

MAC e trame IEEE 802.11

Pietro Nicoletti

Studio Reti s.a.s

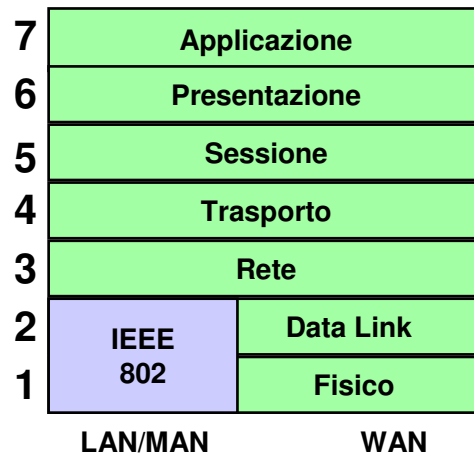
www.studioreti.it

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.

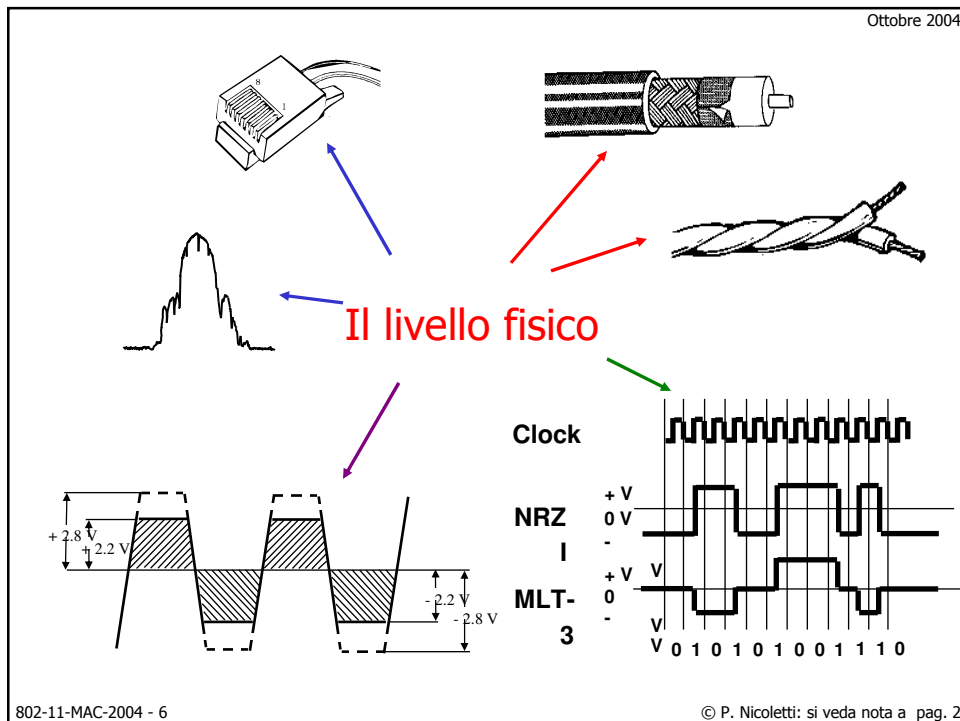
Richiami sulle architetture ISO/OSI e IEEE 802

ISO/OSI e IEEE 802



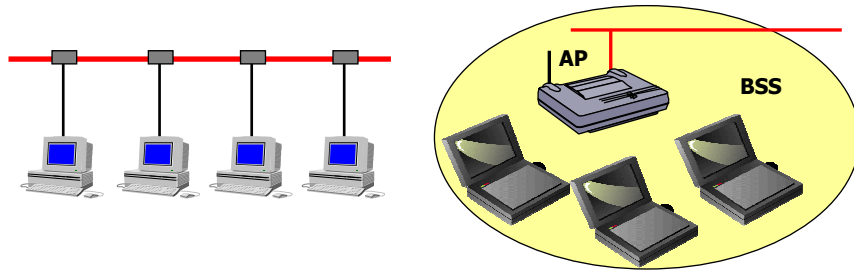
ISO/OSI: Termini principali

- PDU = Protocol Data Unit
 - è una struttura dati generica che può contenere sia dati utili, sia header
- SAP = Service Access Point
 - è un servizio di accesso che serve per il passaggio delle informazioni tra i livelli della pila OSI (una sorta di puntatore software)
 - per passare un'informazione può essere necessario stabilirne la provenienza **SSAP** (Source Service Access Point) e la destinazione **DSAP** (Destination Service Access point)
- A seconda dei vari livelli da cui si osserva un pacchetto avremo: MAC-PDU, LLC-PDU, L3-PDU, L4-PDU ...



Il livello 2: Data Link

- Si occupa di garantire una trasmissione di pacchetti sufficientemente affidabile e verifica la presenza di errori; stabilisce la metodologia per contendere e condividere un mezzo di comunicazione comune quale la rete

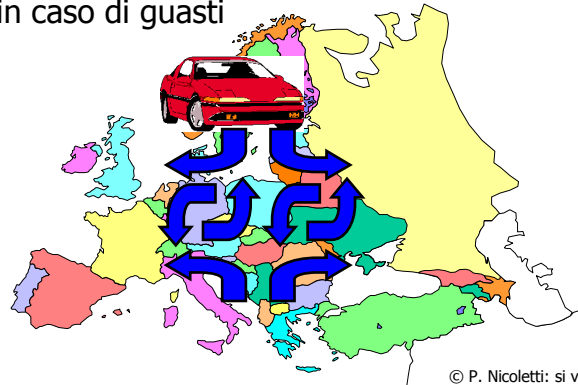


802-11-MAC-2004 - 7

© P. Nicoletti: si veda nota a pag. 2

Il livello 3: Rete

- Definisce gli indirizzi con cui identificare un nodo in rete, si occupa di instradare i messaggi con metodologie diverse a seconda dei protocolli; determina se e quali sistemi intermedi devono essere attraversati per giungere a destinazione e provvede ad instradamenti alternativi in caso di guasti



802-11-MAC-2004 - 8

© P. Nicoletti: si veda nota a pag. 2

Il livello 4: Trasporto

- Il livello 4 accetta dati dal livello 5, li frammenta in pacchetti più piccoli adatti ad essere trasmessi dal livello 3 ed assicura che i pacchetti arrivino tutti nel corretto ordine



Trasporto



Consegna pacco



Firma su ricevuta

I Sottolivelli del livello Data-Link

- IEEE 802 ha suddiviso il livello Data-Link in due sottolivelli:
 - LLC: Logical Link Control
 - MAC: Media Access Control
- LLC è comune a tutte le LAN ed è l'interfaccia verso il livello network.
 - I servizi e i protocolli di questo sottolivello sono descritti nello standard IEEE 802.2
- MAC è specifico per ogni LAN e risolve il problema della condivisione del mezzo trasmissivo.
 - Esistono vari tipi di MAC: ad allocazione di canale fissa o dinamica, deterministici o statistici, ecc.

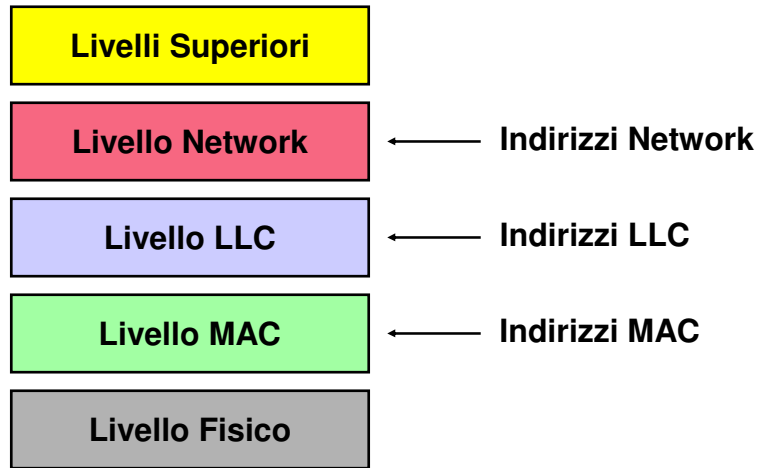
Il sottolivello MAC

- Nelle LAN il livello MAC realizza sempre una rete di tipo broadcast
 - ogni stazione a livello data link riceve le trame inviate da tutte le altre stazioni
- Il broadcast può essere realizzato:
 - con topologie intrinsecamente broadcast quali il bus o l'etere (WM=Wireless Medium)
 - con topologie punto a punto quali l'anello
- I canali trasmissivi sono sufficientemente affidabili e non è necessario in genere correggere gli errori a livello MAC
 - le LAN sono connectionless a livello MAC

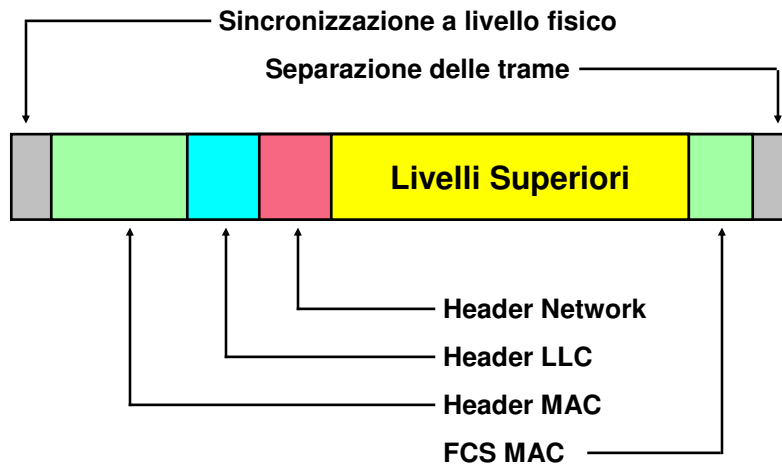
L'importanza del MAC

- Il sottolivello MAC è di fondamentale importanza nelle reti di tipo broadcast
- In tali reti occorre:
 - in trasmissione: determinare chi deve/può utilizzare il canale
 - in ricezione: discriminare quali messaggi sono destinati alla stazione tramite l'utilizzo di indirizzi
 - i nodi o apparati di rete vengono identificati in una LAN tramite degli indirizzi di 6 ottetti o byte denominati "*Indirizzi MAC*"
 - nelle Wireless LAN è necessaria un'ulteriore informazione riguardante la cella o BSS entro la quale s'intende comunicare "*Indirizzo BSSID*"

Gli indirizzi

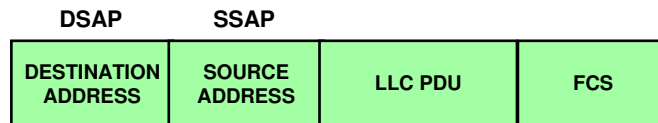


La trama nelle LAN

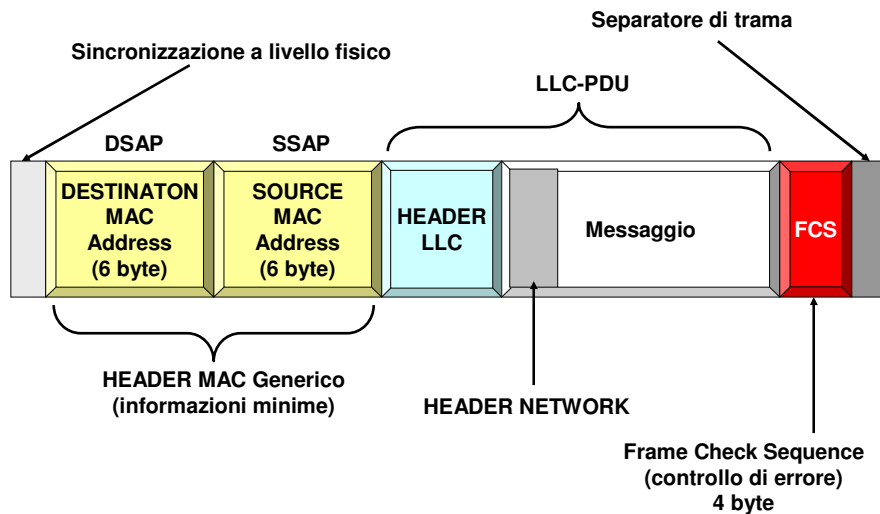


La MAC PDU (Protocol Data Unit)

- I campi principali di una MAC PDU sono:
 - Gli indirizzi (detti SAP: Service Access Point) univoci a livello mondiale:
 - DSAP: Destination SAP
 - SSAP: Source SAP
 - La LLC-PDU contiene l'header LLC e i dati
 - La FCS (Frame Control Sequence): un CRC su 32 bit per il controllo dell'integrità della trama



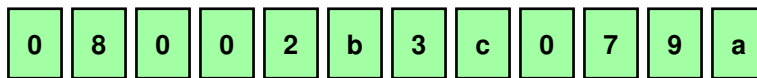
La MAC PDU (Protocol Data Unit)



Gli indirizzi MAC

- Sono standardizzati dalla IEEE
 - sono lunghi 6 byte, cioè 48 bit
 - si scrivono come 6 coppie di cifre esadecimali
- Ad esempio:

00001000000000000010101100111100000011110011010



08-00-2b-3c-07-9a

Gli indirizzi MAC

- Si compongono di due parti grandi 3 Byte ciascuna:
 - I tre byte più significativi indicano il lotto di indirizzi acquistato dal costruttore della scheda, detto anche *vendor code o OUI (Organization Unique Identifier)*.
 - I tre meno significativi sono una numerazione progressiva decisa dal costruttore



OUI assegnato dall'IEEE

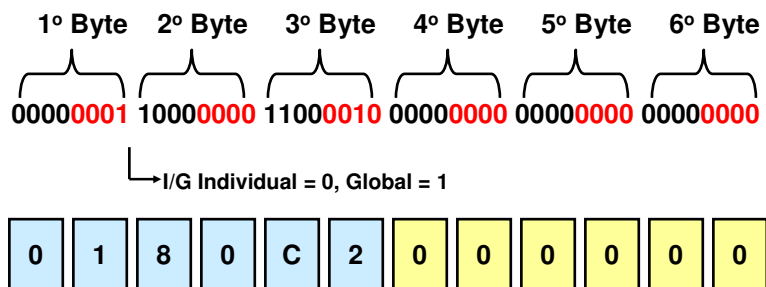
Assegnato dal costruttore

Tipi di indirizzi MAC

- Single: di una singola stazione
 - tipo universale contenuto in ROM
 - tipo locale contenuto in RAM
- Multicast: di un gruppo di stazioni
 - contenuto normalmente in RAM per il periodo del suo impiego
 - contenuto in ROM se riservato dall'IEEE
- Broadcast: di tutte le stazioni (ff-ff-ff-ff-ff-ff)

Indirizzi Multicast o di gruppo

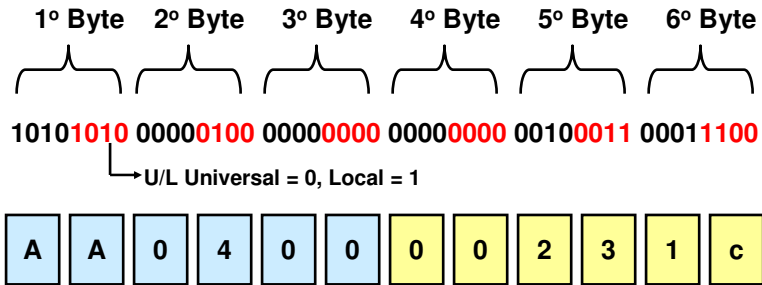
- Il valore del byte più significativo è dispari



01-80-C2-00-00-00

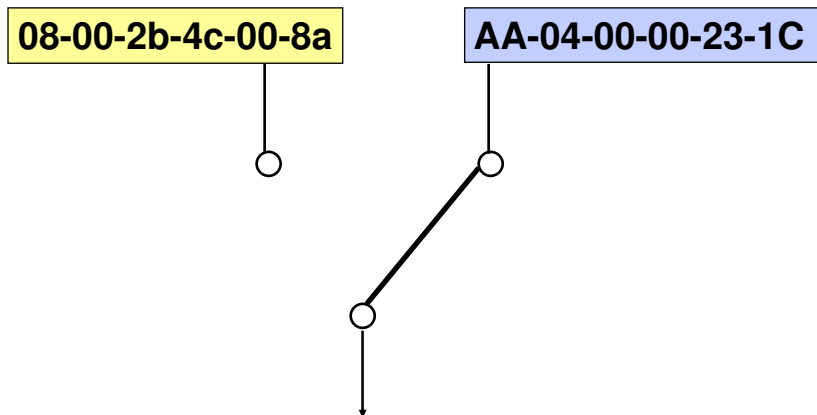
Indirizzo MAC locale

- Assegnato all'interfaccia di rete a livello di configurazione a dai software di rete
- Alternativo all'indirizzo MAC universale



AA-04-00-00-23-1C

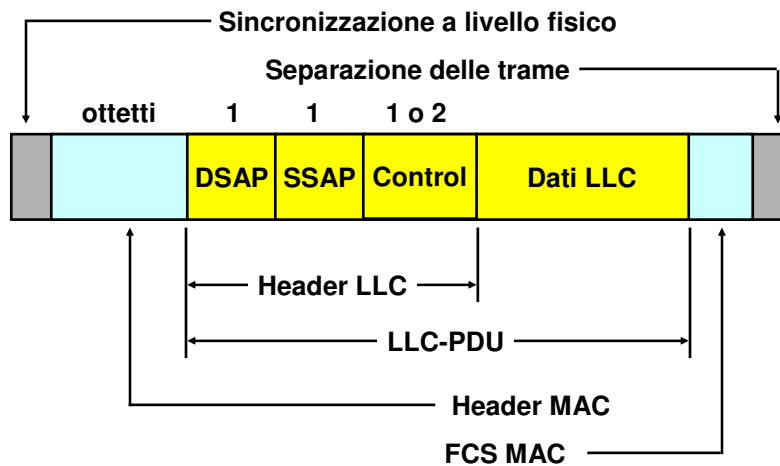
Indirizzo Universale o Locale



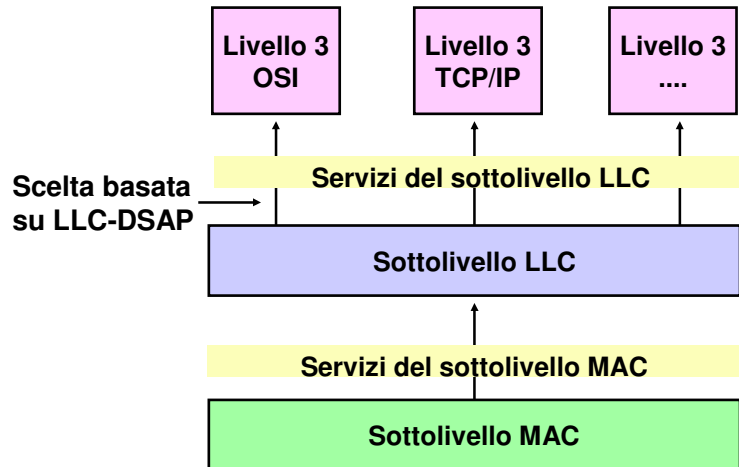
Il sottolivello LLC

- È la versione per le LAN di HDLC
- LLC è utilizzabile con un qualsiasi MAC
- LLC può offrire al Livello 3 i seguenti tipi di servizio:
 - *Tipo 1*: Unacknowledged connectionless service
 - *Tipo 2*: Connection Oriented service
 - *Tipo 3*: Semireliable service
- LLC ha sue PDU (LLC-PDU) molto simili a quelle di HDLC
- LLC ha un suo SAP (LLC-SAP) che viene utilizzato per discriminare tra più protocolli di livello superiore

La LLC-PDU



I servizi LLC verso il livello 3



LLC SAP (Service Access Point)

- Sono grandi un Byte
 - due bit I/G e U riservati
 - 64 indirizzi singoli, globali definibili
 - ff broadcast
 - 00 data link layer itself

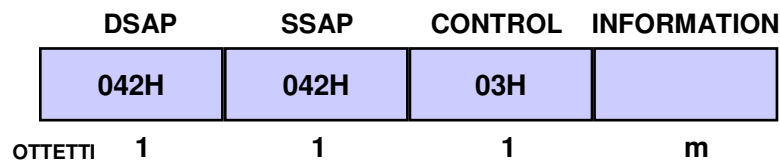
1 0 1 1 1 1 0 1

I/G (Individual=0, Group=1)
 U (Non Universal=0, Universal=1)

- Gli indirizzi universali sono assegnati dall'ISO solo per i protocolli progettati da un comitato di standardizzazione

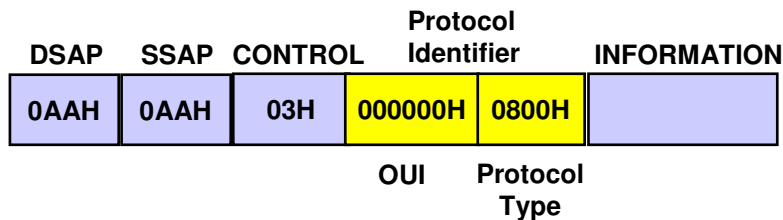
Esempi di SAP-LLC

- Codifiche di DSAP e SSAP
 - 0FEH - protocollo ISO 8473
 - 042H - protocollo IEEE 802.1D Spanning Tree
 - 0AAH - pacchetto LLC di tipo SNAP
- Nel campo control la codifica 03H indica un pacchetto UI (Unnumbered Information)



SNAP PDU

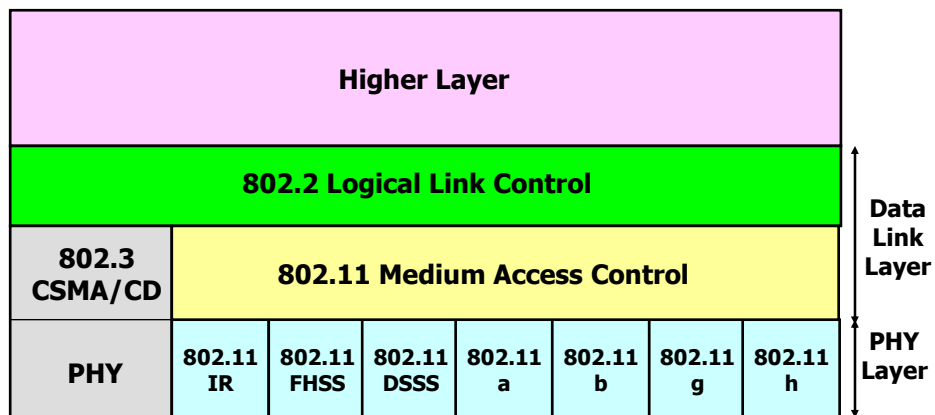
- Subnetwork Access Protocol (SNAP)
 - Si riconoscono dalla codifica 0AAH in DSAP e SSAP
 - Si utilizzano quando i pacchetti LLC contengono dati derivati da protocolli non OSI
 - Esiste un Header aggiuntivo su 5 ottetti detto Protocol Identifier



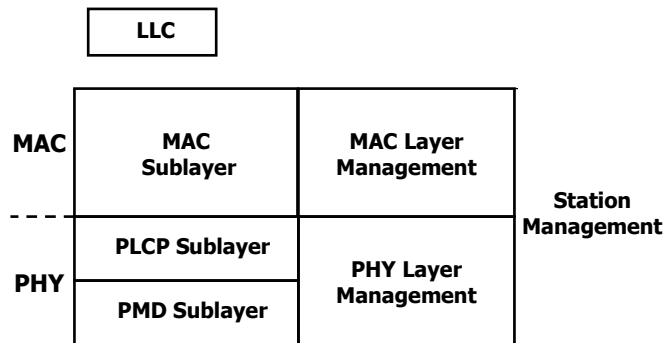
Il Protocol Identifier

- È composto da due parti:
 - L'OUI (su 3 ottetti) che indica chi ha progettato il protocollo
 - Il protocol type (2 ottetti) che identifica il protocollo
- Se l'OUI è uguale a zero il protocol type è quello usato in ethernet v2.0, ad esempio:
 - 6003 Decnet fase IV
 - 6004 LAT
 - 8137/8 IPX
 - 0800 IP
 - 0806 ARP
 - 809B EtherTalk (AppleTalk over Ethernet)

Architettura 802.11 e livelli OSI



Architettura 802.11 e livelli OSI



PLCP = Physical layer convergence procedure
PMD = Physical medium dependent

PLCP: Physical layer convergence procedure

- E' uno strato di adattamento tra il livello fisico strettamente dipendente dalla trasmissione e ricezione sul mezzo trasmissivo e il livello MAC.
 - PLCP specifico per FHSS
 - PLCP specifico per DSSS di 802.11 (1 e 2 Mb/s)
 - PLCP specifico per DSSS di 802.11a (da 6 a 54 Mb/s)
 - PLCP specifico per DSSS di 802.11h (da 6 a 54 Mb/s)
 - PLCP specifico per DSSS di 802.11b (da 1 a 11 Mb/s)
 - PLCP specifico per DSSS di 802.11g (da 1 a 54 Mb/s)
- Definisce per esempio:
 - la velocità a cui si opera
 - il sistema di modulazione del segnale radio

I servizi MAC

- Autenticazione
- Associazione
- Diassociazione
- Distribuzione
- Riassociazione
- Privacy
- Integrazione
- Sincronizzazione

I servizi MAC (parte 1)

- Autenticazione
 - Utilizzata per verificare l'identità delle stazioni che vogliono stabilire fra loro un link diretto di comunicazione
 - Lo standard fornisce il supporto e lascia la possibilità di implementare protocolli di autenticazione diversi
- Associazione
 - Ogni stazione deve associarsi con un access point prima di poter inviare dati attraverso un distribution system
 - E' il primo passo che consente alla stazione di muoversi tra celle diverse

I servizi MAC (parte 2)

- Disassociazione
 - E' la notifica effettuata da una stazione quando lascia la rete o da un access point quando viene disconnesso da tutte le stazioni per problemi di manutenzione
 - Termina una precedente associazione
- Distribuzione
 - Viene utilizzato da tutte le stazioni che devono inviare frame MAC attraverso un distribution system
 - Per effettuare il trasporto dei frame si sfruttano tutte le informazioni di associazione

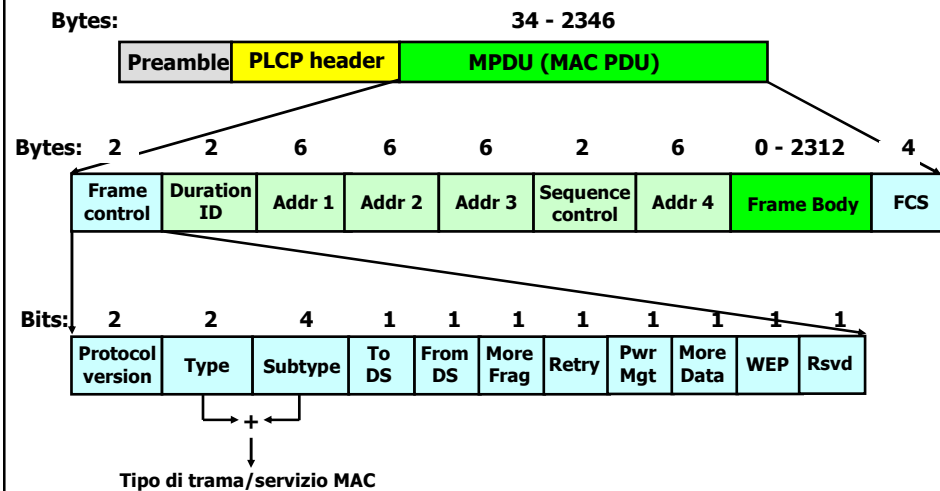
I servizi MAC (parte 3)

- Riassociazione
 - Offre la possibilità a una stazione di modificare lo stato di associazione
 - La stazione può cambiare la sua associazione da un access point a un altro effettuando il trasferimento da una cella ad un'altra
 - Permette la mobilità delle stazioni al di fuori del BSA (roaming)
- Privacy
 - Implementa le politiche di sicurezza, utilizzando algoritmi per criptare e decrittare i messaggi
- Integrazione
 - Permette lo scambio di frame Mac tra un distribution system e una LAN

I servizi MAC: la sincronizzazione

- Lo scopo è quello di sincronizzare le STAs di una stessa BSS ad un clock comune.
- Time Synchronization Function (TSF)
 - In una **ESS** l'AP trasmetterà periodicamente delle trame Beacon, in cui copierà il valore del proprio TSF timer (Timestamp), e le STAs della BSS aggiorneranno a quel valore il proprio TFS timer.
 - In una **IBSS** l'algoritmo è distribuito: ogni STA trasmette trame Beacon con il proprio Timestamp.

Formato della trama 802.11



I campi del Frame Control

- Protocol Version:
 - zero per lo standard 802.11
- Type= tipo di trama:
 - data, management, control
- Subtype = sotto-tipo di trama:
 - ognitipo di trama ha un insieme di sottotipi
- ToDS:
 - bit impostato a 1 se è una trama dati destinata al DS
- FromDS:
 - bit impostato a 1 se è una trama dati uscente dal DS

I campi del Frame Control

- Retry:
 - bit impostato a 1 per tutte le trame dati e di management che sono una ritrasmissione di trame precedenti.
- More fragments:
 - bit impostato a 1 per le trame dati e management che precedono altri frammenti dello stesso MSDU o MMPDU
- Power Management = indica lo stato in cui si porterà la Stazione al termine della sequenza di trame
 - bit impostato a 1 se la stazione si porterà in modalità Power Save mode (PS)
- More Data:
 - il bit impostato a 1 indica ad una Stazione in modalità Power Save che ci sono altre MSDUs o MMPDUs di tipo dati o management bufferizzate nell'Access Point.

I campi del Frame Control

- WEP:
 - se il bit è impostato a 1 indica che il campo del Frame Body ci sono delle informazioni che devono essere processate dall'algoritmo WEP.
- Order:
 - se il bit è impostato a 1 indica che la trasmissione della MSDU è sottoposta a restrizioni

Tipo di trama e servizio MAC (parte 1)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	Announcement traffic indication message (ATIM)
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved

Tipo di trama e servizio MAC (parte 2)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
01	Control	0000-1001	Reserved
01	Control	1010	Power Save (PS)-Poll
01	Control	1011	Request To Send (RTS)
01	Control	1100	Clear To Send (CTS)
01	Control	1101	Acknowledgment (ACK)
01	Control	1110	Contention-Free (CF)-End
01	Control	1111	CF-End + CF-Ack

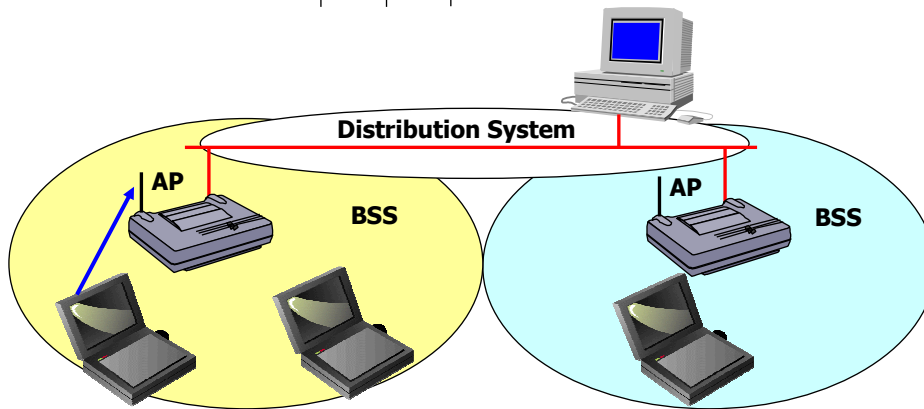
Tipo di trama e servizio MAC (parte 3)

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Trasmissione tra stazioni dello stesso BSS

Bits: 2 2 4 1 1 1 1 1 1 1 1

Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
			0	0						



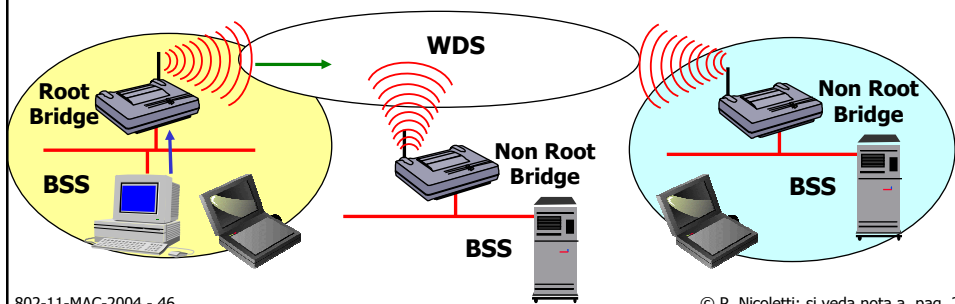
802-11-MAC-2004 - 45

© P. Nicoletti: si veda nota a pag. 2

Trasmissione di trama destinata al Distribution System

Bits: 2 2 4 1 1 1 1 1 1 1 1

Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
			1	0						



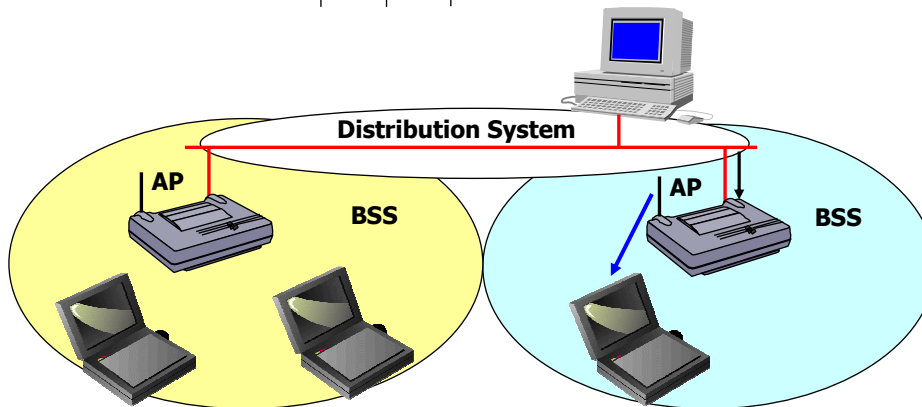
802-11-MAC-2004 - 46

© P. Nicoletti: si veda nota a pag. 2

Trasmissione di trama uscente dal Distribution System

Bits: 2 2 4 1 1 1 1 1 1 1 1

Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
			0	1						



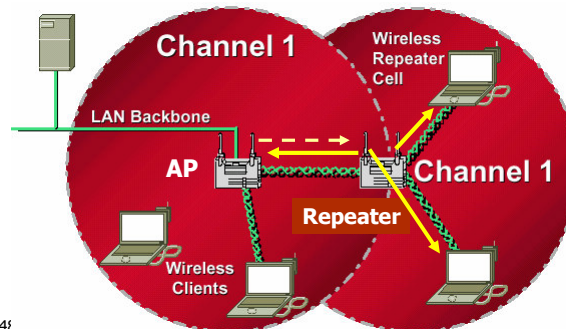
802-11-MAC-2004 - 47

© P. Nicoletti: si veda nota a pag. 2

Trasmissione di trama destinata alla STA di un altro BSS, trasmessa da un AP ad un altro AP attraverso il Wireless Distribution System

Bits: 2 2 4 1 1 1 1 1 1 1 1

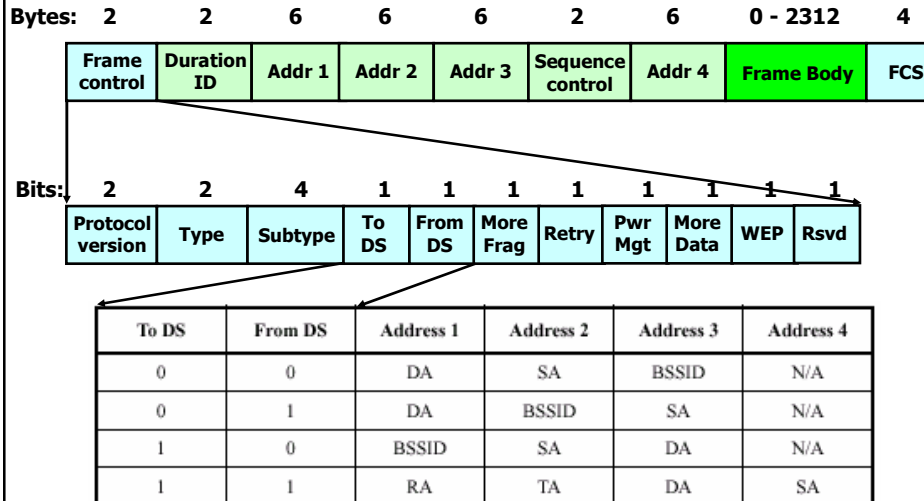
Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Rsvd
			1	1						



802-11-MAC-2004 - 48

Nicoletti: si veda nota a pag. 2

Gli indirizzi MAC in 802.11



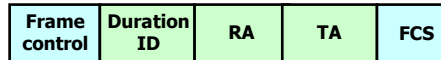
Gli indirizzi MAC in 802.11

- DA = Destination Address indica l'indirizzo MAC del Destinatario
- SA = Source address indica l'indirizzo MAC della stazione che ha trasmesso il messaggio MSDU (MAC Service Data Unit)
- RA = Receiver Address indica l'indirizzo MAC della stazione nel WM che deve ricevere il messaggio
- TA = Transmitter Address indica la stazione che ha trasmesso il messaggio nel WM
- BSSID identifica in modo univoco un BSS

Trame RTS e CTS

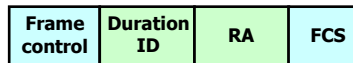
■ Trama RTS

- Il campo Duration contiene il valore in μs del tempo necessario per trasmettere la trama dati o management + CTS + ACK + intervallo SIFS



■ Trama CTS

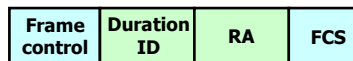
- Il campo Duration contiene il valore in μs ottenuto dal precedente RTS meno il tempo necessario per trasmettere il CTS e il suo intervallo SIFS



Trame ACK e PS-Poll

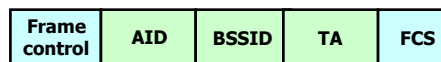
■ Trama ACK:

- Il campo Duration contiene il valore in μs ottenuto dalla precedente trama dati o management ricevuta meno il tempo necessario per trasmettere l'ACK e il suo intervallo SIFS

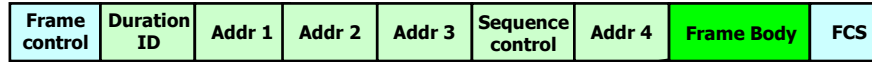


■ Trama PS-Poll:

- Il campo AID contiene l'identificativo di associazione,



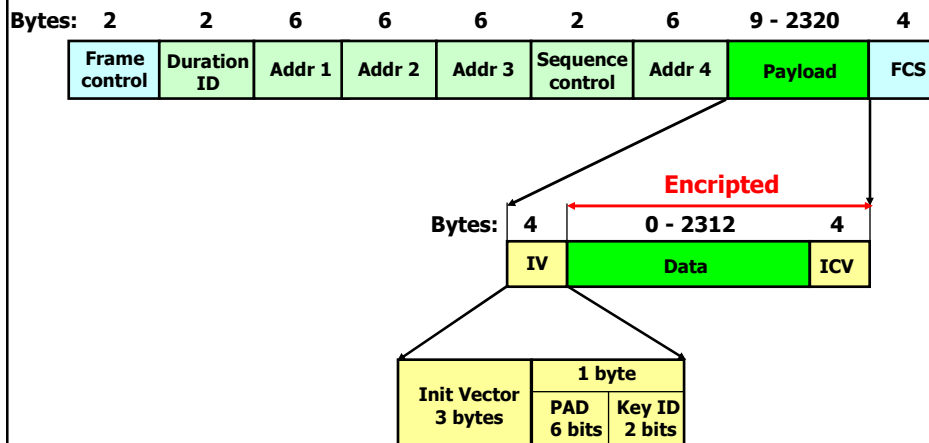
Trama Beacon



Order	Information	Notes
1	Timestamp	
2	Beacon interval	
3	Capability information	
4	SSID	
5	Supported rates	
6	FH Parameter Set	The FH Parameter Set information element is present within Beacon frames generated by STAs using frequency-hopping PHYs.
7	DS Parameter Set	The DS Parameter Set information element is present within Beacon frames generated by STAs using direct sequence PHYs.
8	CF Parameter Set	The CF Parameter Set information element is only present within Beacon frames generated by APs supporting a PCF.
9	IBSS Parameter Set	The IBSS Parameter Set information element is only present within Beacon frames generated by STAs in an IBSS.
10	TIM	The TIM information element is only present within Beacon frames generated by APs.

Trama MSDU con WEP

- Espande il Payload di 8 byte



PLCP Header

- Contiene le informazioni necessarie all'adattamento tra i livelli PMD e MAC
- Il formato e contenuto dell'header cambia in funzione dei vari PLCP specifici per:
 - FHSS
 - DSSS di 802.11 (1 e 2 Mb/s)
 - DSSS di 802.11a (da 6 a 54 Mb/s)
 - DSSS di 802.11h (da 6 a 54 Mb/s)
 - DSSS di 802.11b (da 1 a 11 Mb/s)
 - DSSS di 802.11g (da 1 a 54 Mb/s)

