



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# Protocolli: Prestazioni

Franco CALLEGATI

Dipartimento di Informatica: Scienza e Ingegneria



# Affidabilità

- Controllo dell'errore
  - Rivelazione e correzioni
  - CRC e Internet checksum
- Eventuale recupero dell'errore
  - ARQ e ritrasmissione
- Controllo di flusso e sequenza
  - Ack e ARQ
- Questi temi sono stati trattati lo scorso anno



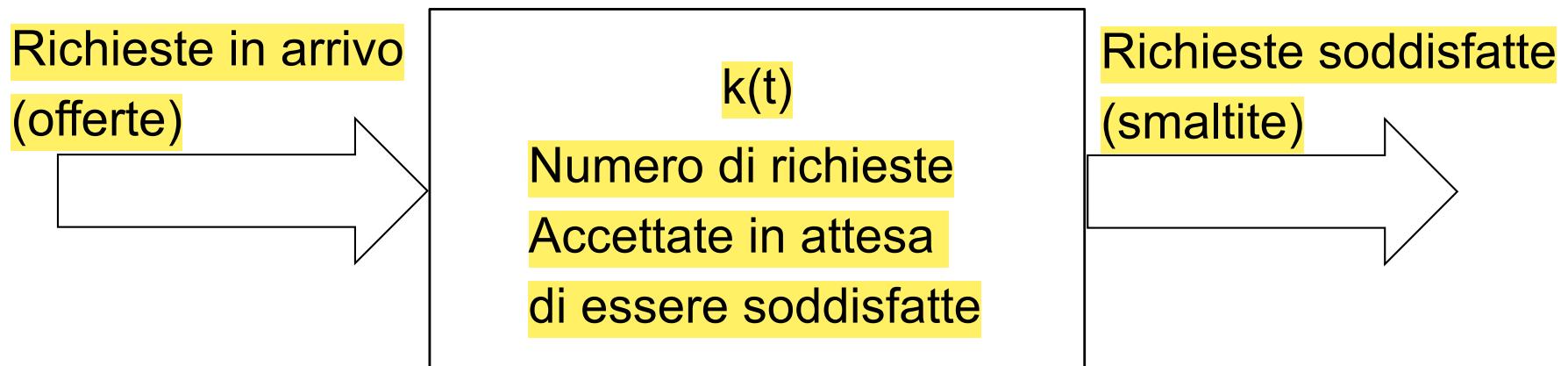
# Funzionalità e prestazioni

- I protocolli sono progettati per garantire
  - Funzionalità
    - La trasmissione dati deve poter avvenire risolvendo i problemi che si riscontrano nell'accesso e nell'uso del canale
  - Prestazioni
    - La trasmissione deve avvenire con successo utilizzando per quanto possibile la capacità messa a disposizione dallo strato fisico



# Le prestazioni in generale

- Un *sistema* deve *smaltire* del *lavoro* che gli viene *offerto* dall'esterno
- Esempio nel caso specifico delle reti di tlc
  - Livello N+1 invia PDU al livello N tramite la relativa interfaccia (e un opportuno SAP)
  - Livello N impiega un certo tempo per soddisfare la richiesta





# Arrivi e partenze

Richieste in arrivo al sistema

$$a(t)$$

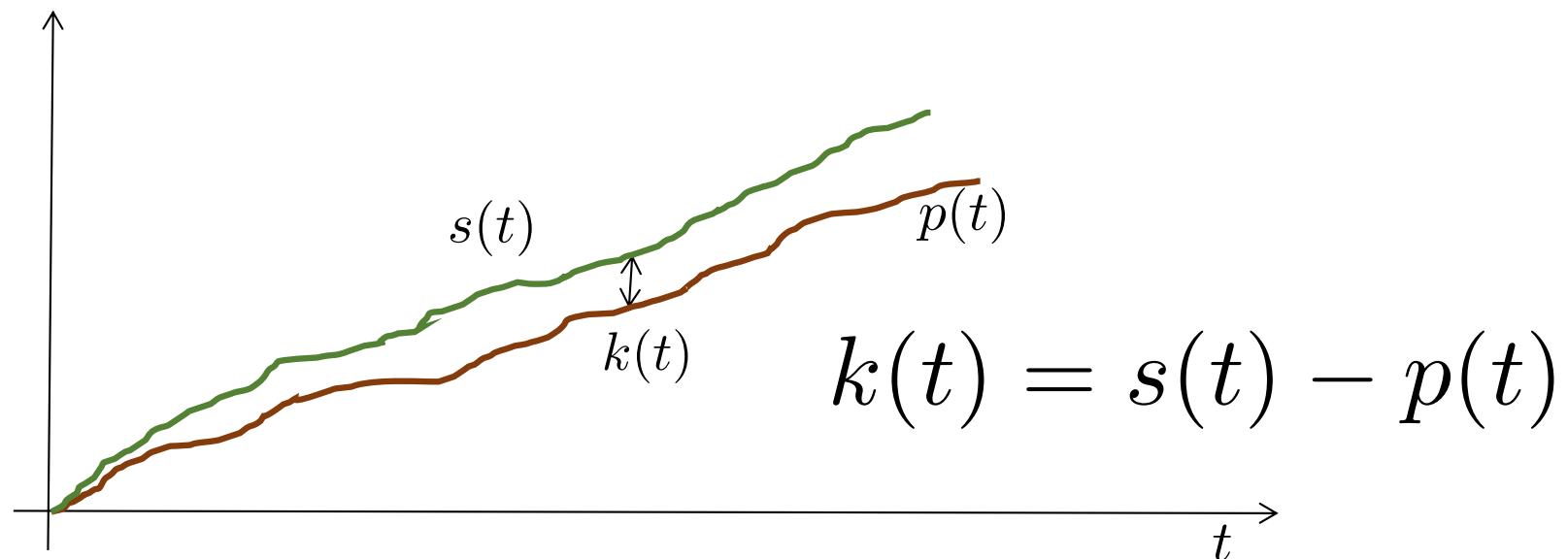
- Numero di richieste di servizio giunte al tempo  $t$

$$s(t)$$

- Numero di richieste accettate al tempo  $t$

$$p(t)$$

- Numero di partenze dal sistema al tempo  $t$





# Richieste offerte e smaltite

- Frequenza media delle richieste offerte

$$\lambda = \lim_{t \rightarrow \infty} \frac{a(t)}{t}$$

- Frequenza media delle richieste smaltite

$$\lambda_s = \lim_{t \rightarrow \infty} \frac{p(t)}{t}$$

- Se il sistema in oggetto non produce lavoro ma lo riceve solamente dall'esterno

$$\lambda_s \leq \lambda$$



# Richieste perdue

$$\lambda_s = \lambda$$

Implica

Accettate uguali a quelle in arrivo

$$s(t) = a(t)$$

Richieste Smallite uguali alle Richieste in Arrivo al sistema (non ci sono richieste perdute)

- Tutte le richieste vengono accettate dal sistema e prima o poi soddisfatte

$$\lambda_s < \lambda$$

implica

Le Richieste Accettate non sono uguali a quelle in Arrivo (quindi ci sono richieste perdute)

$$r(t) = a(t) - s(t)$$

- Dove  $r(t)$  rappresenta le richieste che non vengono accettate e sono *rifiutate o perdute* dal sistema



# Analogamente

- Posso definire

$$\lambda_p = \lim_{t \rightarrow \infty} \frac{r(t)}{t}$$

Frequenza media delle richieste perdute

- Da cui consegue

$$\lambda = \lambda_s + \lambda_p$$

Smaltite + Perdute



# Utente e servizio

- In una rete a pacchetto considerare il semplice «bit rate» del canale non è del tutto corretto
  - I bit sono raggruppati in pacchetti
  - L'unità di servizio è il pacchetto non il bit
    - In altre parole trasmettere una porzione di bit appartenenti ad un pacchetto non ha senso di per se perché solo quando l'intero pacchetto è trasmesso e ricevuto può essere utile.
- **Il riferimento è il tempo di servizio dell'intero pacchetto che solo se completato produce un risultato «utile» per l'utente**

☞ Il tempo necessario per fornire il servizio al pacchetto

$\vartheta$  Tempo richiesto dal servizio di un generico cliente (pacchetto dati, PDU)

- Servizio aleatorio
  - Si fa riferimento in prima battuta al tempo medio
- Servizio deterministico
  - Tempo di servizio costante ed uguale al suo valore medio



Il tempo medio di trasmissione di un pacchetto in una rete a commutazione di pacchetto, basandosi sulla lunghezza del pacchetto e sulla capacità del canale.

# La lunghezza del pacchetto

- $L$  lunghezza del pacchetto in bit
- $C$  capacità del canale in bit per secondo (bitrate)
- Ovviamente

$$\bar{\vartheta} = \frac{L}{C}$$

Tempo di trasmissione medio (rappresenta il tempo che un router (o un altro dispositivo di rete) impiega per caricare un pacchetto sul canale di trasmissione).

Il tempo di propagazione è il tempo che un pacchetto impiega a viaggiare fisicamente da un capo all'altro di un canale di trasmissione, una volta che è stato caricato sul canale.

Tempo di Propagazione = Lunghezza del Canale (D) / Velocità di Propagazione (V)



# Frequenza di servizio

- L'inverso del tempo medio di servizio viene detto frequenza media di servizio

$$\mu = \frac{1}{\bar{\vartheta}}$$

- La frequenza media di servizio è ovviamente legata alla presenza di utenti del sistema
  - Se non vi sono richieste di servizio ovviamente la frequenza di servizio è nulla
  - Se vi sono richieste di servizio il parametro da indicazione di quanto velocemente esse vengono soddisfatte



# Il ruolo di $\mu$

- Di fatto  $\bar{v}$  può essere interpretato come una sorta di capacità massima del servitore
- Se  $\bar{v} = 0.5 \text{ s}$  ne consegue che il servitore al più smaltirà  $\mu = 2 \text{ pacchetti/s}$   
(numero massimo di pacchetti che il servitore può servire in un'unità di tempo)
- Possiamo dire che per il singolo servitore

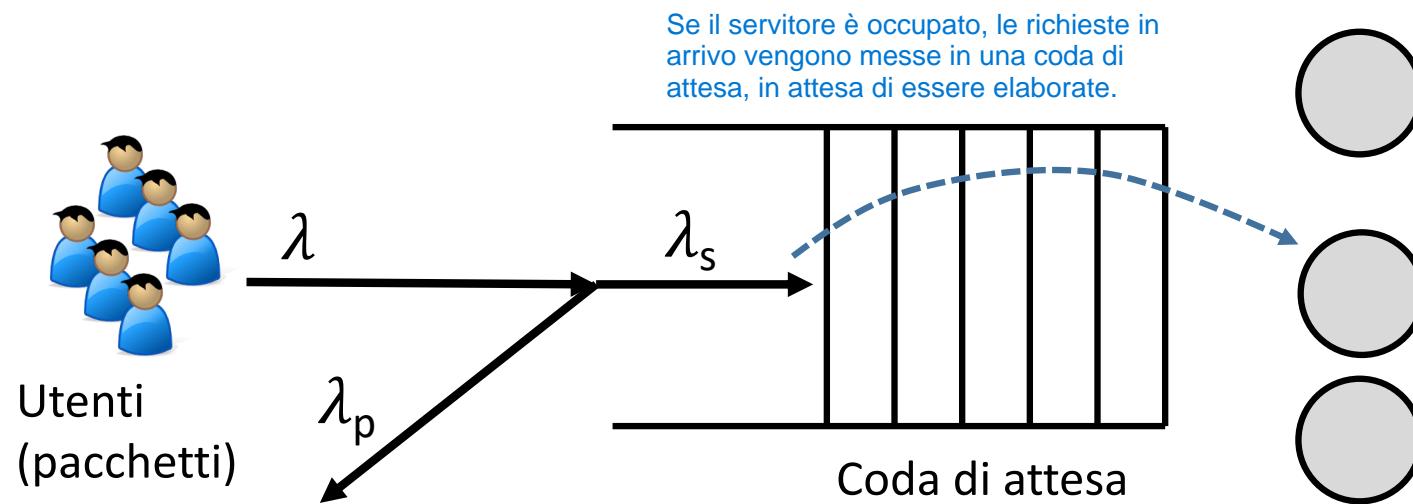
$$\lambda_s^{\max} = \mu$$

Frequenza massima media delle richieste smaltite in un'unità di tempo.  
È il tasso massimo di arrivo delle richieste che un servitore può accettare senza che si verifichi congestione.  
Questo indica che il servitore può servire richieste a una frequenza massima pari alla sua capacità.



# Di quale sistema parliamo

- Per le reti hanno particolare importanza i sistemi a coda



Utenti  
(pacchetti)

Uno o più servitori  
(sistemi di trasmissione)

Nella reti a pacchetto 1 solo servitore  
è il caso di riferimento



# Cosa accade all'utente in un sistema a coda?

- L'utente permane nel sistema per un tempo che tiene conto dell'attesa in coda e del tempo di esecuzione del servizio
- $\bar{\delta}$  tempo medio totale speso dal singolo utente nel sistema a coda che è composto da
  - $\bar{\vartheta}$  tempo <sup>medio</sup>effettivo di servizio (l'utente fa le cose per le quali è entrato nel sistema)
  - $\bar{T}_A$  tempo <sup>medio</sup>speso in coda, ossia tempo di attesa prima di essere effettivamente servito

$$\bar{\delta} = \bar{\vartheta} + \bar{T}_A$$

Tempo medio di Attesa



# Il traffico

- Le prestazioni del sistema che fornisce il servizio dipendono:
  - Dalla numerosità degli arrivi, tipicamente frequenza media di arrivo (utenti per secondo)
  - Dalla durata del servizio, tipicamente la frequenza media di servizio (utenti al secondo) o il tempo medio di servizio (secondi)  
(o richieste)
- Si definisce **traffico** il numero medio di utenti  $\bar{A}$  presenti nel sistema in un dato momento.
- Si dimostra che il prodotto fra frequenza di arrivo e tempo medio di permanenza nel sistema (teorema di Little) da il traffico

$$A = \lambda \bar{\delta}$$

Rappresenta il tempo medio che una richiesta trascorre nel sistema. Include sia il tempo medio di attesa in coda sia il tempo medio di servizio.

Frequenza media di arrivo delle richieste, misurata in unità per secondo (sono le richieste in arrivo, non quelle accettate e dentro il sistema (infatti, in arrivo = serviti+perduti))



# Alcune definizioni conseguenti

- Per analogia si definiscono

$$A_0 = \lambda \bar{\vartheta}$$

Tempo di trasmissione medio

- Traffico offerto (occupazione media di un sistema ideale che serve subito tutti gli utenti senza attesa)

$$A_s = \lambda_s \bar{\vartheta}$$

- Traffico smaltito (occupazione media dei servitori del sistema)
- Ci ricorda che se  $\lambda$ s utenti mediamente entrano per unità di tempo ~~entriano~~ allora  $\lambda$ s devono uscire

$$A_p = \lambda_p \bar{\vartheta}$$

- Traffico perduto (occupazione media di un sistema che serve gli utenti che invece sono stati rifiutati)



# Il traffico smaltito

Riflette la capacità utilizzata rispetto alla capacità totale disponibile.

- $A_s$  da una valutazione della capacità di servizio del sistema considerato
- Se i servitori sono impegnati al 100% il sistema esprime tutta la sua capacità di servizio
- Se i servitori sono  $m$  allora

$$0 \leq A_s \leq m$$

Se il sistema è sfruttato al 100% (tutti i servitori sono operativi e utilizzati senza margini di inutilizzo), il throughput coincide con la capacità massima del sistema

- $A_s$  è spesso indicato con il nome di *throughput*

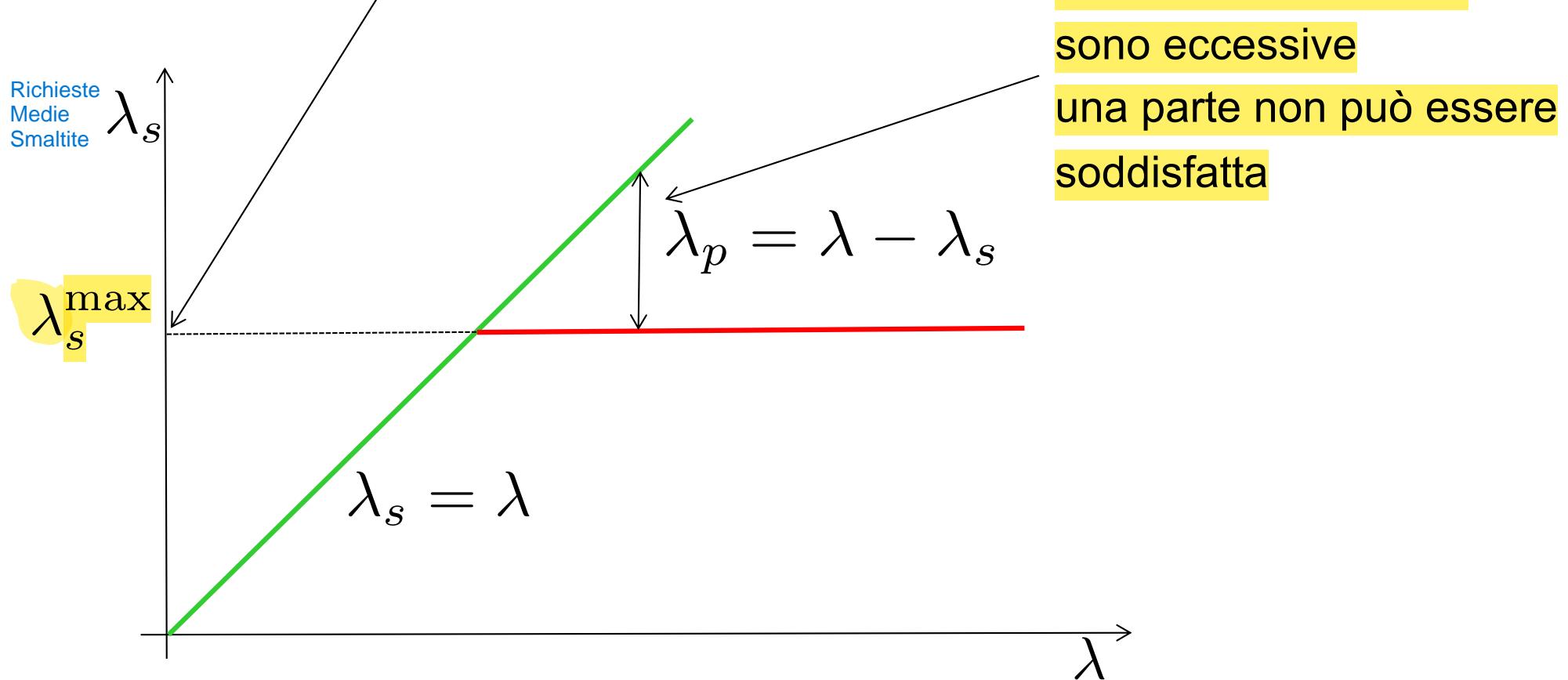
Throughput: misura la quantità effettiva di richieste soddisfatte in un dato intervallo di tempo (È un indicatore fondamentale per valutare le prestazioni di una rete o di un sistema di comunicazione).

# In un sistema ideale

Il sistema ha una capacità massima finita

di smaltire richieste

(dipende dalle condizioni in cui opera)

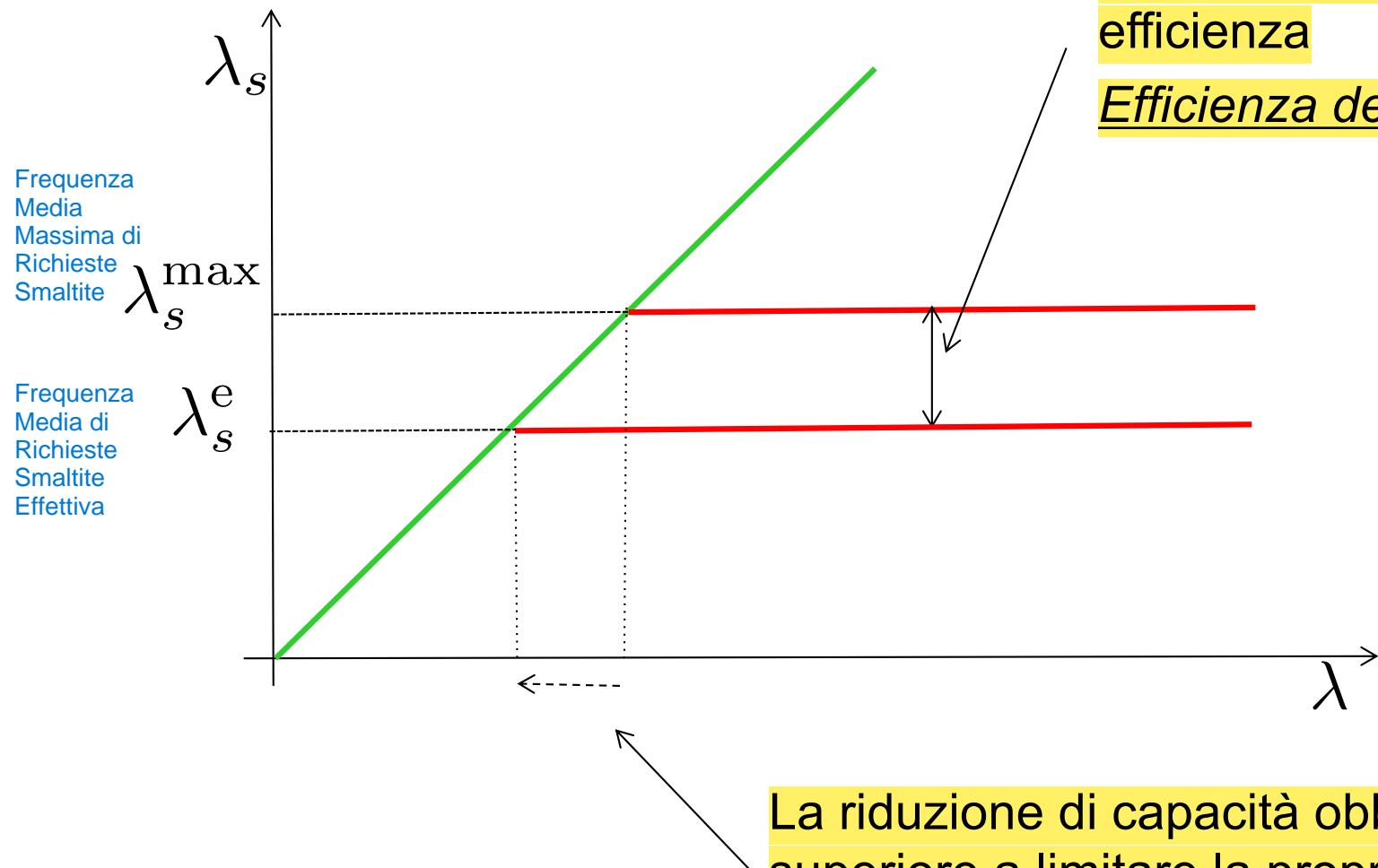


Se le richieste offerte

sono eccessive

una parte non può essere  
soddisfatta

# In un sistema reale



La riduzione di capacità si interpreta come perdita di efficienza

Efficienza del protocollo

$$\eta = \frac{\lambda_s^e}{\lambda_s^{\max}} \leq 1$$

La riduzione di capacità obbliga il livello superiore a limitare la proprie richieste pena la perdita dei dati



# Capacità massima ed efficienza

- Quali sono le prestazioni ideali per un protocollo data link?
  - Poiché il protocollo invia i bit dello strato 3 sul canale la sua capacità massima teorica è la velocità del canale  $C$

- Il tempo medio di servizio minimo possibile sarebbe quindi

$$\bar{\vartheta} = \frac{L}{C} = \frac{1}{\mu}$$

- Se il protocollo richiede maggiore tempo per la completa trasmissione della trama allora

$$\bar{\vartheta}_e = \frac{L}{C_e} > \frac{1}{\mu}$$



C<sub>e</sub>

- La capacità effettiva dipende dal protocollo
- Se le funzionalità richieste o una situazione non ideale richiedono più tempo per ogni PDU allora parte della capacità risulta inutilizzabile per i dati degli utenti
  - PCI necessarie per la segnalazione
  - Errori di trasmissione
  - Ritrasmissioni
  - Tempi morti legati alle dinamiche del protocollo
  - Tempi morti in attesa di accedere al canale



# Unità di misura

- Il traffico è una grandezza adimensionale
  - Moltiplico richieste di servizio per unità di tempo (secondo) per la durata del servizio in unità di tempo (secondi)

$$A_0 = \lambda \bar{\vartheta}$$

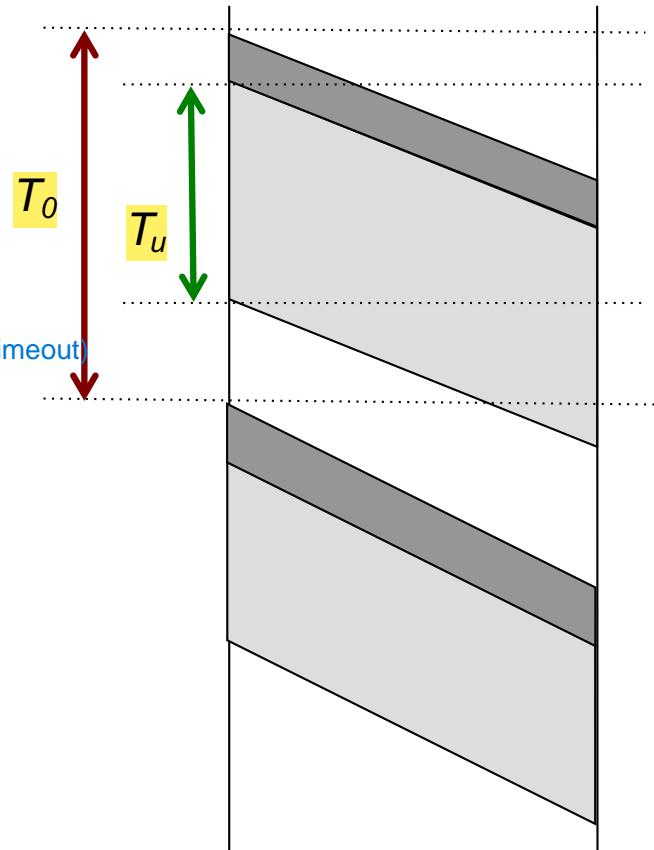
Traffico offerto (occupazione media di un sistema ideale che serve subito tutti gli utenti senza attesa)

- Formalmente si misura con una unità fittizia detta Erlang



# Valutazione efficienza

- Per valutare l'efficienza di solito si fa riferimento alla PDU
- Si confronta:
  - ↳ Tempo di Trasmissione dei soli dati utente
    - La quantità di tempo strettamente utilizzato per inviare i soli dati d'utente (SDU)  $(T_u)$
    - La quantità di tempo utilizzato complessivamente per completare correttamente l'invio della PDU  $(T_0)$ 
      - In funzione delle regole del protocollo
  - ↳ Tempo di Trasmissione + Propagazione di tutto il pacchetto (aggiungendo il tempo di timeout)
    - La quantità di tempo utilizzata complessivamente per completare correttamente l'invio della PDU  $(T_0)$
- L'efficienza è data dal rapporto fra queste due quantità
- Questo problema l'abbiamo studiato lo scorso anno studiando i protocolli ARQ  
(Stop-and-Wait e Sliding Window)



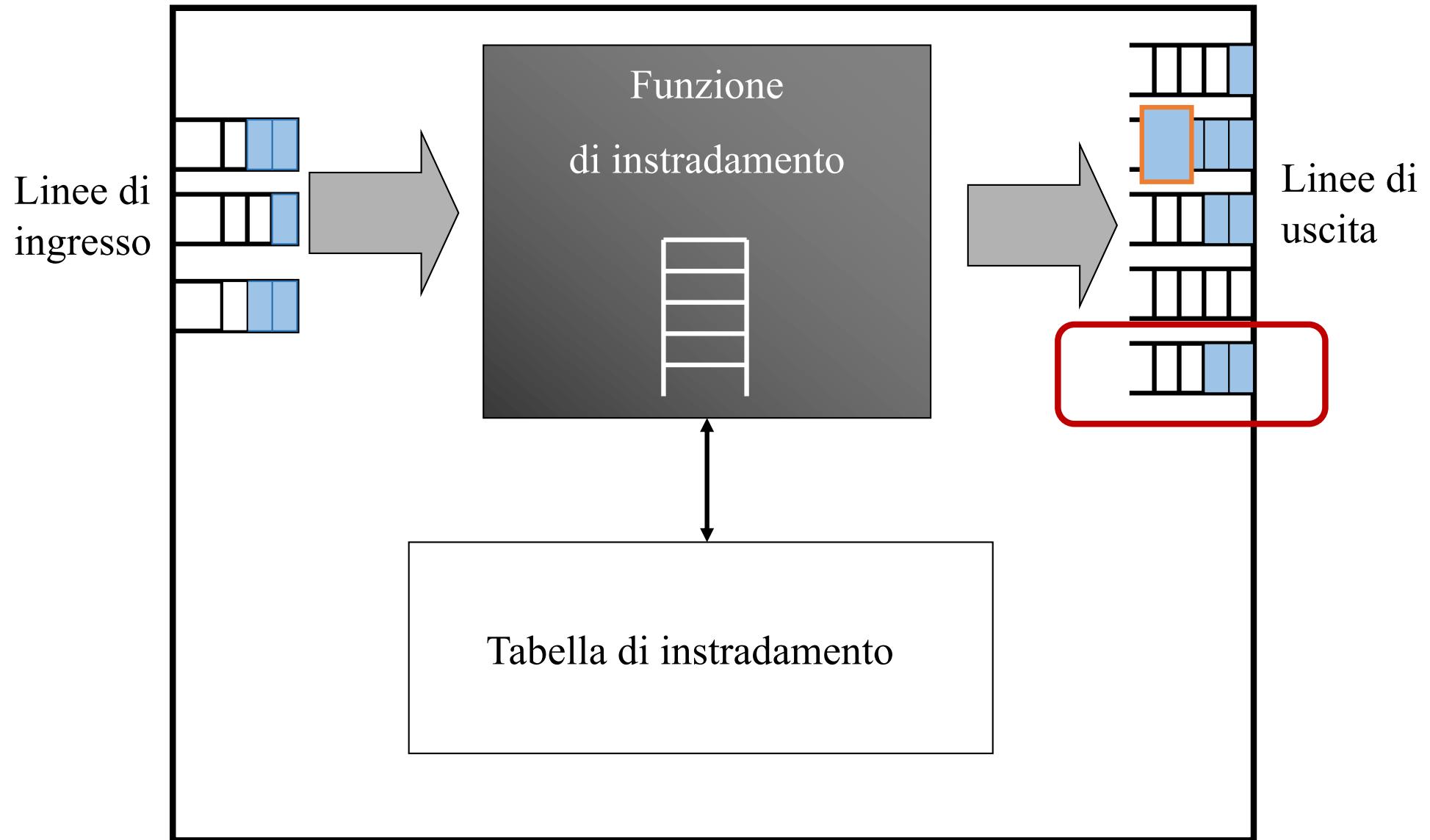
$$\eta = \frac{T_u}{T_0} = \frac{\bar{\vartheta}}{\bar{\vartheta}_e}$$



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# Reti commutate: il sistema a coda con singolo servitore

# Il nodo di commutazione a pacchetto

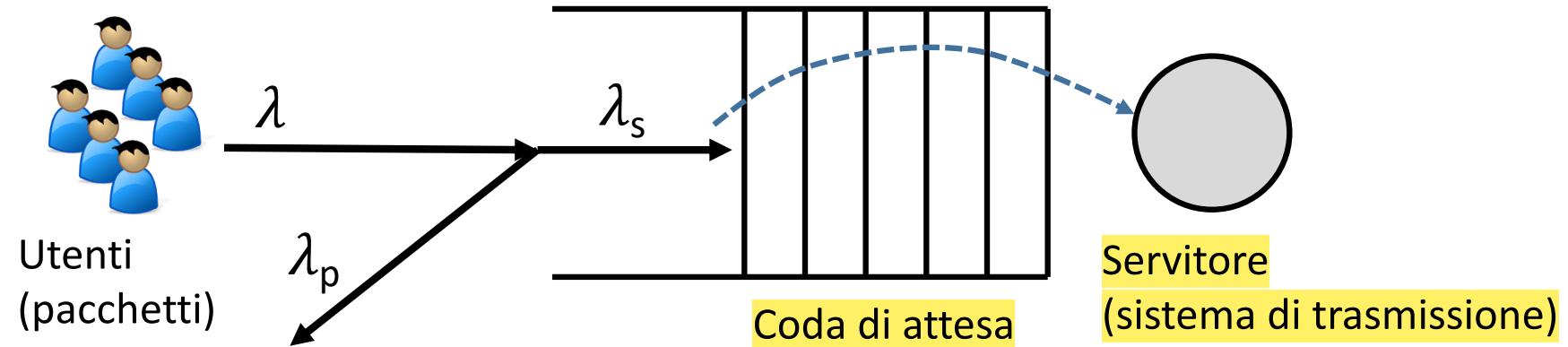


con N uscite avrai N servitori indipendenti, ciascuno responsabile per il proprio flusso di richieste.



# Coda singolo servitore

- Ogni collegamento in uscita viene schematizzato come sistema coda singolo servitore





# Alcune ipotesi semplificative

→ La probabilità di perdita di pacchetti è quindi uguale a zero.

- Le perdite di pacchetti in prima approssimazione sono trascurabili (coda infinita)

$$\lambda_p = 0$$

$$\lambda_s = \lambda$$

- I pacchetti arrivano causalmente con distribuzione di Poisson

$$\Pr \{k \text{ arrivi in un tempo } t\} = P(k, t) = \frac{(\lambda T)^k}{k!} e^{-\lambda T}$$

Intervallo di Tempo

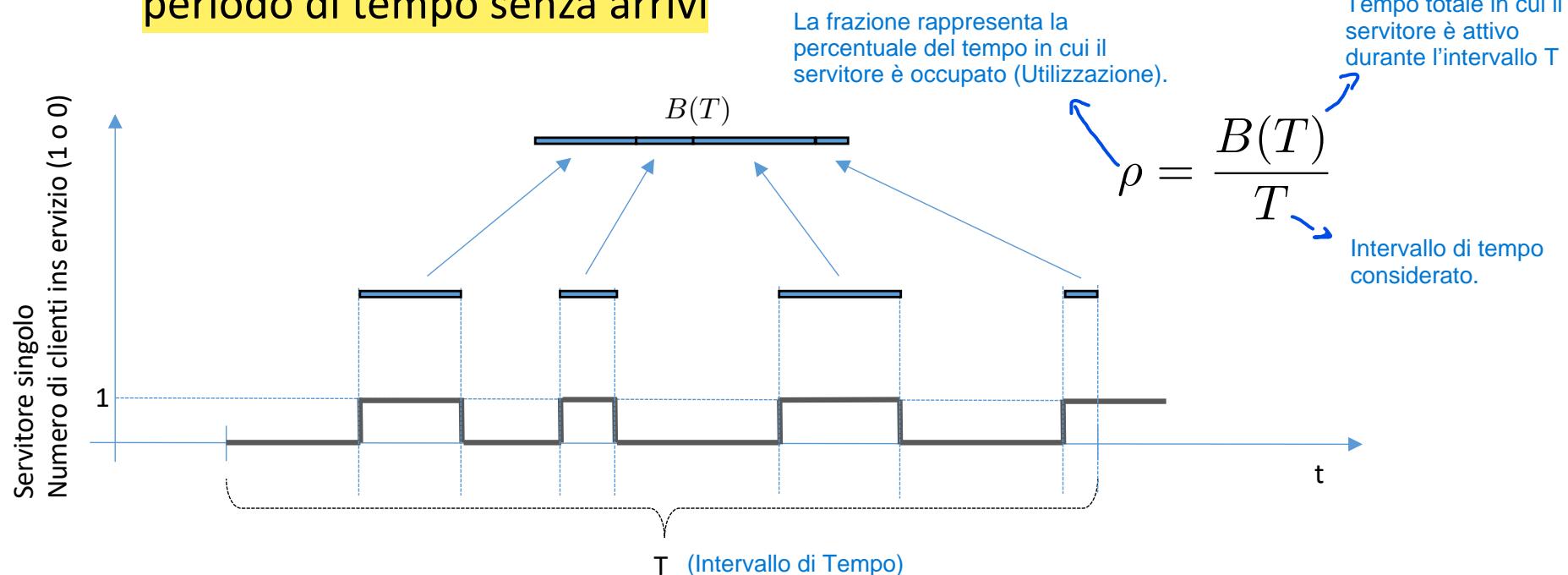
- La dimensione dei pacchetti è casuale con distribuzione esponenziale uguale per tutti i pacchetti

$$\Pr\{\vartheta \leq t\} = F_\vartheta(t) = 1 - e^{-\frac{t}{\vartheta}}$$

- 1) Se i pacchetti hanno dimensioni casuali, il tempo di servizio varia di conseguenza.
- 2) Pacchetti più grandi richiedono più tempo per essere processati, aumentando la probabilità di accumulo nella coda. La variabilità delle dimensioni può causare congestione temporanea, dove i pacchetti successivi devono attendere tempi di servizio più lunghi.
- 3) Un servitore che processa pacchetti di dimensione variabile deve adattarsi dinamicamente, con la possibilità di avere periodi di inattività (pacchetti brevi) seguiti da periodi di alta occupazione (pacchetti lunghi).

# Utilizzazione

- Il servitore alterna fasi di lavoro a fasi di pausa
  - Idealmente vorremmo il servitore sempre attivo
    - Il servitore in pausa è uno spreco di risorse
  - Il servitore può essere attivo solo se ci sono clienti da servire
    - I clienti arrivano in modo casuale e può capitare che ci sia un periodo di tempo senza arrivi





# Servitore occupato

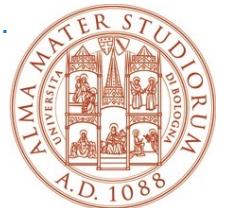
- In un sistema a servitore singolo l'utilizzazione è la percentuale di tempo per cui il servitore è impegnato
- In un sistema ergodico questa è anche la probabilità di trovare il servitore occupato in un istante qualunque
- Quindi

Un sistema ergodico è un sistema che, nel lungo periodo, si comporta in modo prevedibile. Quindi, il comportamento nel breve termine (calcolo in un istante) è rappresentativo di ciò che accade nel lungo periodo.

$$\rho = \Pr\{\text{Servitore occupato}\} = \Pr\{\text{Pacchetto accodato}\}$$

L'utilizzazione è anche la probabilità che il servitore sia occupato in un istante qualunque, in un sistema a servitore singolo e stazionario (ergodico).

Avere un servitore utilizzato tra il 70% e l'80% significa che il sistema è ben sfruttato, evitando inutili sprechi di risorse.  
Se il traffico aumenta temporaneamente, il servitore ha abbastanza capacità residua per assorbire l'aumento senza generare code lunghe o congestione.  
Mantenere l'utilizzazione tra 0.7 e 0.8 è un compromesso ottimale tra efficienza e resilienza a picchi di traffico.



# Traffico e utilizzazione

$$\frac{B(T) / T}{\lambda} = \rho = \frac{\lambda}{\mu}$$

Questa grandezza è significativa perché  
confronta il ritmo di arrivo con quello di  
servizio

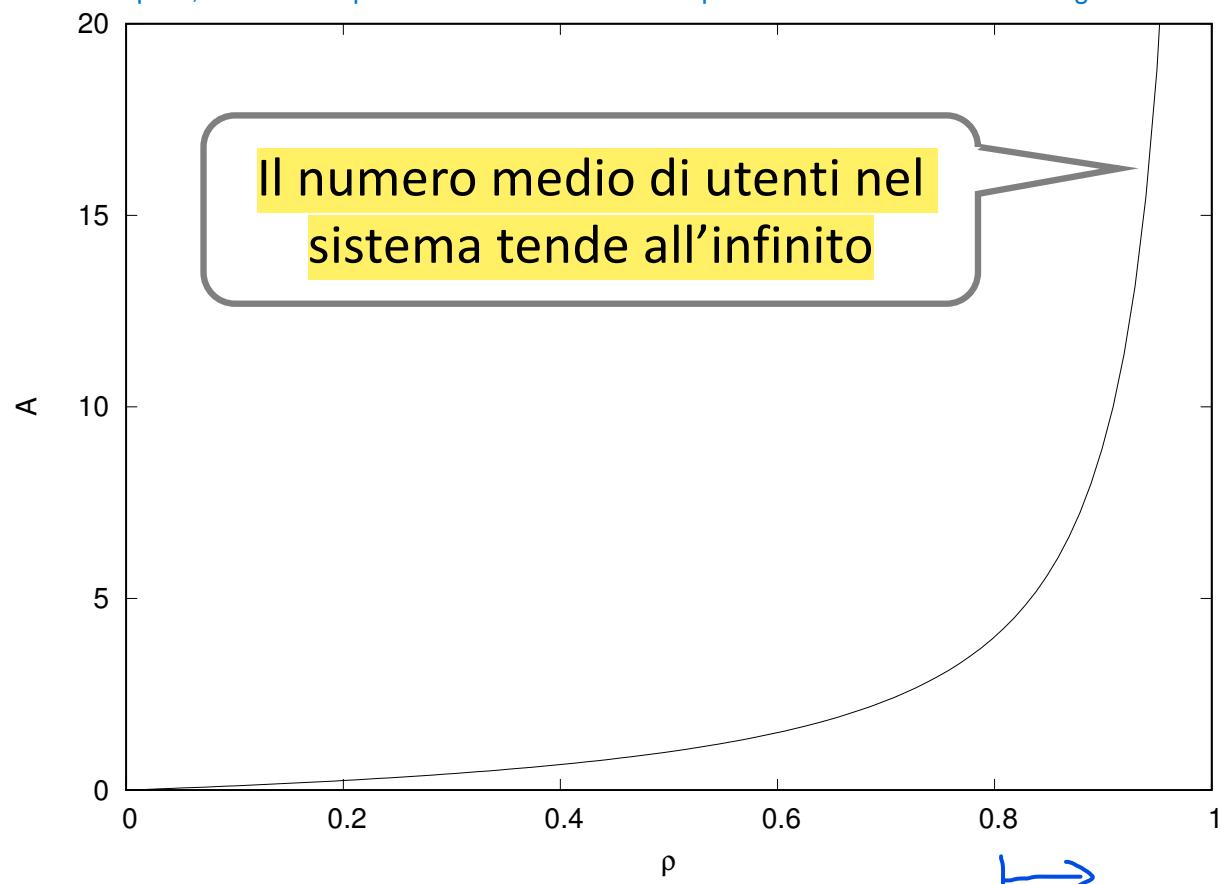
$$\mu = \frac{1}{\vartheta}$$

Questa grandezza è detta  
frequenza di servizio e ci  
dice mediamente quanti  
pacchetti possono essere  
serviti in un dato intervallo di tempo

$$\lambda < \mu$$

Non devo arrivare più  
pacchetti di quelli che  
possono essere serviti

Se l'utilizzazione è troppo alta (ad esempio vicino a 1), significa che il sistema è quasi sempre occupato, e anche un piccolo aumento nel traffico potrebbe causare ritardi o congestione.

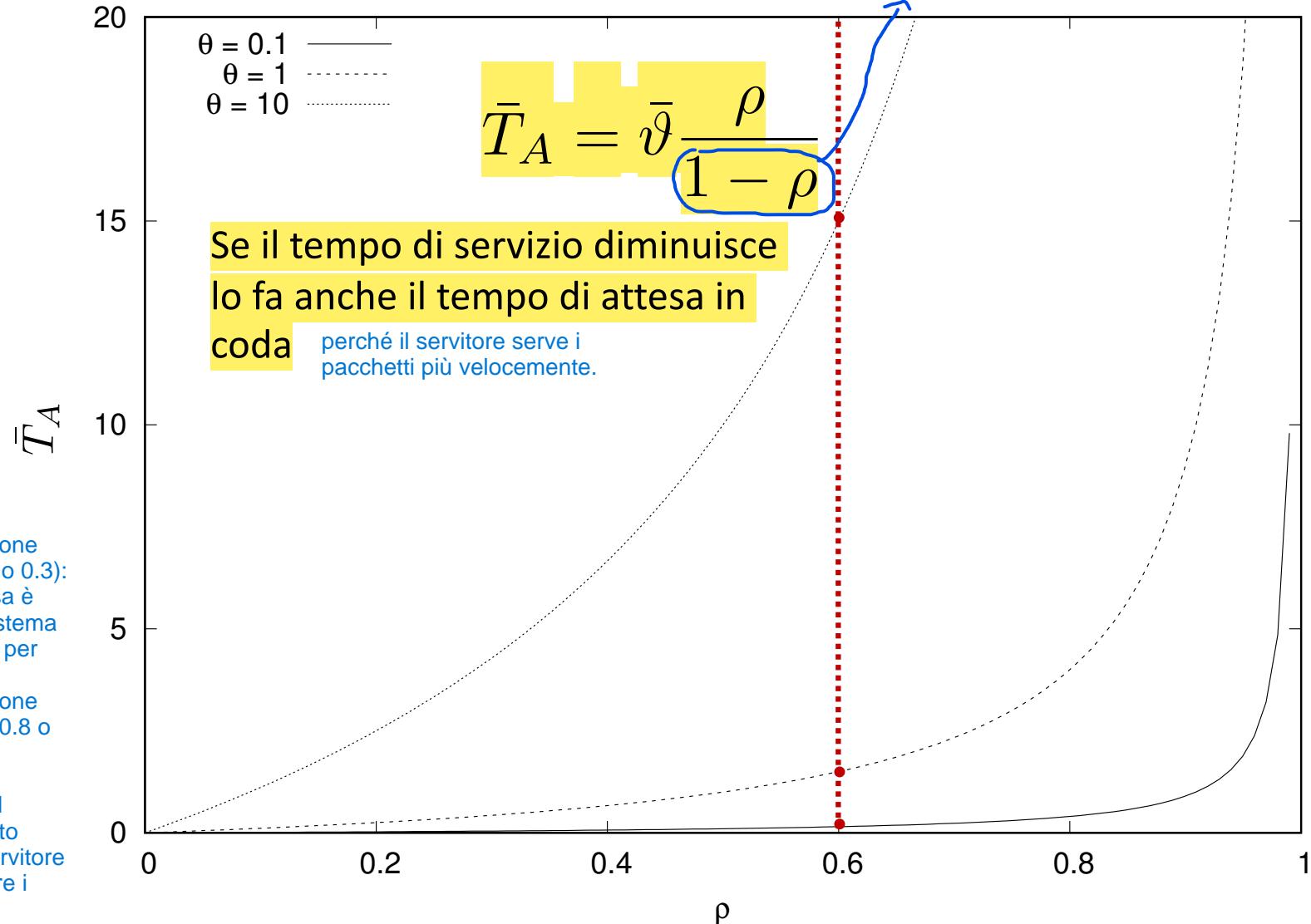


Utilizzazione vicina a 1: Il sistema è quasi congestionato. Un piccolo aumento nel traffico (che è casuale) potrebbe rendere il sistema insostenibile.



# Tempo medio di attesa in coda

Margine residuo del sistema (quanto il servitore è libero per gestire nuovi pacchetti).





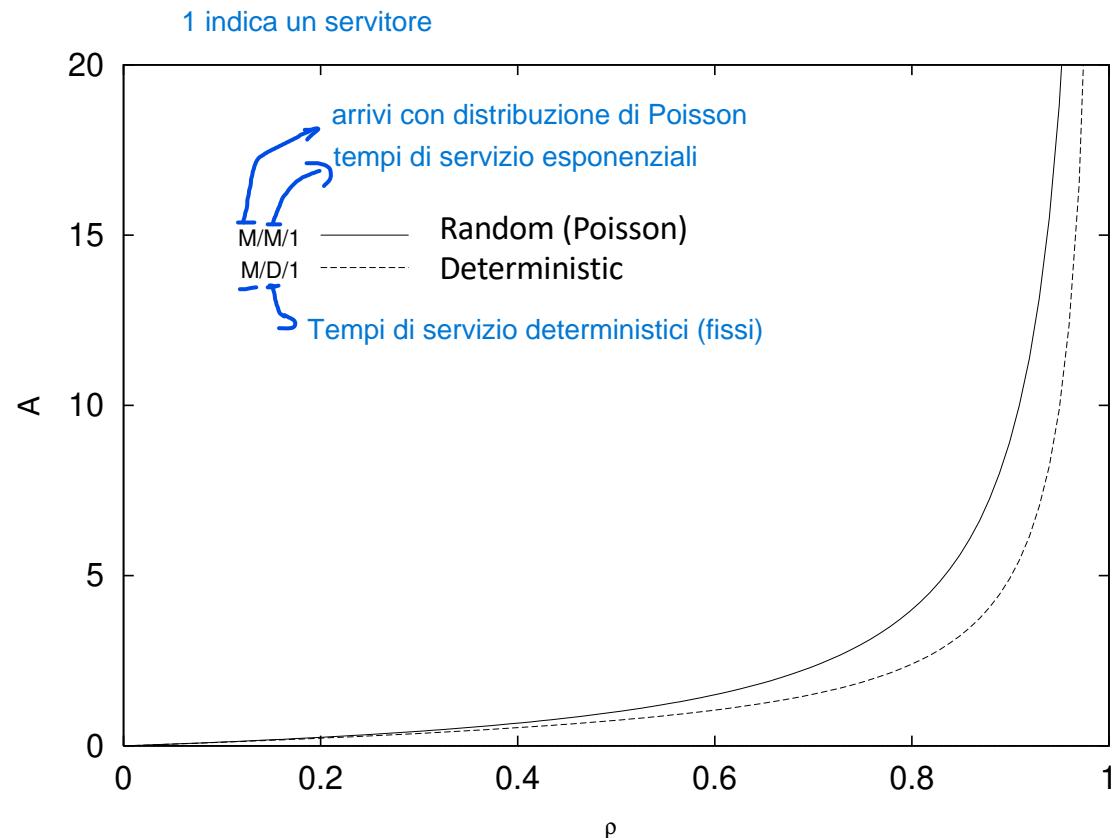
# La statistica del tempo di servizio

- Il traffico nel sistema cambia se cambia la statistica del tempo di servizio (cioè come è distribuito il tempo necessario per servire un pacchetto)
  - I tempi di servizio sono distribuiti casualmente seguendo una distribuzione esponenziale.
  - Servizio casuale con distribuzione esponenziale (M)
  - I tempi di servizio sono costanti e sempre uguali.
  - Servizio deterministico ossia sempre uguale (D)

$$\bar{T}_A = \bar{\vartheta} \frac{\rho}{1 - \rho}$$

$$\bar{T}_A = \bar{\vartheta} \frac{\rho}{2(1 - \rho)}$$

il tempo di attesa è più basso rispetto al caso casuale, poiché non c'è variabilità nel tempo di servizio e i pacchetti vengono serviti con un ritmo regolare.

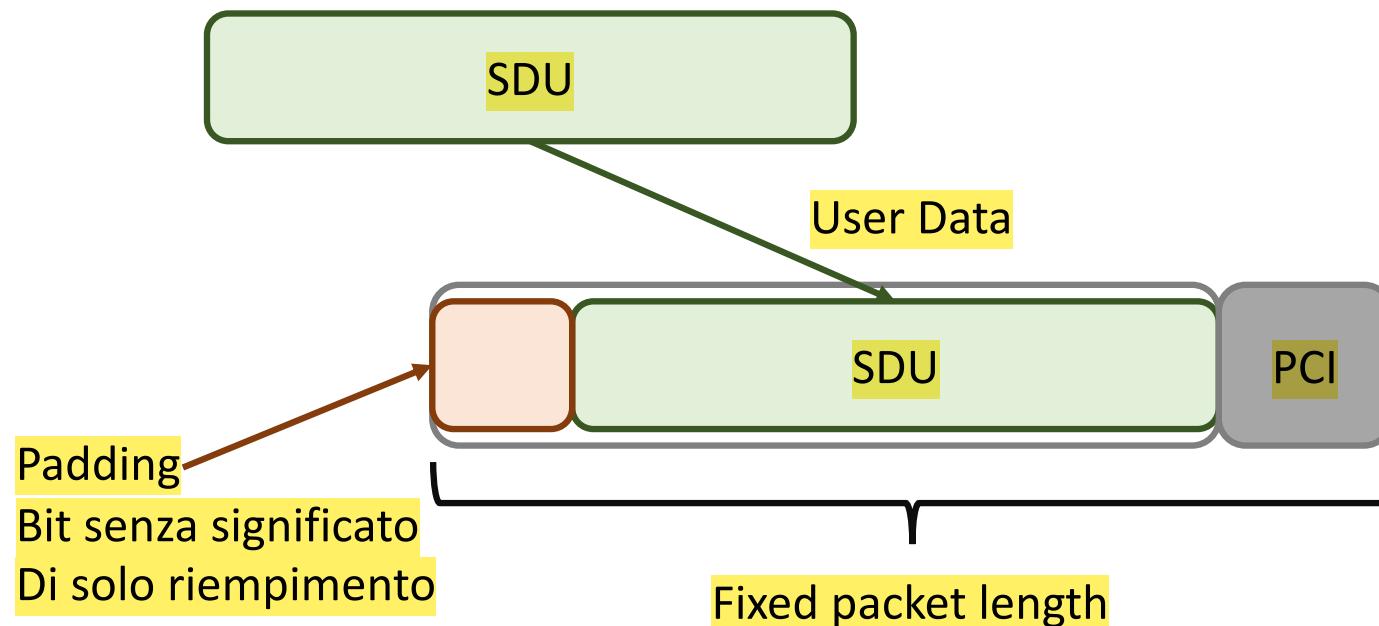




# Un classico problema nella progettazione dei protocolli

- Pacchetti di lunghezza predeterminata e tutti uguali migliorano le prestazioni in caso di accodamento
- I dati di utente arrivano in quantità casuale quindi è necessario il **padding**

Se tutti i pacchetti hanno la stessa lunghezza, è più facile per il sistema gestirli. Questo migliora le prestazioni, specialmente quando ci sono tanti pacchetti in attesa.





# Il compromesso

- I pacchetti di lunghezza fissa migliorano il tempo di attesa in coda → Con pacchetti tutti uguali, il sistema funziona più velocemente e i tempi di attesa in coda si riducono.
- Il padding aumenta la lunghezza dei pacchetti, quindi aumenta il tempo di servizio e quindi peggiora il tempo di attesa in coda
- Cosa conviene?

Conviene usare il padding?

Sì, se vuoi migliorare la regolarità del sistema e gestire meglio le code.

No, se il costo di allungare i pacchetti (padding) rallenta troppo il sistema.

Il padding rende i pacchetti più grandi del necessario. Pacchetti più grandi richiedono più tempo per essere serviti, aumentando i tempi di servizio e, di conseguenza, i tempi di attesa in coda.



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# Local Area Network e Accesso multiplo



# LAN: Local Area Networks

Infrastruttura di telecomunicazioni che consente ad apparati **indipendenti** (stazioni) di comunicare in un' area **limitata** attraverso **un canale fisico condiviso** ad **elevata bit rate** con **bassi tassi di errore**

- **INDIPENDENTI**: assenza di architetture master-slaves
- **LIMITATA**: un' area di dimensioni moderate è spesso privata, non soggetta a regulations
- **CANALE FISICO CONDIVISO**: potrebbe essere un unico mezzo fisico condiviso
- **ELEVATA BIT RATE**: uso esclusivo dell' intera banda anche se per brevi intervalli
- **BASSI TASSI DI ERRORE**: a causa delle piccole distanze si dispone di molta potenza

Le brevi distanze riducono il rischio di perdita o danneggiamento dei dati.



# Scelte per le LAN

Per far funzionare una LAN, è necessario scegliere i giusti protocolli e tecnologie per ogni parte del sistema. Questi protocolli devono seguire il modello OSI

- Le LAN sono *reti di calcolatori* e devono essere implementate scegliendo *protocolli per tutti gli strati dell'OSI*
  - Poiché le LAN coprono un'area piccola, si possono usare soluzioni tecnologiche particolari, diverse da quelle usate per reti più grandi come le WAN.
- Le **dimensioni limitate** rendono convenienti soluzioni particolari per gli **strati 1 e 2**
  - di questo si occupano gli standard per le LAN
- Occorre scegliere
  - Il mezzo trasmissivo
  - La topologia
  - Un eventuale protocollo di accesso al canale

Quale "cavo" o tecnologia useremo per trasmettere i dati?

Come saranno collegati i dispositivi?

Come decidiamo quale dispositivo può inviare dati in un dato momento?



# Mezzo trasmissivo

- Fibra ottica: Sempre più diffusa grazie alla maggiore capacità e al minor costo rispetto al rame.
- Rame (twisted pairs): Ancora usato, soprattutto per i collegamenti finali (ultimo tratto).
- Radio: Utilizzato sempre di più per la flessibilità, anche se meno affidabile rispetto ai cavi.

- In generale nelle reti moderne le fibre ottiche stanno progressivamente sostituendo il rame
  - Maggiore banda e distanza
  - Minore costo
  - Interconnessione più complessa e costosa
- Nelle LAN
  - Per le dimensioni limitate il costo del mezzo incide meno rispetto al costo dell'attacco per le stazioni
    - La penetrazione delle fibre ottiche è più lenta
    - Per gli ultimi metri fino all'attacco, potrebbero sopravvivere le coppie intrecciate (twisted pairs)
- Il mezzo radio, per motivi di affidabilità e di costi non è stato usato fino alla fine degli anni '90, ma sta acquistando un'importanza sempre crescente

Installare e collegare la fibra richiede tecnologie e competenze più avanzate.

si riferisce al costo di collegare ogni dispositivo (stazione) alla rete.



# Topologie

Wide Area Networks

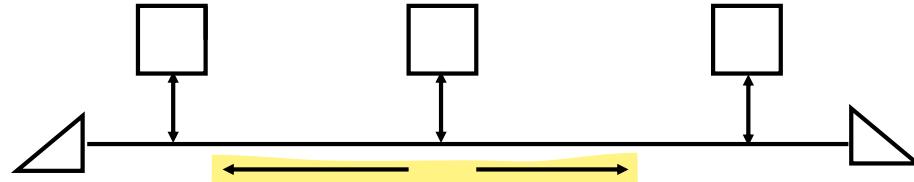
- Topologie tradizionalmente preferita nelle WAN
  - A stella
  - A maglia più o meno completa
  - Architettura gerarchica Dispositivi organizzati in livelli, con nodi superiori che gestiscono nodi inferiori.
- Topologie punto-multipunto per LAN
  - Non adatte per le WAN
    - Nelle WAN è importante avere i collegamenti più lunghi possibile i collegamenti devono coprire lunghe distanze nelle WAN
    - Le prese intermedie sottraggono potenza e aggiungono disturbi imponendo collegamenti più corti
  - Sono state preferite nelle prime proposte di LAN
    - Se i terminali sono pochi non servono nodi di commutazione

→ Le prese intermedie sono meno problematiche.

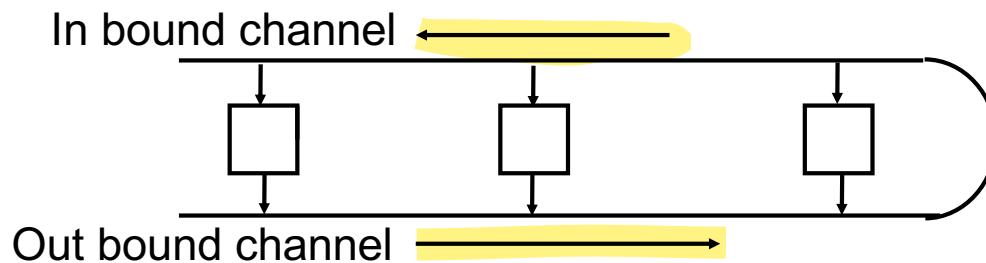
# Topologie punto-multipunto

- **Bus bidirezionale**

Un unico cavo usato da tutti i dispositivi.

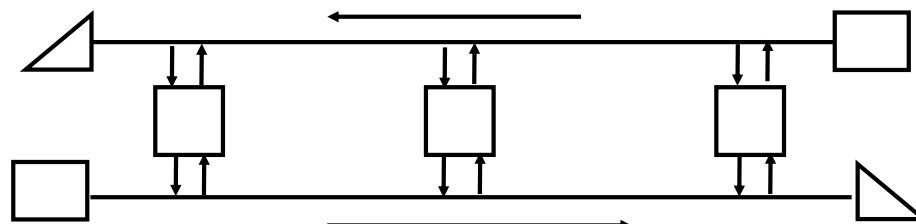


- **Bus unidirezionale**

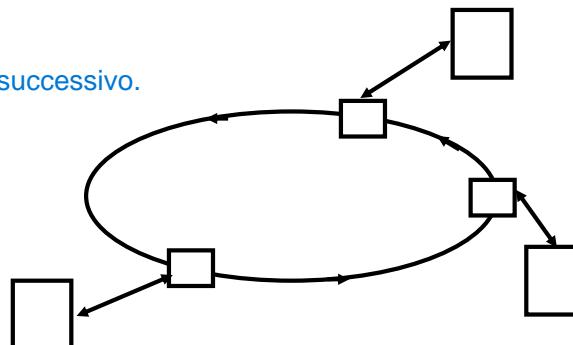


- **Doppio bus (dual bus)**

Due linee separate per migliorare l'affidabilità.



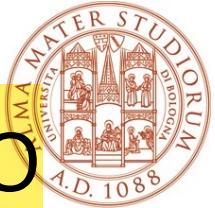
- **Anello**





# Due caratteristiche

- Topologie punto-multipunto = mezzo di trasmissione condiviso = due caratteristiche peculiari
  - Broadcast I dati possono essere inviati a tutti i dispositivi, quindi serve un meccanismo per evitare che ogni dispositivo elabori informazioni non destinate a sé.
    - La LAN fornisce in modo nativo una comunicazione da uno a tutti (broadcast) sul mezzo condiviso
    - Per evitare che tutti i calcolatori leggano i dati di tutte le comunicazioni si deve introdurre un meccanismo di indirizzamento a livello di protocollo LAN
      - Si vuole evitare che lo strato 3 debba elaborare anche le conversazioni degli altri
  - Collisione Più dispositivi possono tentare di inviare dati contemporaneamente, causando interferenze.
    - Su di un mezzo condiviso esiste la possibilità che più utenti inviiano informazioni contemporaneamente
    - Interferenza – perturbazione o distruzione dell'informazione – perdita di trasparenza semantica



# Accesso al canale di collegamento

↳ Ogni collegamento è dedicato a una coppia di dispositivi

- Collegamenti con canali punto-punto e commutati

- Solo sorgente e destinazione hanno accesso al canale quindi la sorgente può liberamente impegnare tutta la capacità certa di raggiungere la destinazione

↳ Più dispositivi condividono il canale, ma questo può causare collisioni.

- Collegamenti con canali ad accesso multiplo

- Più sorgenti possono accedere al canale contemporaneamente determinando quindi la **«collisione»**

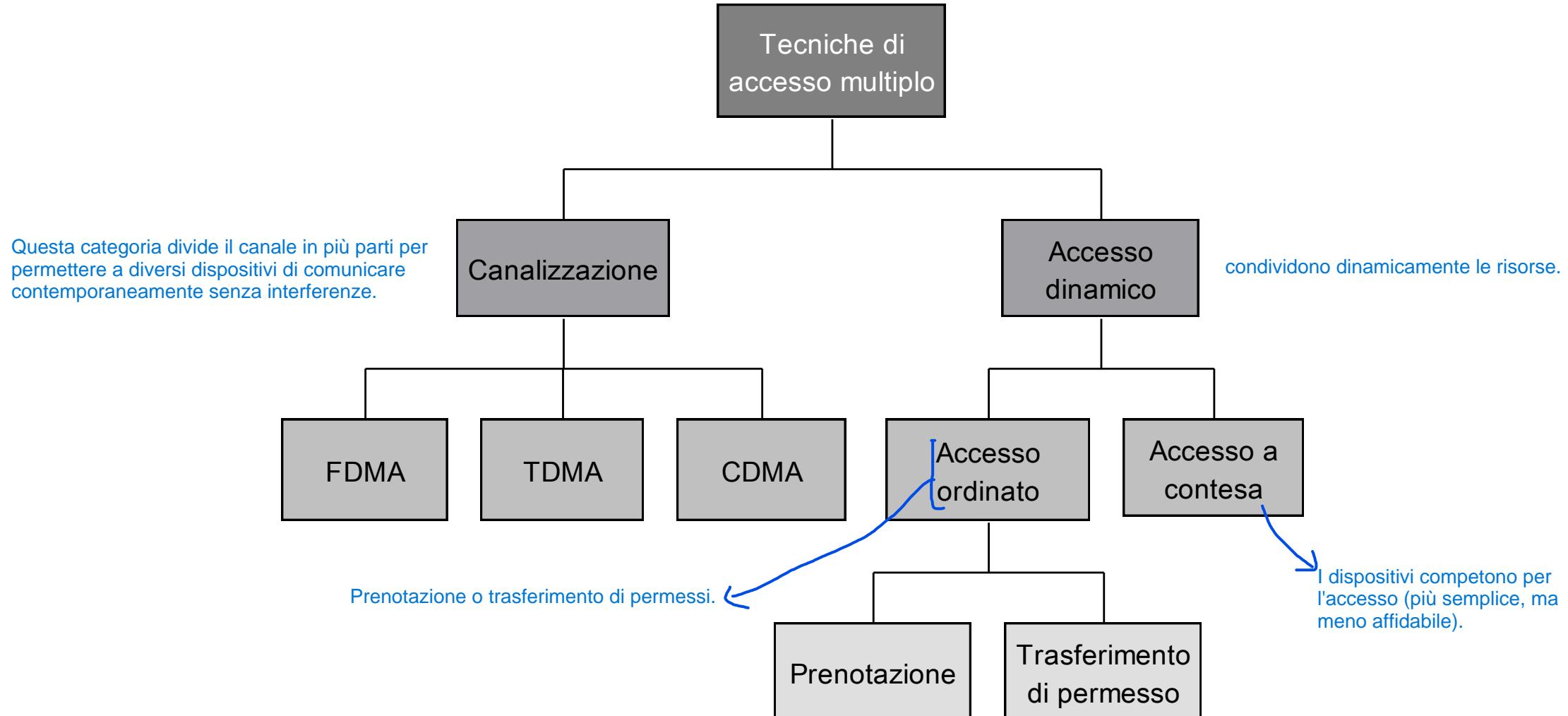
↳ L'accesso è regolato per evitare conflitti.

- Collegamenti con accesso al canale controllato

- Il canale è condiviso ma l'accesso viene controllato in modo centralizzato o distribuito per **evitare** fenomeni di collisione



# Accesso multiplo: tassonomia





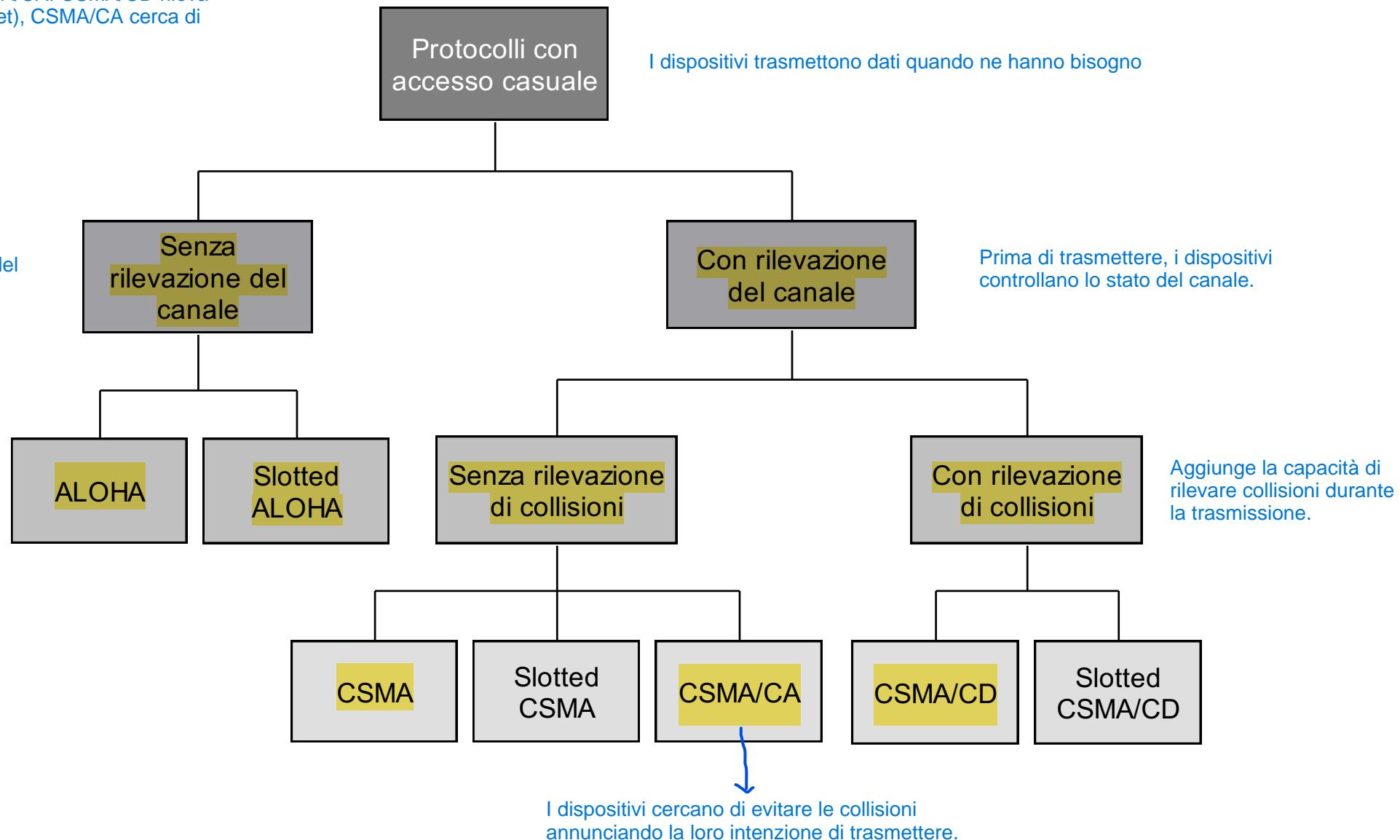
ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# Protocolli ad accesso casuale: funzionalità e prestazioni



# Protocolli ad accesso casuale

ALOHA vs. CSMA: ALOHA non verifica mai lo stato del canale, mentre CSMA lo fa.  
CSMA/CD vs. CSMA/CA: CSMA/CD rileva le collisioni (Ethernet), CSMA/CA cerca di evitarle (Wi-Fi).





# Protocolli Medium Acces Control

- **A CONTESA**

- ammettono collisioni

Se più dispositivi trasmettono contemporaneamente, si possono creare collisioni o errori di trasmissione.

Il MAC risolve questo problema stabilendo regole che indicano:

Quando un dispositivo può accedere e trasmettere sul canale.

Come evitare o gestire collisioni.

I Protocolli MAC servono a gestire come i dispositivi accedono a un mezzo condiviso, come un cavo o un canale wireless, per trasmettere i dati senza interferenze.

- **CAP - Channel Access Procedure**

- E' l'insieme delle procedure che la stazione effettua per realizzare l'accesso al canale

- **CRA - Collision Resolution Algorithm**

- E' l'insieme delle procedure che la stazione effettua per rivelare ed eventualmente recuperare situazioni di collisione

Il CRA è come un "arbitro" che:

Rileva i problemi (collisioni).

Fermare il caos interrompendo le trasmissioni.

Riordina il traffico decidendo quando i dispositivi possono riprovare.



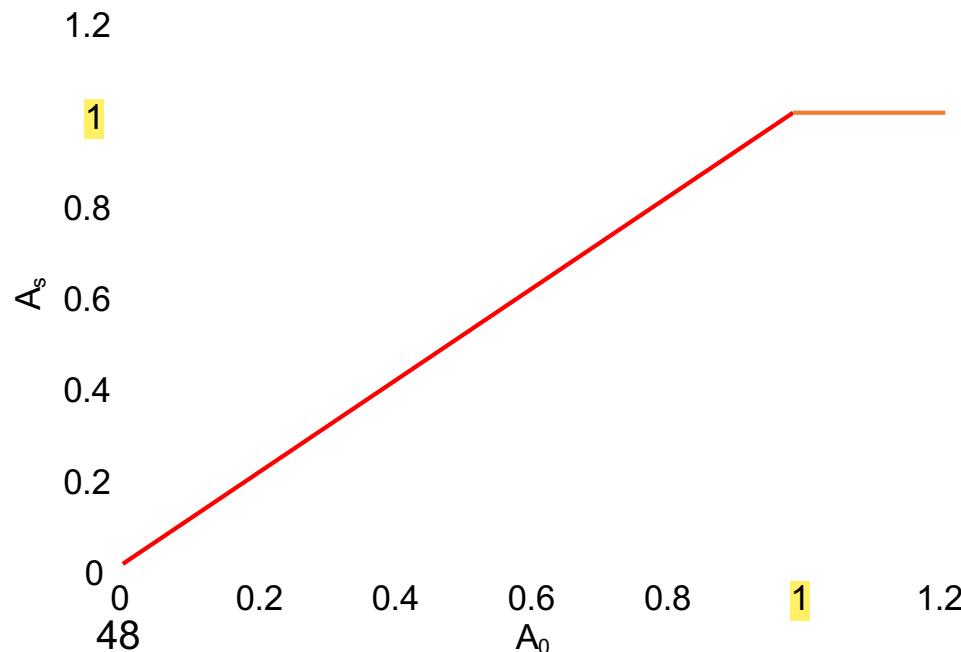
# Parametri caratterizzanti la LAN

- $L$  : lunghezza massima della trama
    - Tutte le trame sono della dimensione massima
  - $C$  : velocità di trasmissione sul mezzo (bitrate)
  - $d$  : massima distanza fra due stazioni della LAN
  - $v$  : velocità di propagazione del segnale
- 
- $\theta = L/C$  : tempo di trasmissione di una trama
  - $d/v$  : tempo di propagazione di un singolo bit sulla LAN
  - $Cd/v$  : massimo numero di bit che possono essere presenti contemporaneamente sulla LAN



# LAN ideale

- Utilizza una CAP ideale
  - Coordina le stazioni per evitare accessi contemporanei al canale di trasmissione
  - Tutte le trame in arrivo vengono trasmesse con successo, quindi  $A_s = A_0$
- Il tempo di propagazione della trama è nullo
- È possibile trasmettere le trame una di seguito all'altra
  - Il canale di trasmissione della LAN può essere utilizzato al 100%



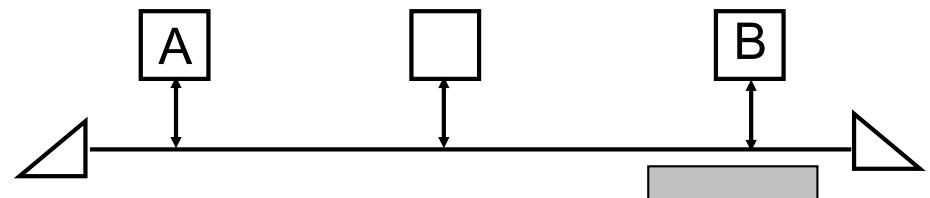
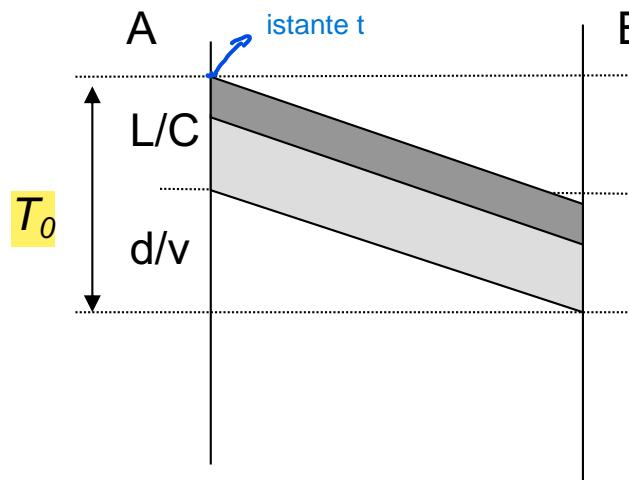
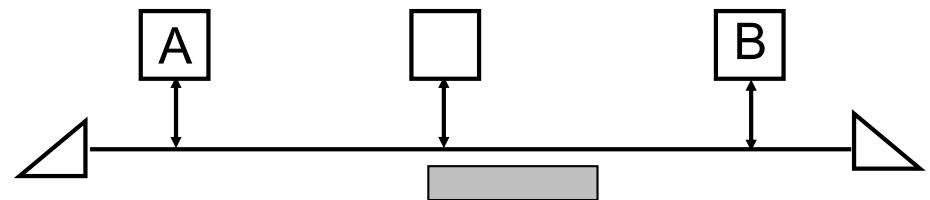
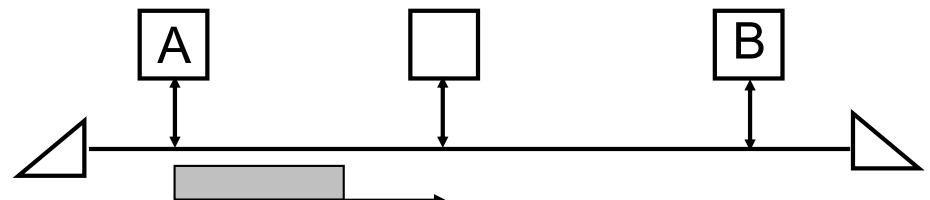
Se  $A_0 < 1$  allora  $\lambda_s = \lambda$

Se  $A_0 \geq 1$  allora  $A_s = 1$

La LAN ideale permette di smaltire tutto il traffico offerto, fino alla saturazione del canale

# Propagazione reale (topologia bus)

- La trama impiega un tempo non nullo per attraversare la LAN
  - $t$  : A inizia la trasmissione
  - $t + L/C$  : A termina la trasmissione
  - $t + d/v$  : B riceve il primo bit
  - $t + L/C + d/v$  : B riceve l'ultimo bit





# Efficienza con MAC ideale

- Una trama tiene impegnata la LAN per  $T_0$
- Il canale di trasmissione non può più essere usato al 100%
- Al massimo viene utilizzato per  $T$  secondi ogni  $T_0$
- **Efficienza del MAC**

quanto, del tempo disponibile, il canale è usato per inviare dati utili.

$$\eta = T/T_0 = (L/C)/(L/C + d/v) = 1/(1+a)$$

Quando un dispositivo invia un pacchetto, il canale è occupato per un certo periodo di tempo, chiamato  $T_0$ . Durante questo tempo, nessun altro dispositivo può trasmettere, quindi il canale di trasmissione non è usato al massimo.

- L'efficienza pone un limite superiore al massimo traffico smaltito  $A_s$

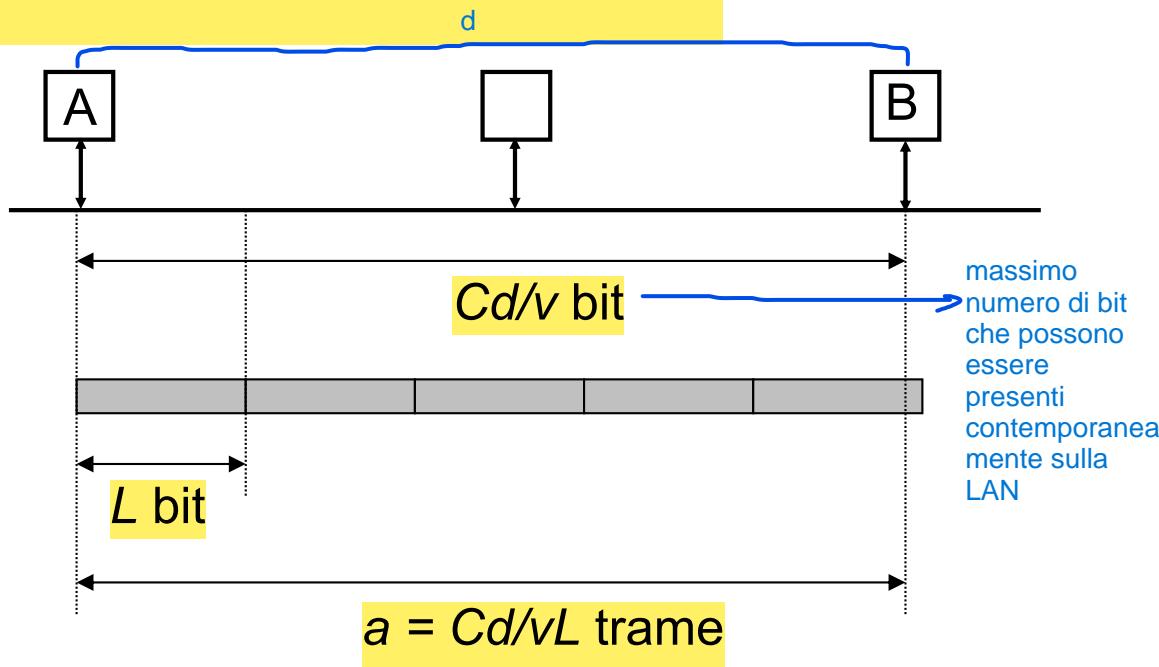
Se la rete supera questo limite, si creano colli di bottiglia, che portano a:  
Ritardi. Collisioni. Rallentamenti nella trasmissione dei dati.

$$a = Cd/vL$$

è interpretabile come la lunghezza della LAN misurata in PDU

- Se  $a$  è grande: Significa che la rete è lunga o i messaggi sono corti. In questo caso, il tempo sprecato aumenta, quindi l'efficienza diminuisce. 50

- Se  $a$  è piccolo: Significa che la rete è breve rispetto alla lunghezza del messaggio. In questo caso, il sistema è più efficiente.





L'efficienza del sistema MAC pone un limite massimo al traffico che la rete può smaltire

# Traffico smaltito dalla LAN

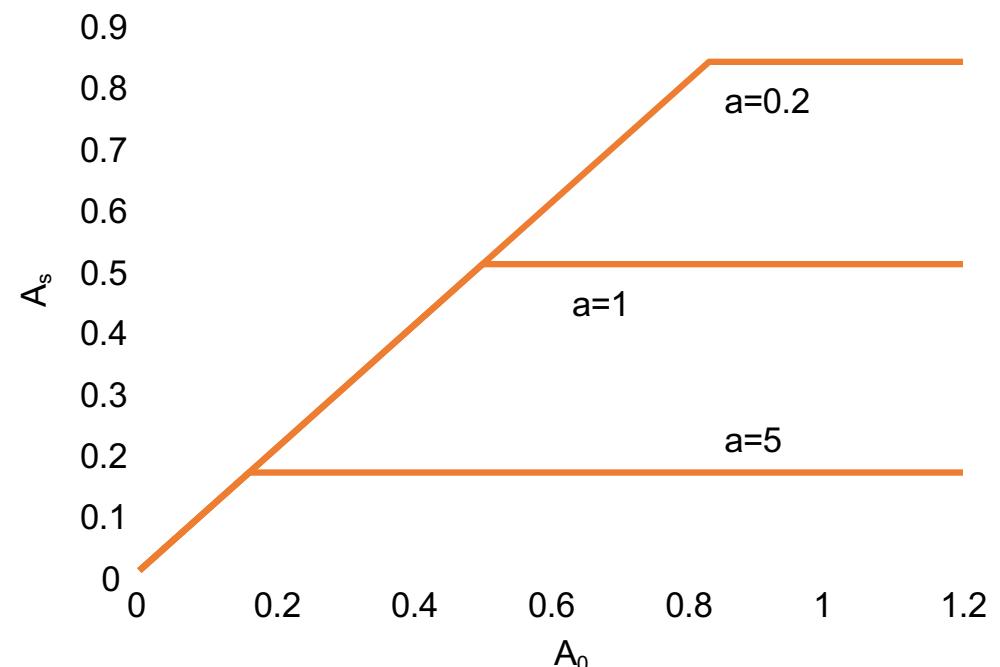
- $A_0 < 1/(1+a)$

- Tutte le trame in arrivo vengono trasmesse
- $S = G = A_0$

- $A_0 \geq 1/(1+a)$

- Il MAC non permette la trasmissione di tutte le trame
- Parte delle trame viene accodata
- $A_s = \eta = 1/(1+a)$

Se il traffico offerto è inferiore all'efficienza massima teorica della rete:  
Tutte le trame in arrivo vengono trasmesse.  
In questo caso, il traffico smaltito è uguale al traffico offerto, cioè non c'è congestione.  
Nessuna trama viene accodata o persa, perché la rete riesce a gestire tutto il traffico che le viene inviato.



Quando il traffico offerto supera la capacità massima teorica del sistema:

La rete non riesce a trasmettere tutte le trame in arrivo.

Una parte del traffico viene accodata, cioè messa in attesa.

In questo caso, il traffico smaltito è limitato dall'efficienza del sistema

Quindi, anche se traffico offerto aumenta, il traffico effettivamente trasmesso rimane costante e non può superare il limite imposto dall'efficienza.



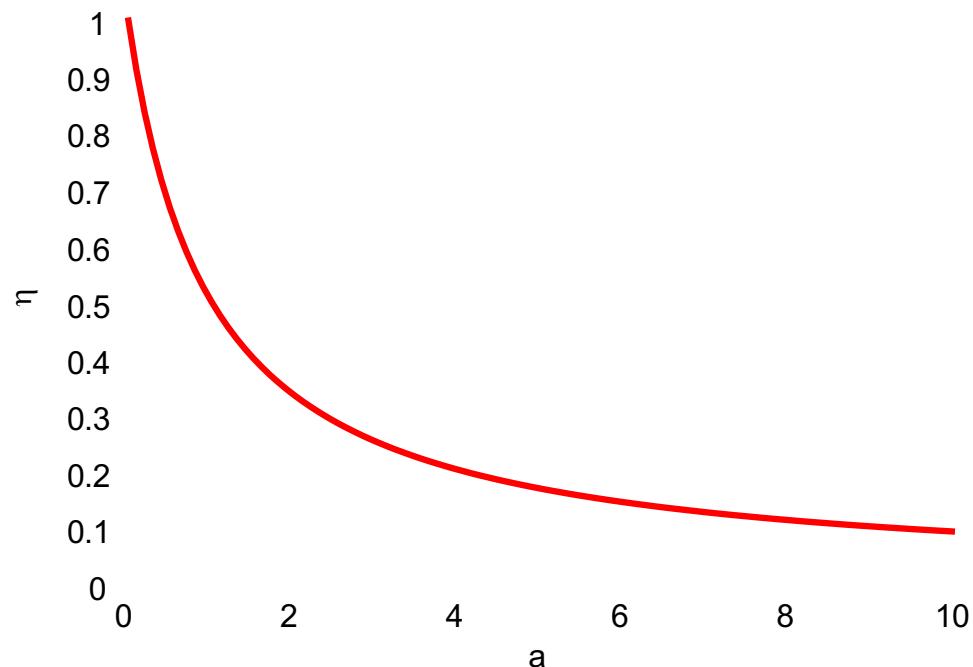
# Esempio numerico

- $C=10 \text{ Mbit/s}$   $d=1 \text{ km}$   $v=200000 \text{ km/s}$   $F=100$ 
  - $d/v = 5 \cdot 10^{-6}$
  - $C d/v = 10 \cdot 10^6 \cdot 5 \cdot 10^{-6} = 50$
  - $a = 50 / 100 = 0,5$     $\eta = 1/1,5 = 0,67$ 
    - $\hookrightarrow$  lunghezza del pacchetto (efficienza)
- $C=100 \text{ Mbit/s}$
- $C d/v = 500$
- $a=500/100=5$     $\eta=1/6$
- $C=1 \text{ Gbit/s}$
- $C d/v = 5000$
- $a=5000/100 = 50$     $\eta=1/51$



# Quale efficienza per le LAN

- $a$  determina le prestazioni della LAN
- Maggiore è la lunghezza del canale in trame, minore risulta il traffico massimo smaltibile (massimo throughput)
  - I protocolli ad accesso multiplo sono efficienti quando le distanze e le velocità di trasmissione<sup>(C)</sup> sono abbastanza limitati





# Protocollo a contesa: ALOHA

- È nato nel 1970 per collegare tra loro le università delle isole Hawaii.
- Prevede stazioni a terra ed un satellite geostazionario
  - Le stazioni trasmettono tutte sul medesimo canale radio (uplink)
  - Il satellite ritrasmette a terra amplificati i dati su un canale diverso (downlink)
- **CAP**
  - Quando un trasmettitore ha una trama da trasmettere la trasmette senza alcun verifica preventiva
  - La trama viene ritrasmessa dal satellite verso tutte le stazioni
  - La stazione trasmittente riceve la propria trama ed ha quindi conferma della corretta trasmissione
- **CRA**
  - Quando due stazioni trasmettono contemporaneamente, i segnali collidono e si interferiscono sull'uplink
  - Il satellite scarta le trame non correttamente ricevute
  - La stazione non riceve la propria trama sul downlink e quindi identifica una collisione
  - Non ritrasmette subito ma fa partire l'algoritmo di **back-off**
    - Sceglie l'istante per la ritrasmessione in modo aleatorio all'interno di un intervallo di lunghezza prefissata  $T_b$  (tempo di back-off)



# Aloha: prestazioni

I pacchetti generati dalle applicazioni, che girano su una stazione specifica, arrivano alla stazione specifica in modo casuale, seguendo la distribuzione di Poisson

- Assumiamo che i pacchetti generati dalle sorgenti di traffico (applicazioni) determinino gli arrivi di trame alle stazioni secondo un **processo di Poisson con frequenza media di arrivo  $\lambda$**

indica la frequenza media con cui le applicazioni generano pacchetti sulla stazione per essere trasmessi al satellite.

- Tenendo conto delle ritrasmissioni, il numero medio di pacchetti trasmessi in effetti al satellite nell'unità di tempo è  $\lambda_r > \lambda$

Le collisioni con successive ritrasmissioni generano delle **correlazioni fra gli arrivi**, ma se l'intervallo di back off è abbastanza lungo rispetto a  $T$  ( $T_b >> T$ ), anche il traffico verso il satellite si può considerare **approssimativamente di Poisson**

Quando due o più pacchetti si scontrano (collisione) e devono essere ritrasmessi, il momento in cui questi pacchetti vengono reinviati non è del tutto casuale, ma è influenzato dal momento della collisione iniziale.



Quindi, invece di arrivare al satellite in modo completamente indipendente, i pacchetti ritrasmessi tendono ad arrivare "in blocco" o in momenti più vicini tra loro, creando una correlazione (un legame temporale).

Tempo di Trasmissione = Tempo di Servizio



# Traffico offerto e smaltito

- Ipotesi:
  - Trame tutte uguali di lunghezza pari a L e quindi richiedono un tempo di trasmissione pari a T
- Traffico offerto dalle applicazioni

$$A_0 = \lambda T \longrightarrow \text{ Traffico iniziale generato dalle applicazioni.}$$

- Traffico offerto al MAC

$$G = \lambda_r T \longrightarrow \text{ Traffico effettivo offerto al sistema MAC, comprensivo di ritrasmissioni.}$$

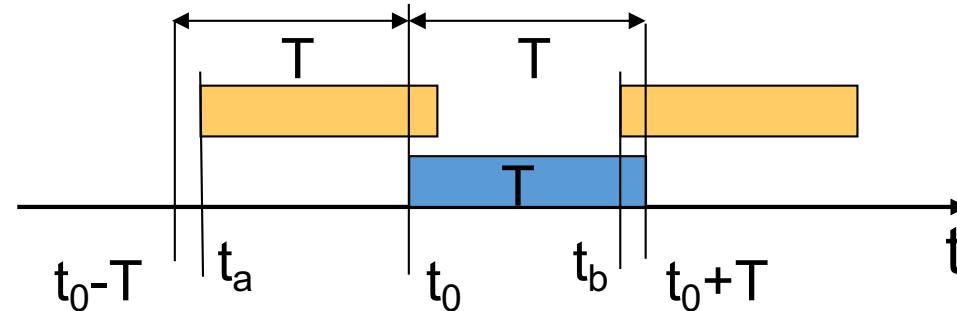
- A causa delle collisioni  $\lambda_r \geq \lambda$
- Il traffico smaltito è pari al traffico offerto che viene trasmesso senza collidere
  - Una trama viene trasmessa senza collidere con probabilità  $P_0$

$$A_s = G P_0 \longrightarrow \text{ Traffico che riesce ad essere trasmesso con successo, senza collisioni.}$$

rappresenta quanto è probabile che un pacchetto venga trasmesso senza collisione.



# Intervallo di vulnerabilità



- Si definisce **intervallo di vulnerabilità**  $T_v$  l'intervallo all'interno del quale una trasmissione può dar luogo a collisione
  - Nel caso di ALOHA vale  $T_v = 2 T$ 
    - La trama considerata inizia in  $t_0$  e finisce in  $t_0 + T$
    - Si ha collisione se
      - il primo bit della trama considerata si sovrapponga all'ultimo bit di una trama precedente
      - Il primo bit di una nuova trama si sovrapponga all'ultimo bit della trama considerata
- Nessuna trama deve essere trasmessa per un tempo  $T$  prima di  $t_0$  e per un tempo  $T$  successivo a  $t_0$
- ↳ L'intervallo di vulnerabilità significa che: Una trasmissione può essere disturbata da altre che iniziano fino a un tempo  $T$  prima o fino a un tempo  $T$  dopo il suo inizio.



# Calcolo del Throughput

- La probabilità di non avere una trasmissione in 2T (probabilità di non collisione) è

$$P_0 = e^{-2\lambda_r T} = e^{-2G}$$

- Quindi il numero medio di trasmissioni aventi successo (traffico smaltito  $A_s$ ) è pari a

$$A_s = G e^{-2G}$$

- Valore massimo di  $A_s$

$$A_s^{max} = 1/(2e) \approx 0.18 \text{ per } G = 0.5$$

Aumentando il Traffico Offerto al MAC, Aumentano il Numero di Pacchetti da Trasmettere e quindi aumenta il numero di collisioni (collisioni producono altre collisioni, aumentando sempre di più, portando il traffico smaltito a circa zero)



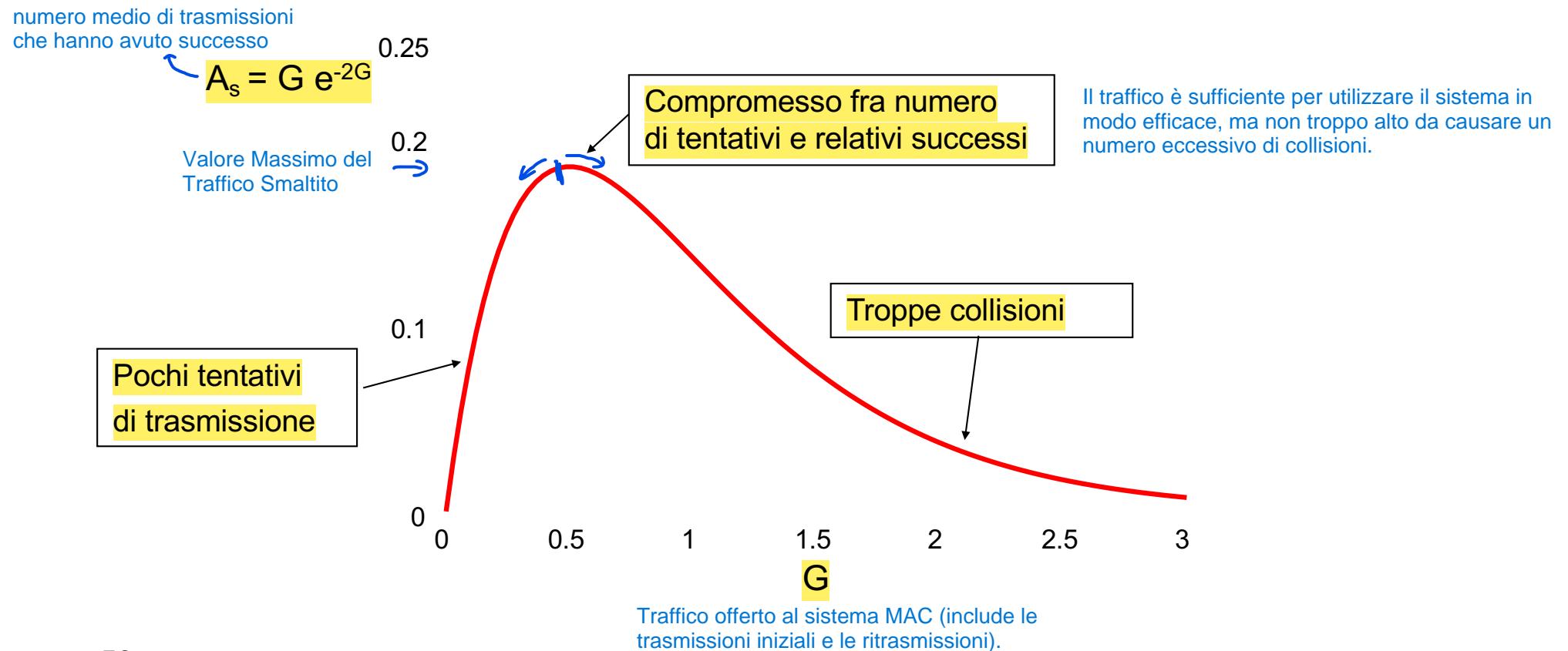
# Aloha: throughput

- $A_s \approx G$  per piccoli valori di  $G$
- $A_s \rightarrow 0$  per grandi valori di  $G$

RIMANERE SEMPRE A VALORI DI  $G < 0.5$

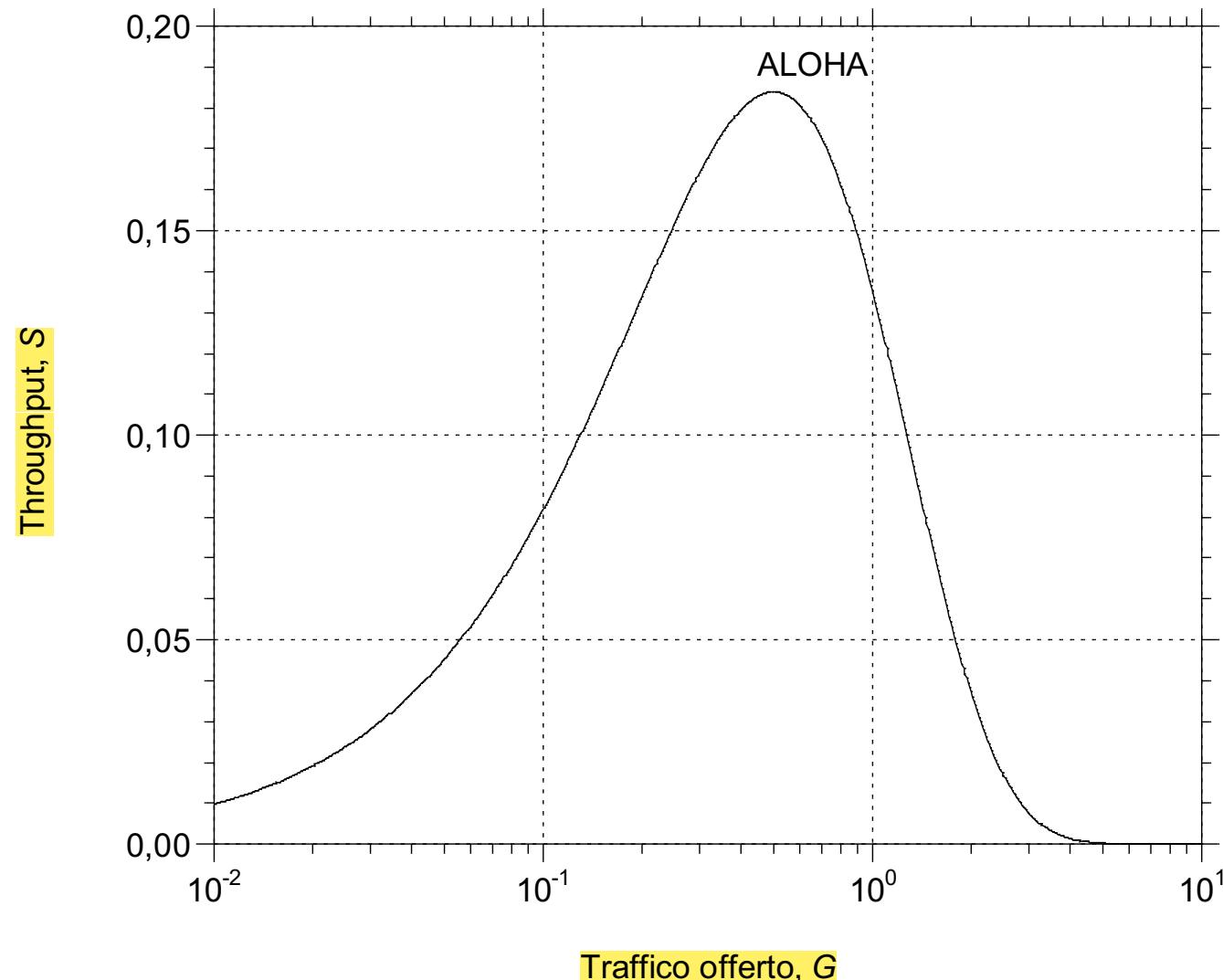
Quando  $G$  è basso, ci sono pochi tentativi di trasmissione. Questo significa che il traffico è gestito facilmente senza collisioni. (Quasi tutto il traffico offerto viene smaltito).

Quando  $G$  aumenta oltre il punto ottimale ( $G>0.5$ ), si verificano troppe collisioni. In questa regione, gran parte del traffico offerto viene perso a causa delle collisioni e delle ritrasmissioni ripetute.





# Per piccoli valori di G



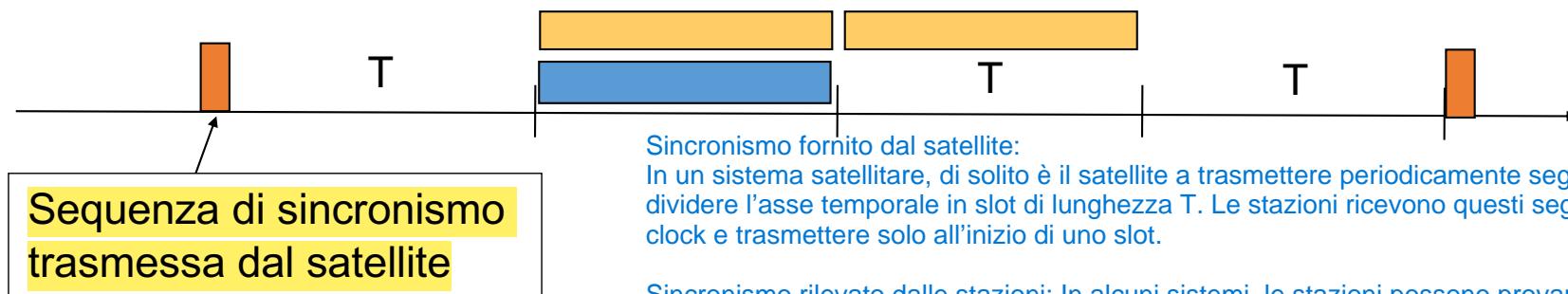
In Aloha puro, le trasmissioni possono iniziare in qualsiasi momento, causando collisioni parziali o complete.  
In Slotted Aloha, le trasmissioni possono iniziare solo all'inizio di uno slot (causando solo collisioni complete, quindi riducendo collisioni perché diminuisce intervallo di vulnerabilità)



# Slotted Aloha

Le stazioni devono mantenere costantemente il sincronismo durante tutta la loro operatività per assicurarsi di trasmettere all'inizio esatto di uno slot (Il satellite trasmette il segnale di sincronismo periodicamente).

- Un possibile miglioramento: **SLOTTED ALOHA.**  
(cioè tutta la rete)
  - Il sistema lavora in modo **sincrono**: l'asse dei tempi viene diviso in intervalli (slot) di lunghezza  $T$  dove  $T$  è il tempo necessario per trasmettere una trama.
  - Le trame vengono trasmesse in corrispondenza di istanti predefiniti



Prima di iniziare le trasmissioni la stazione deve acquisire il sincronismo, inviando trame di tentativo e rivelando come si posizionano rispetto agli slot

Due trame o si sovrappongono completamente o non si sovrappongono per nulla

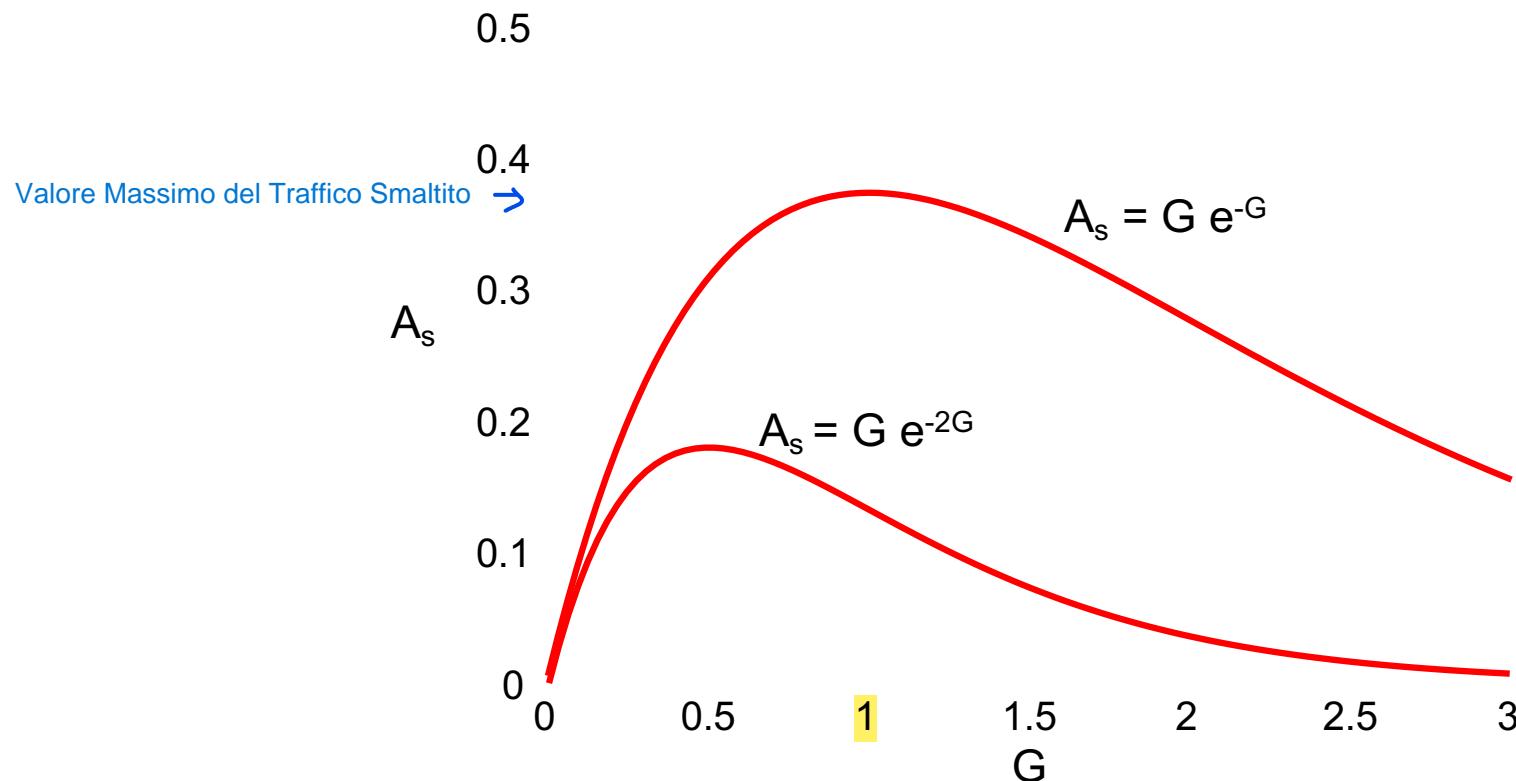
# Slotted Aloha

- L'intervallo di vulnerabilità si riduce a T

-  $P_0 = e^{-G}$

-  $A_s = Ge^{-G}$

- il massimo di  $A_s$  vale  $A_s^{\max} = 1/e \cong 0.36$  per  $G_{\max} = 1$





# Algoritmi di back-off

La decisione di trasmettere in quello slot è probabilistica, cioè:  
La stazione trasmette con una probabilità  $p_b$ .  
Con una probabilità complementare  $(1-p_b)$ , la stazione non trasmette e passa allo slot successivo.  
Se la stazione decide di non trasmettere nel primo slot, passa al successivo slot utile e ripete lo stesso processo

- Aloha classico

- Sceglie a caso (con probabilità uniforme) il nuovo istante di trasmissione nell'intervallo 0 e  $T_b$

- Deve essere  $T_b \gg T$  per rendere piccola la probabilità di una nuova collisione

- Aloha slotted

- Si ritrasmette negli istanti di sincronismo, ci sono due alternative:

- Si prende  $T_b = n_b T$  e si sceglie un numero a caso fra 0 ed  $n_b-1$  (si sceglie uno slot dei disponibili)

- Si ritrasmette nel primo slot utile con probabilità  $p_b$  e si passa allo slot successivo con probabilità  $(1-p_b)$ ; ripetendo l'algoritmo ad ogni slot fino a che non si trasmette (si scorre gli slot disponibili uno ad uno, scegliendo il primo utile per trasmettere secondo  $p_b$ )

- A parità di valore medio del tempo di ritrasmissione, queste due alternative danno prestazioni simili

Entrambi gli approcci (Aloha classico e slotted) hanno prestazioni simili



# Traffico offerto e smaltito

- In condizioni di equilibrio il traffico offerto al sistema deve essere eguale al traffico smaltito

$$A_0 = A_s$$

(il traffico può variare in modo casuale)

- Per effetto delle fluttuazioni statistiche del traffico,  
su brevi intervalli di tempo risulterà

capacità massima del sistema  
= traffico massimo smaltito

$$A_0 \neq A_s$$

- Se  $A_0 < A_s^{\max}$  la dinamica naturale del sistema tende a portarsi in equilibrio il sistema ha la capacità di smaltire tutto il traffico.
- Se  $A_0 > A_s^{\max}$  è impossibile raggiungere una situazione di equilibrio
  - I dati si accumulano nello strato superiore al MAC, in quanto una buona parte di essi non riesce mai ad essere trasmessa

Se il traffico offerto eccede questa capacità, il sistema non può mantenere l'equilibrio, causando perdite e inefficienze.

Con l'aumento delle collisioni:

Si generano più ritrasmissioni.

Le ritrasmissioni contribuiscono a sovraccaricare ulteriormente il sistema.

Il traffico offerto diventa ancora più elevato rispetto alla capacità del sistema ( $A_s^{\max}$ ).

Il sistema entra in una spirale di congestione in cui diventa impossibile ritornare all'equilibrio.



(cioè stazioni che hanno pacchetti in attesa di essere trasmessi a causa di collisioni).

# Numero di stazioni finito e stabilità

- Il traffico offerto dipende dal numero di stazioni backlogged

$k$

Una stazione non backlogged sta generando pacchetti con frequenza media  $\lambda$ , pronti per essere trasmessi.

Una stazione è considerata backlogged quando ha subito collisioni e deve attendere prima di ritrasmettere.

Sia  $\lambda_i$  la frequenza media di arrivo delle trame da ciascuna stazione

- Se la stazione non è backlogged:  $\lambda_i = \lambda$  La stazione continua a generare pacchetti da inviare
- Se la stazione è backlogged non invia nuove trame:  $\lambda_i = 0$

Durante il backlog, la stazione non genera nuovi pacchetti

- Con  $k$  stazioni backlogged il traffico offerto vale

$\lambda$  è la frequenza media di generazione dei pacchetti dalle stazioni.

$$A_0 = \lambda T(N-k)$$

Con  $N$  stazioni totali e  $k$  stazioni backlogged:  
Solo le  $N-k$  stazioni non backlogged contribuiscono al traffico offerto.

- Inoltre

- $G(k)$  è una funzione monotona di  $k$
- $S(G(k))$  ha una forma simile a quella già evidenziata

tempo di trasmissione della trama.

traffico totale offerto al sistema (cioè il traffico generato dalle stazioni non backlogged e backlogged)

traffico smaltito dal sistema, cioè il numero medio di pacchetti che vengono trasmessi con successo.

- I valori di  $k$  che garantiscono condizioni di stabilità si trovano determinando  $k$  tale che  $A_0(k) = S(k)$

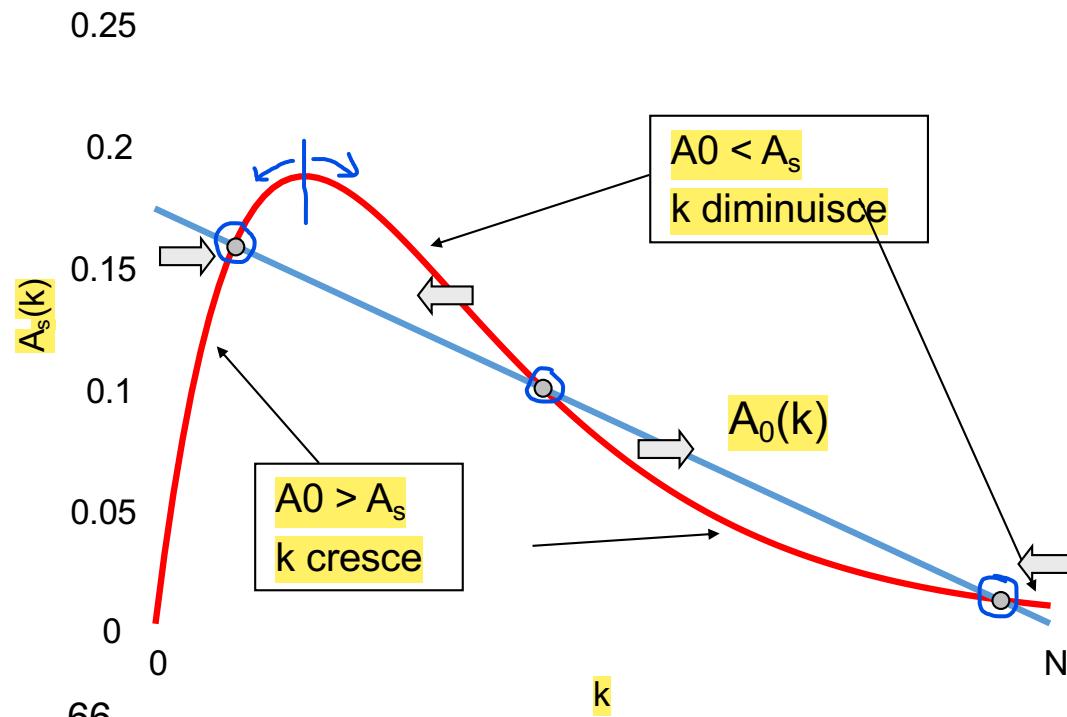
La rete è stabile quando il traffico offerto è esattamente uguale al traffico smaltito, in relazione a  $k$ .



# Stabilità

$A_0(k)$  (traffico offerto): Dipende dal numero di stazioni attive ( $N-k$ ) e dalla frequenza di generazione delle trame lambda. È rappresentato dalla curva blu.  
 $A_s(k)$  (traffico smaltito): Rappresenta quanto traffico il sistema riesce effettivamente a trasmettere senza collisioni. È la curva rossa, che raggiunge un massimo e poi diminuisce a causa delle collisioni.

- Se  $A_0 > A_s$  si accumula traffico  $\Rightarrow$  si hanno collisioni  $\Rightarrow$  le stazioni backlogged aumentano  $\Rightarrow A_0$  cala e  $k$  cresce
- Se  $A_0 < A_s$  si smaltisce più traffico di quello nuovo in arrivo  $\Rightarrow$  si trasmettono trame che hanno colliso in precedenza  $\Rightarrow$  le stazioni backlogged calano  $\Rightarrow A_0$  cresce e  $k$  cala



- **3 punti di stabilità**
  - 2 sono stabili
  - 1 instabile
- **Un aumento eccessivo di  $A_0$  può portare ad una situazione di troppe collisioni**
  - Primo punto (stabile): Qui il sistema è leggero, con poche collisioni e un numero basso di stazioni backlogged. Se  $A_0$  aumenta leggermente, il sistema tende a tornare in questo punto.
  - Secondo punto instabile: Questo è un punto critico. Un piccolo aumento di  $k$  fa sì che il sistema si sposti verso congestimento ( $A_0 > A_s$ ). Questo punto non è stabile perché il sistema tende ad allontanarsi da esso.
  - Terzo punto (stabile): Qui il sistema è in uno stato congestionato, con molte stazioni backlogged. Anche se le collisioni sono frequenti, il sistema rimane "stabili" in questa situazione di congestione.



# Controlled Aloha

- Per ovviare al problema dell'instabilità si possono usare varie tecniche
- Una delle più semplici è fare crescere il tempo di back-off
  - Alla prima collisione si pone  $T_b = T_0$  Il tempo di back-off viene impostato a un valore iniziale.
  - Se la trama ritrasmessa collide di nuovo si pone  $T_b = 2T_0$  e si continua a raddoppiare  $T_b$  ad ogni nuova collisione  $T_b=4T_0, T_b=8T_0$ , e così via.
  - Quando la trasmissione ha successo si ritorna a  $T_b = T_0$
  - Nel caso slotted si puo dimezzare  $p_b$  ad ogni collisione
- Questo algoritmo si dice **back-off esponenziale** e si può dimostrare che elimina l'instabilità
  - Può fare sorgere problemi di fairness: una stazione che ha subito molte collisioni viene tagliata fuori dalle trasmissioni



# Derivati del protocollo Aloha

- Il protocollo Aloha può essere implementato su qualunque mezzo trasmissivo e qualunque topologia
- Ha una efficienza piuttosto bassa ma è circa quanto di meglio si può fare quando i ritardi di propagazione sono grandi come nel caso del satellite
- Se lo si vuole applicare ad una rete locale conviene sfruttare la conoscenza che ogni stazione può acquisire sull'attività delle altre
- Nasce così il protocollo **CSMA Carrier Sensing Multiple Access**
  - Viene proposto su una topologia a Bus bidirezionale
  - È ancora un protocollo ad accesso casuale a contesa



# CSMA: Carrier Sensing Multiple Access

- **Carrier sensing** Protocollo con Accesso Casuale al Canale con Rilevazione del canale (senza rilevazione di collisione)

Ogni stazione che deve trasmettere verifica se il bus (il mezzo di trasmissione condiviso) è libero o occupato.

La stazione non trasmette immediatamente. Invece, avvia un algoritmo di back-off: Aspetta un intervallo di tempo casuale prima di controllare di nuovo se il bus è libero.

La stazione attende che il bus diventi libero e poi: Trasmette con una probabilità  $p$ . Con una probabilità  $1-p$ , la stazione attende il prossimo slot e ripete il controllo.

- Ogni stazione che debba trasmettere **rivela** presenza di segnale sul bus e trasmette solo se è libero
  - Se il bus è occupato si aspetta la fine della trama e poi
    - Si trasmette (caso 1 persistent) La stazione attende che il bus diventi libero e poi trasmette immediatamente.
    - Si fa partire l'algoritmo di back off (caso non persistent o 0 persistent)
    - Si trasmette con probabilità  $p$  e si fa partire l'algoritmo di back off con probabilità  $(1-p)$  (caso  $p$  persistent) (utilizzato nei sistemi slotted CSMA (lunghi tau))

- Una volta iniziata la trasmissione, i dati inviati da una stazione **possono collidere** con quelli di un'altra

Anche con il carrier sensing, le collisioni possono avvenire.

C'è un tempo finito ( $\tau$ ) per cui il segnale di trasmissione si propaga sul bus.

- Questo avviene a causa del ritardo di propagazione non nullo
- Sul bus non c'è un meccanismo immediato di rivelazione delle collisioni: occorre affidarsi a un sistema di Acknowledgement → per confermare che i dati sono stati ricevuti correttamente. Se non si riceve un ACK, la stazione assume che ci sia stata una collisione e ritrasmette.

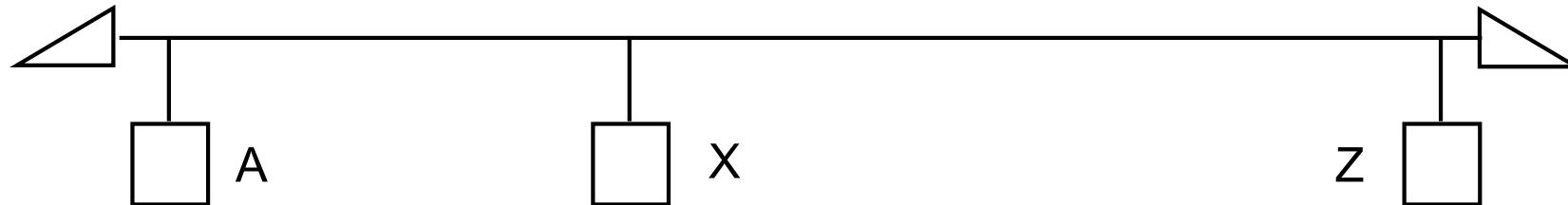
- L'algoritmo di back-off può essere come quello dell'Aloha con  $T_b \gg 2\tau$

ritardo massimo di propagazione



L'intervallo di vulnerabilità rappresenta il periodo di tempo in cui può verificarsi una collisione tra i dati trasmessi da due stazioni.

# CSMA: intervallo di vulnerabilità



- Chiamiamo A e Z le due stazioni più distanti sul Bus e  $\tau$  il tempo di propagazione fra di loro + il tempo necessario per rivelare il segnale

e rileva libero il canale ed inizia a trasmettere.

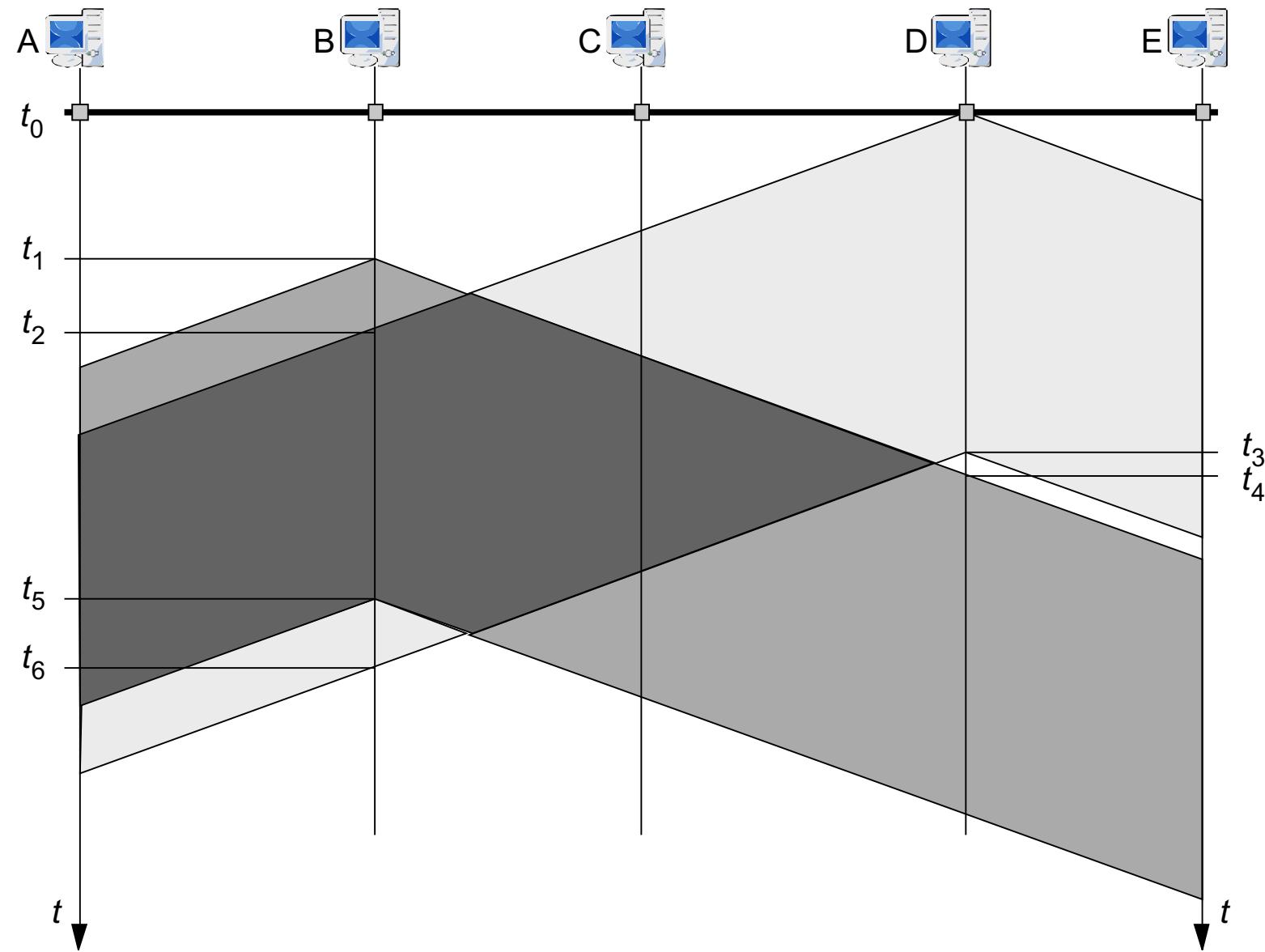
- A esegue il carrier sensing nell'istante  $t_A$  (perché il segnale non ha avuto abbastanza tempo per propagarsi).
  - Se Z fa carrier sensing fra  $t_A$  e  $t_A + \tau$  non rileva attività e può quindi anch'essa iniziare a trasmettere: *si ha collisione*
  - Analogamente se Z ha trasmesso fra  $t_A$  e  $t_A - \tau$  A non rileva il segnale di Z e trasmette in  $t_A$ : *si ha collisione* In questo intervallo, il segnale di Z non è ancora arrivato ad A.
- L'intervallo di vulnerabilità vale  $2\tau$
- Le prestazioni sono tanto migliori dell'Aloha quanto più

Per minimizzare l'impatto delle collisioni

$$\tau/T < 1$$

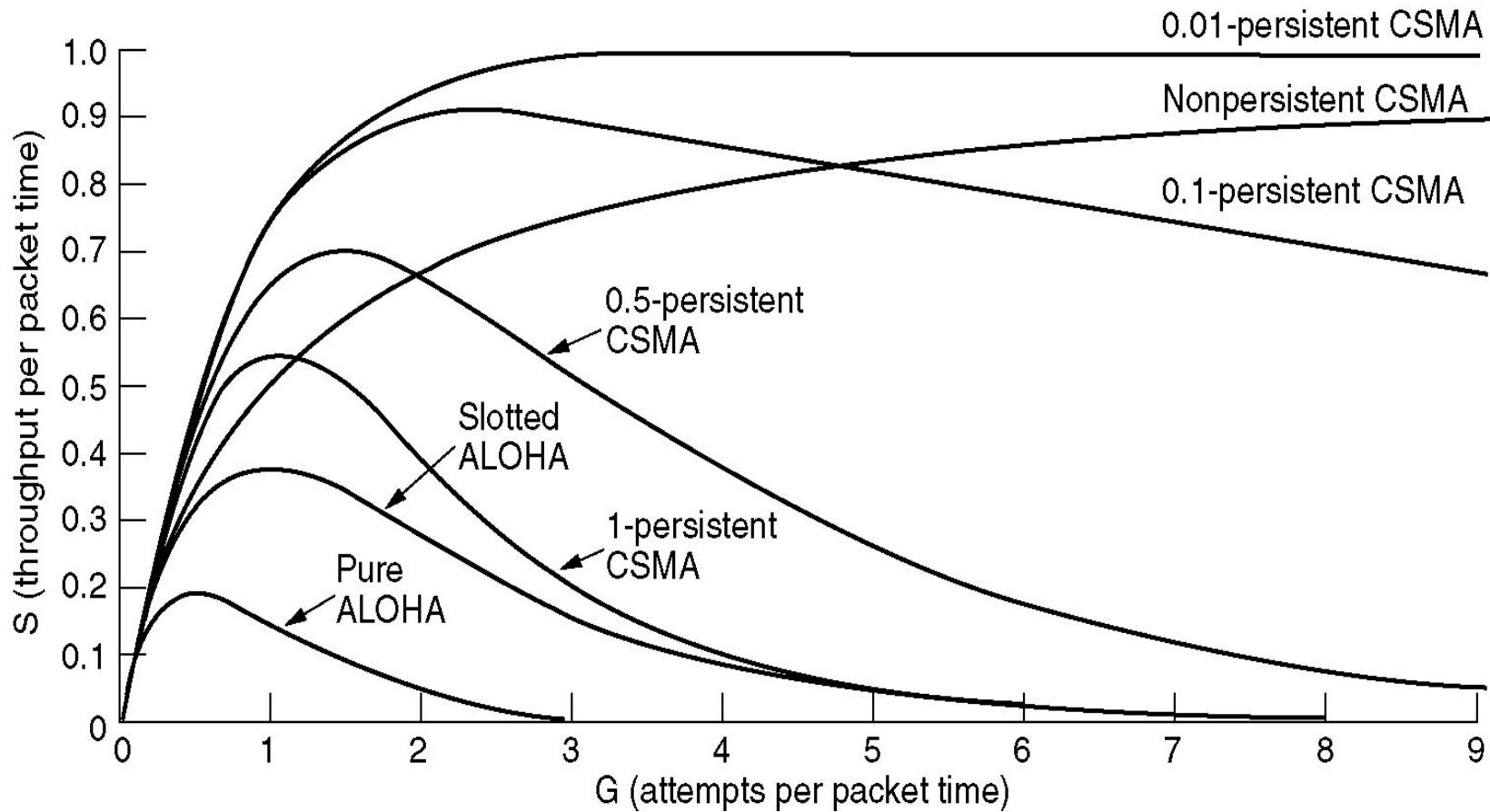
Più piccolo è tau, più migliorano le prestazioni

- In generale le prestazioni dipendono anche dal valore di  $p$



# Persistent e Nonpersistent CSMA

Utilizzazione del canale per Aloha e CSMA





# Versione slotted e problemi di stabilità

- Anche per il CSMA esiste la **versione slotted**
  - In questo caso la misura più opportuna del **tempo di slot** è  $\tau$
  - L'intervallo di vulnerabilità vale  $\tau$  invece che  $2\tau$
- 
- Anche per il CSMA come per tutti i protocolli a contesa **ci sono problemi di stabilità**
  - Si può usare un algoritmo di back-off esponenziale



Quasi Ideale

# CSMA/CD: CSMA con Collision Detect

- Un miglioramento del CSMA è stato proposto da **Metcalfe** nel 1976

- **Collision Detection:**

- Una stazione è in grado di rilevare l'avvenuta collisione *rimanendo in ascolto* sul mezzo mentre trasmette
  - E' un processo analogico basato sulla rilevazione di potenza sul canale (facilitato anche dalla codifica di Manchester adottata)

La codifica Manchester aiuta a rilevare più facilmente variazioni nel segnale, semplificando il processo di collision detection.

Quando una stazione trasmette, monitora il segnale che sta inviando. Se il segnale ricevuto corrisponde a quello trasmesso, significa che non c'è nessuna interferenza e quindi nessuna collisione. Se un'altra stazione inizia a trasmettere contemporaneamente, i due segnali si sovrappongono.

Poiché il segnale codificato in Manchester ha un andamento regolare e prevedibile, qualsiasi variazione dovuta a una collisione risulta evidente e può essere immediatamente rilevata.

- In caso di collisione:

- si ferma subito la trasmissione
  - si invia una particolare sequenza di bits (**jamming**) per informare tutte le altre stazioni dell'avvenuta collisione

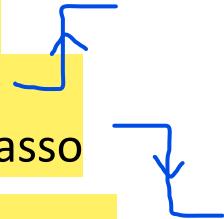
La stazione interrompe subito la trasmissione per evitare di sprecare risorse.

che devono interrompere eventuali trasmissioni o ritrasmissioni.



# Codifica di Manchester

- Rappresentazione dei bit
  - “0” logico: segnale basso (-0.85 Volt) per mezzo tempo di simbolo e segnale alto (+0.85 Volt) per l’altro mezzo
  - “1” logico: segnale alto per mezzo tempo di simbolo e poi segnale basso



- Vantaggi
  - Una transizione al centro di ogni bit, che può essere rivelata mediante un derivatore, facilita
    - L’acquisizione del sincronismo
    - Il carrier sensing
    - Il collision detection
  - Sono disponibili simboli (alto alto e basso basso) per rappresentare *non dati*

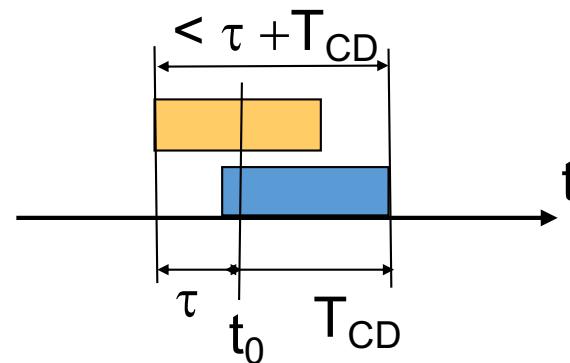
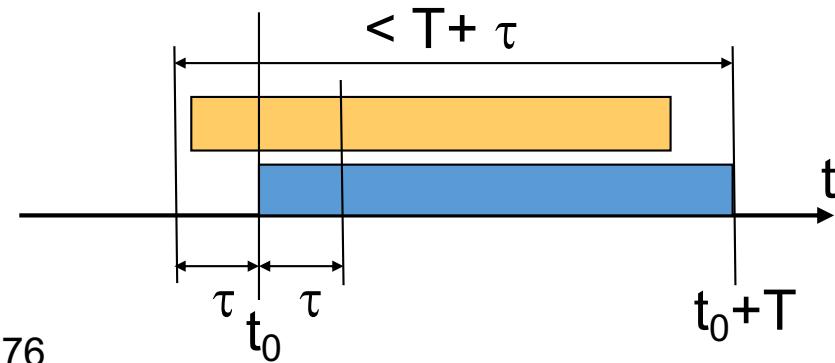
- Svantaggi
  - Per trasmettere a 10 Mbit/s occorre un clock a 20 MHz

(Questo perché ad ogni tempo di bit ho sempre due variazioni (da 1 a 0, o viceversa))  
Si perde metà della Larghezza di Banda Disponibile

- Il protocollo CSMA/CD con codifica di Manchester è stato adottato nella rete Ethernet, standard di mercato per le LAN

# Cosa migliora nel CSMA-CD

- Nei casi in cui avviene collisione
  - Nel CSMA le stazioni continuano la trasmissione dell'intera trama
    - Il canale rimane impegnato inutilmente per un intervallo di tempo all'incirca pari a  $T$
  - Nel CSMA/CD
    - Al più il canale rimane impegnato inutilmente al più per la somma di
      - Un intervallo di vulnerabilità ()
      - Il tempo necessario a rilevare la collisione più il tempo della sequenza di Jamming ( $T_{CD}$ )



MO



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# Protocolli controllati: funzionalità e prestazioni



# TOKEN RING e IEEE 802.5

- Token Ring sviluppato dai laboratori IBM nel 1976;
- Topologia: logicamente un anello ma fisicamente una stella con cavi STP 1
- bit rates: 4 Mbit/s (vecchie versioni), 16 Mbit/s;
- In 1982 IEEE costituisce il comitato 802.5 che standardizza il Token Ring per i livelli fisico e MAC
- Nel 1993 IEEE produce un document (802.5 Q/Draft 3) per l'impiego dei cavi UTP



# Token Ring

- Token Ring sviluppato dai laboratori IBM nel 1976
- E' un protocollo controllato in cui non si possono verificare collisioni
- Richiede una topologia ad anello (ring)
- **Token** = diritto alla trasmissione
  - si può realizzare mediante una trama che gira continuamente sulla linea in cui un bit (**token bit**) indica se è libero o occupato
- L' accesso al mezzo funziona come segue
  - accede al mezzo condiviso chi è in possesso del token
  - la stazione che vuole trasmettere attende che passi un token libero, lo occupa e vi appende le informazioni in coda.



# Definizioni

- **T : tempo di trasmissione**
  - Tempo necessario per la trasmissione di una trama di lunghezza massima
- **$T_{acc}$  : Tempo di accesso**
  - Tempo che una stazione deve attendere per vedere il token libero e quindi essere trasmessa
- **$T_{lat}$  : Tempo di latenza**
  - Tempo che impiega un bit a fare un giro completo dell'anello
  - dipende dalla lunghezza dell'anello e dal ritardo introdotto dalle stazioni
- **THT : Tempo di detenzione del token (Token Holding Time)**
  - Tempo trascorso fra l'arrivo e la partenza del token da una stazione
- **TRT: Token Rotation Time**
  - Tempo che impiega il token a compiere un giro completo dell'anello



# Rimozione delle trame

- La trama deve essere rimossa dall' anello una volta ricevuta.
- Rimozione con **modalità parzialmente diffusiva**
  - la trama viene rimossa dalla **stazione ricevente** che libera anche il token
  - prima di ritrasmettere occorre *leggere* almeno l' indirizzo del destinatario
- Rimozione con **modalità diffusiva**
  - la trama viene rimossa dalla **stazione trasmittente** che libera anche il token
  - la stazione ricevente può appendere un Ack alla trama
  - Ogni stazione può ritrasmettere le trame immediatamente con un ritardo di un solo bit

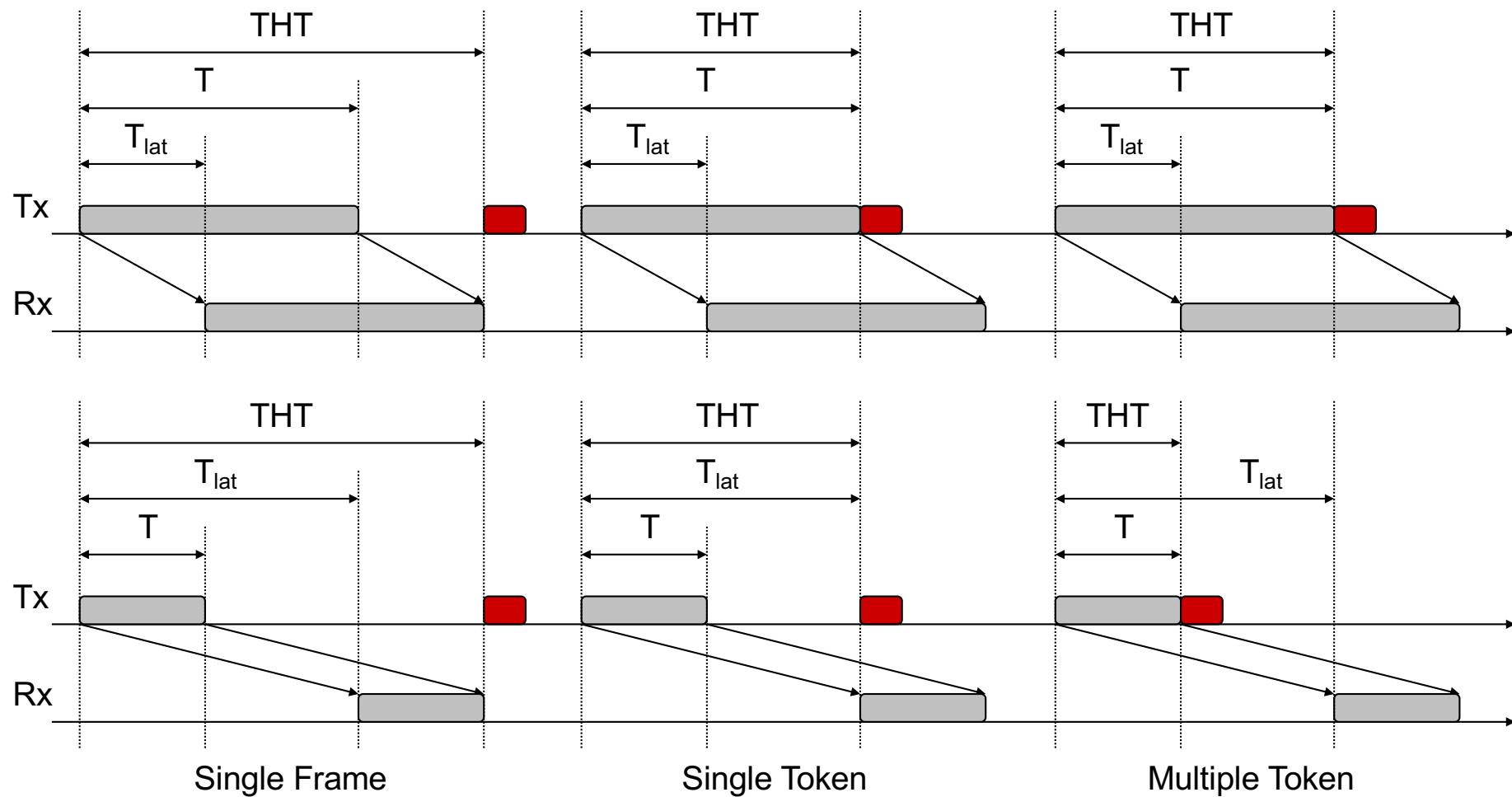


# Rimozione delle trame (segue)

- Con la tecnica parzialmente diffusiva il token si libera prima però si hanno i seguenti svantaggi:
  - cambiamento dell'ordine di trasmissione e maggiore aleatorietà del tempo di accesso
  - mancanza di una verifica di corretta trasmissione
  - aumento del tempo di latenza
- Nella modalità diffusiva, la rigenerazione del token si può avere con tre modalità
  - **Sigle frame**: il token viene rigenerato quando la stazione ha ricevuto l'intera trama trasmessa
  - **Single token**: il token viene rigenerato quando la stazione ha ricevuto il token della trama trasmessa
  - **Multiple token**: il token viene rigenerato appena la stazione ha finito di trasmettere la trama (ha senso solo se il tempo di latenza è maggiore del tempo di trama)

# Rigenerazione del token

- THT dipende da
  - Dimensione massima della trama ( $T$ )
  - Strategia di rigenerazione del token

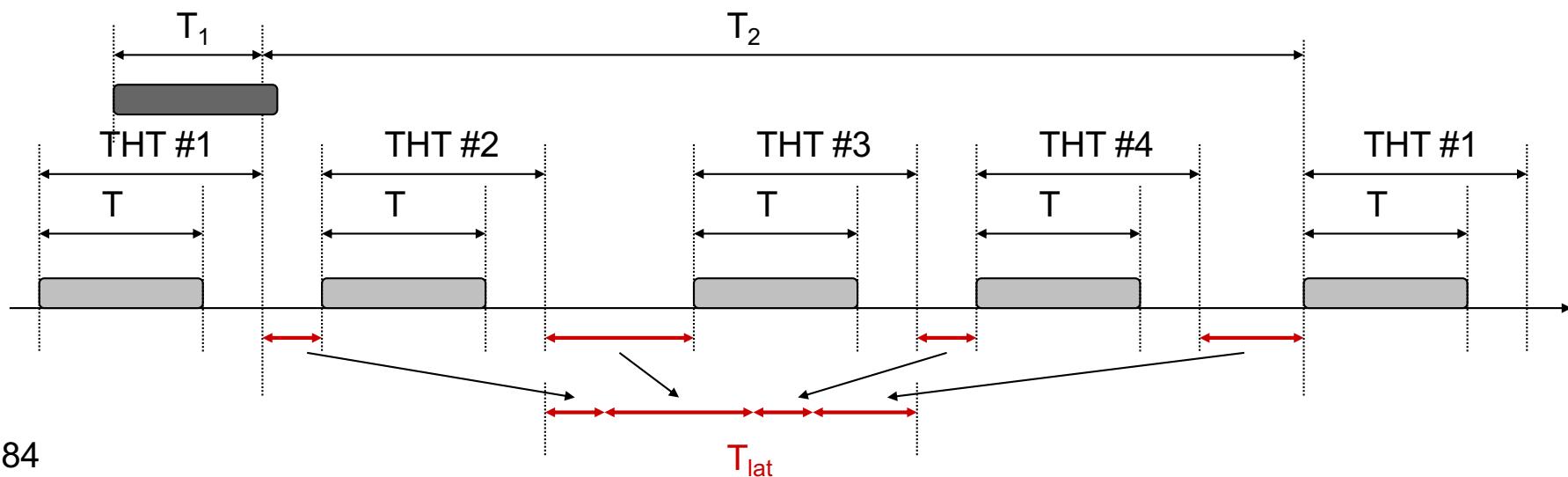


# Tempo di accesso

- n stazioni, trame tutte di lunghezza massima
- Una trama arriva alla stazione 1 durante il suo THT
  - Deve attendere  $T_1$  affinché la stazione 1 lasci il token  
 $T_1 \leq \text{THT}$  e  $E[T_1] = \text{THT}/2$
  - Deve attendere  $T_2$  affinché il token ritorni alla stazione 1  
 $T_2 \leq (n-1) \text{THT} + T_{\text{lat}}$ 
    - Al peggio il token può essere trattenuto per un THT dalle altre n-1 stazioni
    - Il token impiega un  $T_{\text{lat}}$  a percorrere l'anello

$$T_{\text{acc}} = T_1 + T_2 \leq n \text{THT} + T_{\text{lat}} = \text{TRT}$$

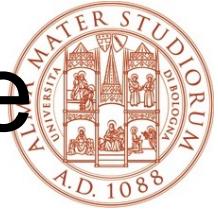
$$E[T_{\text{acc}}] = \text{THT}/2 + (n-1)/2 \text{THT} + T_{\text{lat}} = n \text{THT}/2 + T_{\text{lat}}$$





# Monitor

- In caso di malfunzionamenti di stazioni possono verificarsi situazioni di emergenza che richiedono l'intervento di un supervisore (monitor)
- La funzione di monitor può essere svolte da qualunque stazione
- Un tipico problema è una stazione trasmittente che non rimuove la trama e questa circola indefinitamente nell'anello
  - Per rimuoverla il Monitor dispone di un bit M nel campo token, che è sempre 0 quando un nuovo token viene generato e viene marcato a 1 dal monitor ogni volta che questo riceve una trama: se il monitor riceve una trama con M=1 la rimuove
- Altri possibili malfunzionamenti
  - Token perduto: non circola più nulla nell'anello
  - Token duplicato



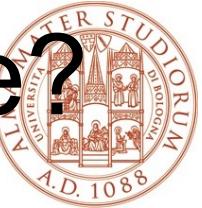
# Sincronizzazione e ritrasmissione bit per bit

- Il sincronismo viene ricavato dal segnale ricevuto e usato per il segnale trasmesso (sincronismo asservito)
- Occorre almeno una stazione nell'anello (ad esempio il Monitor) che genera il sincronismo e lo ripristina con un buffer elastico
- Per rendere minimo il tempo di latenza il ogni stazione ritrasmette ogni singolo bit appena lo ha ricevuto
- Un inconveniente è che le trame devono essere ritrasmesse prima del controllo di correttezza e potrebbero contenere errori



# Token passing o Token bus

- Usa il concetto di token in una topologia a bus
- Le stazioni formano un anello logico in cui ognuna ha un predecessore ed un successore
- La stazione che possiede il token può usarlo per un THT
- Il passaggio del token avviene inviando al successore una trama apposita (give token)
- L'anello logico si forma e si modifica dinamicamente
  - La stazione che vuole uscire dall'anello attende di avere il token e poi lo comunica al predecessore e al successore
  - Per l'ingresso nell'anello occorre che una stazione prima di passare il token faccia un polling invitando chi vuole ad entrare
    - Se più stazioni vogliono entrare si apre una fase a contesa



# Protocolli a contesa o collision free?

- Vantaggi dei protocolli a contesa
  - Maggior semplicità
  - Maggiore efficienza a basso traffico
- Vantaggi dei protocolli collision free
  - Tempo di consegna di una trama superiormente limitato in modo deterministico
  - Assenza di problemi di stabilità
  - Miglior sfruttamento della capacità del canale ad alto traffico
- I protocolli collision free sono stati ritenuti migliori per applicazioni con problemi di real time
  - In queste applicazioni il token bus è stato preferito rispetto al token ring
    - Se si capita un malfunzionamento e contemporaneamente il monitor ha un guasto, il token ring si blocca per un tempo imprevedibile
- Comunque il protocollo divenuto standard di mercato è l' Ethernet e gli altri stanno sparendo



# MAC del Token Ring

- E' un protocollo controllato in cui non si possono verificare collisioni
- Token = diritto alla trasmissione
  - si puo' realizzare mediante una trama che gira continuamente sulla linea
- L'accesso al mezzo funziona come segue
  - accede al mezzo condiviso chi e' in possesso del token
  - la stazione che vuole trasmettere attende che passi un token libero, lo occupa e vi appende le informazioni in coda.
- Tempo di accesso:
  - tempo che la stazione deve attendere per vedere il token libero
- Tempo di latenza
  - tempo che impiega un bit a fare un giro completo dell'anello
  - dipende dalla lunghezza dell'anello e dal ritardo introdotto dalle stazioni



# Rimozione delle trame

- La trama deve essere rimossa dall'anello una volta ricevuta.
- Rimozione con modalità diffusiva
  - la trama viene rimossa dalla stazione trasmittente che libera anche il token
- Rimozione con modalità parzialmente diffusiva
  - la trama viene rimossa dalla stazione ricevente che libera anche il token
- Con la tecnica parzialmente diffusiva il token si libera prima però si hanno i seguenti svantaggi:
  - cambiamento dell'ordine di trasmissione e maggiore aleatorietà del tempo di accesso
  - mancanza di una verifica di corretta trasmissione
  - aumento del tempo di latenza a causa della necessità di memorizzare almeno il token e l'indirizzo del destinatario in ciascuna stazione.



# Rimozione delle trame (segue)

- Nella modalità diffusiva, la rigenerazione del token si può avere con tre modalità
  - Single frame: il token viene rigenerato quando la stazione ha ricevuto l'intera trama trasmessa
  - Single token: il token viene rigenerato quando la stazione ha ricevuto il token della trama trasmessa
  - Multiple token: il token viene rigenerato appena la stazione ha finito di trasmettere la trama (ha senso solo se il tempo di latenza è maggiore del tempo di trama)



# Tempo di accesso

- Si stabilisce un limite THT (token holding time) per il tempo di utilizzo del token per ogni stazione
- Tempo di rotazione del token (TRT): tempo impiegato da un token lasciato libero a tornare libero alla stessa stazione
- Con  $n$  stazioni si ha

$$TRT \leq n \cdot THT$$

- Il tempo di accesso è limitato superiormente a  $TRT + \text{tempo di latenza}$



# Monitor

- In caso di malfunzionamenti di stazioni possono verificarsi situazioni di emergenza che richiedono l'intervento di un supervisore (monitor)
- La funzione di monitor può essere svolte da qualunque stazione
- Un tipico problema è una stazione che non rimuove la trama dopo che ha fatto il giro e questa circola indefinitamente nell'anello
- Per rimuoverla il Monitor dispone di un bit  $M$  nel campo token, che è sempre 0 quando un nuovo token viene generato e viene marcato a 1 dal monitor ogni volta che questo riceve un a trama: se il monitor riceve una trama con  $M=1$  la rimuove.



# Sincronizzazione

- Per rendere minimo il tempo di latenza il ogni stazione ritrasmette ogni singolo bit appena lo ha ricevuto
- Come conseguenza le trame vengono ritrasmesse anche se contengono errori
- Il sincronismo viene ricavato dal segnale ricevuto e usato per il segnale trasmesso (sincronismo asservito)
- Occorre almeno una stazione nell'anello (ad esempio il Monitor) che ripristina il sincronismo con un buffer elastico



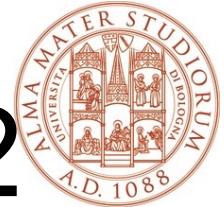
ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# PROGETTO IEEE 802

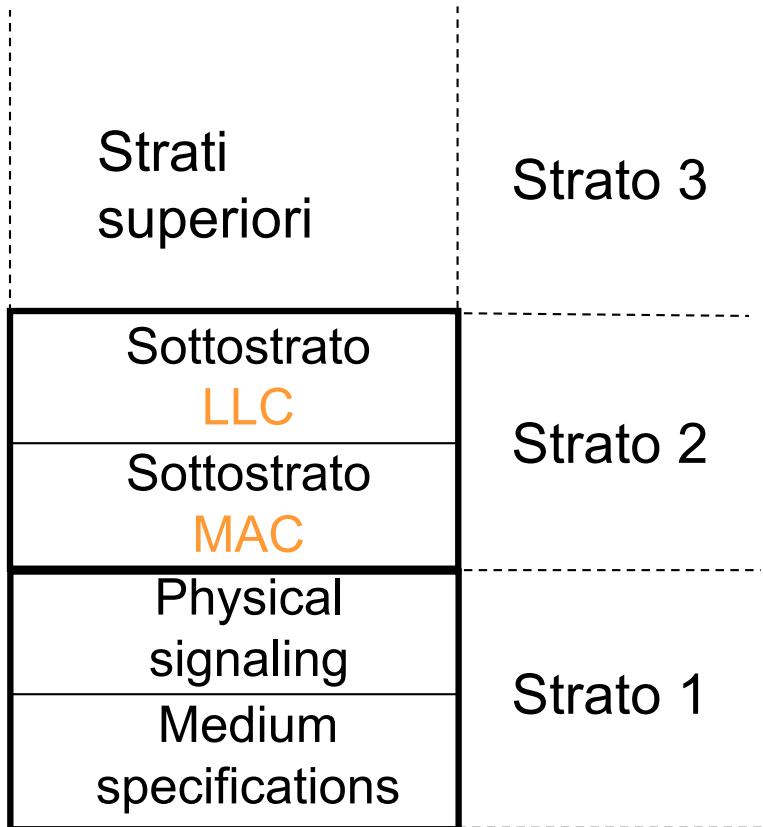


# Progetto IEEE 802

- Molti altri protocolli a contesa e collision free sono stati proposti soprattutto nei tardi anni '70
- Nel 1980 parte il **Progetto IEEE 802** per tentare di definire degli standard per LAN
  - IEEE ha già avuto un grande successo con lo standard **IEEE 488**, per applicazioni ai **banchi di misura** comandati da un calcolatore
    - Propone un' **architettura master-slave**
    - Si rifà ad uno standard di mercato proprietario: lo **HP-IB** (Hewlett Packard Interface Bus)
- Si organizza in commissioni che producono documenti denominati **IEEE 802.x**
  - diventeranno standard ISO col nome **IS 8802/x**



# Scelta importante di IEEE 802



- Lo strato 2 viene diviso in due sottostrati
  - LLC = Logical Link Control
  - MAC = Medium Access Control
- Lo strato LLC è indipendente dal mezzo fisico, dalla topologia e dal protocollo di accesso
- Anche lo strato 1 viene diviso in due



# Commissioni e documenti IEEE 802

- **IEEE 802.1** : descrizione generale del progetto, modello di riferimento
  - Non ha mai finito i suoi lavori
  - Contiene anche parte di standard che non trovano facilmente posto in altri documenti
- **IEEE 802.2** : Sottostrato LLC, interfaccia con gli strati superiori
- **IEEE 802.3** : Rete locale basata su CSMA/CD, ispirata alla rete Ethernet (per Intel)
- **IEEE 802.4** : Rete locale basata su Token Passing Bus (per Boing)
- **IEEE 802.5** : Rete locale basata su Token Ring, ispirata alla rete Token Ring di IBM
- **IEEE 802.6** : Reti in Area Metropolitana o MAN (Metropolitan Area Networks)

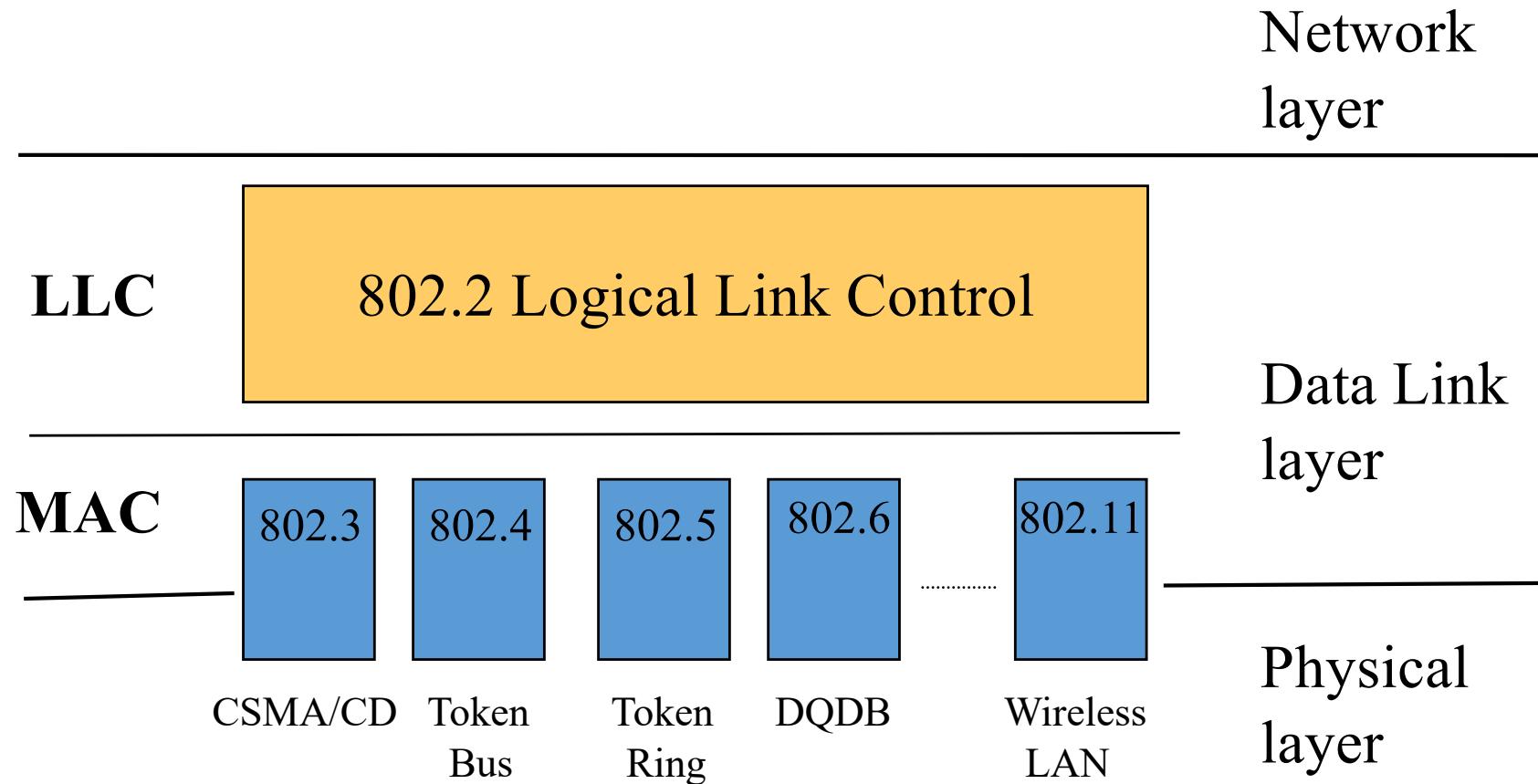


# Commissioni e documenti IEEE 802

- IEEE 802.7 : Studi sulle tecnologie a larga banda
- IEEE 802.8 : Studi sulla tecnologie in fibra ottica
- IEEE 802.9 : ISLAN (Isochronous LAN)
- IEEE 802.10 : LAN/MAN security
- IEEE 802.11 : WLAN (Wireless LAN)
- IEEE 802.12 : Reti locali a 100 Mbit/s basate su Demand Priority (standard AnyLAN di HP)
- IEEE 802.13 : non esiste
- IEEE 802.14 : Cable modem per impianti di TV via cavo
- IEEE 802.15 : Personal Area Networks (Bluetooth)
- IEEE 802.16 : Accesso wireless a banda larga per utenti residenziali
- IEEE 802.17 : Resilient Packet Ring (RPR)



# PROGETTO IEEE 802





ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# Rete Ethernet e IEEE 802.3



# Rete Ethernet

- Nasce da sviluppi della Xerox nel 1976, poi si forma in consorzio comprendente
  - Digital Equipment Corporation (DEC)
  - Intel
  - Xerox
- Il consorzio nel 1978 mette a punto lo standard a 10Mbit/s chiamato DIX
- Nel 1983 il DIX diviene con poche modifiche lo standard IEEE 802.3
- È basato sul protocollo di accesso CSMA/CD



# CSMA/CD

- Protocollo Carrier Sensing Multiple Access with Collision Detection
  - Limita molto ma non elimina la possibilità che due stazioni parlino in contemporanea
  - È quindi possibile la collisione fra due o più flussi informativi risultante in perdita di trame (layer 2 PDU)
- Permette un'utilizzazione molto efficiente della banda disponibile sul mezzo trasmissivo
- Non è in grado di garantire in modo certo i tempi di consegna delle trame (ritardo di accesso)

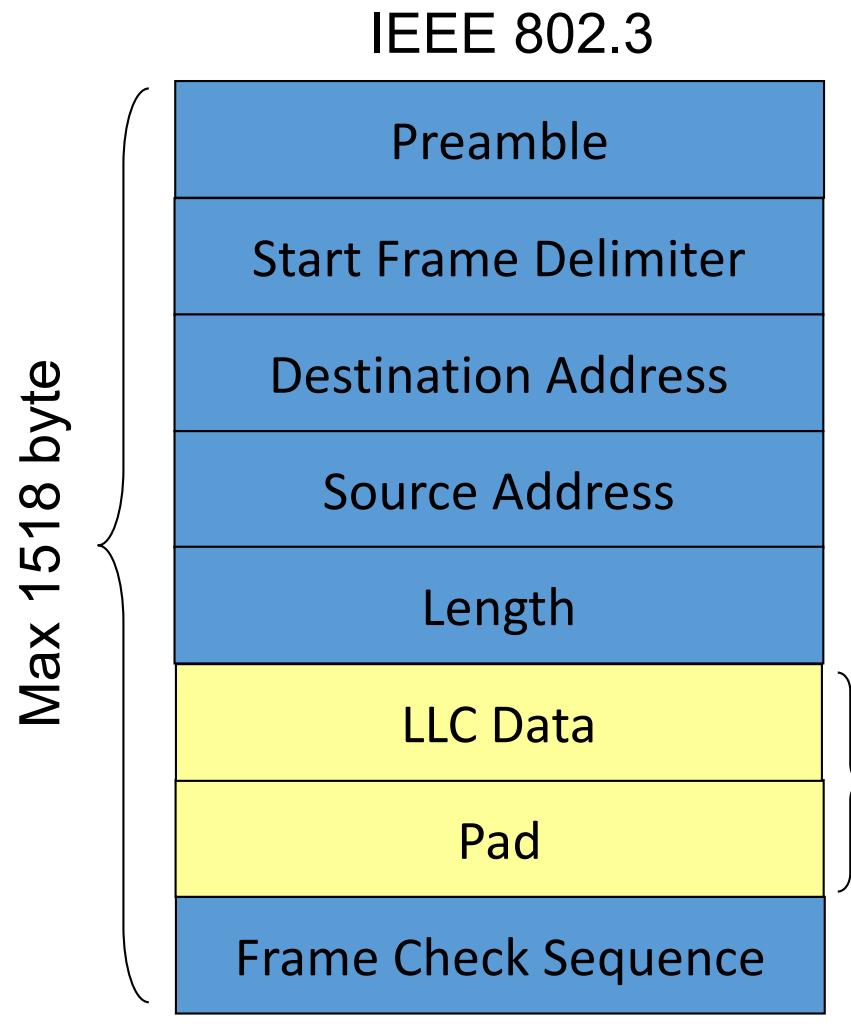


# Slot time

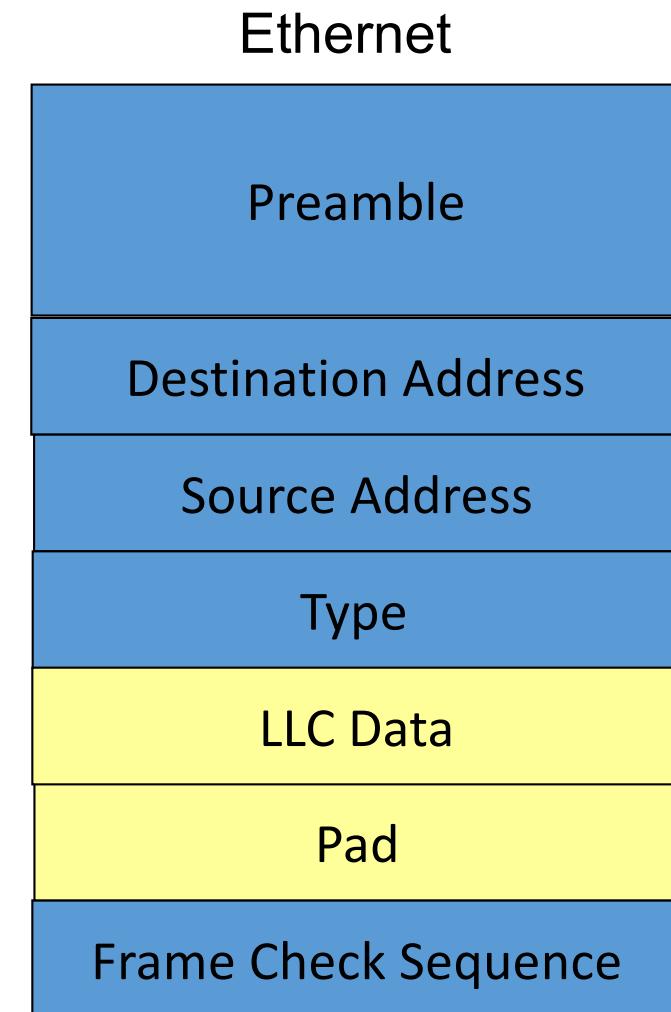
- Slot time = tempo necessario per trasmettere
  - 512 bit in reti a 10 e 100 Mbit/s
  - 4096 bit in reti a 1 Gbit/s
- La trama deve avere una dimensione minima uguale allo slot time
- Lo slot time deve essere superiore alla somma:
  - Del tempo di andata e ritorno del segnale
  - Del tempo necessario per rilevare la collisione e lanciare la sequenza di jamming
- Sequenza di jamming = 33 bit
  - La sequenza di jamming deve essere abbastanza lunga da garantire il riconoscimento di una collisione nel circuito di CD
- Fissata la dimensione dello slot time
  - Ogni trama di dimensione minore viene scartata
  - Viene imposto il tempo di propagazione massimo e quindi la conseguentemente la dimensione massima della rete



# Formato del Frame



$b_0$   $b_7$   
Ordine di trasmissione





# Campi del frame

- **Preamble**

- 7 byte tutti uguali a 10101010; producono, a 10 Mbps, un'onda quadra a 10 Mhz per 5,6  $\mu$ s, che consente al ricevitore di sincronizzare il suo clock con quello del trasmettitore.

- **SFD**

- uguale a 10101011 ha la funzione di flag di inizio frame

- **Lunghezza / Tipo**

- Per IEEE 802.3 la lunghezza indica quanti byte ci sono nel campo dati (da 0 a 1500)
    - Il tipo di payload è dato da LLC
    - I primi 4 bit sono sempre 0
  - Per Ethernet indica il Tipo di payload contenuto nel campo dati
    - Uno dei primi 4 bit è ≠0

- **Dati**

- contiene il payload del livello superiore.



# Campi del frame

- **Pad** (da to pad = riempire)
  - Se il frame (esclusi preambolo e delimiter) è più corto di 64 byte, con questo campo lo si porta alla lunghezza di 64 byte
- **Frame Checking sequence**
  - Contiene i bit di ridondanza per il codice di controllo dell' errore, di tipo polinomiale di grado 32
- **Indirizzi**
  - Sono composti da 48 bit (6 byte)
  - Sono cablati nella scheda di rete
  - Sono univoci a livello mondiale; i primi 3 byte individuano il costruttore e gli altri 3 numerano progressivamente le schede
  - E' possibile specificare
    - un singolo destinatario (unicast)  
**00-60-b0-78-e8-fd**
    - un indirizzo di gruppo (multicast): il primo bit deve essere a 1
    - un invio a tutte le stazioni (broadcast)  
**ff-ff-ff-ff-ff-ff**



# Cattura di pacchetti Ethernet

ConnessioneDEISNET\_DNS.cap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **tcp** Expression... Clear Apply Save

Source	Destination	Src Port	Dst Port	Protocol	Length	Info
192.168.10.199	137.204.57.85	1058	80	TCP	62	nim->http [SYN] Seq=1075430079 Win=65535 Len=0 MSS=1460 SACK_PER
137.204.57.85	192.168.10.199	80	1058	TCP	62	http->nim [SYN, ACK] Seq=1126214783 Ack=1075430080 Win=5840 Len=
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim->http [ACK] Seq=1075430080 Ack=1126214784 Win=65535 Len=0
192.168.10.199	137.204.57.85	1058	80	HTTP	790	GET / HTTP/1.1
137.204.57.85	192.168.10.199	80	1058	TCP	60	http->nim [ACK] Seq=1126214784 Ack=1075430816 Win=6624 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim->http [ACK] Seq=1075430816 Ack=1126217704 Win=65535 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim->http [ACK] Seq=1075430816 Ack=1126220624 Win=65535 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	HTTP	186	HTTP/1.1 200 OK (text/html)

Frame 6: 790 bytes on wire (6320 bits), 790 bytes captured (6320 bits)

Ethernet II, Src: DellComp\_89:b3:e9 (00:06:5b:89:b3:e9), Dst: D-Link\_c6:fa:6f (00:50:ba:c6:fa:6f)

Destination: D-Link\_c6:fa:6f (00:50:ba:c6:fa:6f)  
Source: DellComp\_89:b3:e9 (00:06:5b:89:b3:e9)  
Type: IP (0x0800)

Internet Protocol Version 4, Src: 192.168.10.199 (192.168.10.199), Dst: 137.204.57.85 (137.204.57.85)

Transmission Control Protocol, Src Port: nim (1058), Dst Port: http (80), Seq: 1075430080, Ack: 1126214784, Len: 736

Hypertext Transfer Protocol

0000	00 50 ba c6 fa 6f 00 06 5b 89 b3 e9 08 00 45 00 .P...o.. [.....E.
0010	05 08 01 87 40 00 80 06 00 00 c0 a8 0a c7 89 cc ....@... .....
0020	39 55 04 22 00 50 40 19 c2 c0 43 20 ac 80 50 18 9U.".P@..C..P.
0030	ff ff 91 8b 00 00 47 45 54 20 2f 20 48 54 54 50 .....GE T / HTTP
0040	2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69 6d /1.1..Ac cept: im
0050	61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78 age/gif, image/x
0060	2d 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f -xbitmap, image/
0070	6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65 jpeg, im age/pjpe
0080	67 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 g, appli cation/v
0090	6e 64 2e 6d 73 2d 70 6f 77 65 72 70 6f 69 6e 74 nd.ms-po werpoint
00a0	2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e , applic ation/vn



ConnessioneDEISNET\_DNS.cap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp Expression... Clear Apply Save

Source	Destination	Src Port	Dst Port	Protocol	Length	Info
192.168.10.199	137.204.57.85	1058	80	TCP	62	nim->http [SYN] Seq=1075430079 Win=65535 Len=0 MSS=1460 SACK_P
137.204.57.85	192.168.10.199	80	1058	TCP	62	http->nim [SYN, ACK] Seq=1126214783 Ack=1075430080 Win=5840 Len=0
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim->http [ACK] Seq=1075430080 Ack=1126214784 Win=65535 Len=0
192.168.10.199	137.204.57.85	1058	80	HTTP	790	GET / HTTP/1.1
137.204.57.85	192.168.10.199	80	1058	TCP	60	http->nim [ACK] Seq=1126214784 Ack=1075430816 Win=6624 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim->http [ACK] Seq=1075430816 Ack=1126217704 Win=65535 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim->http [ACK] Seq=1075430816 Ack=1126220624 Win=65535 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	HTTP	186	HTTP/1.1 200 OK (text/html)

Frame 6: 790 bytes on wire (6320 bits), 790 bytes captured (6320 bits)

Ethernet II, Src: DellComp\_00:b3:c0 (00:0c:5b:00:b3:c0), Dst: D-Link\_c6:fa:6f (00:50:ba:c6:fa:6f)

Destination: D-Link\_c6:fa:6f (00:50:ba:c6:fa:6f)

Address: D-Link\_c6:fa:6f (00:50:ba:c6:fa:6f)

.... .0. .... .... .... = LG bit: Globally unique address (factory default)

.... .0. .... .... .... = IG bit: Individual address (unicast)

Source: DellComp\_00:b3:c0 (00:0c:5b:00:b3:c0)

Type: IP (0x0800)

Internet Protocol Version 4, Src: 192.168.10.199 (192.168.10.199), Dst: 137.204.57.85 (137.204.57.85)

Transmission Control Protocol, Src Port: nim (1058), Dst Port: http (80), Seq: 1075430080, Ack: 1126214784, Len: 736

Hypertext Transfer Protocol

0000	00	50	ba	c6	fa	6f	00	06	5b	89	b3	e9	08	00	45	00	.P...o..	[.....E.
0010	03	08	01	87	40	00	80	06	00	00	c0	a8	0a	c7	89	cc	....@...	.....
0020	39	55	04	22	00	50	40	19	c2	c0	43	20	ac	80	50	18	9U.".P@..C..P.	
0030	ff	ff	91	8b	00	00	47	45	54	20	2f	20	48	54	54	50	.....GE	T / HTTP
0040	2f	31	2e	31	0d	0a	41	63	63	65	70	74	3a	20	69	6d	/1.1..Ac	cept: im
0050	61	67	65	2f	67	69	66	2c	20	69	6d	61	67	65	2f	78	age/gif,	image/x
0060	2d	78	62	69	74	6d	61	70	c2	20	69	6d	61	67	65	2f	-xbitmap,	image/
0070	6a	70	65	67	2c	20	69	6d	61	67	65	2f	70	6a	70	65	jpeg,	im age/pjpe
0080	67	2c	20	61	70	70	6c	69	63	61	74	69	6f	6e	2f	76	g,	application/v
0090	6e	64	2e	6d	73	2d	70	6f	77	65	72	70	6f	69	6e	74	nd.ms-po	werpoint
00a0	2c	20	61	70	70	6c	69	63	61	74	69	6f	6e	2f	76	6e	, applic	ation/vn
00b0	64	2e	6d	73	2d	65	78	63	65	6c	2c	20	61	70	70	6c	d.ms-exc	el, appl



ConnessioneDEISNET\_DNS.cap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **tcp** Expression... Clear Apply Save

Source	Destination	Src Port	Dst Port	Protocol	Length	Info
192.168.10.199	137.204.57.85	1058	80	TCP	62	nim- <b>http</b> [SYN] Seq=1075430079 Win=65535 Len=0 MSS=1460 SACK_PEE
137.204.57.85	192.168.10.199	80	1058	TCP	62	http-nim [SYN, ACK] Seq=1126214783 Ack=1075430080 Win=5840 Len=0
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim- <b>http</b> [ACK] Seq=1075430080 Ack=1126214784 Win=65535 Len=0
192.168.10.199	137.204.57.85	1058	80	HTTP	790	GET / HTTP/1.1
137.204.57.85	192.168.10.199	80	1058	TCP	60	http-nim [ACK] Seq=1126214784 Ack=1075430816 Win=6624 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim- <b>http</b> [ACK] Seq=1075430816 Ack=1126217704 Win=65535 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim- <b>http</b> [ACK] Seq=1075430816 Ack=1126220624 Win=65535 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	HTTP	106	HTTP/1.1 200 OK (text/html)

Frame 6: 790 bytes on wire (6320 bits), 790 bytes captured (6320 bits)

Ethernet II, Src: DellComp\_89:b3:e9 (00:06:5b:89:b3:e9), Dst: D-Link\_c6:fa:6f (00:50:ba:c6:fa:6f)

Destination: D-Link\_c6:fa:6f (00:50:ba:c6:fa:6f)

Source: DellComp\_89:b3:e9 (00:06:5b:89:b3:e9)

Address: DellComp\_89:b3:e9 (00:06:5b:89:b3:e9)

.... .0. .... .... .... = LG bit: Globally unique address (factory default)

.... .0. .... .... .... = IG bit: Individual address (unicast)

Type: IP (0x0000)

Internet Protocol Version 4, Src: 192.168.10.199 (192.168.10.199), Dst: 137.204.57.85 (137.204.57.85)

Transmission Control Protocol, Src Port: nim (1058), Dst Port: http (80), Seq: 1075430080, Ack: 1126214784, Len: 736

Hypertext Transfer Protocol

Hex	Dec	Text
0000	00 50 ba c6 fa 6f	.P...o... [.....E.
0010	03 08 01 87 40 00 80 06	....@....
0020	00 00 c0 a8 0a c7 89 cc	9U.".P@..C..P.
0030	39 55 04 22 00 50 40 19	.....GE T / HTTP
0040	c2 c0 43 20 ac 80 50 18	/1.1.Ac cept: im
0050	ff ff 91 8b 00 00 47 45	age/gif, image/x
0060	54 20 2f 20 48 54 54 50	-xbitmap, image/
0070	2d 78 62 69 74 6d 61 70	jpeg, im age/pjpe
0080	2c 20 69 6d 61 67 65 2f	g, applic ation/v
0090	70 65 67 2c 20 69 6d	nd.ms-po werpoint
00a0	61 74 69 6f 6e 2f 76	, applic ation/vn
00b0	65 6c 2c 20 61 70 70 6c	d.ms-exc el, appl



ConessioneDEISNET\_DNS.cap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **tcp** Expression... Clear Apply Save

Source	Destination	Src Port	Dst Port	Protocol	Length	Info
192.168.10.199	137.204.57.85	1058	80	TCP	62	nim-ntp [SYN] Seq=1075430079 Win=65535 Len=0 MSS=1460 SACK_P
137.204.57.85	192.168.10.199	80	1058	TCP	62	http-nim [SYN, ACK] Seq=1126214783 Ack=1075430080 Win=5840 Len=0
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim-ntp [ACK] Seq=1075430080 Ack=1126214784 Win=65535 Len=0
192.168.10.199	137.204.57.85	1058	80	HTTP	790	GET / HTTP/1.1
137.204.57.85	192.168.10.199	80	1058	TCP	60	http-nim [ACK] Seq=1126214784 Ack=1075430816 Win=6624 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim-ntp [ACK] Seq=1075430816 Ack=1126217704 Win=65535 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
192.168.10.199	137.204.57.85	1058	80	TCP	54	nim-ntp [ACK] Seq=1075430816 Ack=1126220624 Win=65535 Len=0
137.204.57.85	192.168.10.199	80	1058	TCP	1514	[TCP segment of a reassembled PDU]
137.204.57.85	192.168.10.199	80	1058	HTTP	186	HTTP/1.1 200 OK (text/html)

Frame 6: 790 bytes on wire (6320 bits), 790 bytes captured (6320 bits)  
Ethernet II, Src: DellComp\_89:b3:e9 (00:06:5b:89:b3:e9), Dst: D-Link\_c6:fa:6f (00:50:ba:c6:fa:6f)  
Destination: D-Link\_c6:fa:6f (00:50:ba:c6:fa:6f)  
Source: DellComp\_89:b3:e9 (00:06:5b:89:b3:e9)  
Type: IP (0x0800)  
Internet Protocol Version 4, Src: 192.168.10.199 (192.168.10.199), Dst: 137.204.57.85 (137.204.57.85)  
Transmission Control Protocol, Src Port: nim (1058), Dst Port: http (80), Seq: 1075430080, Ack: 1126214784, Len: 736  
Hypertext Transfer Protocol

Hex	Dec	Text
0000	00 50 ba c6 fa 6f 00 06 5b 89 b3 e9 08 00 45 00	.P...o.. [....E.
0010	03 08 01 87 40 00 80 06 00 00 c0 a8 0a c7 89 cc	....@... .....
0020	39 55 04 22 00 50 40 19 c2 c0 43 20 ac 80 50 18	9U.".P@. ..C ..P.
0030	ff ff 91 8b 00 00 47 45 54 20 2f 20 48 54 54 50	.....GE T / HTTP
0040	2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69 6d	/1.1..Ac cept: im
0050	61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78	age/gif, image/x
0060	2d 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f	-xbitmap , image/
0070	6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65	jpeg, image/pjpe
0080	67 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76	g, applic ation/v
0090	6e 64 2e 6d 73 2d 70 6f 77 65 72 70 6f 69 6e 74	nd.ms-po werpoint
00a0	2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e	, applic ation/vn
00b0	64 2e 6d 73 2d 65 78 63 65 6c 2c 20 61 70 70 6c	d.ms-exc el, appl



# Delimitazione delle trame

- Assenza di trame = assenza di segnale sul canale
- Preambolo di sincronismo e SFD delimitano l' inizio
- L' assenza di segnale indica il termine di un frame
- Due frame devono essere separati almeno da un Inter-Frame Gap (IFG)
  - 96 tempi di bit
    - 10 Mbps Ethernet 9,6  $\mu$ sec
    - 100 Mbps Ethernet 960 nsec
    - 1000 Mbps Ethernet 96 nsec



# Collision Domain

- Collision domain = l'insieme delle stazioni connesse alla medesima rete Ethernet che possono collidere in trasmissione
- Per garantire il corretto funzionamento del CSMA-CD si devono imporre vincoli alla dimensione massima della LAN
  - In funzione della dimensione delle trame
  - In funzione della velocità di trasmissione
- Inoltre il mezzo trasmittivo impone dei vincoli sulle dimensioni dei collegamenti (attenuazione, rumore)
- La dimensione fisica del collision domain è conseguenza delle tecnologie adottate per lo strato fisico

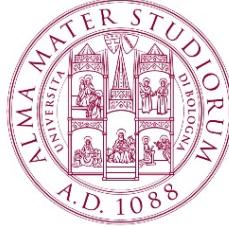


# Broadcast domain

- Una trama MAC con

Destination address = ff. ff: ff: ff: ff: ff: ff

- Viene ricevuta da tutte le interfacce della LAN
- Realizza una comunicazione broadcast dalla sorgente a tutte le destinazioni della LAN
- Dominio di broadcast = insieme di stazioni raggiungibili con l'invio dalla medesima trama inviata con indirizzo broadcast
  - In condizioni normali una singola LAN è anche un singolo dominio di broadcast



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# Soluzioni per lo strato fisico dell' Ethernet



# Ethernet classica a 10 Mbit/s

- **Proposta iniziale: 10base5**
  - 10: velocità 10 Mbit/s con codifica Manchester (clock a 20 MHz)
  - base: trasmissione in banda base (contrapposto a broad)
  - 5: segmenti fino a 500 metri (con max 100 stazioni)
  - Cavo coassiale a  $50 \Omega$ , diametro della cavità 6.15 mm (thick wire)
    - Attacco al cavo con prese a vampiro a cui si collegano apparati attivi detti Transceiver
    - Stazioni collegate mediante cavi transceiver (drop cable) lunghi fino a 40 m
- Cavo thin wire troppo rigido, non si presta al cablaggio di un edificio
  - Occorre distribuire capillarmente prese a muro per raggiungere tutte le stazioni



# Ethernet classica a 10 Mbit/s

- **10base2** (thin wire Ethernet)
  - Cavo coassiale sottile a  $50 \Omega$  ma con diametro della cavità di 2.95 mm, molto flessibile
  - Segmenti fino a 180 metri con max 30 stazioni
  - Il transceiver è integrato nella scheda a bordo del computer
    - collegamento con connettori BNC e computer in serie sul segmento con connettori a T (daisy chain)
  - Di solito si installa un backbone 10base5 (cablaggio verticale) che interconnette segmenti 10base2 per raggiungere le prese a muro (cablaggio orizzontale)
    - occorrono repeaters



# Coppie intrecciate o Twisted Pair

- Agli inizi degli anni '90 si approfondiscono gli studi sulle coppie bifilari in due varianti
  - **Shielded twisted pair STP**
    - Nel cavo ogni coppia è avvolta in un conduttore che fa da schermo
    - Maggiore costo del cavo
    - Lo schermo deve essere messo a massa
  - **Unshielded twisted pair UTP**
    - Meno costose e più semplici da posare
- Vengono studiati modi per migliorare le prestazioni
  - Aumentare il diametro dei conduttori e migliorare la qualità del dielettrico
  - Migliorare la regolarità e infittire il passo di avvolgimento
- Vengono definiti livelli di qualità detti Categorie
  - Standardizzate da Cat. 1 a Cat 7

# Twisted Pair

GIÁ FATTO



(a)

da Tanenbaum



(b)

- (a) Category 3 UTP.
- (b) Category 5 UTP.

Categoria	Velocità (Mbit/s)
1	2
2	4
3	10
4	16
5	100



# Ethernet classica a 10 Mbit/s (segue)

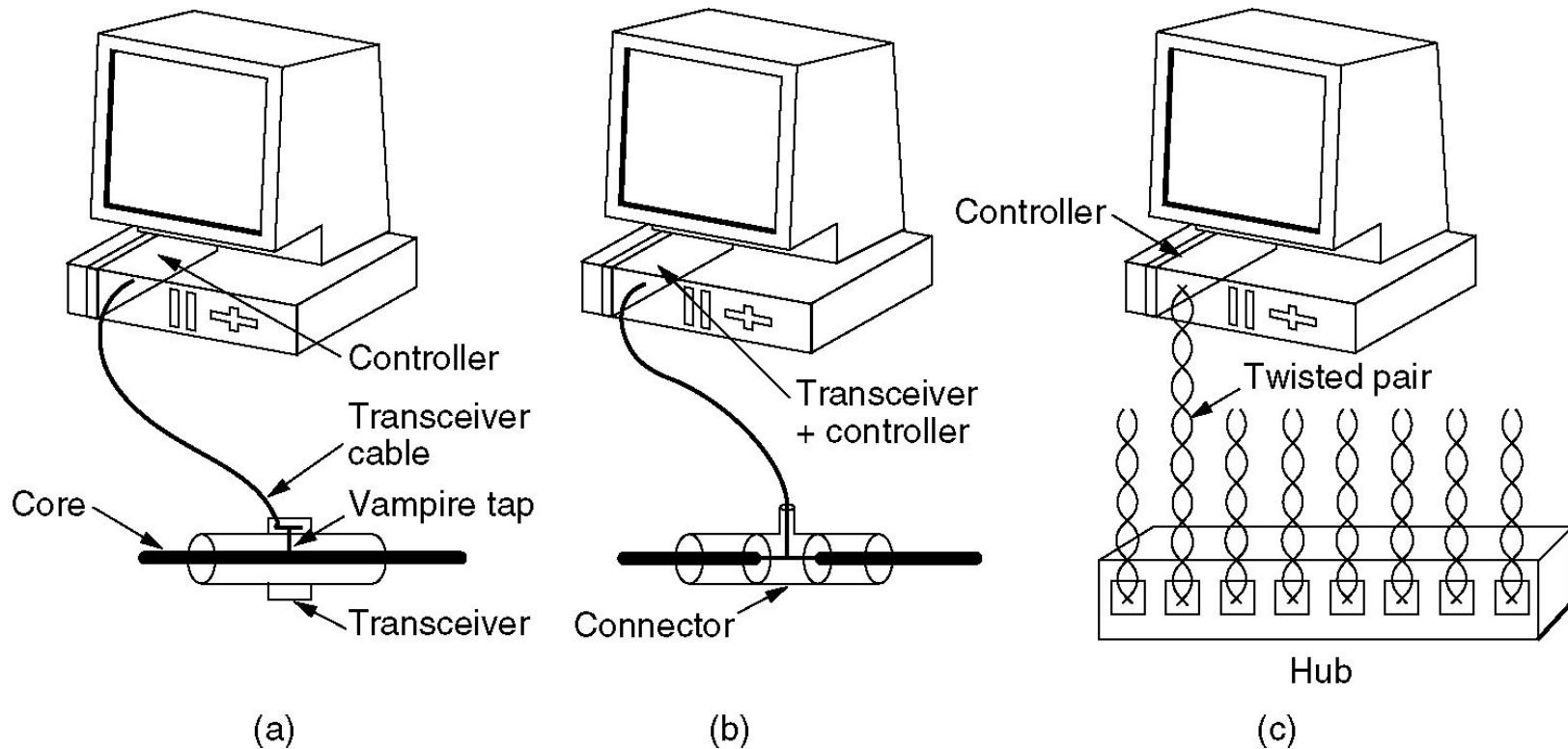
- **10baseT**
  - Usa coppie simmetriche intrecciate senza schermatura UTP (Unshielded Twisted Pairs)
  - occorrono UTP di categoria 3 per arrivare a 100 m
  - Ogni stazione ha una UTP tutta a sua disposizione collegata alla porta di un Hub con connettore RJ45
    - RJ45 simile a RJ11 con 4 contatti
  - Gli Hub fungono da multiport repeater per il cablaggio orizz.
  - Il cablaggio verticale può essere fatto con altri multiport repeater (topologia a stella)
- **10baseF**
  - Alternativa con cavo in fibra ottica multimodo
  - Fino a 2000 m di distanza
  - Ancora costosa a causa dei connettori e degli attacchi per le stazioni
  - La 10baseF spesso viene usata per il cablaggio verticale



# Ethernet Cabling

Three kinds of Ethernet cabling.

(a) 10Base5, (b) 10Base2, (c) 10Base-T.



da Tanenbaum



# Evoluzione dell' Ethernet

- 1992: IEEE riconvocò il comitato 802.3 con l'esigenza di definire LANs più veloci
  - prima proposta: di **mantenere 802.3 tale e quale**, rendendola solo più veloce,
  - Altra proposta: ridefinirla totalmente con nuove caratteristiche (traffico real-time, voce digitale,... )
- Il comitato 802.3 alla fine decise per la prima
- I fautori della seconda formarono un loro comitato **802.12** e la standardizzarono comunque
  - questo standard non ha però avuto successo

# IEEE 802.3 u – Fast Ethernet a 100 Mbit/s



- Diametro massimo di un collision domain: 250 m
- **100baseT4**
  - Ogni stazione è collegata con 4 UTP di cat. 3
  - Lunghezza fino a 100 m
  - Clock a 25 MHz
  - Codifica 8B/6T: 8 bit (256 comb.) da trasmettere vengono codificati in 6 simboli Ternari (729 comb.)
    - Restano diverse combinazioni *non dati*
    - Su ognuna delle UTP la velocità è 33.333.. Mbit/s
  - Un UTP sempre in direzione Hub-stazione, un UTP sempre stazione-Hub, gli altri 2 vanno a rinforzare una direzione alternativamente portandola a 100 Mbit/s



# IEEE 802.3 u – Fast Ethernet (segue)

- **100baseTX**

- 2 coppie UTP di cat. 5, fino a 100m
- Clock a 125 MHz
- Codifica 4B/5B (come in FDDI): 4 bit vengono mappati in 5 bit
  - Velocità netta 100 Mbit/s full duplex
  - Restano combinazioni libere per non dati

- **100base FX**

- Cavo in fibra ottica multimodo
- Fino a 2000 m



# IEEE 802.3 z - Gigabit Ethernet

- Standard per definire una rete Ethernet a 1 Gbit/s; i collision domain dovrebbero diventare di 25 m; per portarli a 200 m si usa:
  - Carrier extension
  - Frame bursting
- **1000baseSX e 1000baseLX**
  - Due alternative in fibra ottica, la prima multimodo, la seconda mono o multi modo
  - Codifica 8B/10B
  - Generatori a Laser
  - Distanze 550 m o 5000 m (solo con LX monomodo)

# IEEE 802.3 z - Gigabit Ethernet (segue)



- **1000baseCX**
  - Usa 2 coppie intrecciate e schermate STP (nel cavetto ogni coppia è schermata e tutto l'insieme delle coppie è di nuovo schermato)
  - Soluzione costosa e meno performante delle OF
- **1000baseT**
  - 4 coppie UTP di cat. 5
  - Clock a 125 MHz
  - Codifica: 2 bit sino codificati su 1 simbolo a 5 livelli
    - È disponibile 1 livello come non dato
    - Velocità netta 1Gbit/s half duplex



# Multigigabit Ethernet

- Ora si parla di 10Gigabit Ethernet (allo studio dal 2002 come IEEE 802.3 ae)
  - Applicabile solo su fibra ottica e non su rame
  - Diversi tipi di fibre e modalità di trasmissione
    - Distanze fino a diversi Km
- La maggioranza dei computer sul mercato non può sfruttare la velocità superiori al Gigabit
  - Vengono usate per il backbone
  - Backbone anche su estensioni di diversi Km: sono una moderna alternativa per le MAN
- Lo standard IEEE802.17 (RPR) è una possibile proposta alternativa per i backbone MAN



# Carrier Ethernet

- Requisiti tecnologici
  - Diversi per trasporto e accesso
- Ethernet nasce per le LAN ossia per l' accesso
- La penetrazione nello strato di trasporto richiede l' introduzione di nuove funzionalità
  - Segnalazione e gestione
  - Indirizzamento
- Sono in fase di definizione una serie di nuovi standard per introdurre queste funzioni
  - Indirizzamento gerarchico multilivello
  - Recupero dei guasti

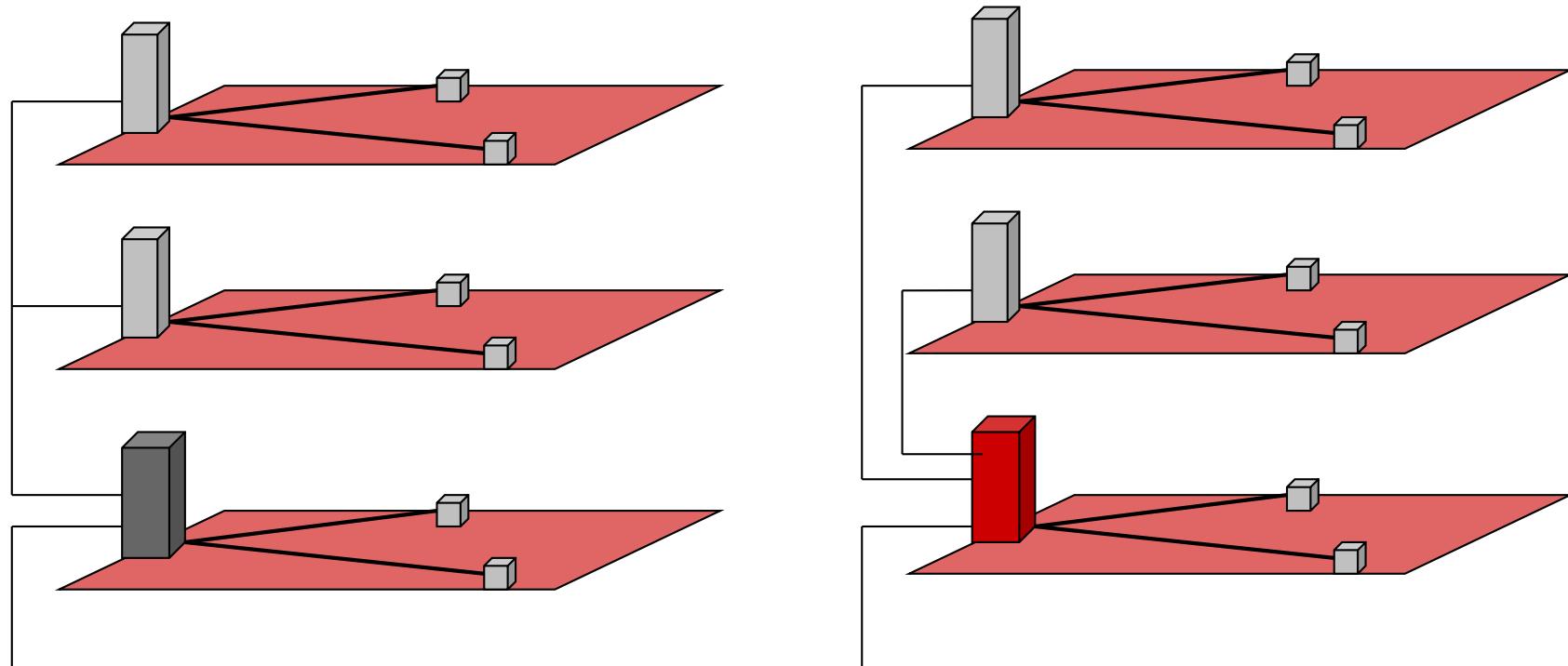


ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

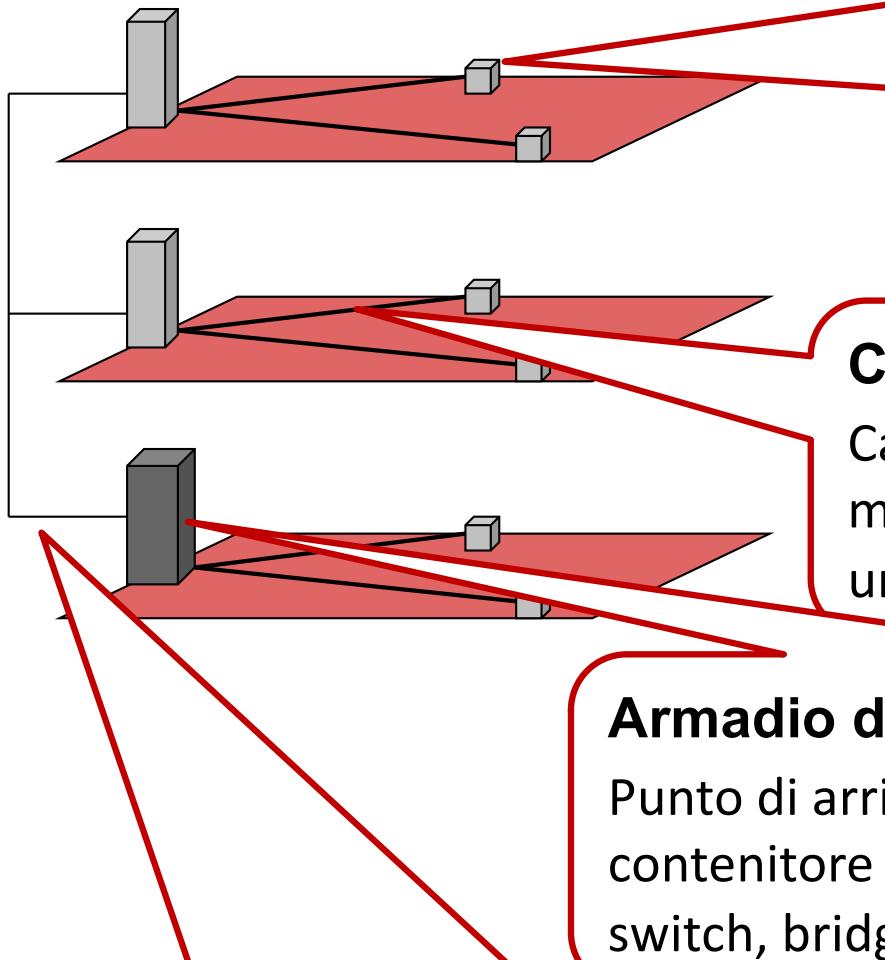
# Il cablaggio delle LAN moderne

# Cablaggio strutturato

- Un unico cablaggio per tutti i servizi di telecomunicazioni degli edifici
  - EIA/TIA 568 (standard di mercato)
  - ISO 11801
  - La soluzione più utilizzata è basata su UTP
    - In un nuovo edificio vengono posati cavetti con diverse coppie (tipicamente 4) che poi finiscono in prese a muro RJ11 o RJ45 per tutti i servizi di telecom.
- Il cablaggio è organizzato in modo gerarchico



# Componenti del cablaggio strutturato



## Prese a muro

Punti di accesso alla LAN per l'utente finale. Localizzate in prossimità delle postazioni di lavoro

## Cablaggio orizzontale o di piano

Cavidotti e cavi che collegano le prese a muro con l'armadio di rete realizzando una topologia a stella

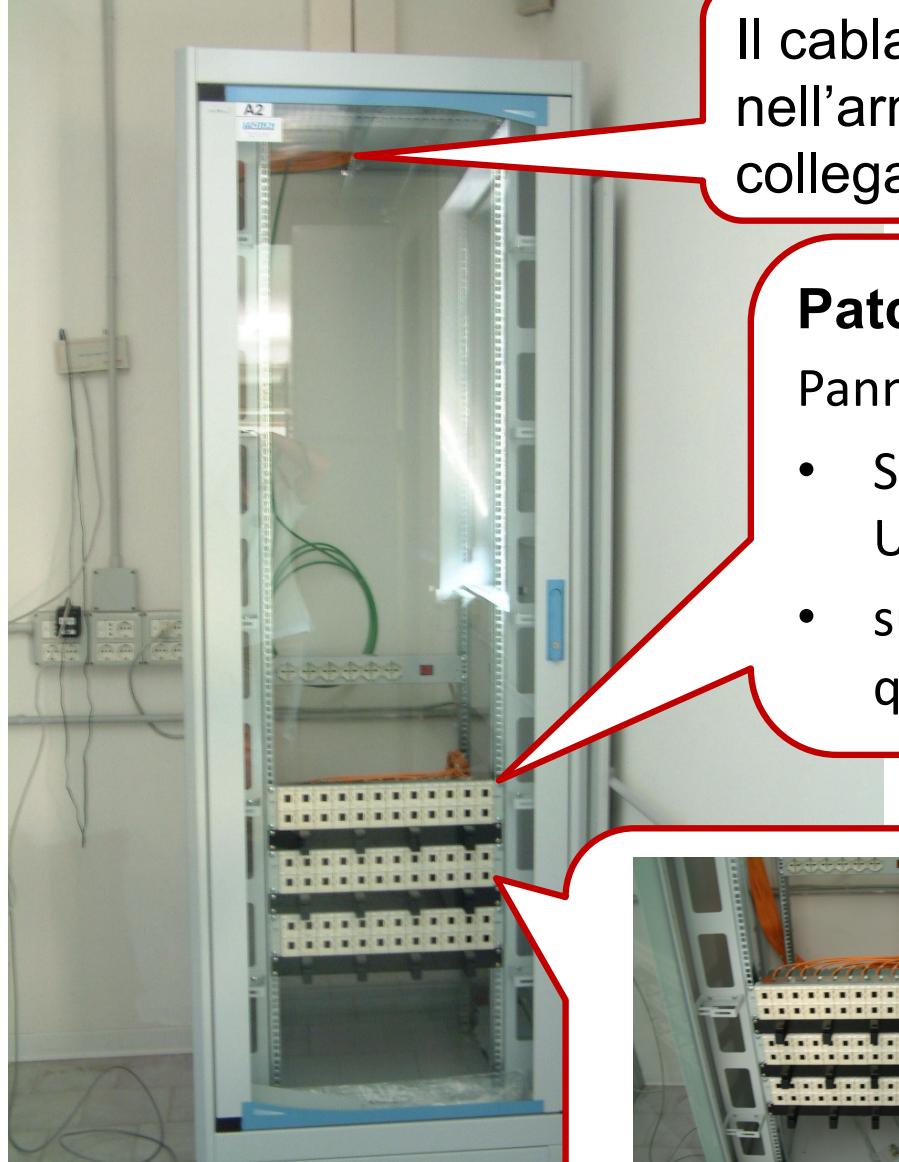
## Armadio di rete

Punto di arrivo del cablaggio orizzontale e contenitore degli apparati attivi della LAN (hub, switch, bridge, router)

## Cablaggio verticale

Interconnette più armadi di rete per realizzare una LAN estesa

# Armadio di rete



Il cablaggio orizzontale entra nell'armadio di rete e i vari cavi sono collegati al retro dei **patch panel**

## Patch panel

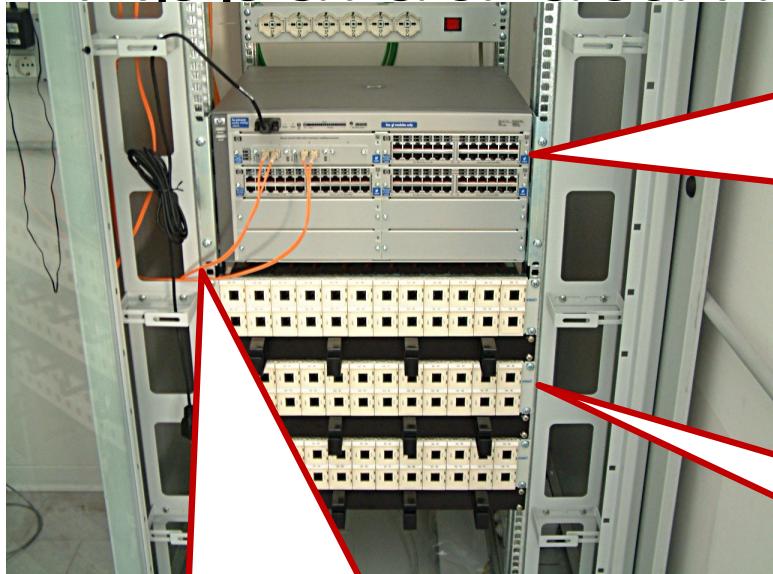
Pannello che presenta

- Sul retro un insieme di connettori per cavi UTP
- sul fronte un insieme di prese standard (in questo caso RJ45 per cavi UTP)



Riporta all'interno dell'armadio di rete i punti di connessione al cablaggio rappresentati dalle prese a muro

# Apparati attivi nell'armadio



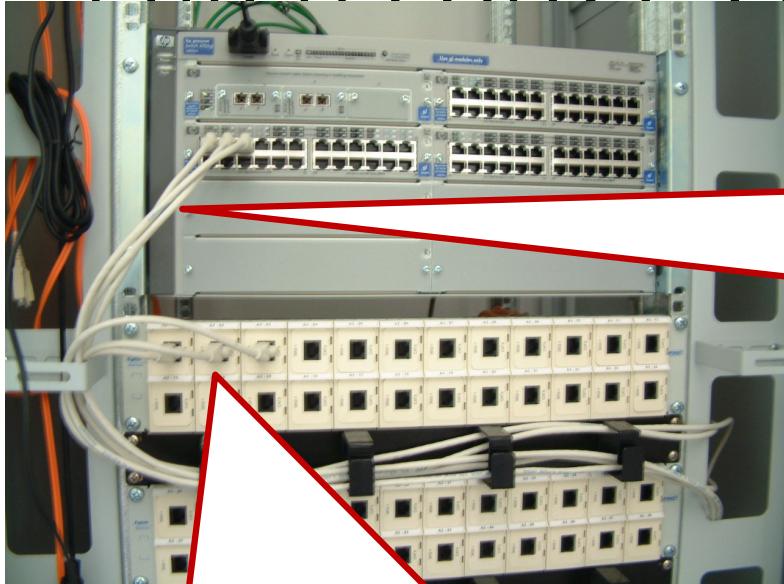
L'armadio di rete ospita gli apparati attivi, in questo caso uno switch equipaggiato con:

- Tre moduli da 24 porte fast Ethernet UTP
- Un modulo con 2 porte Ethernet in fibra

Switch e path panel sono affiancati ma in queste condizioni non esiste alcuna connettività di LAN

Le porte in fibra qui già connesse tipicamente servono per realizzare il cablaggio verticale

# Patch cord e connettività

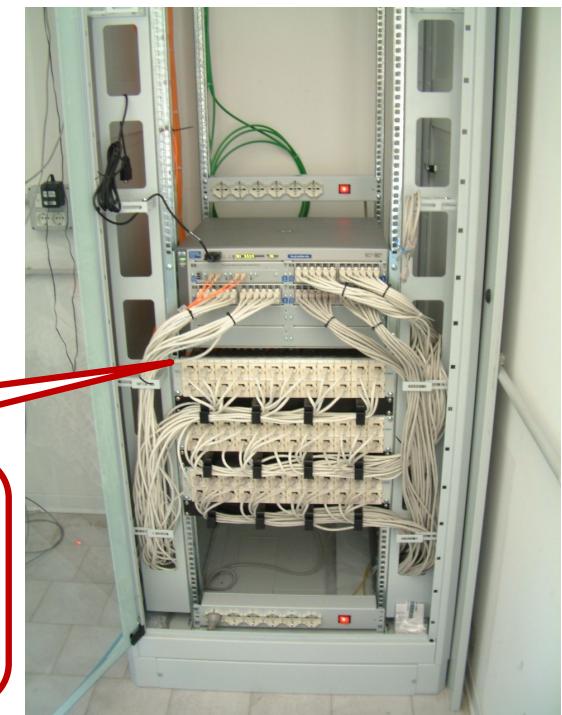


La connettività della LAN viene realizzata collegando le porte dei patch panel con le porte dello switch tramite spezzoni di cavo detti **patch cord**.

## Patch cord

Determina se e a quale porta della switch sia connessa una presa a muro

Per garantire connettività a tutte le prese a muro il numero di porte dei patch panel deve essere equivalente al numero di porte dello switch





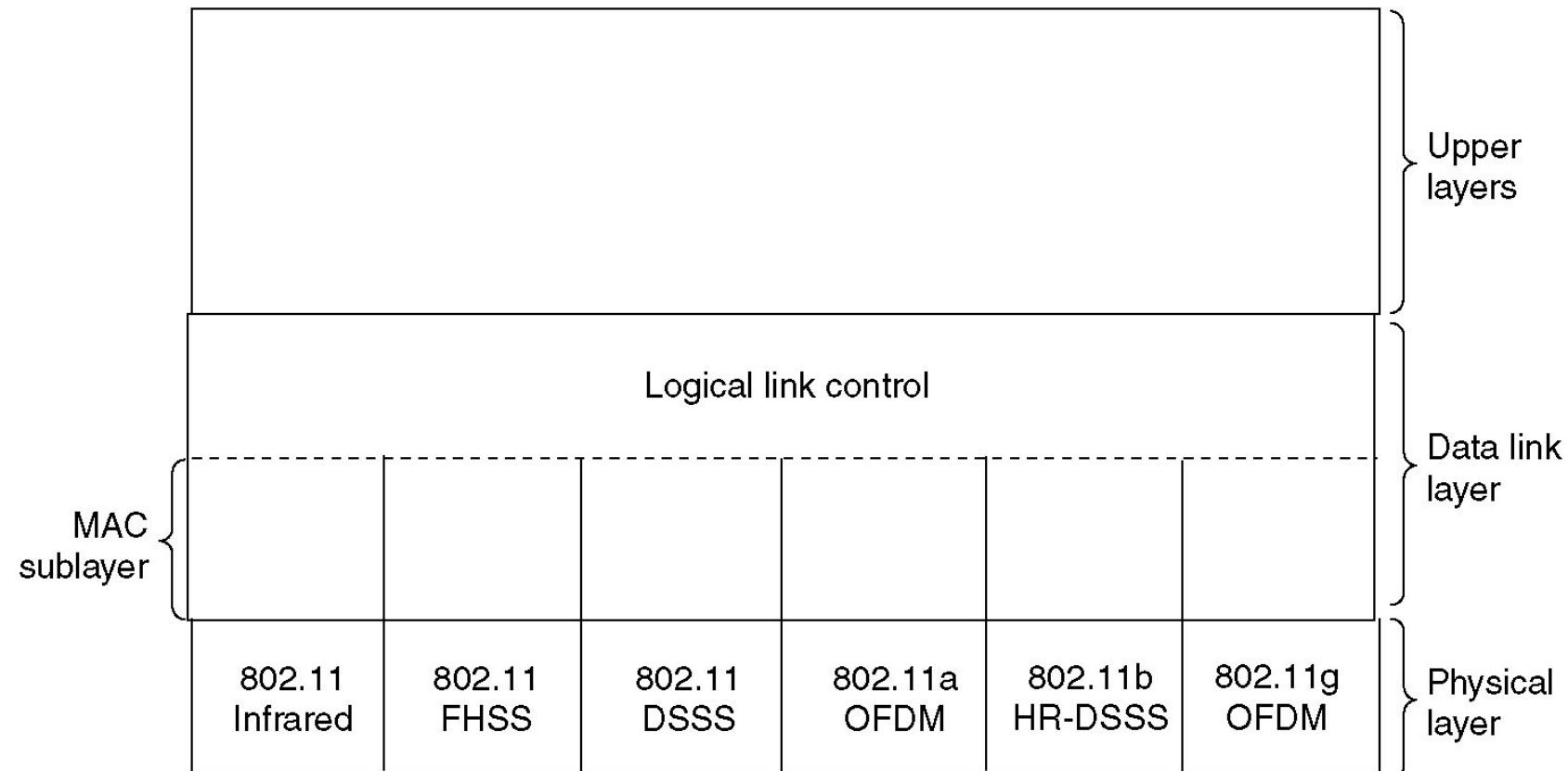
ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# WIRELESS LAN (Wi-Fi)



# Lo standard IEEE 802.11

- Il mezzo radio è stato ignorato nei primi standard 802
- A partire dal 1997 compare un nuovo standard per fornire l'accesso a reti locali via radio





# Lo strato fisico 802.11

- Si occupa della trasmissione fisica delle trame secondo le specifiche stabilite
- Interagisce con lo strato MAC per segnalare l' attività del canale (necessario per il protocollo di accesso)
- La prima versione (1997) prevedeva tre tecniche di trasmissione a **1Mb/s e 2Mb/s**
  - infrarossi (scarsamente usata)
  - FHSS
  - DSSS
- Utilizza la banda **ISM** (Industrial, Scientific, Medical) a **2.4 GHz** (83.5 Mhz da 2.40 a 2.4835 Ghz)
  - disponibile per applicazioni industriali, scientifiche e mediche senza necessità di chiedere licenze



# Uso della banda ISM

- Proprio perché l' utilizzo è libero, occorre una regolamentazione per evitare abusi e per ridurre le interferenze
  - limitazioni sulla potenza massima trasmessa
  - utilizzo di tecniche Spread Spectrum
  - specifiche di utilizzo
    - FHSS: 79 canali da 1 Mhz ciascuno  
tempo di permanenza su un canale  $\leq$  400 ms (dwell time)  
su 30 secondi occorre utilizzare almeno 75 canali diversi
    - DSSS: processing gain  $\geq$  10 dB
- In Italia, il D.M. 28 Maggio 2003 stabilisce
  - obbligo di richiesta di autorizzazione al Ministero per offrire servizi Wi-Fi nella banda ISM su suolo pubblico
  - obbligo di identificazione degli utenti di tali servizi
  - nessun obbligo su suolo privato



# Lo strato fisico 802.11a

- Emesso nel 1999, implementa il Wi-Fi a banda larga
- Utilizza la banda **ISM a 5 GHz**
  - $5.15 \div 5.25 + 5.25 \div 5.35 + 5.725 \div 5.825$
  - meno utilizzata di quella a 2.4 GHz
  - maggiore larghezza di banda disponibile (300 MHz)
  - solo limiti sulla potenza massima trasmessa
- Fa uso di OFDM
  - 52 sottoportanti (48 per i dati, 4 per la sincronizzazione)
  - 312.5 kHz di banda per sottoportante
- 12 canali da 20 MHz ciascuno
- Bit rate: **6, 9, 12, 18, 24, 36, 48, 54 Mb/s**
  - ottenute con codifiche diverse e modulazioni BPSK, QPSK, 16-QAM, 64-QAM
  - scelte in base alla distanza da coprire

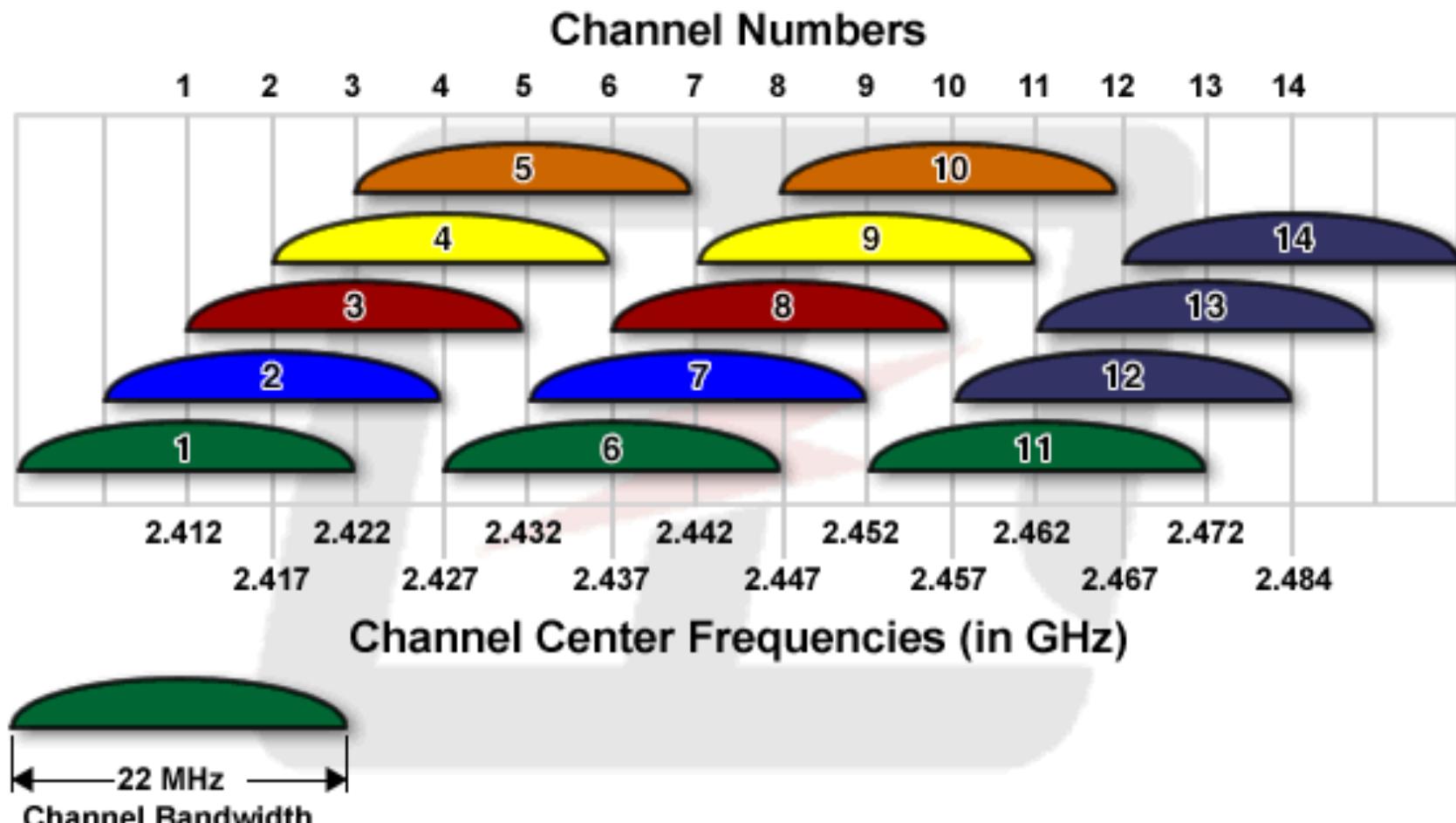


# Lo strato fisico 802.11b

- Emesso nel 1999, implementa il Wi-Fi a banda larga
- Utilizza la banda **ISM** a **2.4 GHz**
- Fa uso di **High-Rate DSSS (HR-DSSS)**
- 14 canali (13 in Europa) da 5 MHz ciascuno
  - il segnale spread spectrum occupa 22 MHz
- Bit rate: **1, 2, 5.5, 11 Mb/s**
  - 1 e 2 Mb/s ottenuti con sequenza PN di Barker a 11 chip e modulazioni DBPSK e DQPSK (compatibile con 802.11)
  - 5.5 e 11 Mb/s ottenuti con una complessa codifica spread spectrum a 11 Mchip/s (Complementary Code Keying – CCK) e modulazione DQPSK
- Riesce ad adattare la bit rate alle condizioni del canale
  - **Dynamic Rate Shifting**



# Canalizzazione 802.11b



IEEE 802.11 RF Channelization Scheme

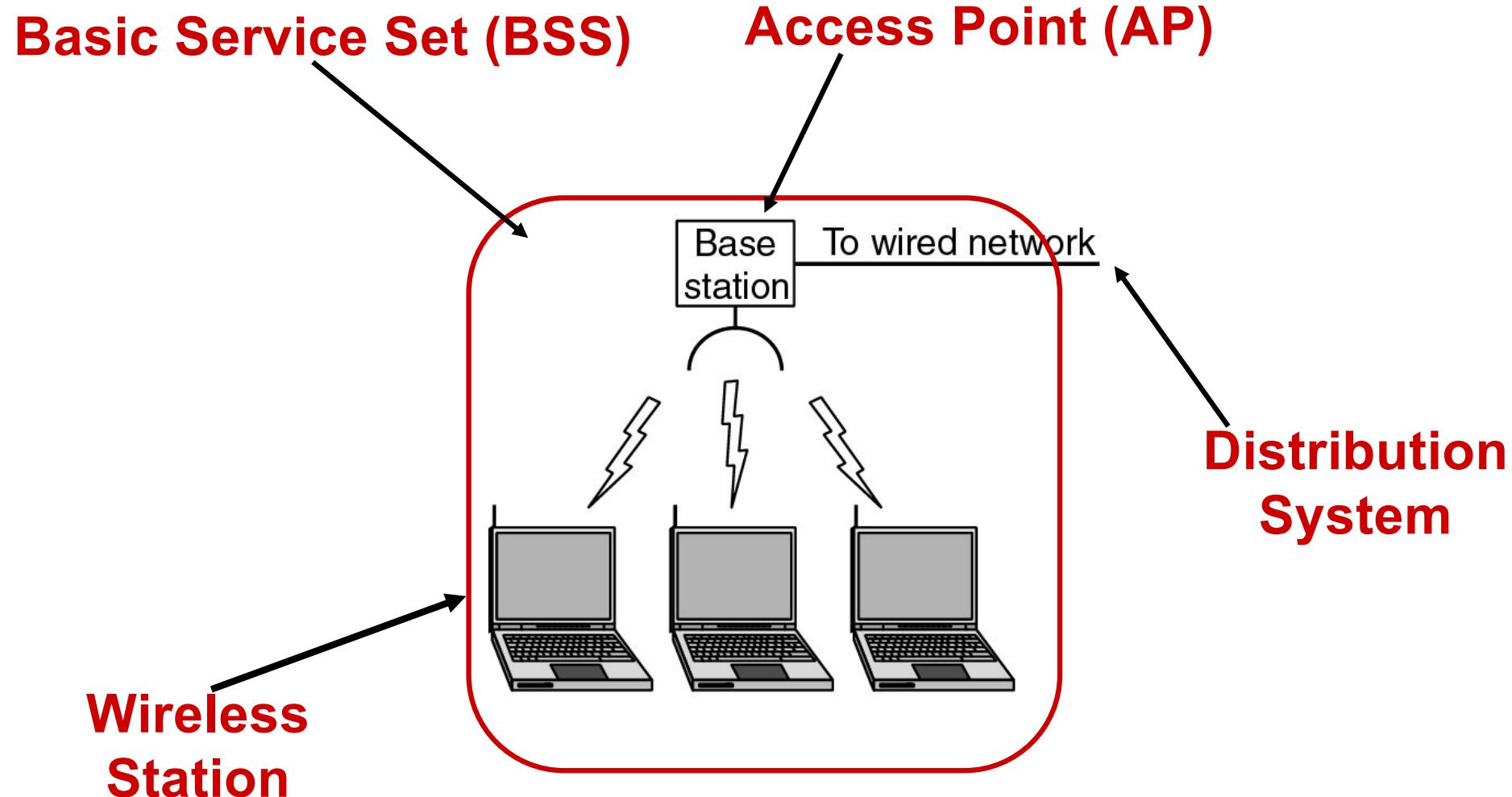


# Lo strato fisico 802.11g

- Emesso nel 2003
- Come 802.11b, utilizza la banda **ISM** a **2.4 GHz**
- Come 802.11a, fa uso di OFDM, ma può usare anche HR-DSSS
- Bit rate
  - HR-DSSS: **1, 2, 5.5, 11 Mb/s**
  - OFDM: **6, 9, 12, 18, 24, 36, 48, 54 Mb/s**



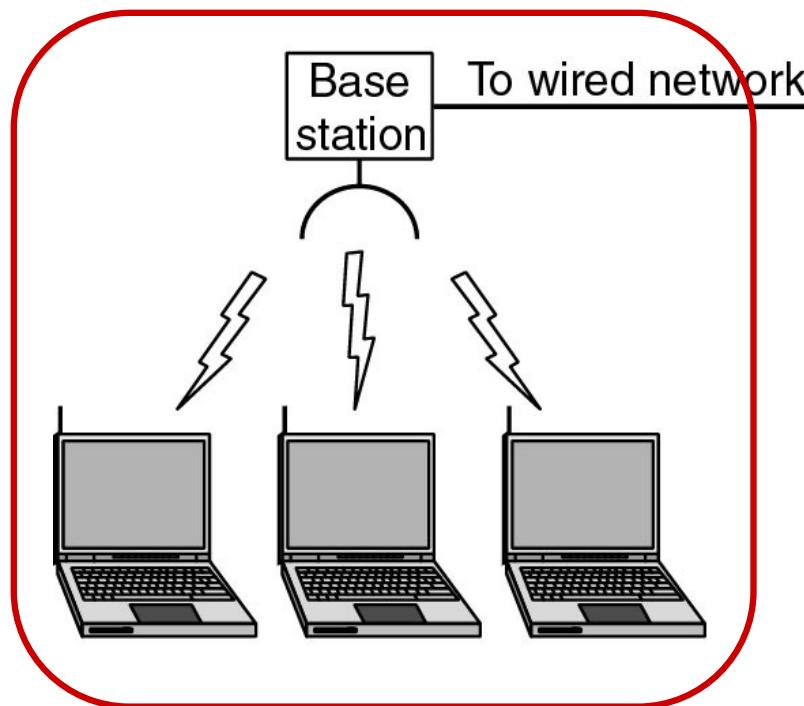
# Architettura di rete 802.11





# Architettura di rete 802.11

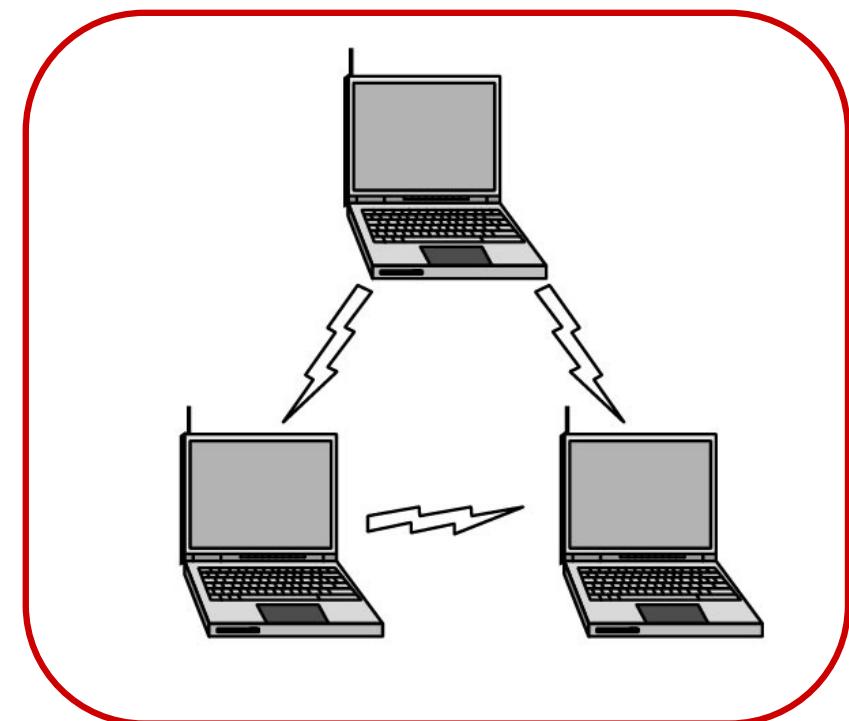
## Modalità Infrastrutturata (Infrastructure BSS)



Le stazioni comunicano attraverso l' AP (anche se non si vedono direttamente)

Da A.S. Tanenbaum, "Reti di Calcolatori"

## Modalità Ad-Hoc (Independent BSS)

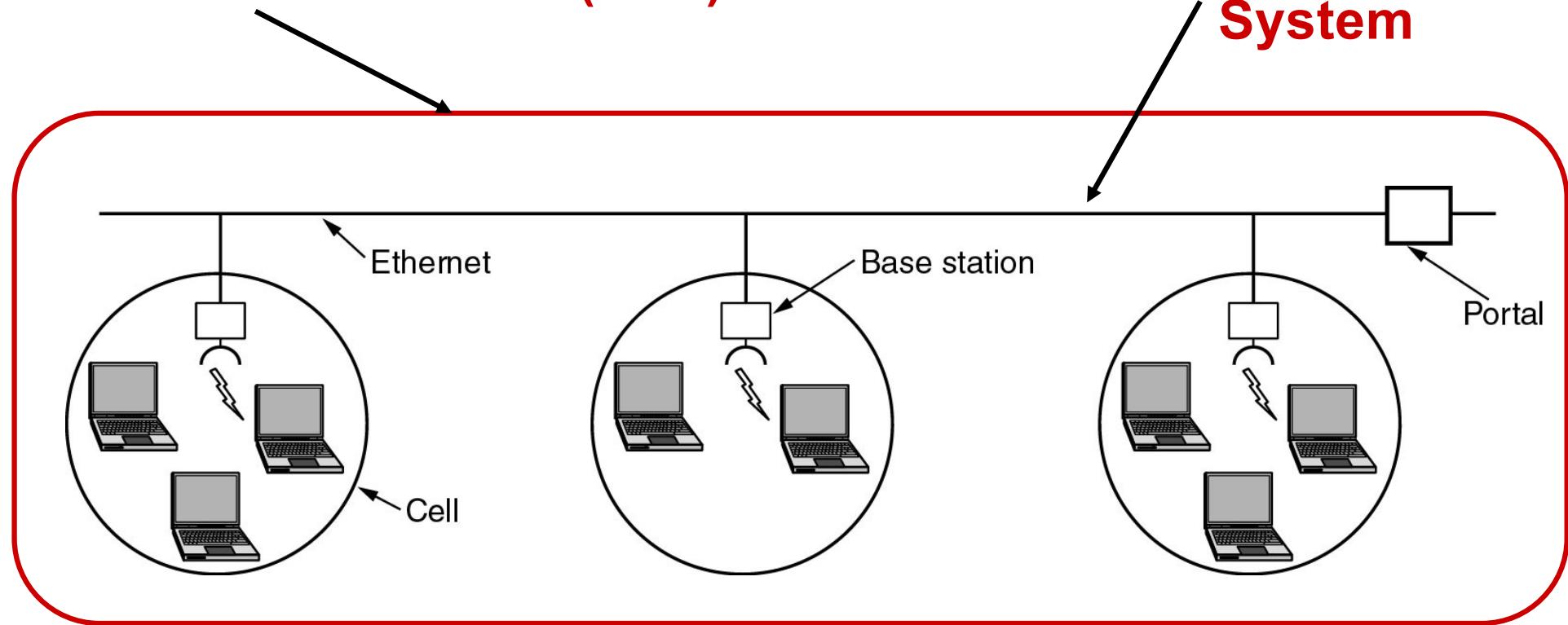


Le stazioni comunicano in modalità peer-to-peer e solo se si vedono direttamente

# Architettura di rete 802.11

## Extended Service Set (ESS)

## Distribution System



Occorre gestire l' associazione delle stazioni agli AP

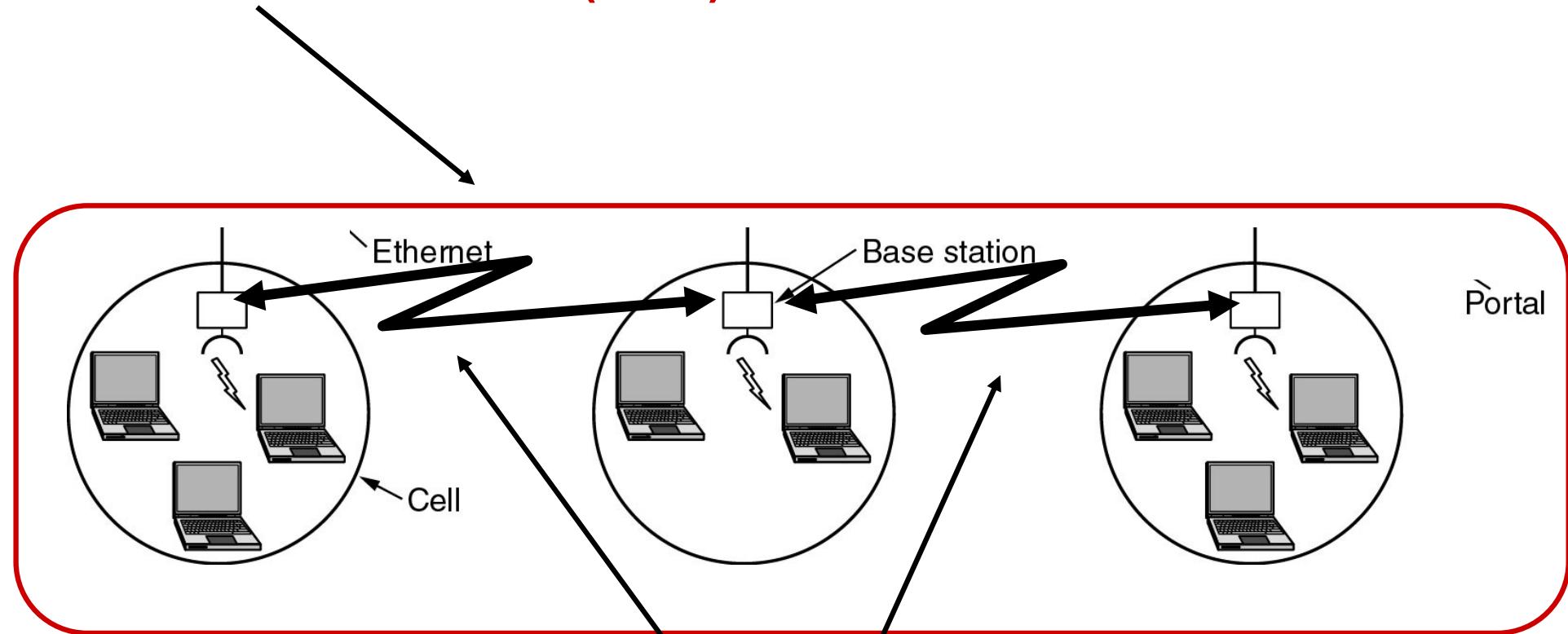
Permette la mobilità delle stazioni trasparente agli strati superiori

Gli AP sono configurati come bridge tra WLAN e LAN, così l' intero ESS è visto come un' unica LAN (unico dominio di broadcast)



# Architettura di rete 802.11

## Extended Service Set (ESS)



**Wireless  
Distribution  
System**

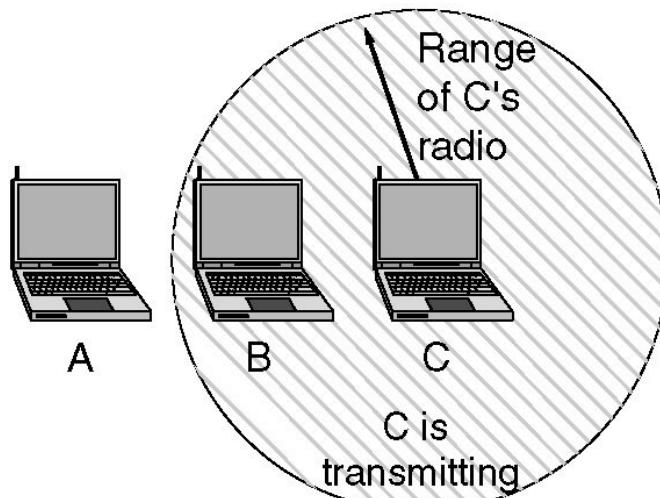


# Problemi di accesso multiplo al canale

- A differenza delle LAN cablate, in cui tutti ricevono quello che viene trasmesso sul mezzo condiviso, nelle WLAN ci sono problemi specifici

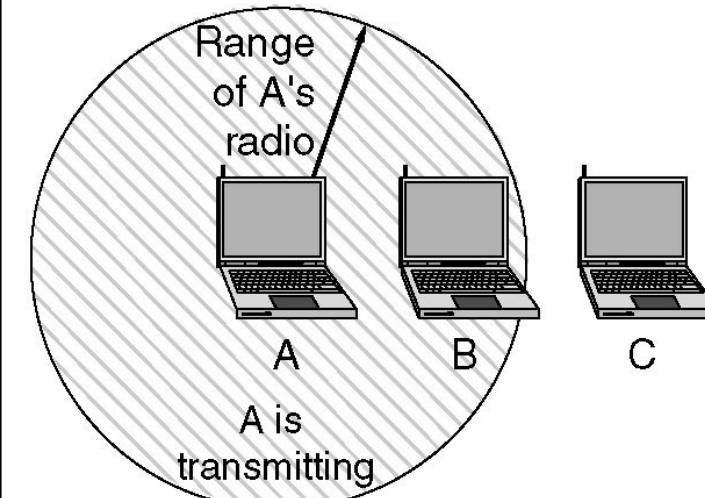
## stazione nascosta

A wants to send to B  
but cannot hear that  
B is busy



## stazione esposta

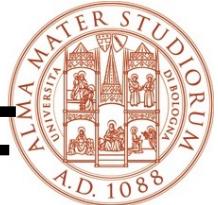
B wants to send to C  
but mistakenly thinks  
the transmission will fail





# Problemi di accesso multiplo al canale

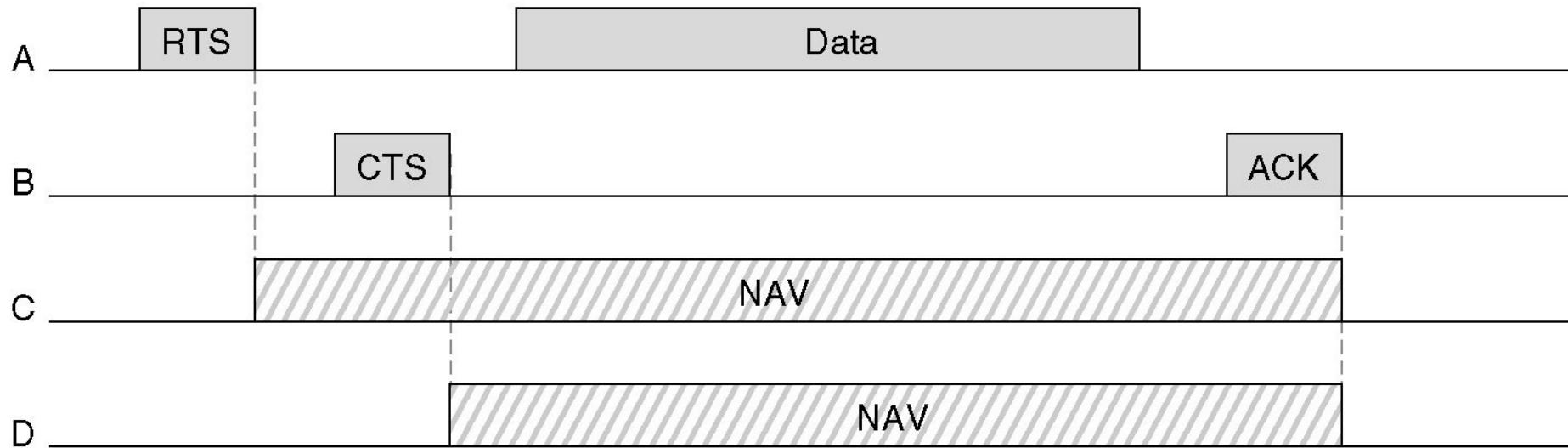
- Il problema della stazione nascosta rende maggiormente problematico l' uso del **carrier sensing**, rispetto alle reti cablate
- La natura half-duplex delle interfacce WLAN impedisce l' uso di **collision detect**
- Il protocollo di accesso multiplo CSMA/CD usato da 802.3 non è utilizzabile nelle WLAN
- Si usa il **Carrier Sensing Multiple Access** con **Collision Avoidance (CSMA/CA)** in due modalità
  - **Distributed Coordination Function (DCF)**
    - l' accesso al canale è gestito in modo distribuito
  - **Point Coordination Function (PCF)**
    - l' accesso al canale è gestito dall' AP



# Protocollo MAC 802.11 – DCF

- Prima di inviare una trama, il mittente invia al destinatario un **Request To Send (RTS)**
  - le altre stazioni che lo ricevono sanno che il canale sta per essere occupato e quanto a lungo lo sarà (la durata del frame è contenuta nel RTS)
- Se il destinatario è in grado di ricevere, risponde con un **Clear To Send (CTS)**
  - a questo punto anche le stazioni che vedono il destinatario ma non il mittente sanno che il canale sarà occupato e conoscono la durata del frame
- L'unico ad accorgersi se una trama è errata è il ricevitore
  - invia un **ACK** al mittente per ogni trama ricevuta correttamente
  - se scade un time-out prima della ricezione dell' ACK, il mittente ritrasmette il frame (preceduto da un nuovo RTS)

# Protocollo MAC 802.11 – DCF



Da A.S. Tanenbaum, “Reti di Calcolatori”

Time →

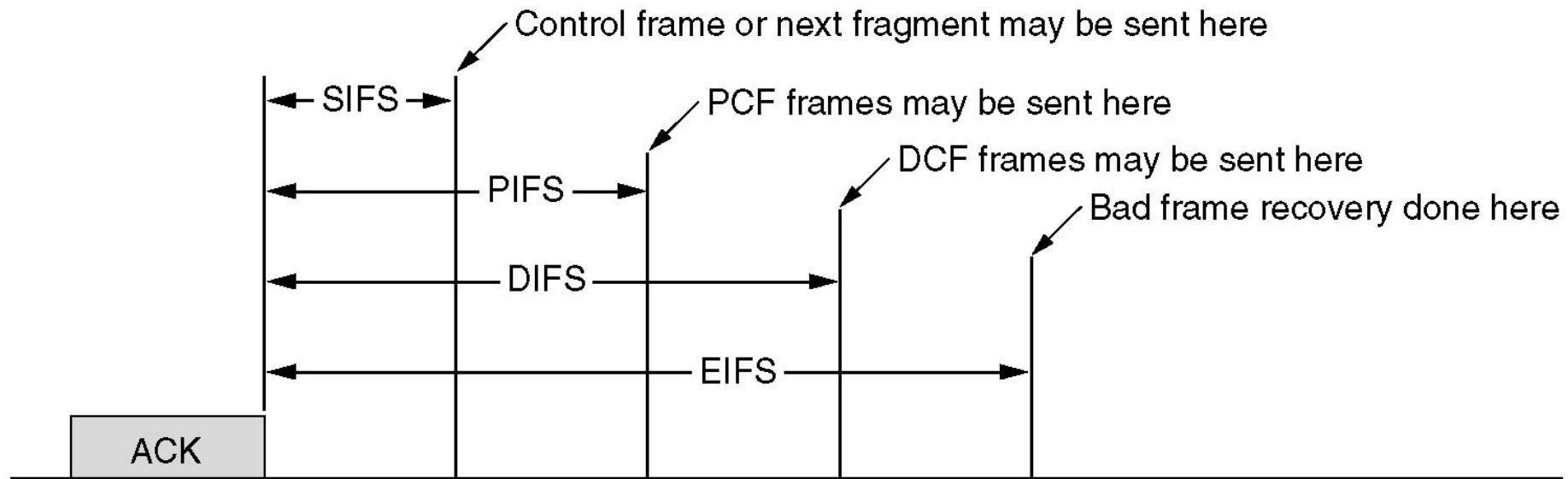
- Le stazioni C e D si accorgono (in tempi diversi) che il canale non è disponibile ed effettuano un carrier sensing virtuale
  - il Network Allocation Vector (NAV) mantiene il canale virtuale occupato
- In caso di collisione tra due RTS, si applica un meccanismo di backoff esponenziale binario
  - si aspetta un tempo casuale entro un intervallo crescente come  $2^n$



# Protocollo MAC 802.11 – PCF

- Nel caso di rete infrastrutturata, l' AP gestisce l' utilizzo del canale a polling, attribuendolo a turno alle stazioni che hanno bisogno di trasmettere
- L' AP trasmette periodicamente un segnale di **beacon** che permette
  - la sincronizzazione delle stazioni
  - la rilevazione della presenza dell' AP
  - la possibilità di entrare nel processo di polling
- Quando una stazione viene attivata, essa scandisce i canali disponibili e cerca i beacon di eventuali AP con cui associarsi
  - tra le altre cose, il beacon mostra il **SSID** (se impostato) che identifica l' AP

# Protocollo MAC 802.11 – PCF



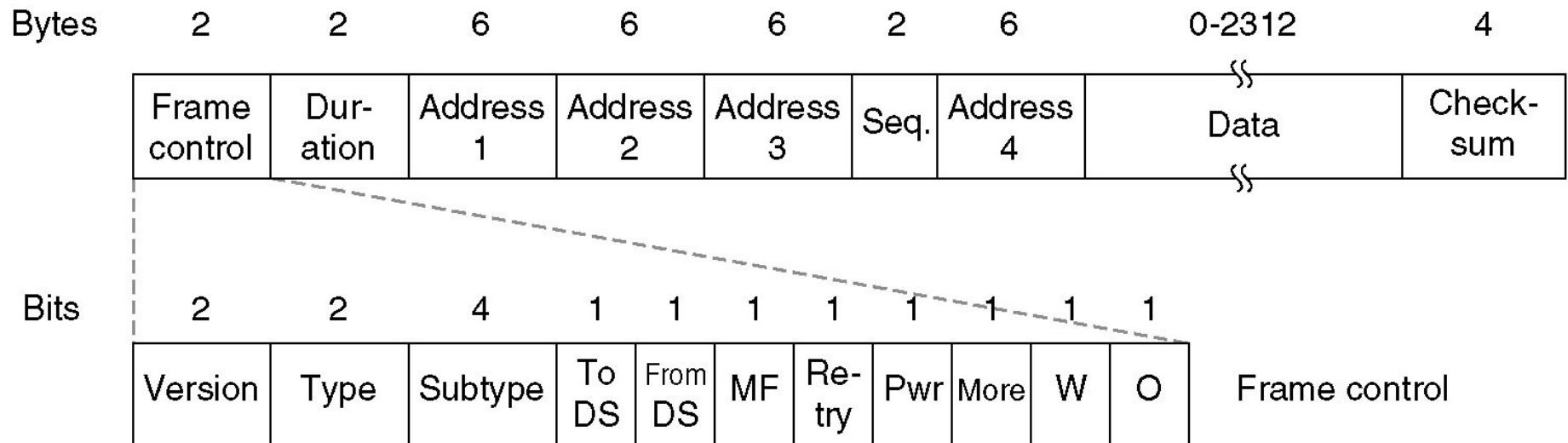
Da A.S. Tanenbaum, "Reti di

Time →

- dopo SIFS (Short InterFrame Spacing) ci si aspetta che qualcuno trasmetta un ACK, un CTS o un frammento di trama successivo
- altrimenti, dopo PIFS (PCF InterFrame Spacing) ci si aspetta che intervenga l' AP (beacon, polling, ...)
- altrimenti, dopo DIFC (DCF InterFrame Spacing) le altre stazioni possono provare ad accedere (con un RTS)
- altrimenti, dopo EIFS (Extended InterFrame Spacing) chi ha ricevuto un frame inatteso può segnalarlo



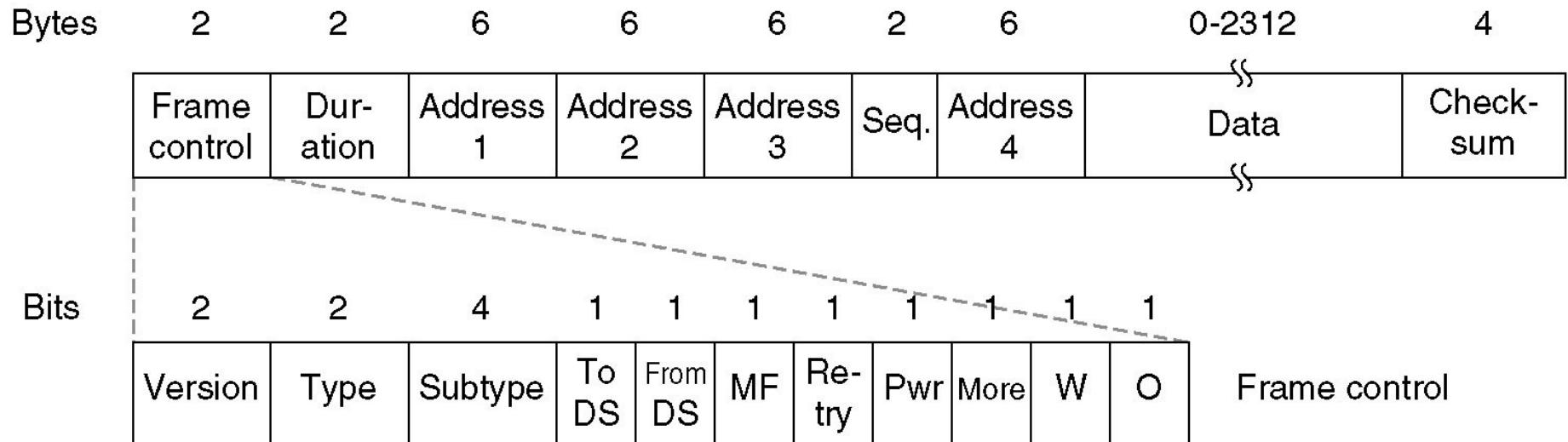
# Trama MAC 802.11



- Type = data, control, management
  - Subtype = RTS, CTS, ACK, ...
  - To DS, From DS = diretto a o proveniente dal sistema di distribuzione
  - MF = More Fragments
  - Retry = è una ritrasmissione
  - Pwr = gestione dell' alimentazione delle stazioni (sleep, wake-up)
  - More = altri frame a seguire
  - W = dati cifrati con WEP
  - Q53 mantenere l' ordine di sequenza dei frame
- Da A.S. Tanenbaum, "Reti di Calcolatori"



# Trama MAC 802.11



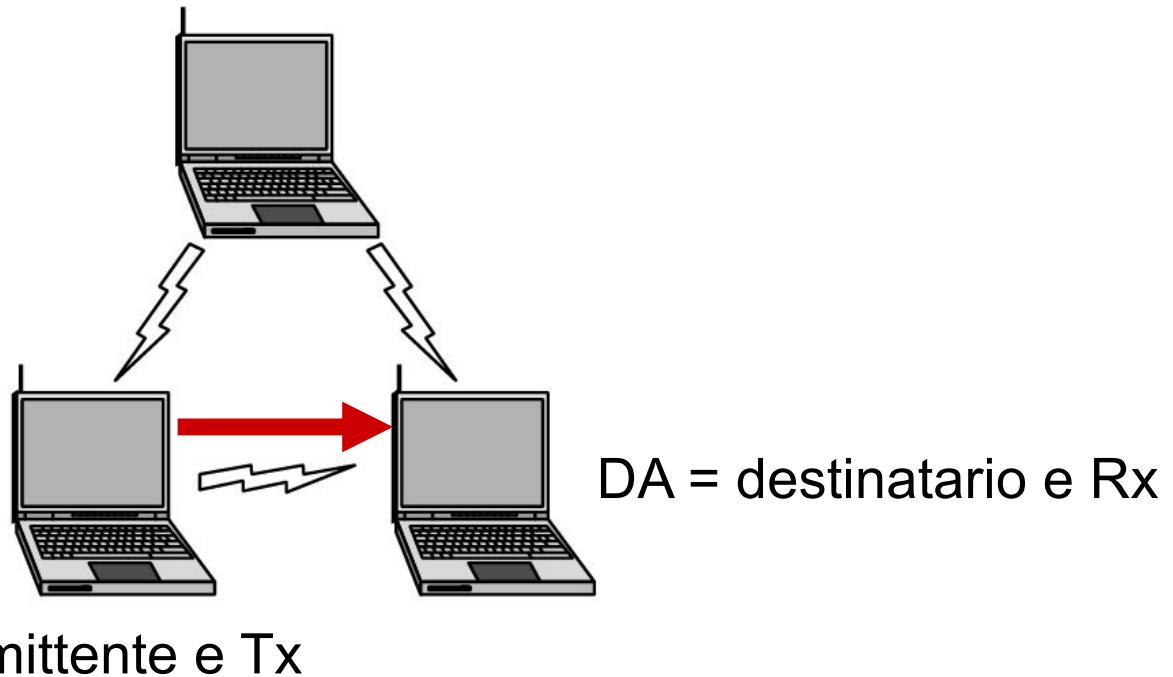
Da A.S. Tanenbaum, "Reti di Calcolatori"

- Duration = durata del frame e del relativo ACK
- Address 1...4 = indirizzi MAC (48 bit) di mittente, destinatario, Tx e RX radio (usati secondo le situazioni specifiche)
- Sequence = numerazione delle trame in sequenza
- Checksum = codice di controllo d' errore



# Indirizzamento 802.11

IBSS (Ad-Hoc)



Address 1 = DA

Address 2 = SA

Address 3 = BSSID (casuale generato da una delle stazioni nell' IBSS)

Address 4 = N/A

To DS = 0

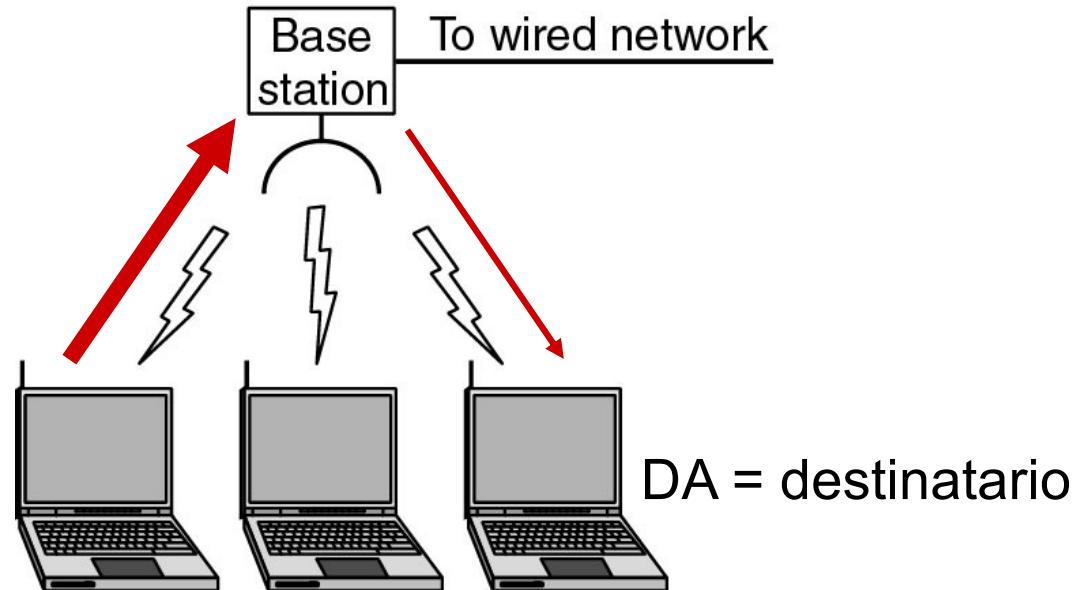
From DS = 0



# Indirizzamento 802.11

BSS/ESS Uplink  
(anche verso LAN)

BSSID = Rx



Address 1 = BSSID (MAC address dell' AP)

Address 2 = SA

Address 3 = DA

Address 4 = N/A

To DS = 1

From DS = 0



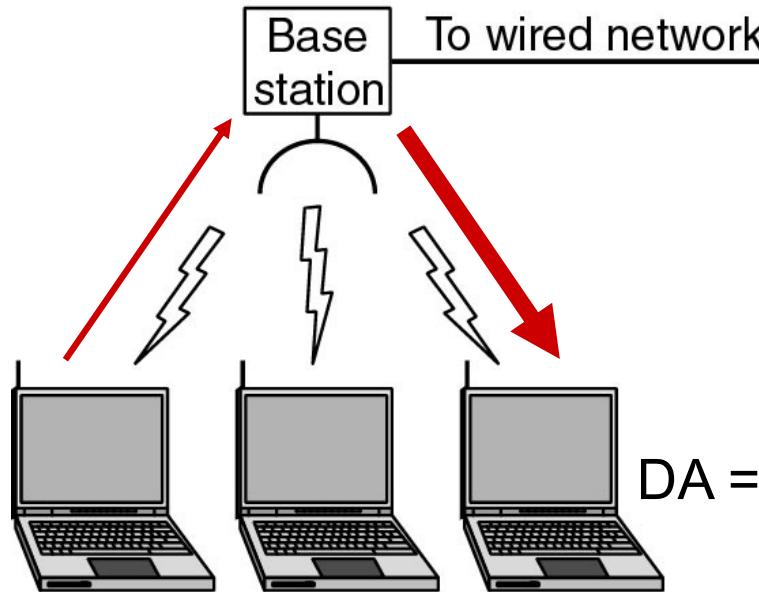
# Indirizzamento 802.11

BSS/ESS Downlink  
(anche da LAN)

BSSID = Tx

SA = mittente

DA = destinatario e Rx



Address 1 = DA

Address 2 = BSSID (MAC address dell' AP)

Address 3 = SA

Address 4 = N/A

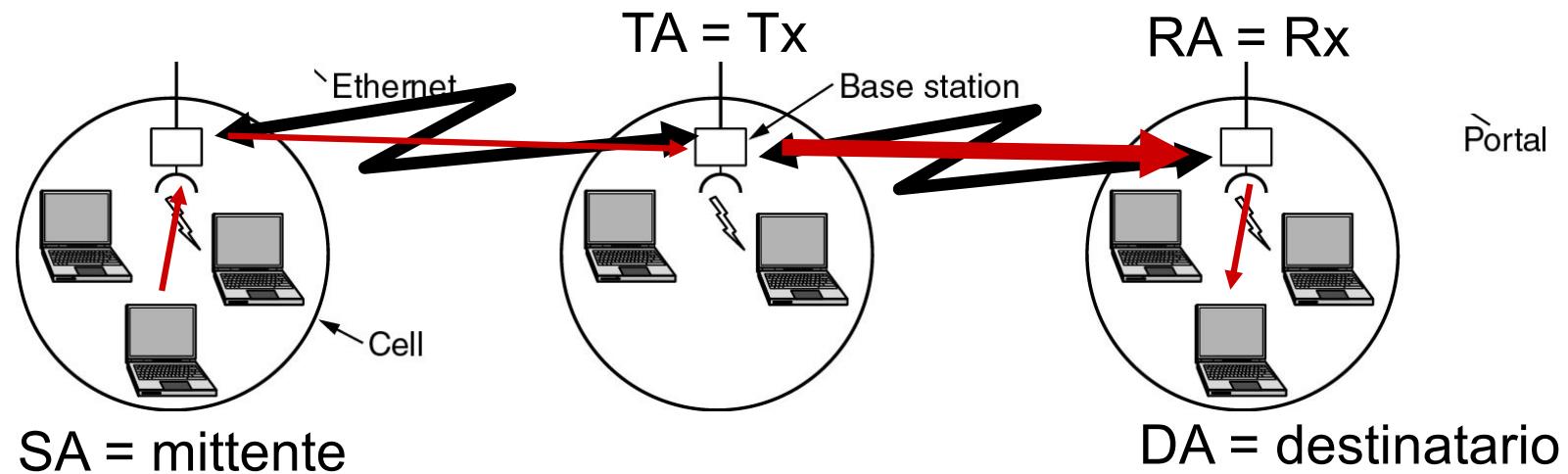
To DS = 0

From DS = 1



# Indirizzamento 802.11

## ESS con Wireless Distribution System



Address 1 = RA

Address 2 = TA

Address 3 = DA

Address 4 = SA

To DS = 1

From DS = 1



ALMA MATER STUDIORUM  
UNIVERSITÀ DI BOLOGNA

# Interconnessione di LAN



# Alternative di interconnessione di LAN

- A volte può essere conveniente suddividere una LAN in più spezzoni o interconnettere LAN o reti di tipo diverso
- Servono apparati di interconnessione che a seconda della funzionalità prendono il nome di
  - Repeaters
  - Bridge
  - Routers
  - Gateways



# REPEATER

- Apparato attivo che collega 2 o più mezzi di trasmissione
- Opera a livello dello **strato 1** OSI
- Permette l'estensione del mezzo di trasmissione
  - Amplifica il segnale
  - Rigenera i bit entranti e li sincronizza
- Permette di estendere una topologia LAN
  - Utilizza più “spezzoni” di mezzo trasmittivo, ciascuno dei quali deve sottostare alle norme di standard
  - Le “parti” della LAN devono essere equivalenti per quanto riguarda il livello 2 (MAC)
- Nella rete Ethernet il diametro complessivo non deve superare i 2500 metri



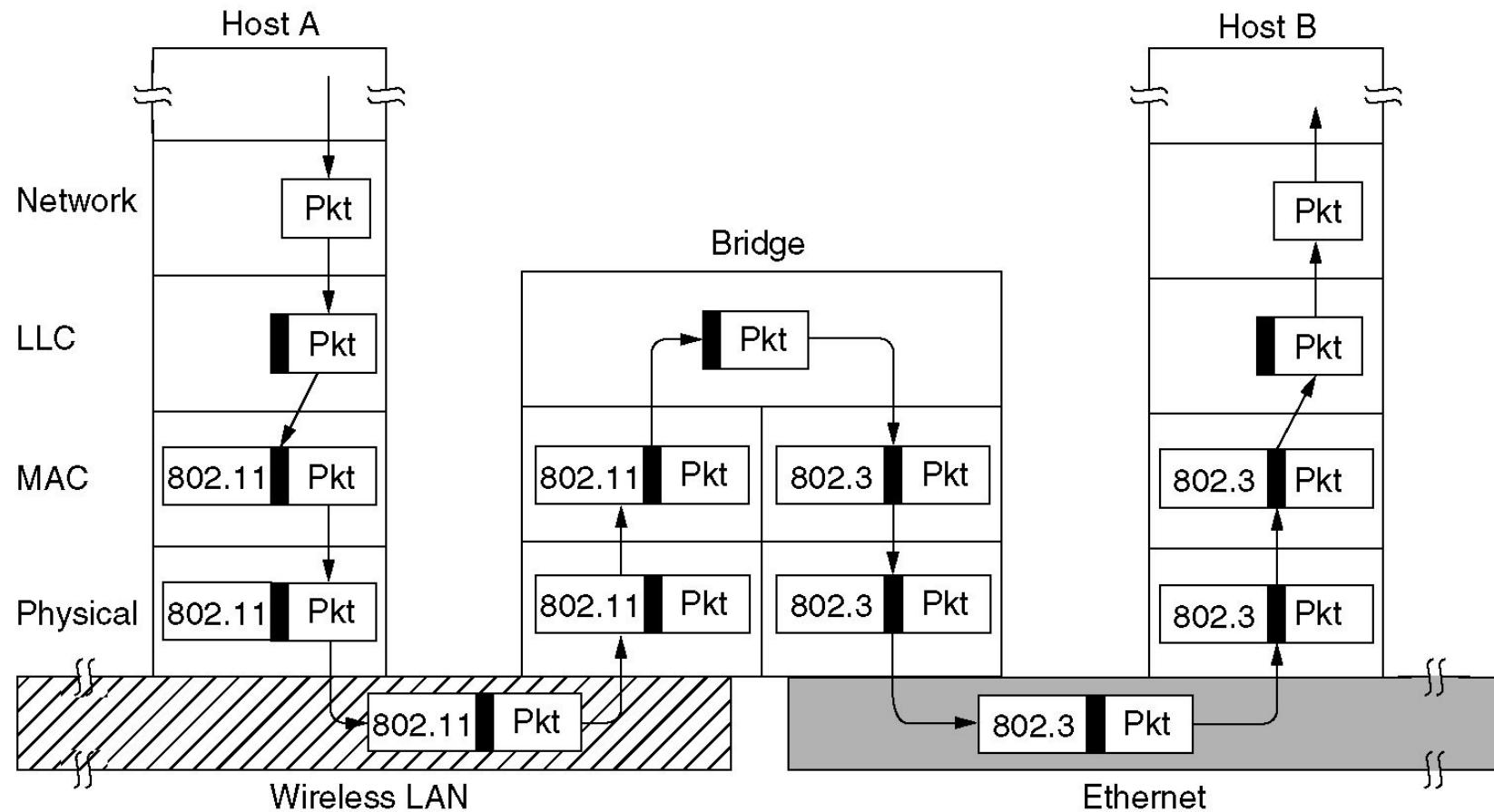
# Bridge

- Opera a livello dello strato 2 OSI
- Può interconnettere LAN di tipo diverso (Ethernet con Token ring, ...)
  - Esegue più protocolli MAC
  - Effettua conversioni del formato di trama
- Nel caso di reti Ethernet separa i domini di collisione
  - Il vincolo dei m. 2500 si applica al collision domain
  - Tramite bridge si possono realizzare LAN di dimensione superiore
- Learning bridge e Filtering bridge
  - Impara quali stazioni sono connesse ad una porta analizzando il "source address" delle trame MAC
  - Invia la trama solo sulla porta di uscita dove si trova il destinatario analizzando il destination address della trama MAC
    - Esegue una funzione di instradamento a livello di trama
  - Separa il traffico dei diversi domini di collisione



# Bridge da 802.x a 802.y

Operation of a LAN bridge from 802.11 to 802.3.



da Tanenbaum

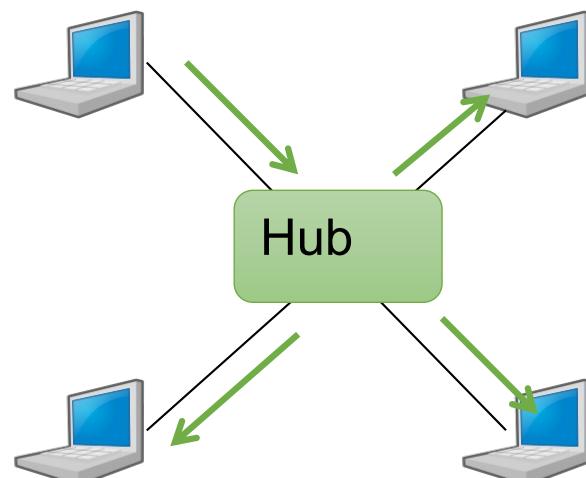


# SWITCH

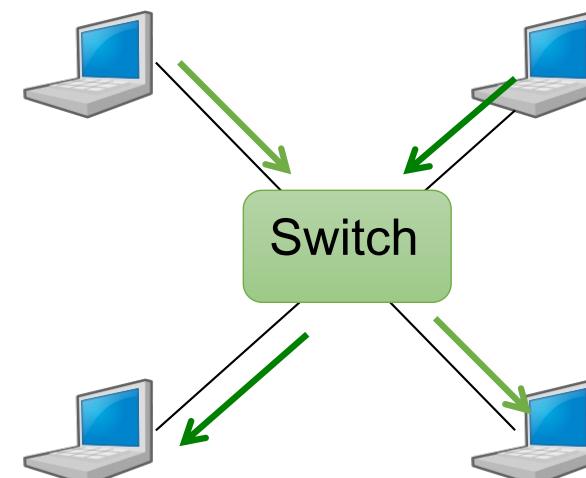
- È un bridge ad alta densità di porte
- Tipicamente ad ogni porta è connessa una sola stazione
- È in grado di trasferire contemporaneamente trame da più porte di ingresso a più porte di uscita
  - Opera una funzione di commutazione a livello 2 basata sull'indirizzo MAC
- Uno switch Ethernet svolge una funzione simile all'hub ma garantendo maggiori prestazioni

# Differenza fra hub e switch

- Hub
  - bus collassato = mezzo condiviso, trasmissione broadcast delle trame
  - Capacità aggregata = capacità della singola porta
- Switch
  - Sistema di commutazione = ri-trasmissione selettiva delle trame
  - Capacità aggregata superiore a quella della singola porta



Esempio: hub fast ethernet  
Si trasferiscono 100 Mbit/s



Esempio: switch fast ethernet  
Si trasferiscono 200 Mbit/s



# Learning Switch

