

Wireless-LAN e standard IEEE 802.11

Pietro Nicoletti

Studio Reti s.a.s

Piero[at]studioreti.it

Nota di Copyright

- Questo insieme di trasparenze (detto nel seguito slides) è protetto dalle leggi sul copyright e dalle disposizioni dei trattati internazionali. Il titolo ed i copyright relativi alle slides (ivi inclusi, ma non limitatamente, ogni immagine, fotografia, animazione, video, audio, musica e testo) sono di proprietà degli autori indicati a pag. 1.
- Le slides possono essere riprodotte ed utilizzate liberamente dagli istituti di ricerca, scolastici ed universitari afferenti al Ministero della Pubblica Istruzione e al Ministero dell'Università e Ricerca Scientifica e Tecnologica, per scopi istituzionali, non a fine di lucro. In tal caso non è richiesta alcuna autorizzazione.
- Ogni altra utilizzazione o riproduzione (ivi incluse, ma non limitatamente, le riproduzioni su supporti magnetici, su reti di calcolatori e stampate) in toto o in parte è vietata, se non esplicitamente autorizzata per iscritto, a priori, da parte degli autori.
- L'informazione contenuta in queste slides è ritenuta essere accurata alla data della pubblicazione. Essa è fornita per scopi meramente didattici e non per essere utilizzata in progetti di impianti, prodotti, reti, ecc. In ogni caso essa è soggetta a cambiamenti senza preavviso. Gli autori non assumono alcuna responsabilità per il contenuto di queste slides (ivi incluse, ma non limitatamente, la correttezza, completezza, applicabilità, aggiornamento dell'informazione).
- In ogni caso non può essere dichiarata conformità all'informazione contenuta in queste slides.
- In ogni caso questa nota di copyright non deve mai essere rimossa e deve essere riportata anche in utilizzi parziali.

Gli standard IEEE per le Wireless-LAN

■ 802.11

- Standard di base che lavora intorno ai 2,4 GHz e con data rate di 1 e 2 Mbps
- Specifica per il livello fisico l'uso di che prevede due tecniche trasmissive:
 - DSSS = Direct Sequence Spread Spectrum
 - FHSS = Frequency-Hopping Spread Spectrum

■ 802.11b

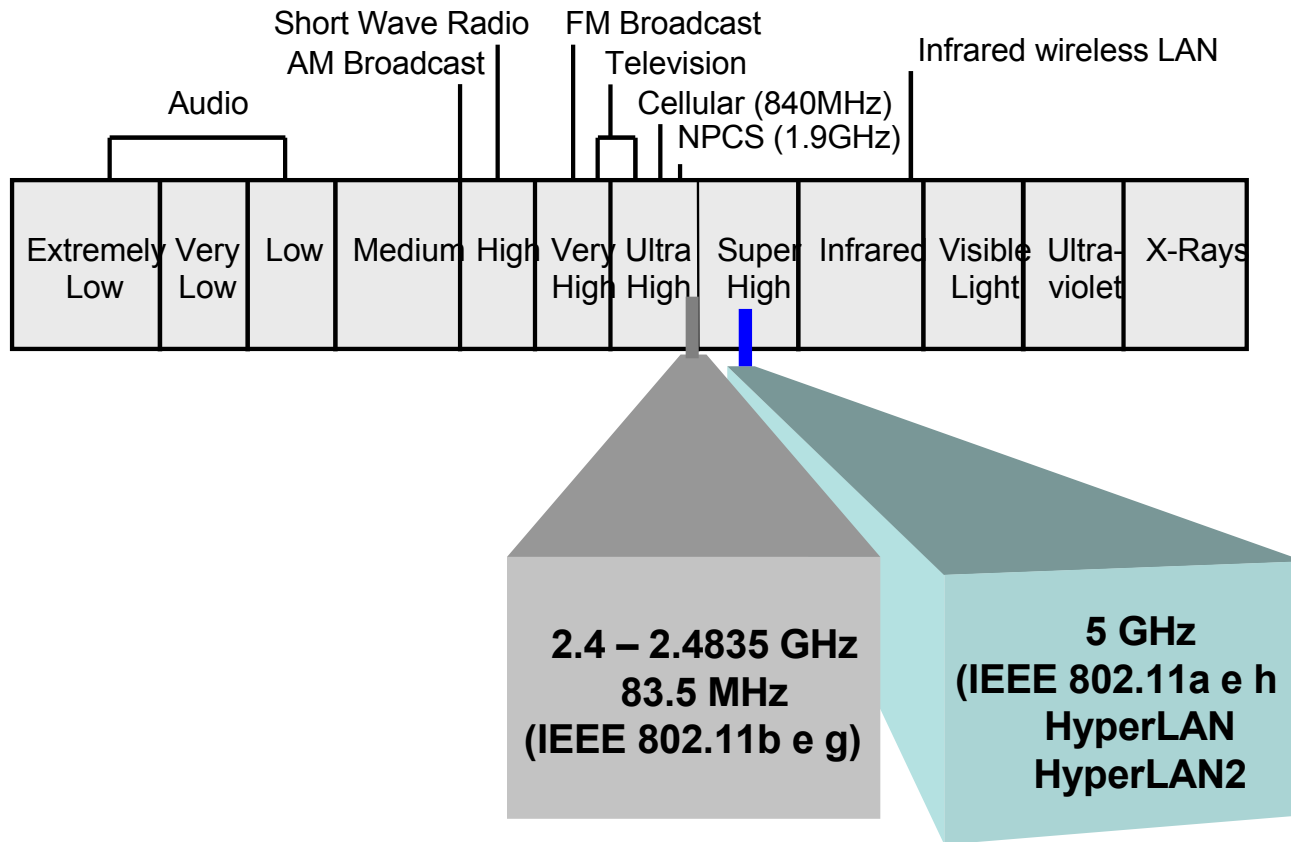
- Estensione di 802.11, specifica per il livello fisico l'uso di HR/DSSS (High Rate DSSS) che lavora intorno ai 2,4 GHz e con data rate di 5.5 Mbps fino a 11 Mbps
- Attualmente è lo standard più diffuso

Gli standard IEEE per le Wireless-LAN

■ 802.11a

- Estensione di 802.11 operante nella banda intorno ai 5 GHz e che permette di ottenere data rate fino a 54 Mbps
- Specifica per il livello fisico l'uso della tecnica di modulazione OFDM (Orthogonal Frequency Division Multiplexing)
- Non conforme alle normative Europee ETSI

Gli standard IEEE per le Wireless-LAN



Evoluzione degli standard

- Obiettivo: incremento della velocità
- 802.11g approvato e pubblicato il 27 Giugno 2003
 - opera intorno ai 2,4 GHz come 802.11b
 - velocità incrementata fino a 54 Mb/s
 - backward compatibility con 802.11b
- 802.11h approvato e pubblicato il giorno 11 Settembre 2003
 - opera intorno ai 5 GHz come 802.11a
 - apporta le modifiche e le aggiunte alle specifiche dello standard 802.11a necessarie per l'adeguamento alle normative Europee ETSI

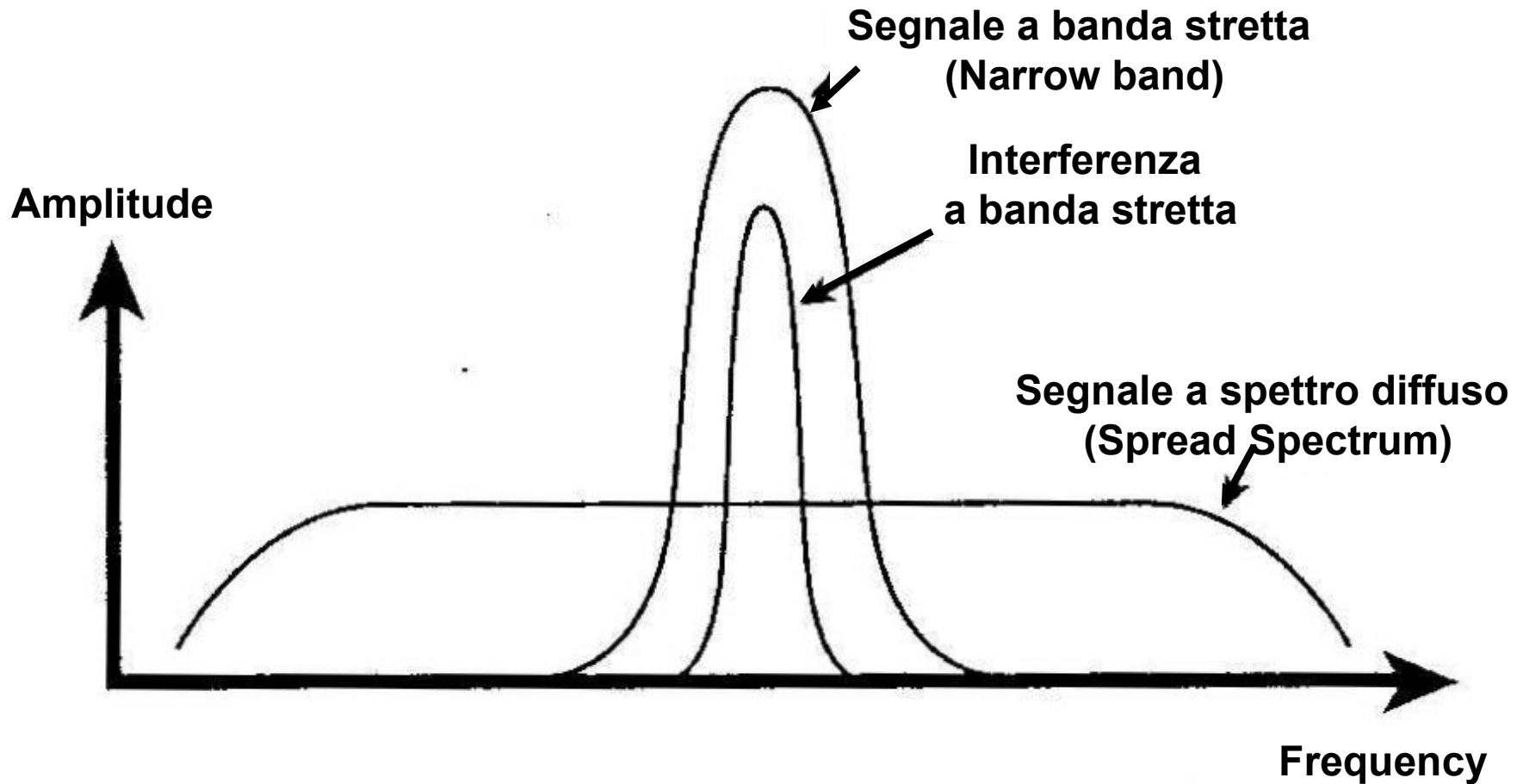
802.11g: velocità supportate

- Le velocità a cui può operare sono:
 - in compatibilità 802.11
 - 1 e 2 Mb/s
 - in compatibilità 802.11b
 - 5,5 e 11 Mb/s
 - velocità tipiche di 802.11g
 - 6, 9, 18, 22, 24, 33, 36, 48, 54 Mb/s

Modulazioni a spettro diffuso

- Obiettivo:
 - aumentare la velocità di trasmissione dati (data-rate)
 - ridurre il rapporto segnale/rumore
- Diffonde la potenza del segnale su di un range di frequenze esteso
 - Il processo di diffusione rende il segnale molto meno soggetto ad interferenze rispetto ad un segnale in banda stretta
- Metodi per ottenere uno spettro diffuso:
 - frequency hopping
 - direct sequence.

Modulazioni a confronto: a banda stretta e spettro diffuso



Frequency-Hopping Spread Spectrum

- Il segnale viene modulato su una portante che si sposta di frequenza in frequenza più volte nel tempo, su di un'ampia porzione di banda, seguendo un pattern prestabilito denominato ***hopping pattern***.
- Velocità di trasmissione (data rate):
 - 1 Mb/s con modulazione 2-level GFSK
 - 2 Mb/s con modulazione 4-level GFSK
- Le sequenze di hopping ed il numero di canali coinvolti varia a seconda dei paesi
 - 79 hopping set per USA e gran parte dell'Europa
 - 23 hopping set per il Giappone
 - 27 hopping set per la Spagna
 - 35 hopping set per la Francia

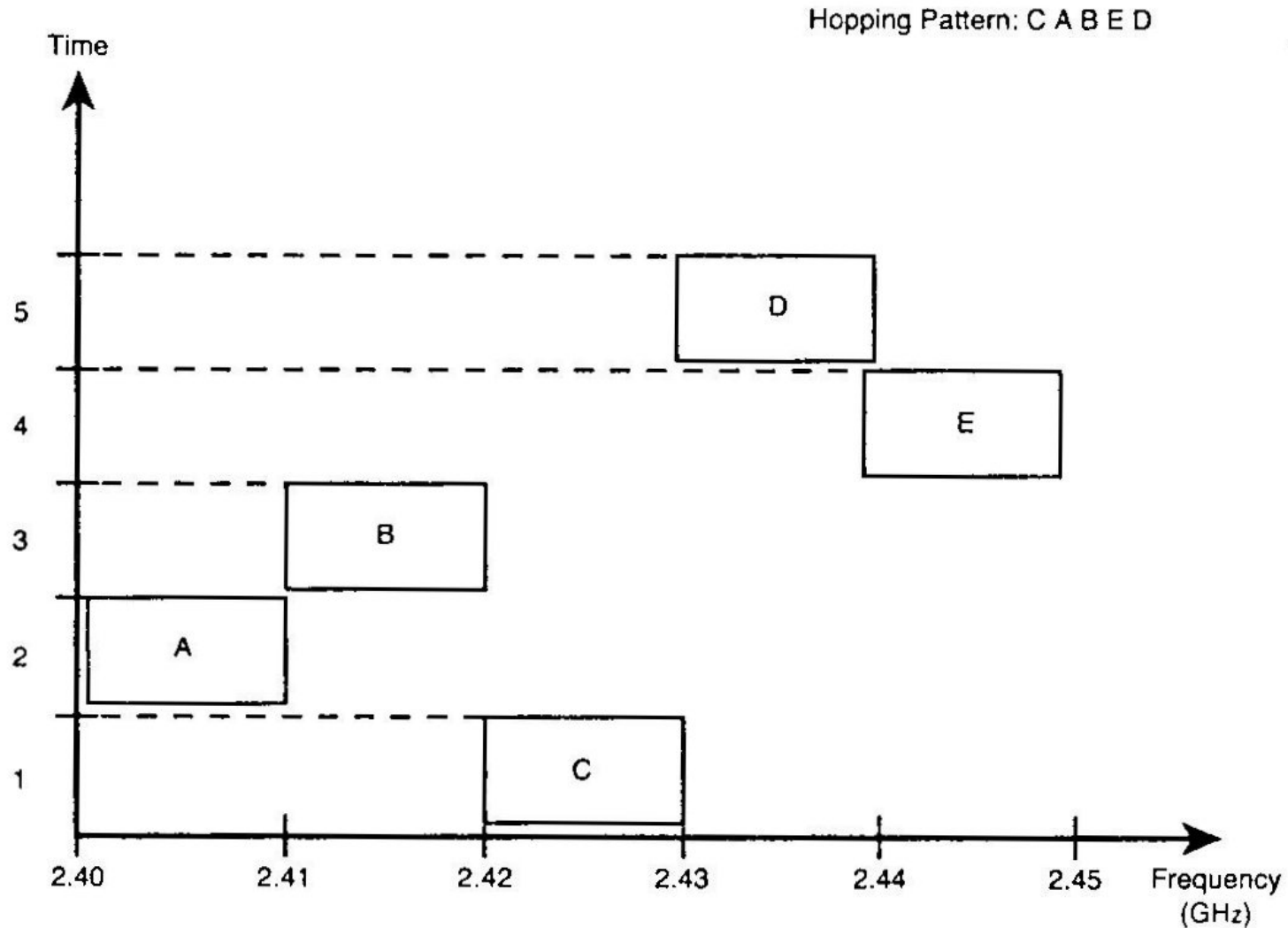
Frequency-Hopping Spread Spectrum -Timing

- Tempo di switching e sistemazione sul successivo canale
 - Channel switching/settling time = 224 μ s
- Tempo massimo di permanenza sul canale
 - max dwell time = 390 TU pari a 400 ms
 - valore raccomandato di dwell time = circa 19 ms
 - all'aumentare del tempo di permanenza aumenta la probabilità di essere disturbati da interferenze
- Se la trasmissione ad una data frequenza risulta troppo disturbata, il segnale viene ritrasmesso nel salto successivo

Sequenze di HOP

- Sequenza di HOP scelta in modo da collocare diverse reti nella stessa area geografica
 - 3 set di 26 sequenze per USA e Europa eccetto Francia e Spagna
 - ogni sequenza impiega 26 differenti frequenze o canali
 - Set 1: $x =$
{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75}
 - Set 2: $x =$
{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}
 - SET 3: $x =$
{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,74,77}

Esempio di sequenza di Hopping



802.11: Canali di Hopping per USA e Europa (incrementi di 1 MHz) Freq. in GHz

Channel #	Value	Channel #	Value	Channel #	Value
2	2.402	28	2.428	54	2.454
3	2.403	29	2.429	55	2.455
4	2.404	30	2.430	56	2.456
5	2.405	31	2.431	57	2.457
6	2.406	32	2.432	58	2.458
7	2.407	33	2.433	59	2.459
8	2.408	34	2.434	60	2.460
9	2.409	35	2.435	61	2.461
10	2.410	36	2.436	62	2.462
11	2.411	37	2.437	63	2.463
12	2.412	38	2.438	64	2.464

802.11: Canali di Hopping per USA e Europa (incrementi di 1 MHz) Freq. in GHz

Channel #	Value	Channel #	Value	Channel #	Value
13	2.413	39	2.439	65	2.465
14	2.414	40	2.440	66	2.466
15	2.415	41	2.441	67	2.467
16	2.416	42	2.442	68	2.468
17	2.417	43	2.443	69	2.469
18	2.418	44	2.444	70	2.470
19	2.419	45	2.445	71	2.471
20	2.420	46	2.446	72	2.472

802.11: Canali di Hopping per USA e Europa (incrementi di 1 MHz) Freq. in GHz

Channel #	Value	Channel #	Value	Channel #	Value
21	2.421	47	2.447	73	2.473
22	2.422	48	2.448	74	2.474
23	2.423	49	2.449	75	2.475
24	2.424	50	2.450	76	2.476
25	2.425	51	2.451	77	2.477
26	2.426	52	2.452	78	2.478
27	2.427	53	2.453	79	2.479
—	—	—	—	80	2.480

DSSS = Direct Sequence Spread Spectrum

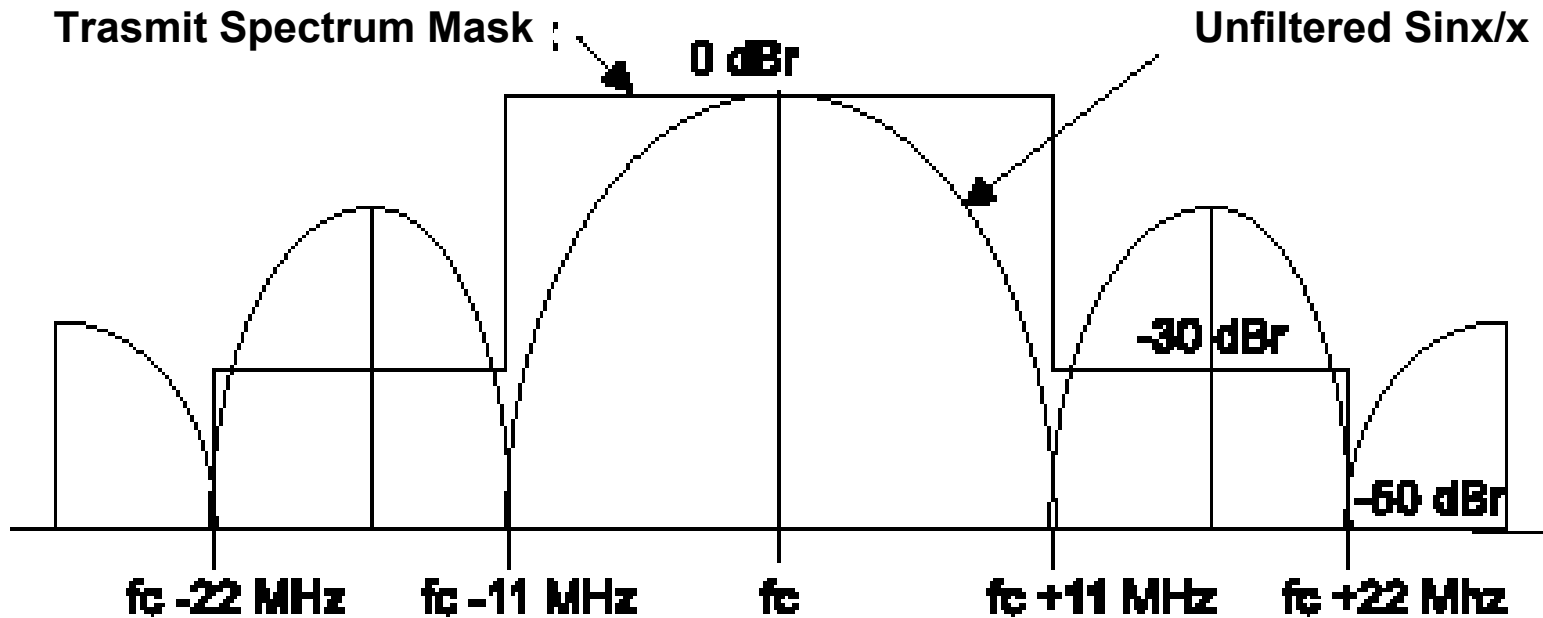
■ Nella tecnica DSSS

- un flusso di bit viene convertito in un flusso di simboli
 - il simbolo rappresenta un certo numero di bit secondo la tecnica di codifica
- il simbolo viene convertito in un segnale che viene assunto dallo spreader (diffusore)
- lo spreader combina il suo segnale d'ingresso con una sequenza Pseudo-Noise denominata *chip sequence*
 - 11-chip Barker sequence su 802.11
 - CCK (complementary code keying) su 802.11b
- il risultato di questa combinazione è un segnale con una banda più larga
 - viene diffuso su uno spettro più ampio di frequenze

802.11 DSSS

- Opera a 1 o 2 Mb/s
 - 1 Mb/s con modulazione Differential Binary Phase Shift Keying (DBPSK)
 - 2 Mb/s con modulazione Differential Quadrature Phase Shift Keying (DQPSK)
- 14 canali disponibili con frequenze che variano da:
 - 2,412 GHz a 2,484 GHz
 - i canali distano normalmente di 5 MHz da quelli adiacenti eccetto il canale 14, pensato appositamente per il Giappone
 - non utilizzabili in tutti gli stati in quanto dipendenti dalle regolamentazioni in materia di utilizzo di frequenze
 - ogni canale copre un spettro di frequenze di 22 MHz

802.11 DSSS: maschera teorica dello spettro trasmissivo



802.11b: Estensione delle prestazioni fino a 11Mb/s

- Adotta la tecnica di modulazione HR/DSSS (High Rate DSSS)
- Lavora intorno ai 2,4 GHz e con data rate di 1, 2, 5.5 e 11 Mbps
 - Modulazione Differential Binary Phase Shift Keying (DBPSK) per le velocità 1 e 5,5 Mbps
 - Modulazione Differential Quadrature Phase Shift Keying (DQPSK) per le velocità 2 e 11 Mbps
- Interopera con i prodotti 802.11 che adottano la tecnica DSSS
- Adotta lo schema di codifica CCK (complementary code keying) per la sequenza di Pseudo-Noise invece dello schema 11-chip Barker sequence per le velocità di 5,5 Mb/s e 11 Mb/s

Coesistenza di canali

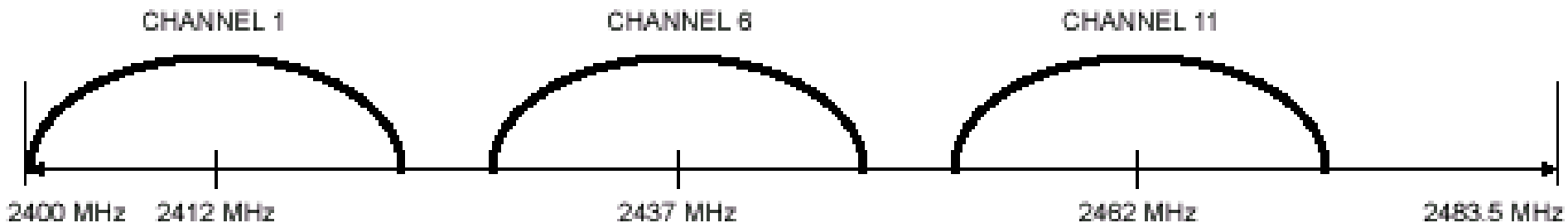
- I canali non sovrapposti
 - distano tra loro almeno 25 MHz dalla frequenza centrale e possono operare simultaneamente nella medesima area
- i canali sovrapponibili
 - sono quelli che operano in aree adiacenti relativamente vicine e parzialmente sovrapposte;
 - essi devono distare tra loro almeno 15 MHz
 - il segnale rispetto all'interferenza deve essere
 - almeno 6 dB al di sopra del segnale d'interferenza a 2 Mb/s
 - almeno 12 dB al di sopra del segnale d'interferenza a 11 Mb/s

Canali DSSS ed utilizzo nei vari stati

CHNL_ID	Frequency	Regulatory domains					
		X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32' France	X'40' MKK
1	2412 MHz	X	X	X	—	—	—
2	2417 MHz	X	X	X	—	—	—
3	2422 MHz	X	X	X	—	—	—
4	2427 MHz	X	X	X	—	—	—
5	2432 MHz	X	X	X	—	—	—
6	2437 MHz	X	X	X	—	—	—
7	2442 MHz	X	X	X	—	—	—
8	2447 MHz	X	X	X	—	—	—
9	2452 MHz	X	X	X	—	—	—
10	2457 MHz	X	X	X	X	X	—
11	2462 MHz	X	X	X	X	X	—
12	2467 MHz	—	—	X	—	X	—
13	2472 MHz	—	—	X	—	X	—
14	2484 MHz	—	—	—	—	—	X

USA: canali DSSS non sovrapposti e canali sovrapponibili

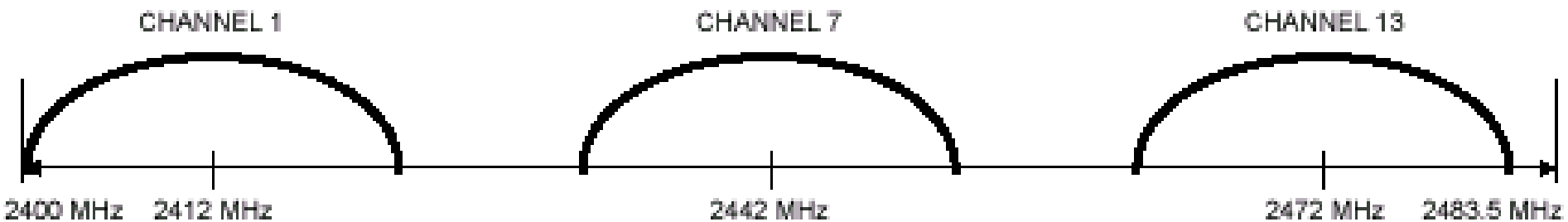
- 3 canali non sovrapposti che possono coesistere nella medesima area
 - 1,6,11



- 4 canali sovrapponibili che possono coesistere in aree adiacenti parzialmente sovrapposte
 - 1, 4, 7, 11

Europa: canali DSSS non sovrapposti e canali sovrapponibili

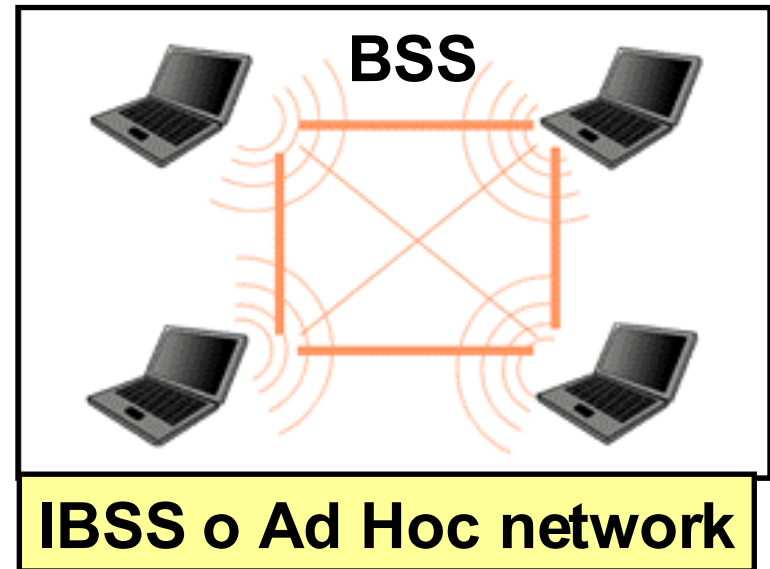
- 3 canali non sovrapposti che possono coesistere nella medesima area:
 - 1, 7, 13



- 5 canali sovrapponibili che possono coesistere in aree adiacenti parzialmente sovrapposte
 - 1, 4, 7, 10, 13

802.11-Topologie di rete: IBSS

- Independent Basic Service Set denominata anche rete Ad-Hoc
 - gruppo di stazioni (STA) che sono localizzate nella medesima area (BSA=Basic Service Area) e che costituiscono un insieme denominato Basic Service Set (BSS)
 - nella topologia IBSS si realizzano comunicazioni peer-to-peer tra le stazioni
 - mezzo trasmissivo condiviso della WLAN: l'etere



Non c'è bisogno di Access Point

Rete Indipendent Basic Service Set - IBSS

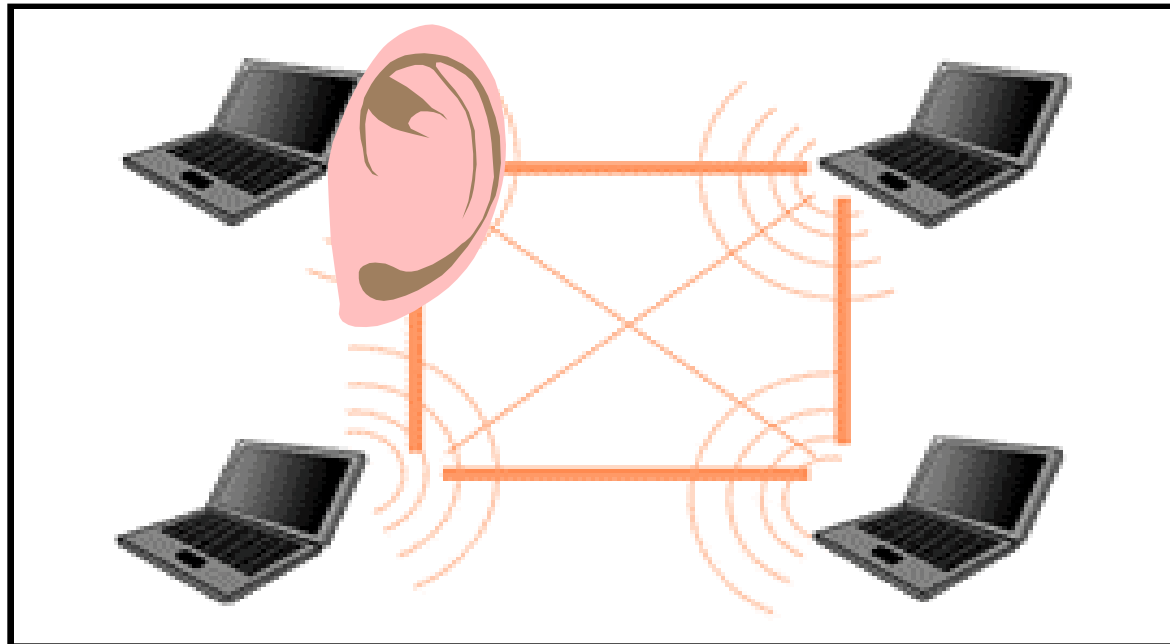
- Le stazioni “STA” localizzate nell’area “BSA” sono sotto il controllo di una funzione di coordinamento che può essere di tipo:
 - Distribuito, caso comune
 - DCF = Distributed Coordination function
 - la funzione DCF è presente in tutte le stazioni
 - Concentrato, col concetto Master/slave
 - PCF = Point Coordination Function
 - viene effettuato un polling dal Master
- La funzione di coordinamento serve alla stazione per stabilire se è abilitata alla trasmissione/ricezione di pacchetti in un determinato BSS attraverso l’etere o WM (WM=Wireless Medium)

Inserimento di una stazione in un IBSS

- In ogni stazione è presente la funzione DCF che serve partecipare ad un determinato BSS e per realizzare la condivisione del mezzo trasmissivo di tipo:
 - CSMA/CA = Carrier Sense Multiple Access with Collision Avoidance
- La stazione che vuole partecipare ad un certo BSS deve sintonizzarsi e sincronizzarsi con le altre stazioni
 - è necessario effettuare una scansione, che nel caso di reti Ad-Hoc, è in genere di tipo ***passive-scanning***

Passive scanning

- La stazione sta in ascolto
 - scandisce tutti i possibili canali rimanendo in ascolto per un certo tempo su ognuno di essi in attesa di un *beacon*
 - confronta lo SSID contenuto nel con il proprio per stabilire se può comunicare in quel IBSS

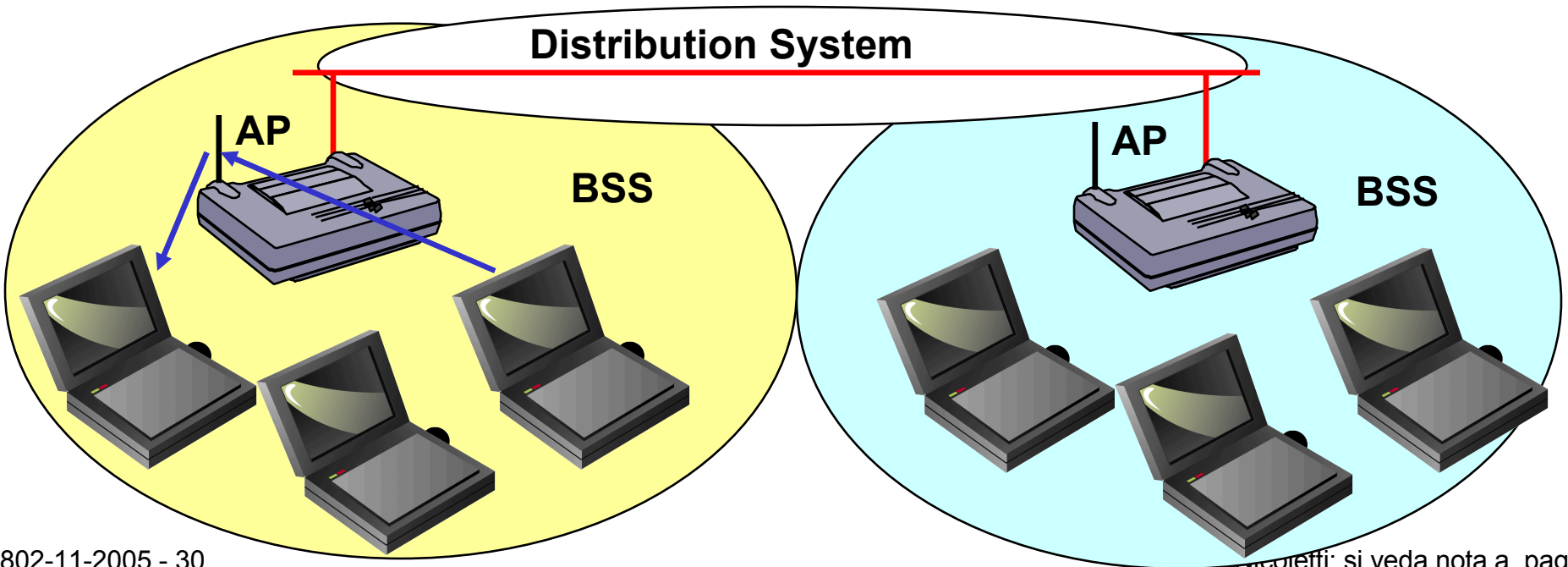


Beaconing

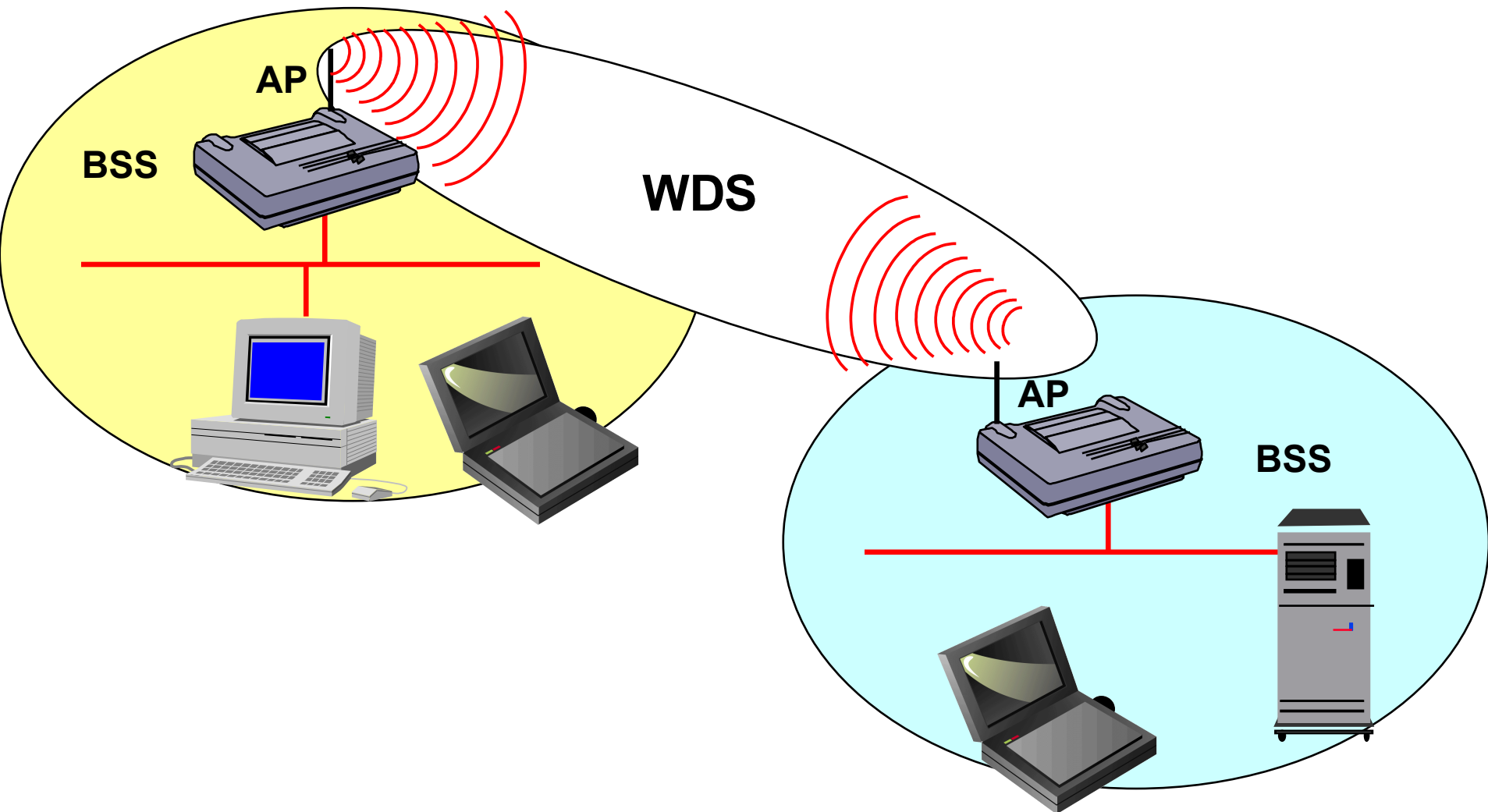
- I beacon sono dei pacchetti speciali di Management che contengono le informazioni di Service Set ID (SSID) e timestamp necessarie alla sincronizzazione della stazione
- In rete Ad-Hoc tutte le stazioni partecipano alla generazioni di pacchetti di beacon

802.11-Topologie di rete: ESS

- **Rete denominata anche di tipo Infrastructure:**
 - presenza di una LAN di distribuzione denominata Distribution System, che interconnette diversi BSS;
 - ad ogni BSS fa capo un Access Point
 - le stazioni possono comunicare solo tramite AP
 - trame ricevute e inviate tramite AP



802.11-Topologie di rete: ESS con Wireless Distribution System (WDS)

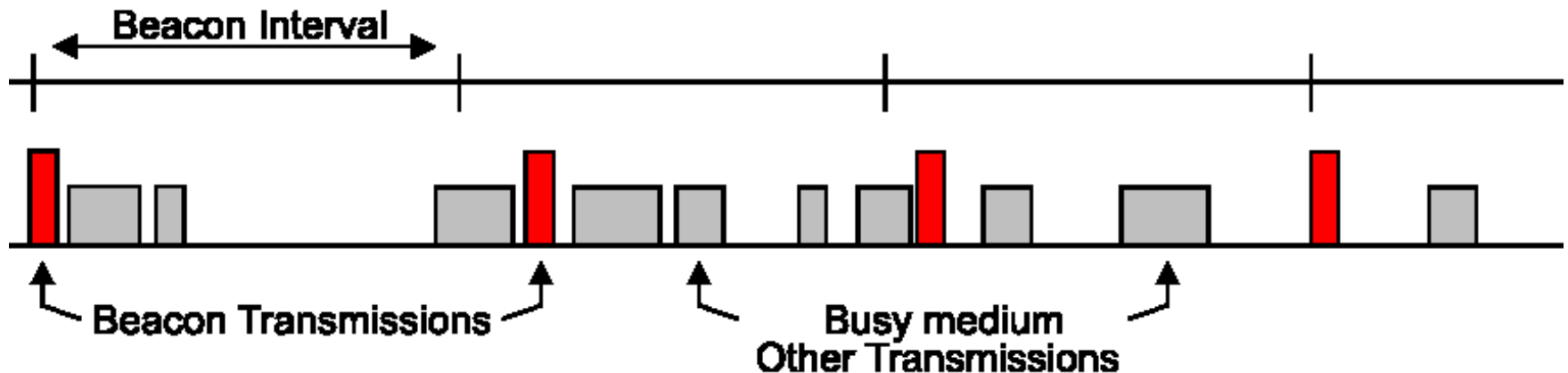


Scanning in una rete

- Lo scanning può essere:
 - di tipo **Passive** basato sulla trasmissione periodica di Beacon
 - di tipo **Active** dove l'AP risponde alle richieste di sondaggio da parte delle Stazioni attraverso i Probe-Request inviando le conferme di Probe-Response

Generazione del Beacon in una rete ESS

- Ad ogni Target Beacon Trasmssion Time (TBTT) l'AP prepara una trama Beacon. Se il mezzo è libero trasmette altrimenti ritarda la trasmissione della trama Beacon.



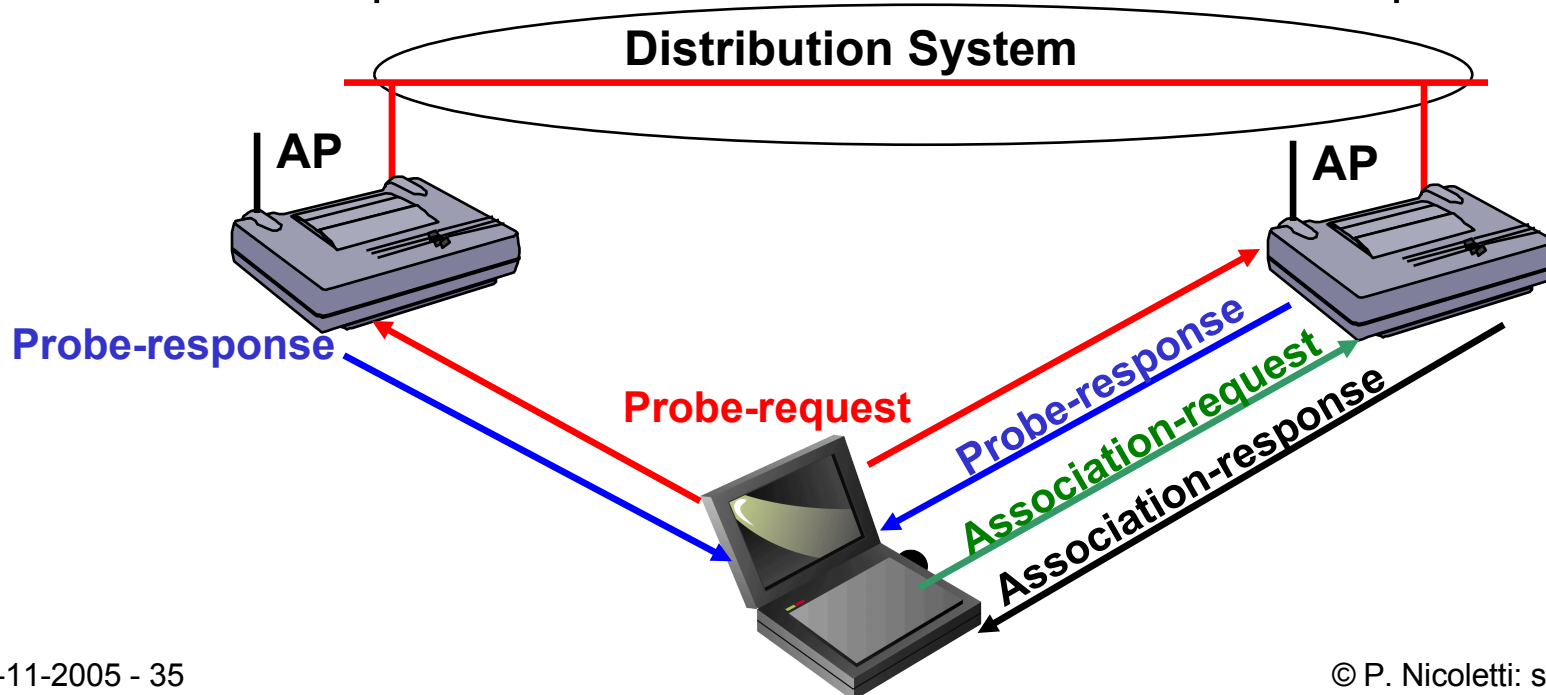
Active Scanning

- Adottato sulle reti di tipo di ESS in cui l'Access Point (AP) ha l'incarico di rispondere al probe-request
- La stazione che vuole entrare a far parte di un rete:
 - invia un pacchetto di Management di tipo *Probe-Request* in broadcast con gli identificativi della rete cercata ESS-ID
 - rimane in attesa per un certo tempo per la ricezione di pacchetto di *Probe-Response*
 - se non riceve risposta passa al canale successivo (nel caso in cui non abbia un canale fisso preimpostato)

Active Scanning e associazione

■ Procedura

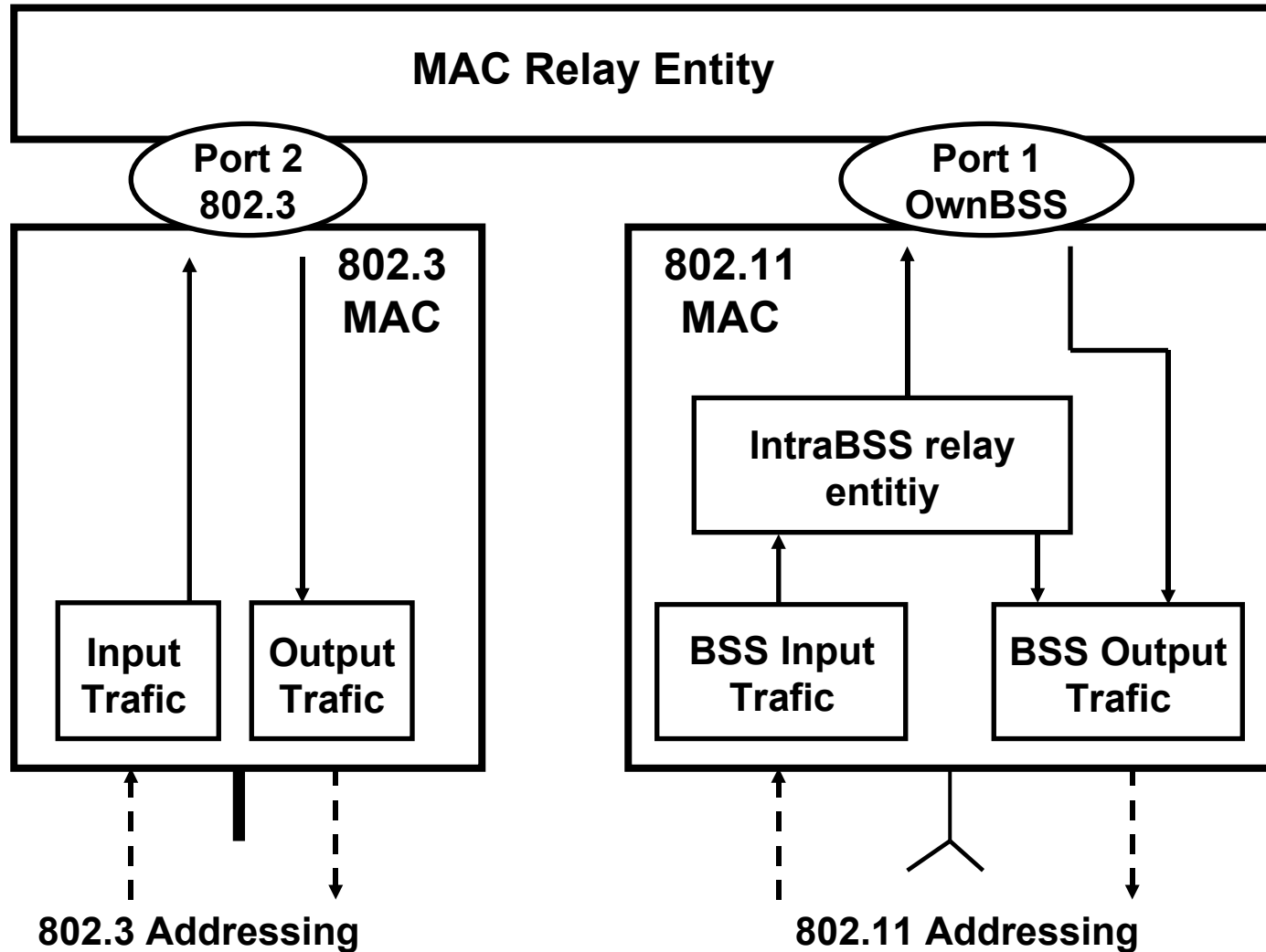
- La STA invia le trame Probe-Request
- Gli AP rispondono con un Probe-Response
- La stazione seleziona l'AP migliore e invia a questo una richiesta di associazione con una trama Association-Request
- L'AP risponde inviando una trama Association-Response



Access Point (AP)

- Viene definito genericamente come un'entità che permette la distribuzione dei servizi MAC via wireless medium (WM) per le stazioni ad esso associate
- In genere è una sorta bridge locale che interfaccia la rete wireless con una wired
 - Copre una ben determinata area
 - Consente ai dispositivi di passare da una cella all'altra garantendo la connettività
 - Può essere utilizzato semplicemente come ripetitore di segnale
 - Le funzioni di bridging sono fondamentali per effettuare la traduzione di trame e il buffering tra la rete wired e wireless

Architettura di un AP transparent bridged



Access Point, Repeater o Bridge?

- L'Access Point è tipicamente un apparato con ridotte funzioni e capacità di Lookup in tabella
 - Viene configurato come “*Root Access Point*”
 - Realizza le funzione di DCF e di apparato di associazione per le stazioni presenti nel BSS (Active Scanning)
 - Configurazione di default dell'AP
 - Dispone solo di una tabella delle associazioni dove sono presenti gli indirizzi MAC riguardanti le stazioni wireless associate all'AP

Access Point: funzioni di inoltra

- Alla ricezione di un pacchetto dal WM
 - Se l'indirizzo MAC di destinazione è presente nella tabella delle stazioni associate al AP il pacchetto viene ritrasmesso nel WM
 - Se l'indirizzo MAC di destinazione non è presente nella tabella delle stazioni associate al AP il pacchetto viene tradotto e trasmesso nella porta Wired (tipicamente Ethernet)

Principio simile a quello della Default Route

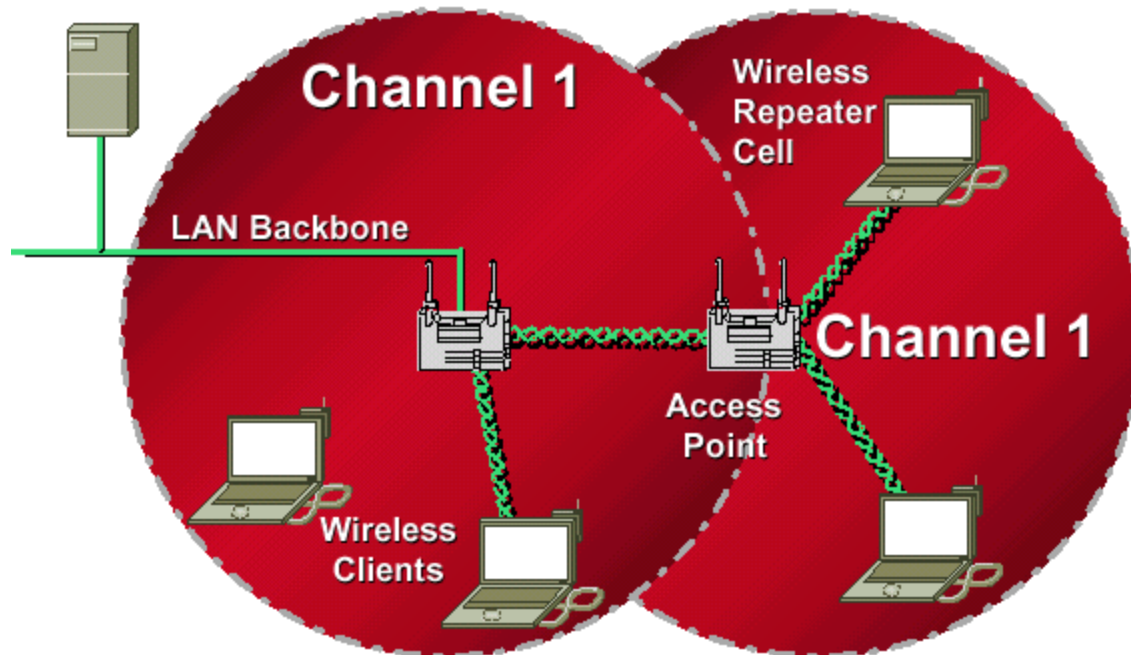
- Alla ricezione di un pacchetto dalla porta Wired
 - Se l'indirizzo MAC di destinazione è presente nella tabella delle stazioni associate al AP il pacchetto viene tradotto e trasmesso nel WM
 - Se l'indirizzo MAC di destinazione non è presente nella tabella delle stazioni associate al AP il pacchetto viene scartato

Repeater, Access Point o Bridge?

- Il Repeater è un apparato Access Point o Bridge che viene configurato come “*Repeater Access Point*”
 - Le stazioni in portata radio del Repeater risultano associate al Root Access Point
 - Nessuna stazione è associata direttamente al Repeater
 - Alla ricezione di un pacchetto dal WM il repeater lo ritrasmette nel WM

L'Access Point impiegato come Repeater nel Wirelss Medium (WM)

- Access Point come Repeater nel WM:
 - utilizzo dello stesso canale
 - ripetizione delle trame con peggioramento delle prestazioni della rete
 - la stazione che si trova nell'area di sovrapposizione si aggancia al segnale migliore



Bridge, Access Point o Repeater?

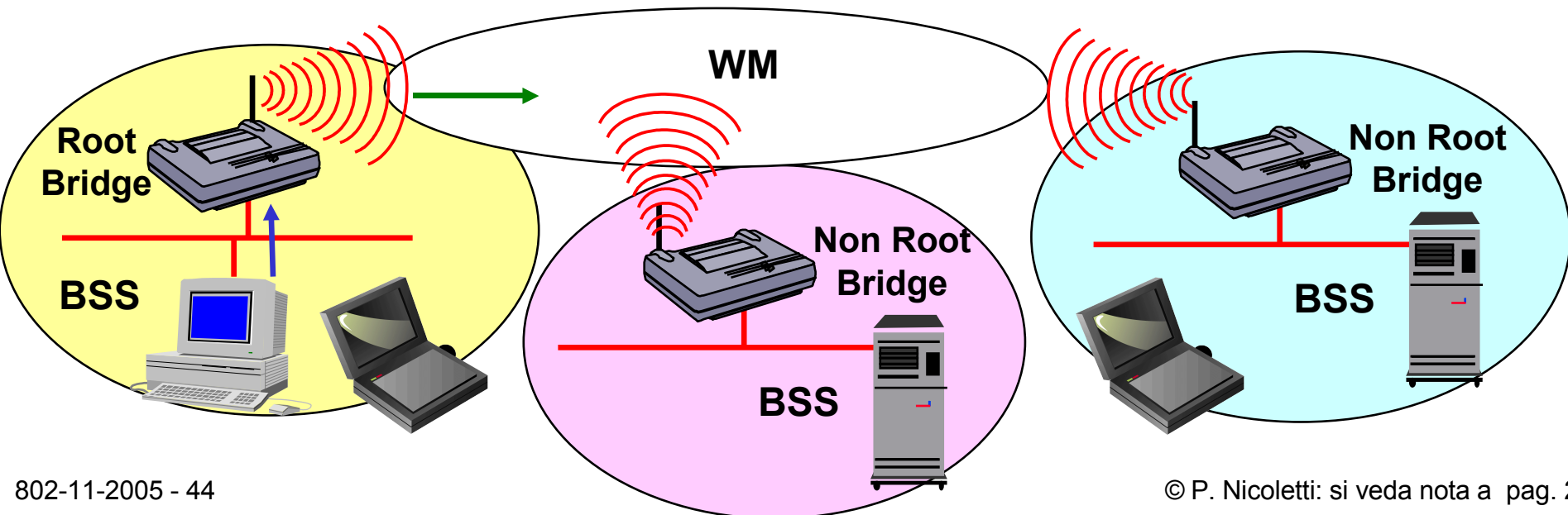
- Il Bridge è un apparato con tutte le funzioni tipiche di un bridge standard incluso lo spanning tree 802.1D
 - Ha in tabella le informazioni di tutte le stazioni attive nella BLAN (che hanno trasmesso dati nell'intervallo dell'ageing time)
 - Viene tipicamente impiegato nelle applicazioni Outdoor per connettere delle LAN via wireless in modalità Point-to-Point o Point-to-Multipoint
 - Un Bridge Wireless deve essere configurato come “**Root Bridge**”
 - Nel caso Point-to-Point l'altro Bridge deve essere configurato come “**Non Root Bridge**”
 - Nel caso Point-to-Multipoint i restanti Bridge devono essere configurati come “**Non Root Bridge**”

Non Root Bridge

- Può trasmettere dati sul WM ad un'altra stazione nel WM o un altro Bridge solo attraverso il Root Bridge al quale è associato
- Può ricevere dei dati dal WM solo dal Root Bridge
- Non c'è comunicazione diretta tra due Bridge Non Root

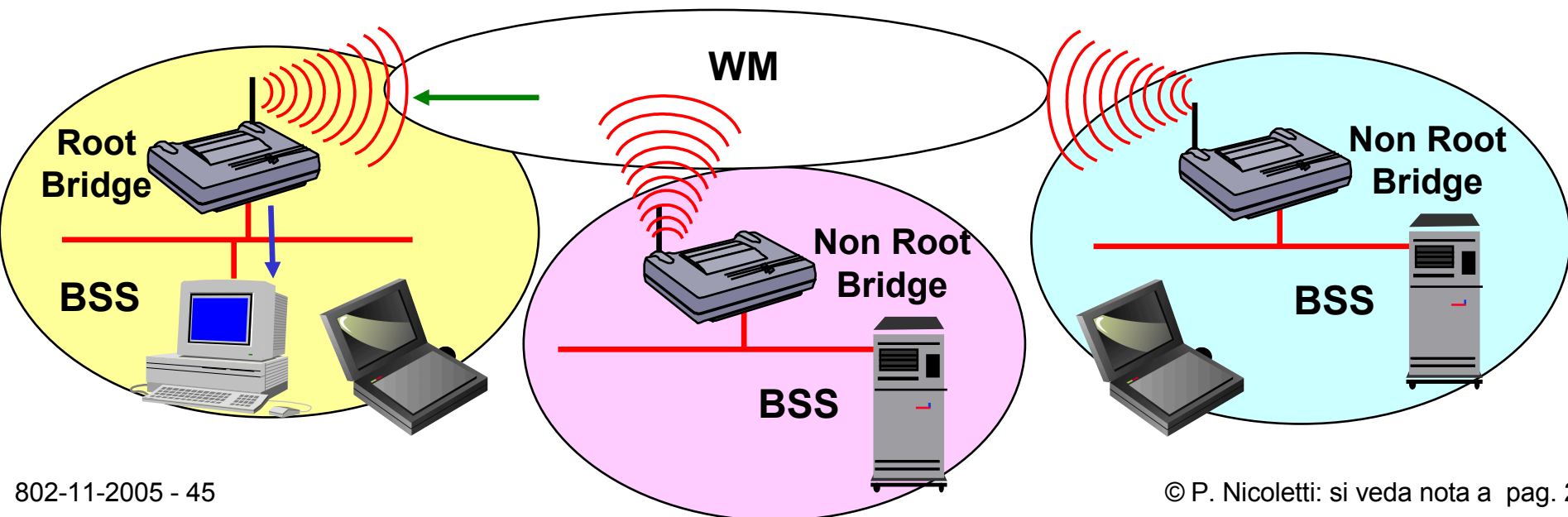
Root Bridge: inoltra parte 1^a

- Alla ricezione di un pacchetto dalla porta Wired:
 - Se la stazione di destinazione appartiene alla parte Wired il pacchetto viene scartato
 - Se la stazione di destinazione appartiene o è raggiungibile dalla parte Wireless il pacchetto viene tradotto e trasmesso nel WM



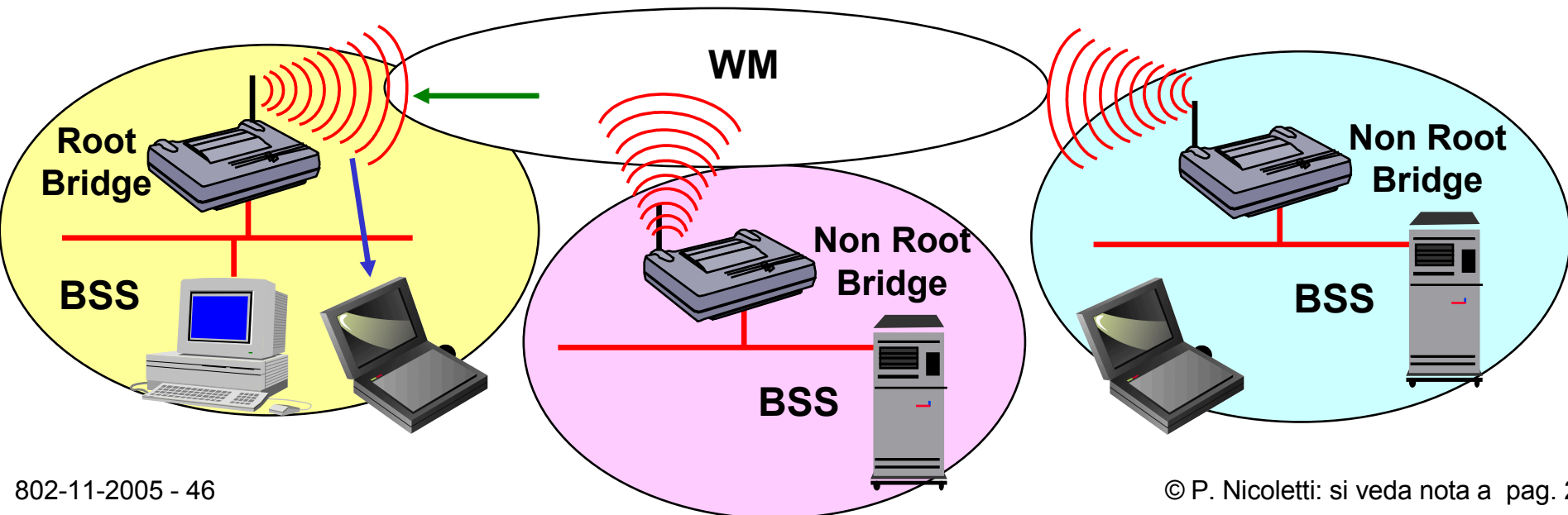
Root Bridge: inoltra parte 2^a

- Alla ricezione di un pacchetto dal WM:
 - Se la stazione di destinazione appartiene o è raggiungibile dalla parte Wired il pacchetto viene tradotto e trasmesso nella porta Wired



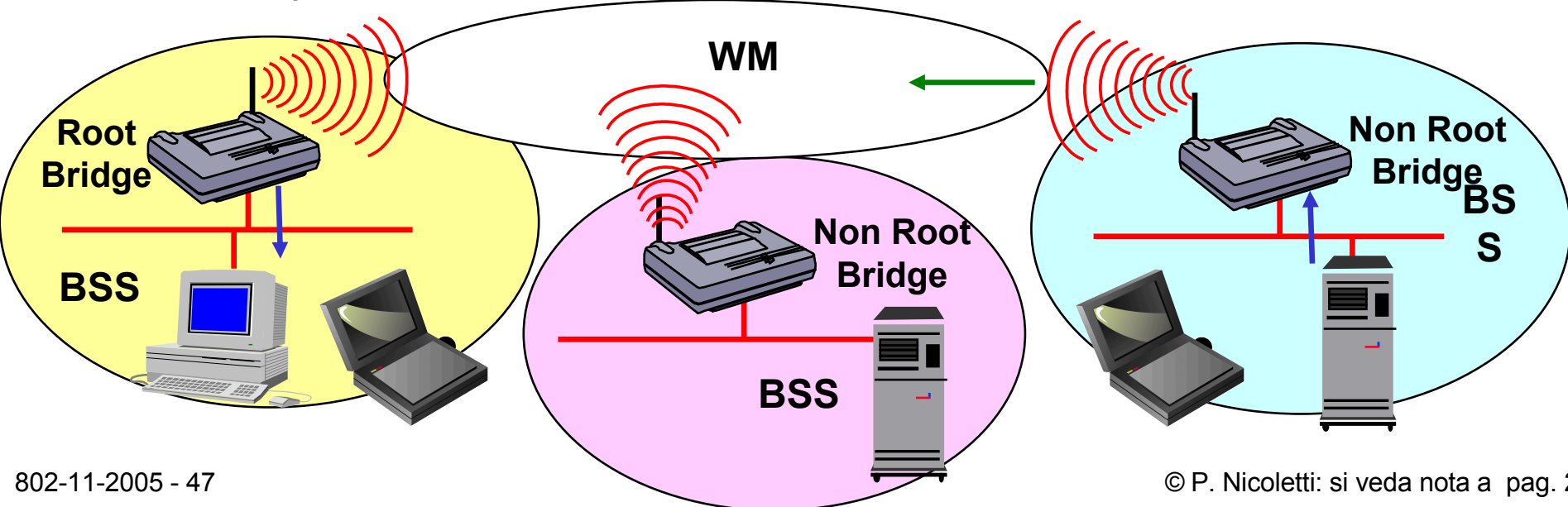
Root Bridge: inoltra parte 3^a

- Alla ricezione di un pacchetto dal WM:
 - Se la stazione di destinazione è associata o è raggiungibile dalla parte Wireless il pacchetto viene ritrasmesso nel WM



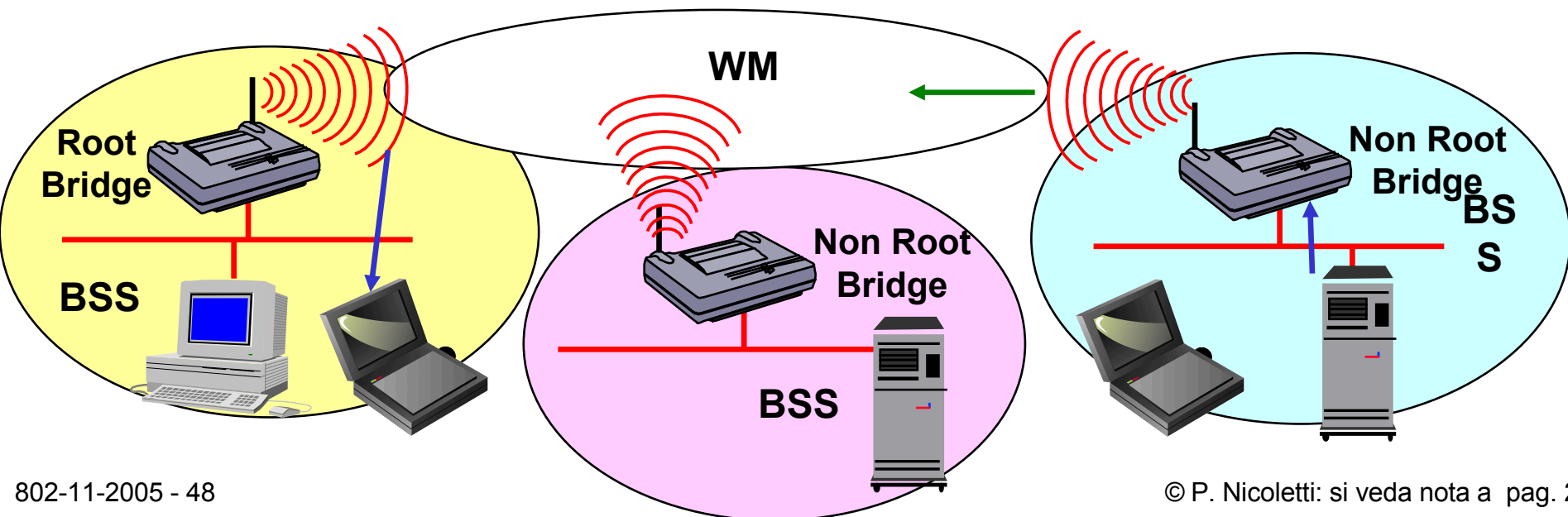
Non Root Bridge: inoltra parte 1^a

- Alla ricezione di un pacchetto dalla porta Wired:
 - Se la stazione di destinazione appartiene alla parte Wired il pacchetto viene scartato
 - Se la stazione di destinazione è raggiungibile tramite il Root Bridge e si trova sulla sua LAN cablata il pacchetto viene tradotto e trasmesso nel WM
 - Successivamente il Root Bridge traduce e trasmette il pacchetto sulla sua LAN cablata



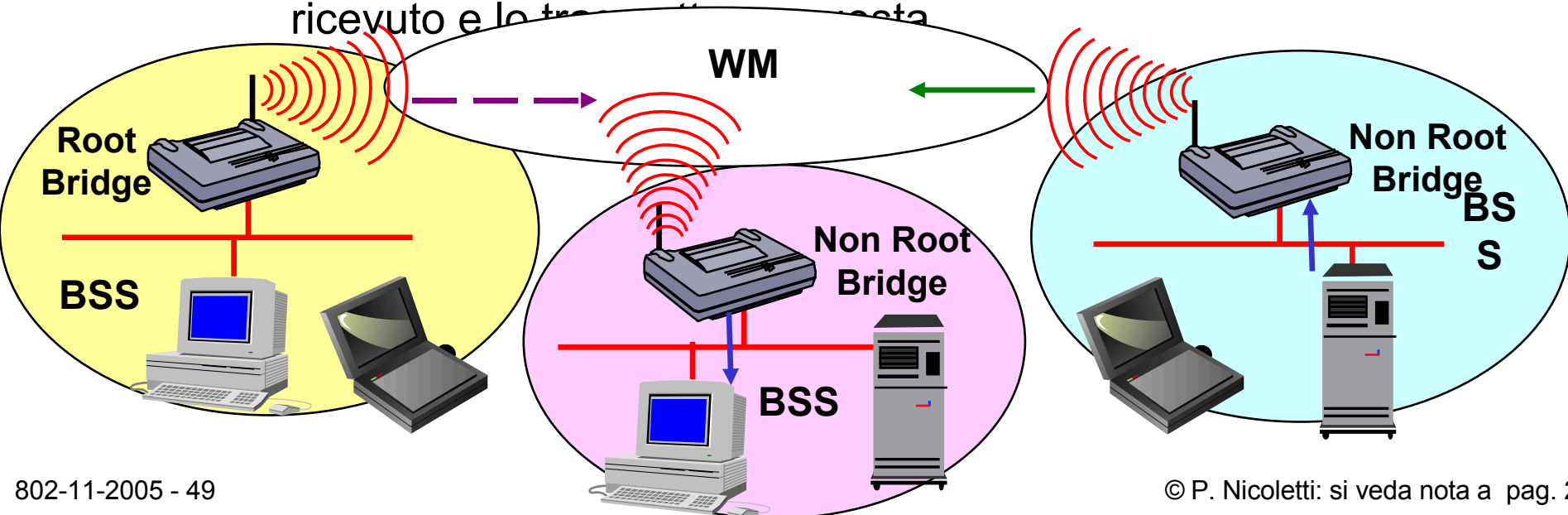
Non Root Bridge: inoltra parte 2^a

- Alla ricezione di un pacchetto dalla porta Wired:
 - Se la stazione di destinazione è raggiungibile tramite il Root Bridge ed è ad esso associata il pacchetto viene tradotto e trasmesso nel WM
 - Successivamente il Root Bridge ritrasmette il pacchetto nel WM



Non Root Bridge: inoltra parte 3^a

- Alla ricezione di un pacchetto dalla porta Wired:
 - Se la stazione di destinazione è raggiungibile tramite il Root Bridge ed è connessa alla LAN cablata di un altro Non Root Bridge il pacchetto viene tradotto e trasmesso nel WM
 - Successivamente il Root Bridge ritrasmette il pacchetto nel WM
 - Il Non Root Bridge che può raggiungere l'indirizzo MAC di destinazione tramite la LAN cablata traduce il pacchetto ricevuto e lo trasmette alla stazione



Il MAC di 802.11

- Due metodi di accesso al mezzo trasmissivo
 - DCF (Distributed Coordination function) implementa il metodo accesso CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) con Acknowledgement ACK
 - PCF (Point Coordination Function) basato sul polling effettuato dall'Access Point verso le stazioni per abilitarle a trasmettere dei dati
 - pensato per applicazioni real-time

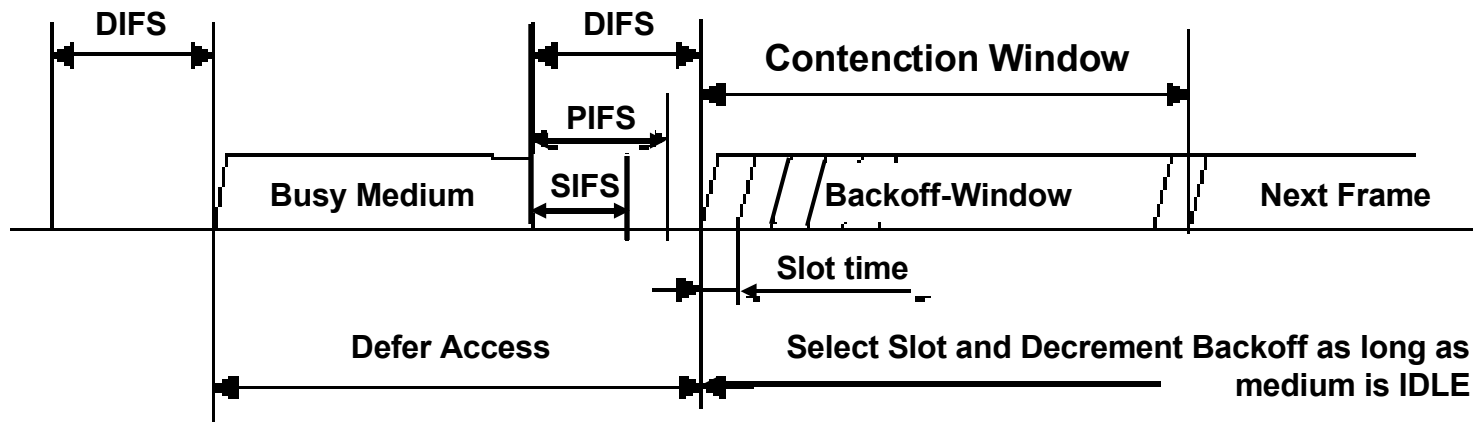
CSMA-CA: Carrier Sense Multiple Access Collision Avoidance

- Nelle reti wireless a differenza di quelle wired la comunicazione è half duplex, per cui, non potendo “ascoltare” mentre si trasmette (listen while talking) come nello standard 802.3 (Ethernet), le STA devono poter evitare le collisioni
 - La STA “ascolta” (Carrier Sense) il WM prima di trasmettere (listen before talking).
 - Se è libero per un tempo maggiore di DIFS (Distributed coordination function Interframe Space) trasmette, altrimenti attende che la trasmissione si fermi e calcola, per evitare le collisioni (CA), un tempo di backoff usando una funzione random (exponenzial random backoff).
 - La STA con il valore del back-off time più piccolo vincerà la contesa.

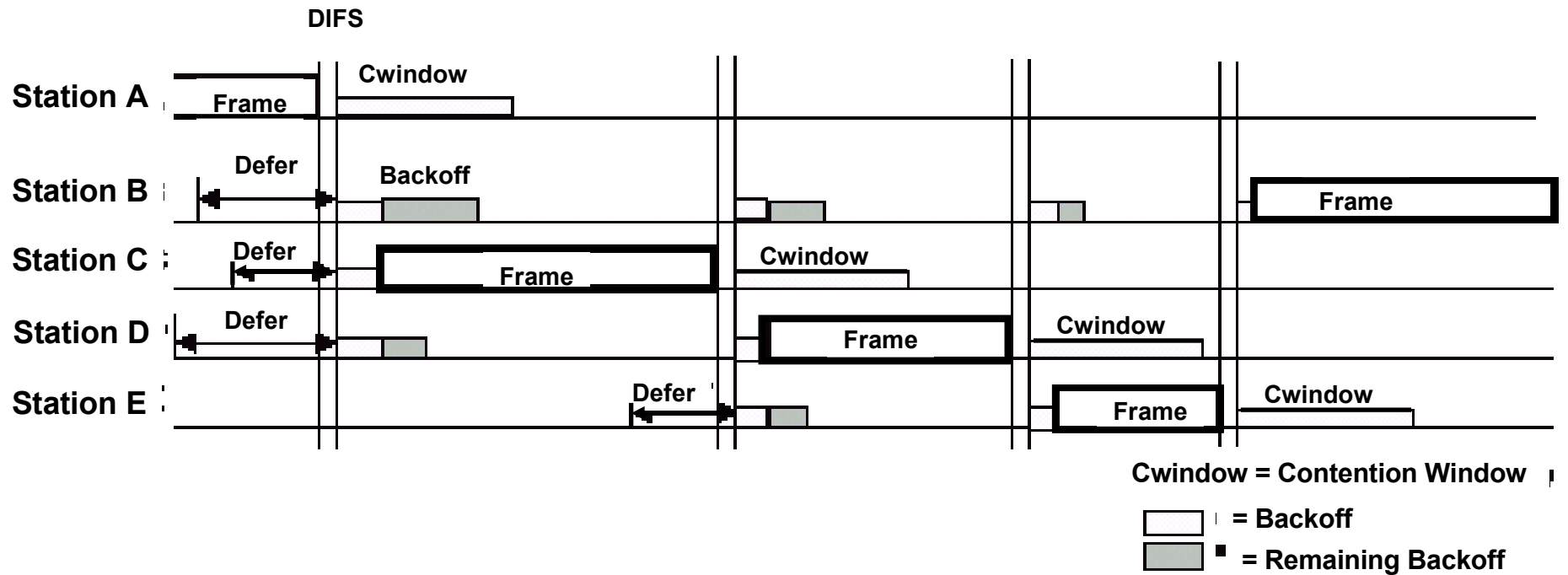
CSMA-CA: Inter Frame Spacing e contesa

- Tipi di Inter Frame Spacing
 - DIFS: DCS Inter Frame Space
 - PIFS: PCF Inter Frame Space
 - SIFS: Short Inter Frame Space
- $\text{BackoffTime} = \text{Random()} * \text{SlotTime}$

Immediate access when medium is free \geq DIFS

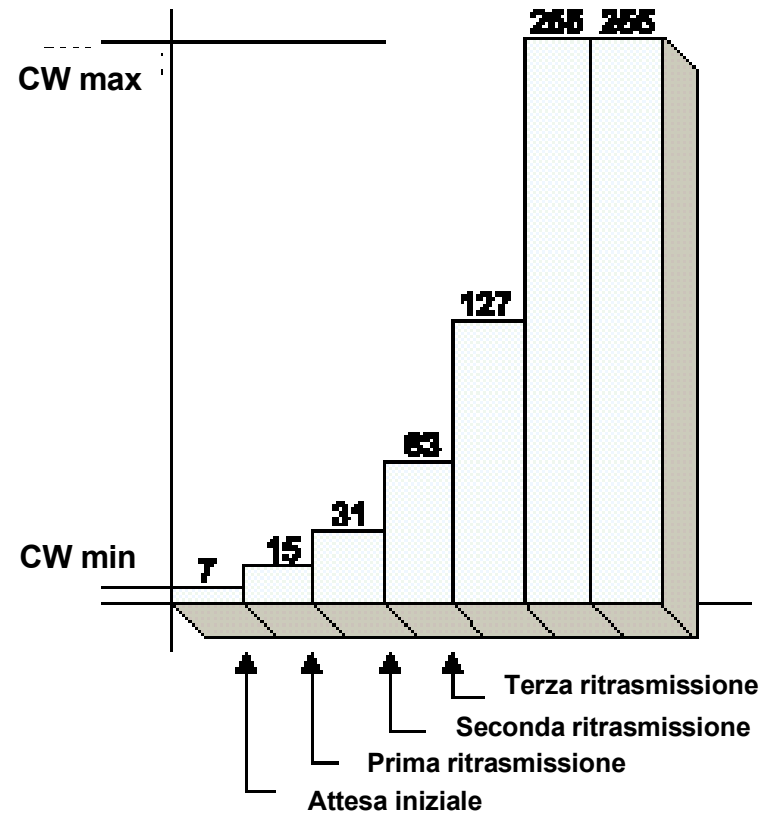


Procedura di Backoff



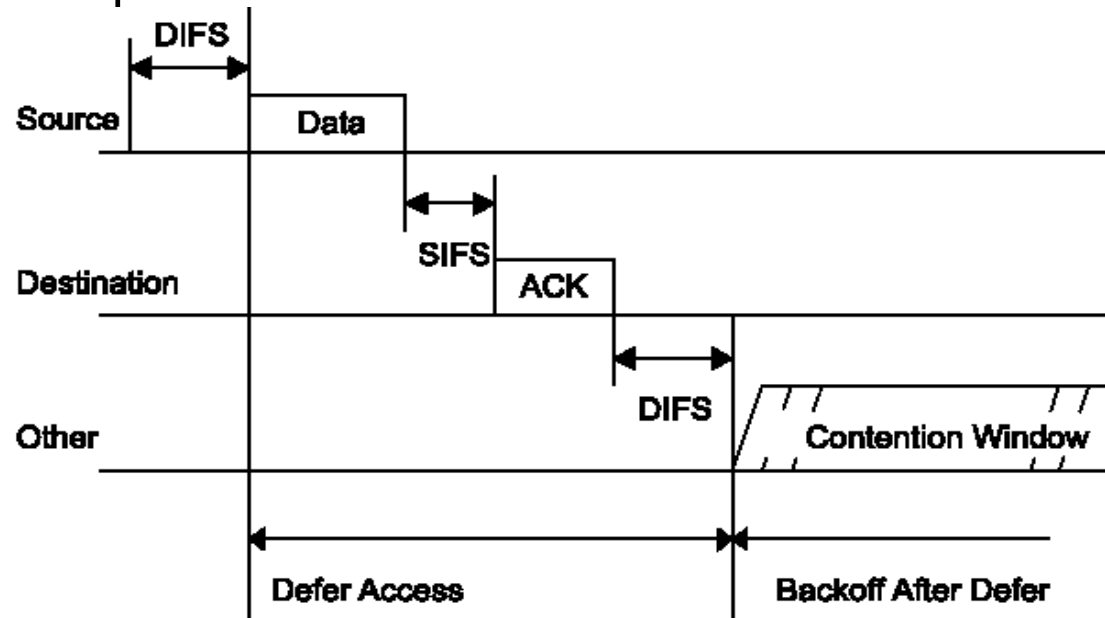
CSMA-CA: Exponential Random Backoff

- Utilizzato quando:
 - la STA vuole iniziare a trasmettere sul mezzo che però risulta occupato;
 - prima di ogni ritrasmissione;
 - dopo ogni trasmissione di MPDU avvenuta con successo
- BackoffTime = $\text{Random()} * \text{SlotTime}$
 - Valore random scelto nei valori compresi tra CWmin (Collision window min) e CWmax
 - $\text{CWmin} \leq \text{CW} \leq \text{CWmax}$



CSMA-CA e Acknowledgement ACK

- Acknowledgement ACK: Serve per confermare la ricezione corretta di una trama (CRC corretta)
 - La stazione ricevente STA invia una trama di ACK dopo aver atteso per il tempo dell'interspazio SIFS (Short Inter Frame Spacing).
 - Se la stazione Source non riceve l'ACK, entro un certo tempo, imposta l'Exponential Random Backoff e ritrasmette la trama.



CSMA-CA e Acknowledgement ACK

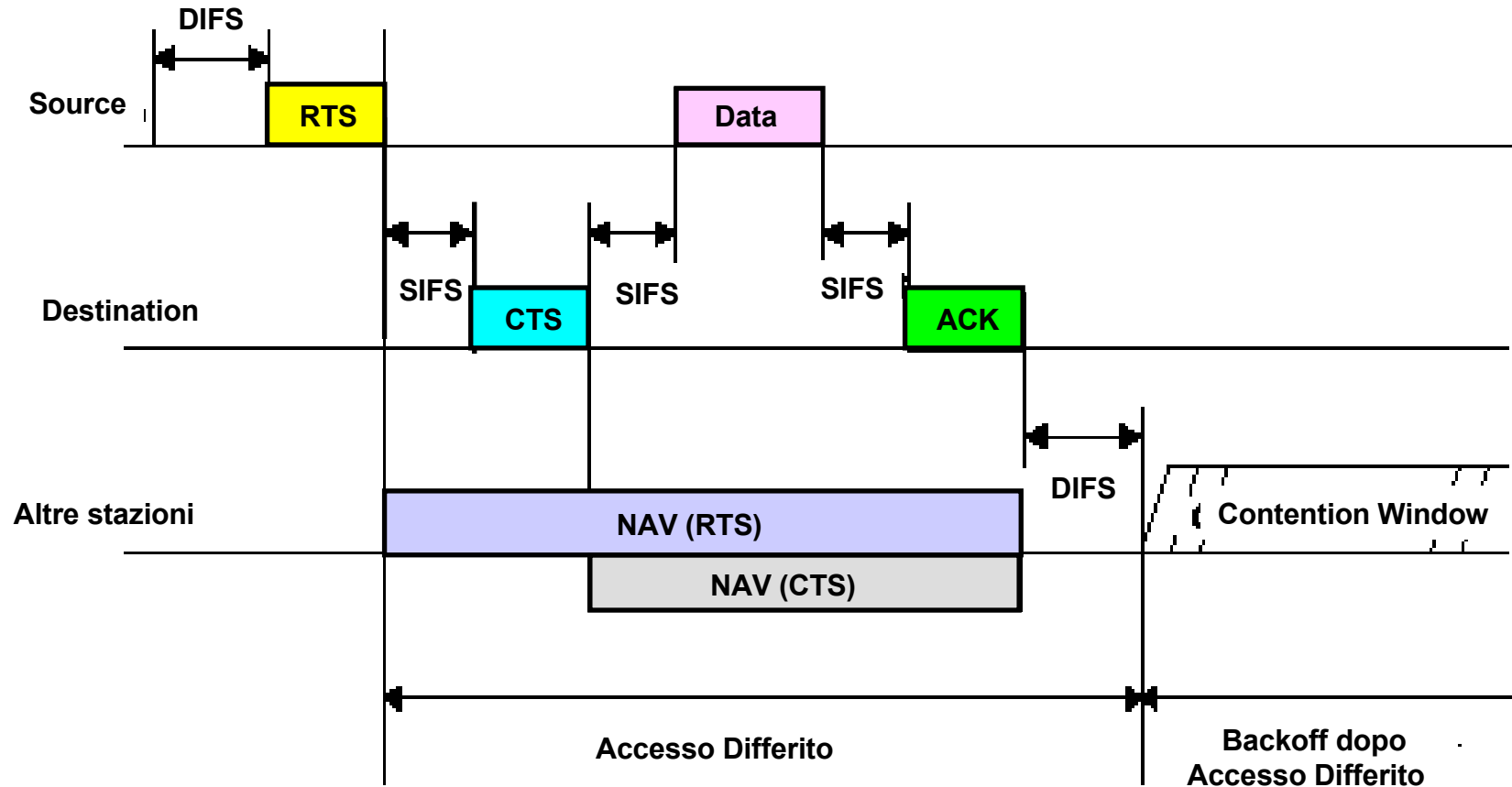
- L'Acknowledgement non viene inviato in risposta a pacchetti Multicast o Broadcast
- Se il pacchetto inviato dalla stazione trasmittente del WM è destinato al Distribution System (DS) l'Access Point invia l'ACK a fronte della corretta ricezione del pacchetto.
- Se il pacchetto è proveniente dal DS e destinato ad una stazione del WM, quindi viene trasmesso dall'AP, la stazione destinataria a fronte della corretta ricezione invia l'ACK
 - se l'Access Point non riceve l'ACK, entro un certo tempo, imposta l'Exponential Random Backoff e ritrasmette la trama.

RTS/CTS e carrier sense virtuale

- Durante la trasmissione una stazione non può rilevare la collisione perché non è in grado di ascoltare la propria trasmissione
- Per prevenire la collisione si realizza un carrier sense virtuale attraverso l'impiego di messaggi **RTS** e **CTS** che contengono informazioni sulla durata della trasmissione successiva
 - Le stazioni non destinatarie dei messaggi caricano le informazioni di durata della trasmissione nel registro **NAV** (Network Allocation Vector)
 - Per il periodo di tempo caricato nel registro NAV la stazione non può trasmettere pacchetti, quindi si evita la collisione

Nota: RTS = Request To Send, CTS = Clear To Send

Procedura di trasmissione tramite RTS e CTS



Frammentazione delle trame

- Opzionale la frammentazione, obbligatoria la funzione di riassettaggio delle trame
- Utile in ambienti rumorosi dove la qualità del segnale è scadente
 - Pacchetti più piccoli sono meno influenzabili dal rumore d'ambiente
 - La frammentazione crea un overhead che consuma banda trasmissiva

Roaming

- Lo standard 802.11 supporta il roaming attraverso le funzioni di scanning e riassociazione.
- Essa utilizza la funzione di scanning, oppure le informazioni ottenute da precedenti scansioni, per trovare un altro AP.
 - E' la STA ad accorgersi che collegamento con l'AP è di scarsa qualità (attenuazione elevata e SNR)
 - Invia una Richiesta di Riassociazione al nuovo AP.
 - Se l'AP invia una trama di Risposta positiva la STA viene associata al nuovo AP altrimenti la STA con lo scanning cerca un altro AP.
- Se accetta la Richiesta di Riassociazione l'AP
 - Informa il DS della riassociazione.
 - Il vecchio AP viene informato attraverso il DS.

Power Management su Infrastructured network (ESS)

- Una stazione si può porre in 3 stati:
 - *Transmit*
 - *Awake*: la STA è alimentata completamente.
 - *Doze*: la STA non è abilitata né a trasmettere né a ricevere. Basso consumo energetico.
- Ogni stazione può lavorare in due modi:
 - Active Mode (AM)
 - Power Save mode (PS)

Power Management - Active Mode

- La stazione può ricevere le trame in qualsiasi momento.
- La stazione è sempre in stato Awake.

Power Management – Power Save Mode (PS)

- La stazione rimane in ascolto dei Beacons
- Se in uno di questi è contenuto l'elemento TIM (Traffic Indication Map) che, tramite Association IDentifier (AID) la identifica, la stazione comprende che l'AP ha MSDU (MAC Service Data Unit) bufferizzate per lei
 - La stazione trasmette un trama PS-Poll all'AP, che solo allora trasmette subito (anche senza ACK) le MSDU
 - Una stazione in modalità PS resterà in stato doze tranne che per ascoltare i Beacons, per trasmettere il PS-Poll, riceverne risposta e per ricevere le MSDUs bufferizzate

Power Management: Access Point e stazione in Power Save

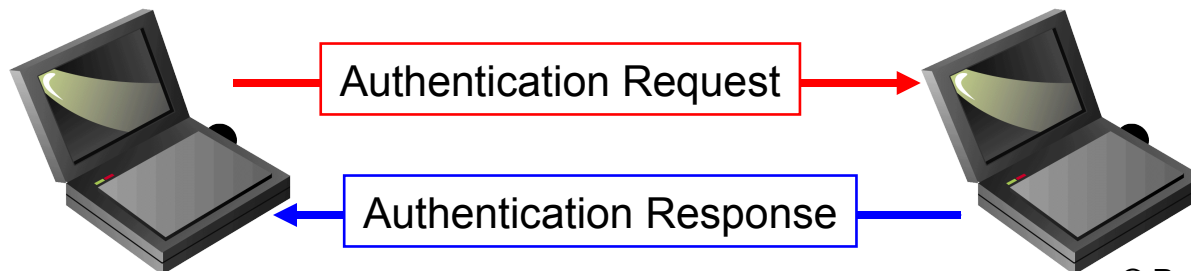
- Se una STA entra in modalità Power Save (PS) avvisa l'AP settando a 1 il bit PwrMgt del Frame Control
- Se alcune STAs (anche una) in una BSS si trovano in modalità PS, l'AP bufferizza tutte le trame broadcast e multicast e le invia subito dopo il successivo Beacon contenente il DeliveryTIM (DTIM)

Autenticazione e segretezza

- Il servizio di autenticazione stabilisce l'identità della STA come membro di un insieme di STAs. Due tipi di servizi di autenticazione:
 - Open System.
 - Shared Key.
- Tra AP e STA in una BSS, tra due STAs in una IBSS.
- Per il servizio di Autenticazione controllata e segretezza (privacy) si adotta l'algoritmo Wired Equivalent Privacy (WEP)
 - Si può utilizzare WEP anche solo per la cifratura dei messaggi

Autenticazione di tipo “Open System”

- Configurazione di default su AP e interfacce di rete
 - Pericolosa se non si adottano altri sistemi di autenticazione più sofisticati che si sovrappongono a quella di tipo “Open System”
- Consta di due passaggi effettuati attraverso trame di servizio di tipo Autenticazione.
 - una stazione richiede l'autenticazione a un'altra stazione o a un Access Point inviando un frame di richiesta di autenticazione e si pone in attesa
 - L'AP o l'altra stazione invia un secondo frame contenente l'esito dell'autenticazione.



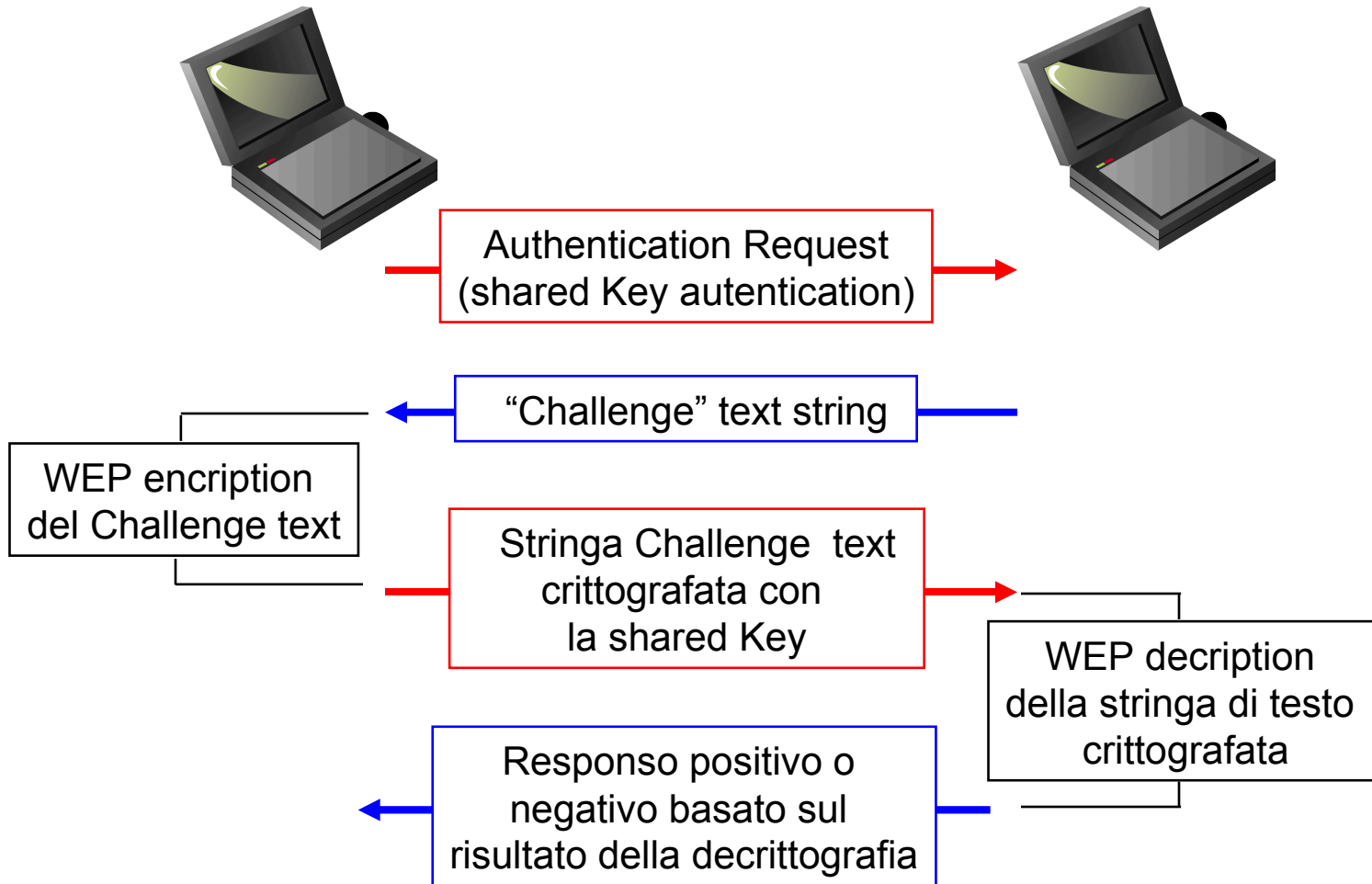
WEP e autenticazione di tipo “Shared Key”

- Autenticazione “Shared Key” realizzata in 802.11 tramite l’adozione di WEP (Wireless Equivalent Privacy).
 - Ipotizza la conoscenza da parte di tutte le STAs di una chiave
- WEP svolge due funzioni:
 - Autenticazione dell’utente
 - Rende la trasmissione di dati relativamente sicura attraverso la cifratura del messaggio

WEP: passi di autenticazione

- Passi di autenticazione:
 - Richiesta d'autenticazione inviata dalla stazione A alla stazione B
 - La stazione B dopo aver ricevuto il frame di richiesta risponde con un frame di 128 ottetti chiamato Challenge Text generato dall'algoritmo WEP.
 - La stazione A copia il Challenge Text in un frame di autenticazione, lo cripta con la chiave pubblica e poi lo invia a B.
 - La stazione B decripta il testo ricevuto con la sua chiave e lo confronta con il testo che aveva inviato in precedenza. Se i due risultano uguali allora B comunica ad A che l'autenticazione ha avuto successo altrimenti lo informa che la sua richiesta è stata rifiutata.

WEP: passi di autenticazione



WEP privacy

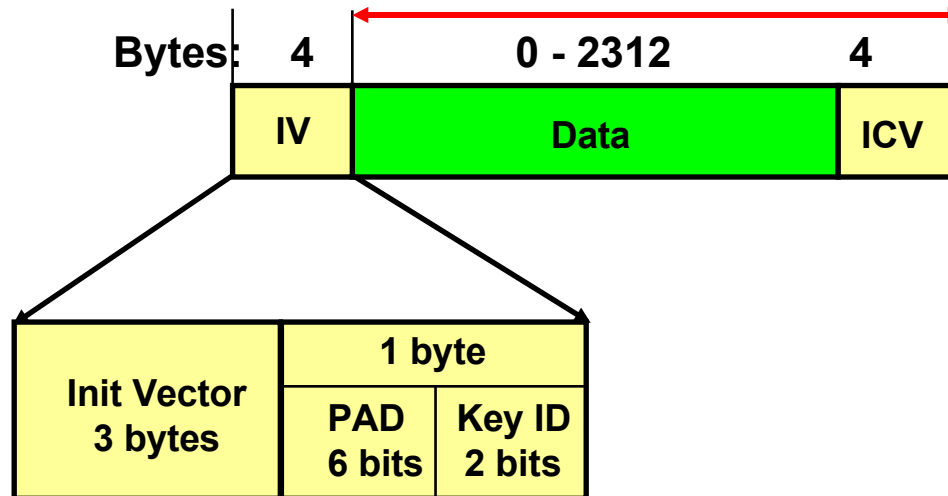
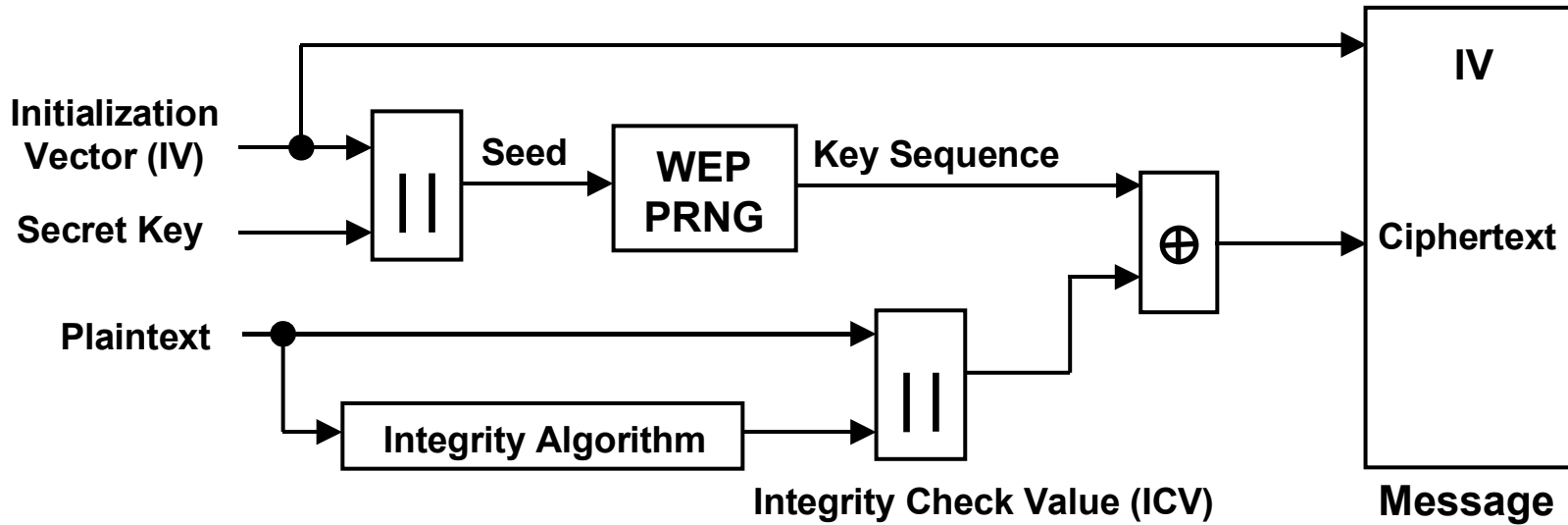
■ Privacy

- Le trasmissioni sono virtualmente “ascoltabili” da chiunque si trovi nell’area
- Sono dunque necessari algoritmi per criptare le comunicazioni
- L’algoritmo WEP (Wireless Equivalent Privacy) usa una chiave per ogni coppia di comunicanti
 - WEP genera chiavi crittografiche segrete che sono utilizzate sia dalla stazione sorgente che da quella destinataria per crittografare i frame da trasmettere (Crittografia a chiave simmetrica)
 - ***Non è però sufficientemente sicuro!***

WEP prima parte

- L'algoritmo WEP si compone dei seguenti passi:
 - Si applica l'algoritmo di integrità al Frame per generare un ICV (Integrity Check Value) di 32 bit inviati insieme ai dati e controllati dal ricevitore per proteggere le informazioni trasmesse da eventuali modifiche non autorizzate.
 - Si genera la Key Sequence da un generatore pseudo-casuale che riceve come input la chiave segreta e il vettore di inizializzazione IV. La Key Sequence ha la stessa lunghezza del Frame + ICV.
 - Si effettua l'OR Esclusivo (X-OR) tra i bit Frame + ICV e la Key Sequence e si genera il testo crittografato.
 - Le due stazioni conoscono la chiave pubblica e non la lunghezza della Key Sequence.

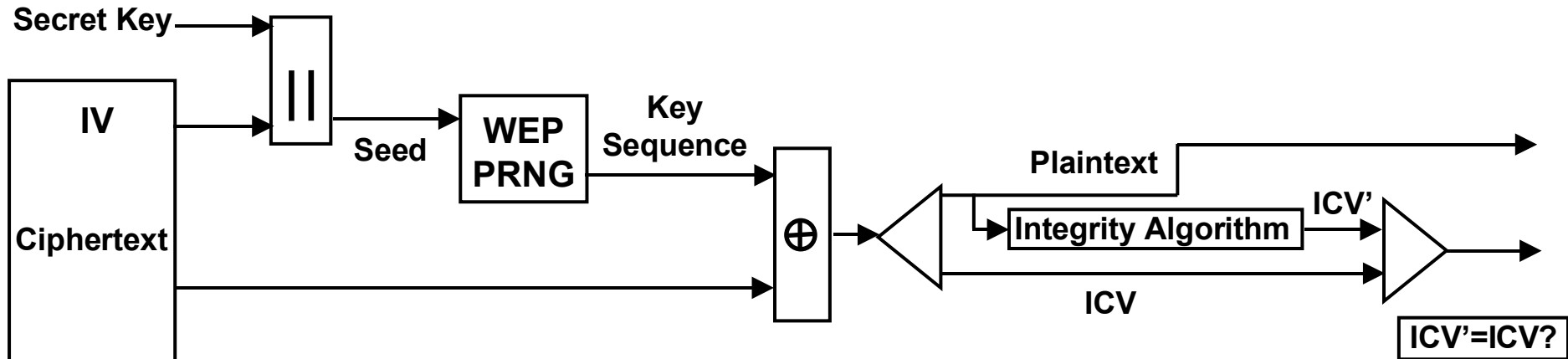
WEP prima parte: cifratura



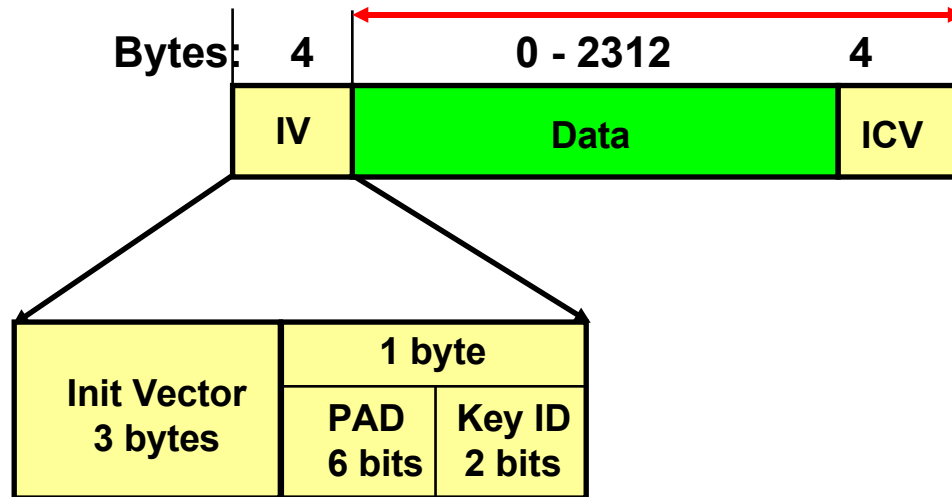
WEP (Wireless Equivalent Privacy)

- L'algoritmo WEP, passi finali:
 - Il ricevitore decifra il testo utilizzando la chiave pubblica e genera la stessa Key sequence utilizzata per criptare il frame.
 - La stazione calcola l'Integrity Check e lo confronta con la sequenza ricevuta decriptata. Se non c'è corrispondenza allora la MSDU non viene inviata all'entità LLC e si invia una "Failure Indication" al Mac Management.

WEP seconda parte: decifratura



Message



TKIP (Temporal Key Integrity Protocol)

- Soluzione che permette di cambiare la chiave WEP ad ogni pacchetto trasmesso
- Prevede tre meccanismi:
 - MIC (Message Integrity Check) è un algoritmo che *previene la modifica dei messaggi*
 - TSC (TKIP Sequence Counter) *previene gli attacchi di tipo replay* basati sul riutilizzo del vettore di inizializzazione utilizzando la chiave dopo averla craccata
 - TEK (Temporal Encryption Key) è un algoritmo che serve come base per creare delle chiavi uniche per ogni pacchetto

Mobilità degli utenti wireless

- Obiettivo: mantenere la connessione di utenti che si spostano su celle differenti da quella iniziale
- Realizzabile tramite IAPP (Interaccess Point Protocol)
 - 802.11F
 - Definisce la modalità con la quale i punti di accesso comunicano attraverso il backbone al fine di passarsi il controllo dei vari utenti mobili
 - Prevede due protocolli base Announce Protocol e Handover Protocol
 - Realizzato inizialmente da un gruppo di produttori guidati da Aironet Wireless Communications, Lucent technologies e Digital Ocean

IAPP: protocolli base

■ Announce Protocol

- Coordina gli access point
- Informa gli altri access point della nuova attività di un access point
- Informa l'access point interessato della nuova configurazione di rete

■ Handover Protocol

- Informa l'access point che una sua stazione si è riassociata con un altro access point
- Il vecchio access point invia i frame destinati alla stazione al nuovo access point
- Il nuovo access point modificherà il suo database per far pervenire i frame alla sua nuova stazione