RETI DI CALCOLATORI
Autunno 2018
docente: Laura Ricci
Lezione 15:
IL LIVELLO DATA LINK
ALOHA, CSMA, ARP

03/12/2018

MATERIALE DIDATTICO

Forouzan

- paragrafo 5.1
- paragrafo 5.2
- paragrafo 5.3
- paragrafo 5.4

IL LIVELLO DI LINEA

- livelli applicazione, trasporto e IP: associati con competenze "più informatiche"
- i livelli più bassi
  - livello data link o medium access control (MAC)
  - livello fisico

  sono stati tipicamente competenza degli "ingegneri elettronici",
  - ma, negli ultimi tempi il livello data link utilizza anche funzioni sw ed è quindi di competenza anche dell'informatico.
- livello fisico si occupa di problemi relativi alle caratteristiche dei mezzi fisici su cui vengono trasmessi il bit
  - inteferenza tra laptop vicini
  - perdita di intensità di un'onda elettromagnetica nel momento che si propaga
  - come rappresentare i bit con livelli di voltaggio, quando sono trasmessi su un cavo
  - in questo corso non lo tratteremo.

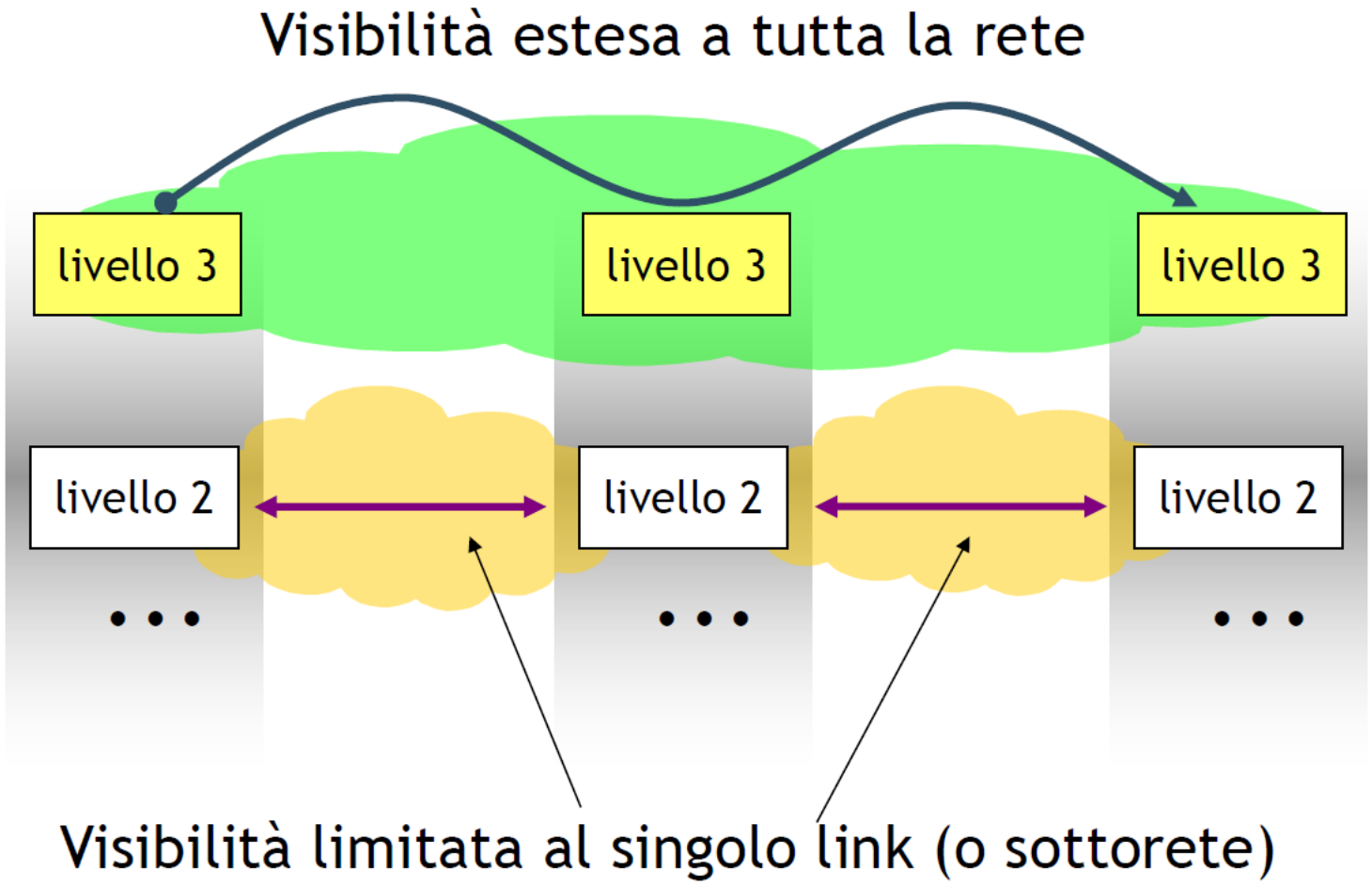
IL LIVELLO DI LINEA: SERVIZI

- framing:
  - incapsulamento di un datagram in un frame
  - aggiunge header e trailer
- controllo di accesso al canale per canali broadcast
  - broadcast channel: linea o mezzo condiviso
    - traditional Ethernet (pre ~2000)
    - 802.11 wireless LAN
  - MAC: Medium Access Control, coordina chi trasmette e chi riceve in canali con molte stazioni collegate (broadcast channel)
- link addressing
  - indirizzi "MAC" (Media Access Control) negli header dei frame identificano i nodi mittente e destinatario
  - diversi dagli indirizzi IP
  - indicati anche come indirizzi fisici

IL LIVELLO DI LINEA: SERVIZI

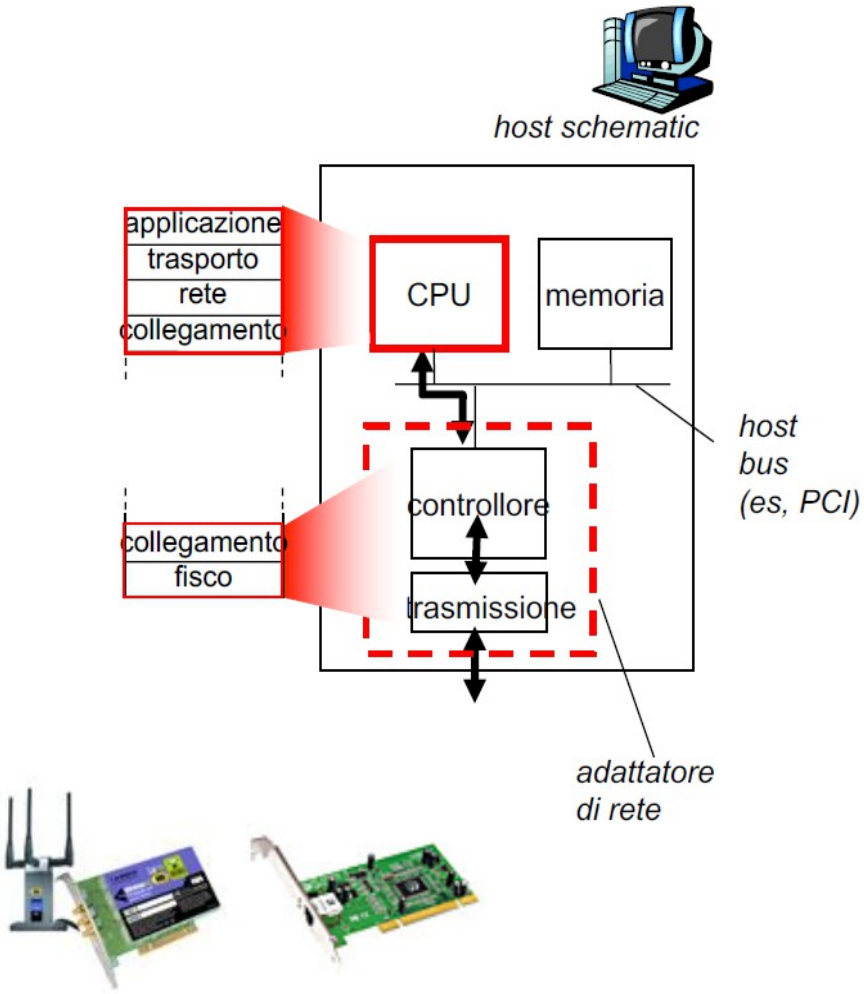
- controllo del flusso
  - controllo velocità di trasmissione dei pacchetti
  - evita che il mittente possa inviare più pacchetti di quelli che il ricevente può ricevere
  - simile al livello TCP
- Individuazione degli errori
  - errori causati dall'attenuazione del segnale, rumore, etc.
  - il destinatario individua la presenza di errori
    - segnala al mittente di ritrasmettere i dati, oppure elimina il frame
- correzione degli errori
  - individuare l'errore e "riparare" il frame

IL LIVELLO DATA LINK

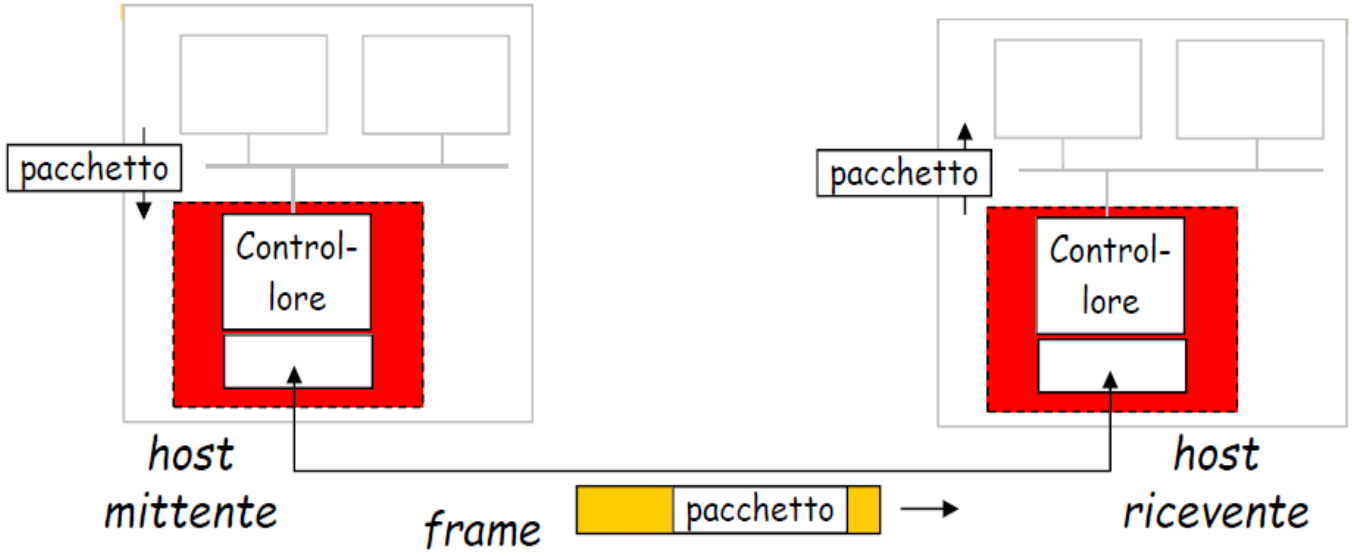


DOVE E' IMPLEMENTATO IL LIVELLO DATA LINK?

- in tutti gli host
- è realizzato in un adattatore NIC, network interface card.
  - scheda di rete Ethernet, 802.11
  - implementa il livello data link e fisico
- è una combinazione di hardware, software e firmware
- alcune funzionalità (gestione degli indirizzi, preparazione della trama) sono svolte in software dall'host



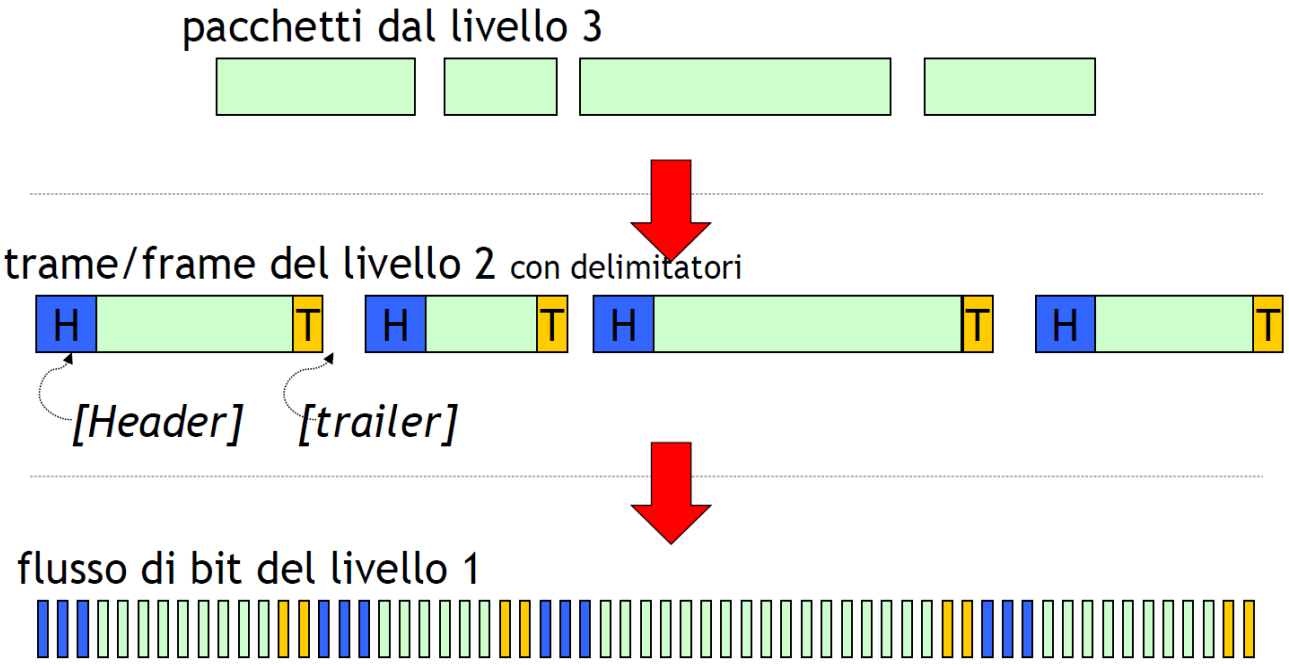
DATA LINK: STRUTTURA



- Lato mittente
  - incapsula un pacchetto in un frame
  - imposta i bit di rilevamento degli errori, controllo del flusso, etc.
- Lato destinatario
  - individua gli errori, controllo flusso, etc.
  - estrae i pacchetti e li passa al nodo ricevente

SERVIZI: FRAMING

- frame: gruppi di bit trattati come una unica unità
  - unità di trattamento dati per il rilevamento degli errori
- tipicamente in arrivo da una unica sorgente e diretto ad un'unica destinazione
- composto da header, dati e trailer
  - header: indirizzi fisici (MAC) mittente e destinazione
  - trailer: informazioni per il controllo degli errori



FRAMING: FUNZIONI

- ha lo scopo di formare un elemento di trasmissione del livello data link (frame) incapsulando il pacchetto di strato superiore
- l'entità ricevente deve essere in grado di riconoscere senza ambiguità l'inizio e la fine di ogni frame (funzione di delimitazione)
- ad ogni frame viene aggiunto all'inizio e alla fine una sequenza fissa di bit, denominata flag
  - l'entità ricevente esamina il flusso binario entrante e delimita le frame riconoscendo i flag di apertura e di chiusura
- problema della simulazione del flag all'interno della frame

FRAMING: ESEMPIO DI FUNZIONE DI DELIMITAZIONE

- una possibile configurazione del Flag di delimitazione è

  01111110

- per evitare la simulazione si utilizzano le funzioni di
  - Bit stuffing
    - in emissione, si aggiunge uno "0" dopo ogni sequenza di cinque "1" consecutivi all'interno della frame indipendentemente da quale sia il bit successivo
  - Bit destuffing
    - in ricezione si contano gli "1" consecutivi
    - quando sono ricevuti cinque "1" consecutivi, si esamina la cifra successiva
      - se è un "1": la sequenza di cifre binarie è un Flag
    - se un 0": questo è un bit di stuffing e deve quindi essere eliminato

ESEMPIO DI STUFFING

- **Sequenza originale**

1 0 1 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 0 0 1 1 1 1 1 0 0

- **Sequenza trasmessa**

1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 1 1 0 1 1 1 1 1 0 0 0 1 1 1 1 1 0 1 0 0

bit di stuffing

- **Sequenza ricevuta**

1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 1 1 0 1 1 1 1 1 0 0 0 1 1 1 1 1 0 1 0 0

0 dopo cinque "1" consecutivi: bit di stuffing bit eliminato

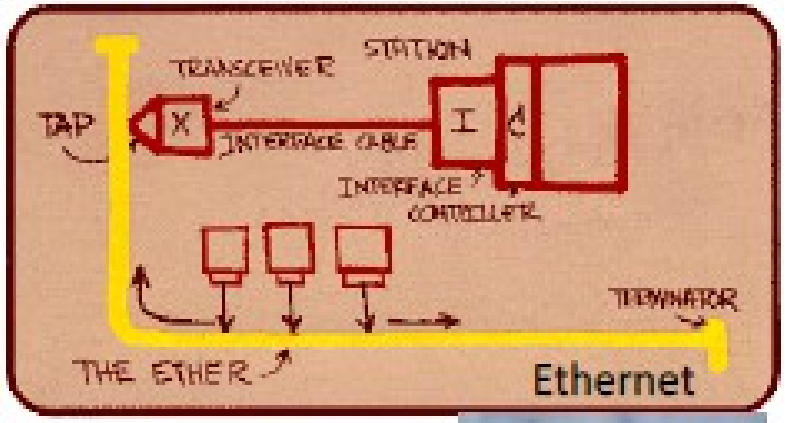
bit di stuffing bit eliminato

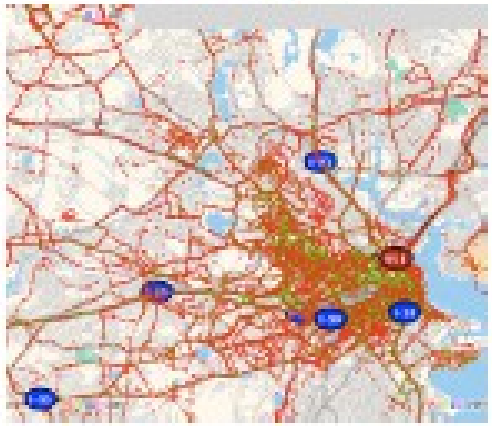
bit di stuffing bit eliminato

bit di stuffing bit eliminato

MEDIA ACCESS CONTROL

- Il problema: arbitrare l'accesso a un mezzo di trasmissione condiviso tra un insieme di diversi utenti.





QUALI BROADCAST MEDIA? ESEMPI

- reti satellitari:
  - il primo esempio: il progetto Aloha
- comunicazioni radio:
  - cellular wireless networks: "EDGE", "3G", "4G", etc.
  - wireless LANs: "802.11", WiFi standard
  - il broadcast è una proprietà intrinseca di queste reti, anche se presenta problemi quali interferenza tra la trasmissione di nodi diversi
- Ethernet (prima generazione):
  - utilizza una rete cablata a cui diversi end host e switches possono essere connessi
  - ogni pacchetto trasmesso può essere "letto" dagli altri nodi della rete

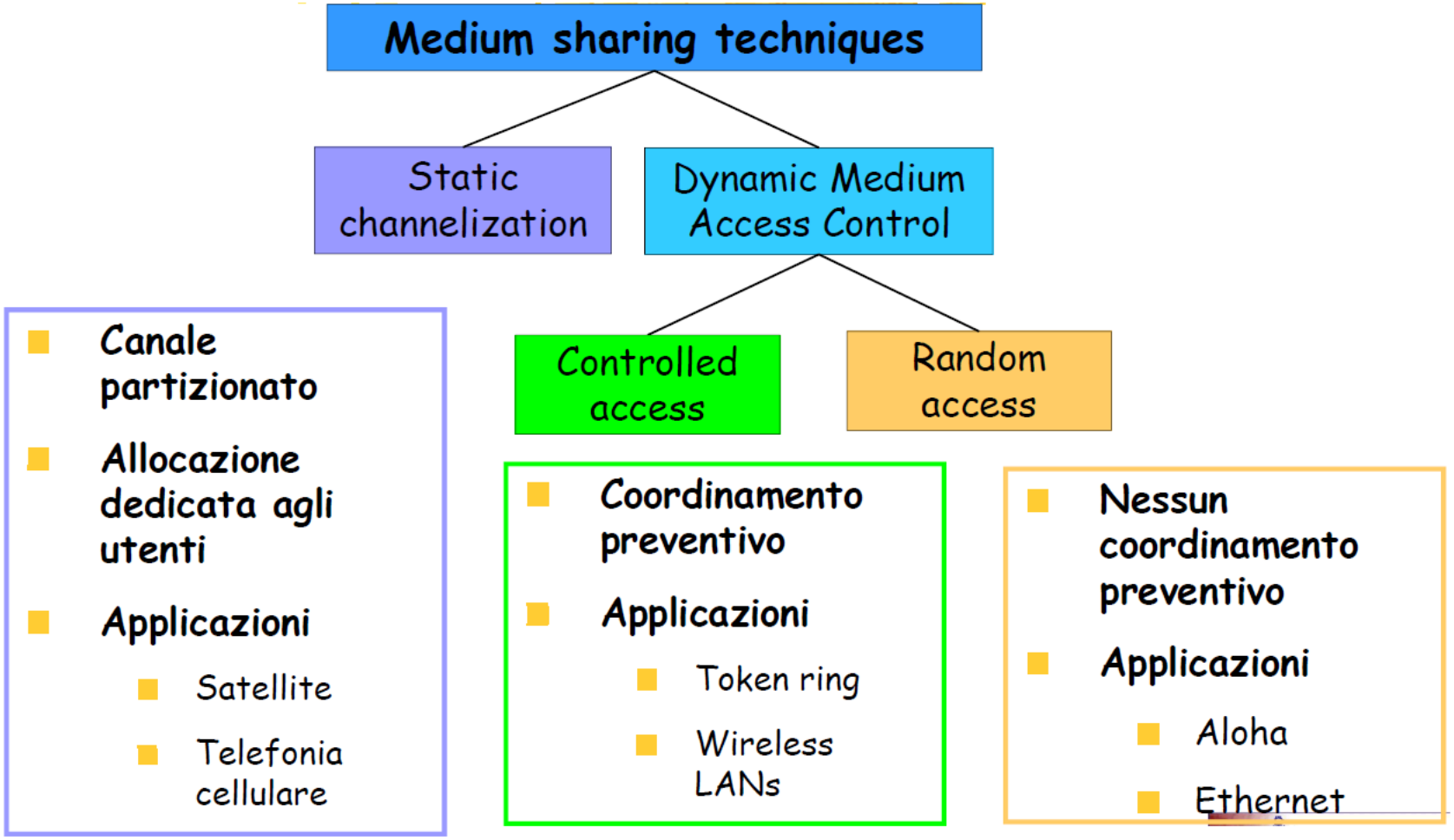
BROADCAST MEDIA: PROBLEMI

- dato un broadcast media condiviso:
  - occorre evitare che più nodi inviino i dati contemporaneamente
  - altrimenti si creano delle collisioni
  - necessari algoritmi che determino quale nodo può trasmettere

- Protocolli a suddivisione del canale (canalizzazione statica)
  - suddivide del canale in "parti più piccole" (slot di tempo, frequenza, codice)
  - le parti vengono allocate ad un nodo per utilizzo esclusivo

- Protocolli ad accesso dinamico
  - Protocolli ad accesso casuale (random access)
    - i canali non vengono divisi e si può verificare una collisione
    - i nodi coinvolti ritrasmettono ripetutamente i pacchetti
  - Protocolli ad accesso controllato (controlled access)
    - ciascun nodo ha il suo turno di trasmissione, ma i nodi che hanno molto da trasmettere possono avere turni più lunghi.

PROTOCOLLI AD ACCESSO MULTIPLO



TDMA ED FDMA

- il meccanismo più semplice per arbitrare gli accessi ad un mezzo condiviso:
  - Time Division Multiple Access (TDMA)
    - ogni utente utilizza il mezzo condiviso per un intervallo di tempo fisso (slot)
    - round robin degli utenti
  - Frequency Division Multiple Access (FDMA)
    - ad ogni utente viene dato un intervallo di frequenze
- simile alla tecnica del circuit switching
- garanzia di performance: ogni slot dedicato solo ad una comunicazione
- in genere implementato mediante una entità centralizzata, come una base station che decide come attribuire i time slot o le frequenze agli utenti
  - usata nelle reti di cellulari

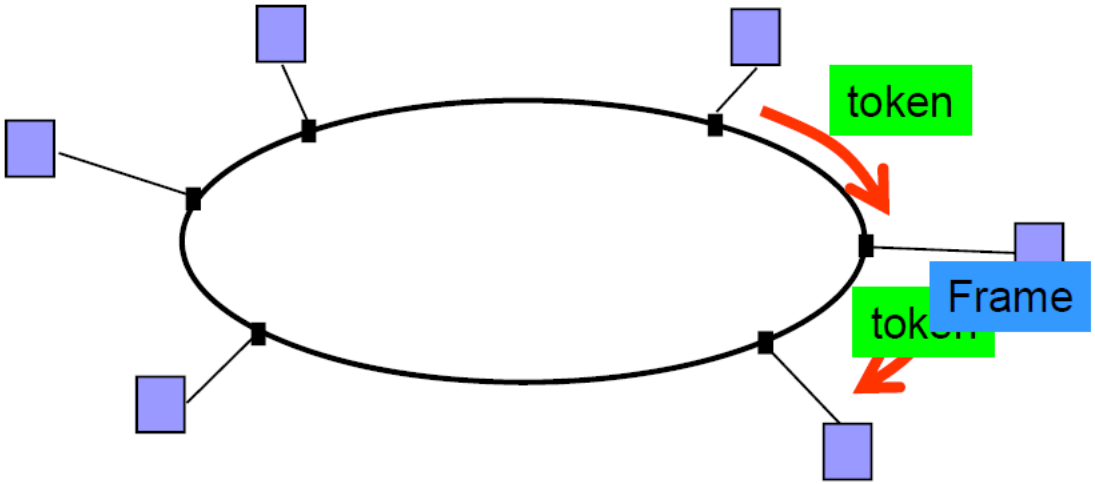
TDMA ED FDMA

- non molto adatti
  - per reti tipo WiFI che si sviluppano in modo non strutturato senza una registrazione formale o comunque un processo di sottoscrizione
  - in caso di "traffico irregolare" tipico di Internet:
    - alcuni time slot o canali possono risultare inutilizzati in alcuni time slot, se non ci sono dati da inviare

- in caso di traffico irregolare:
  - preferibile utilizzare un protocollo distribuito in cui il canale condiviso non viene partizionato e tutti "se lo contendono" quando hanno da inviare dei dati (contention based MAC protocols)

- differenza tra TDMA/FDMA e contention-based MAC protocols
  - simile alla differenza tra circuit and packet switching.

PROTOCOLLI AD ACCESSO CONTROLLATO

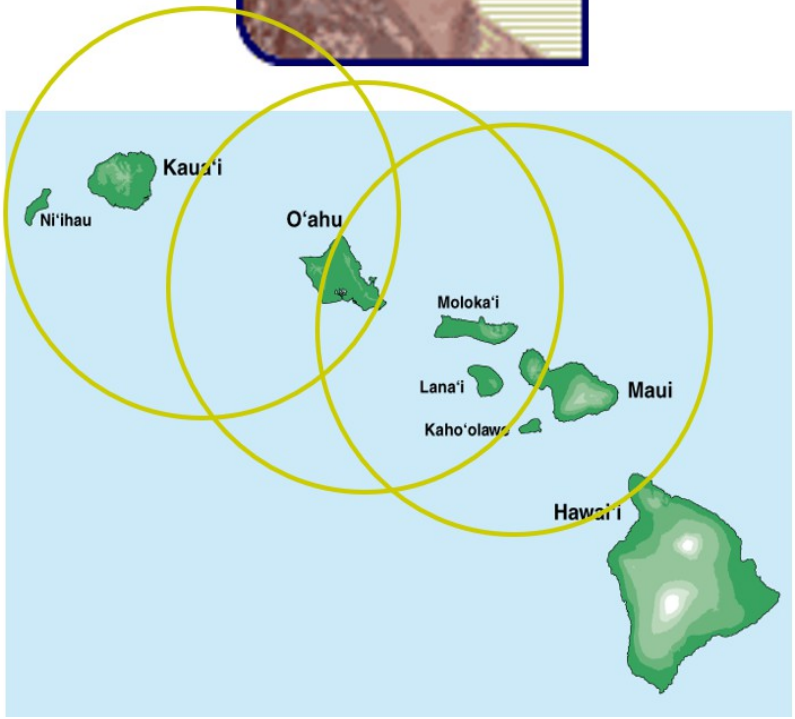


- la stazione che detiene il token può trasmettere
- non sono possibili collisioni

RANDOM ACCESS MAC PROTOCOLS

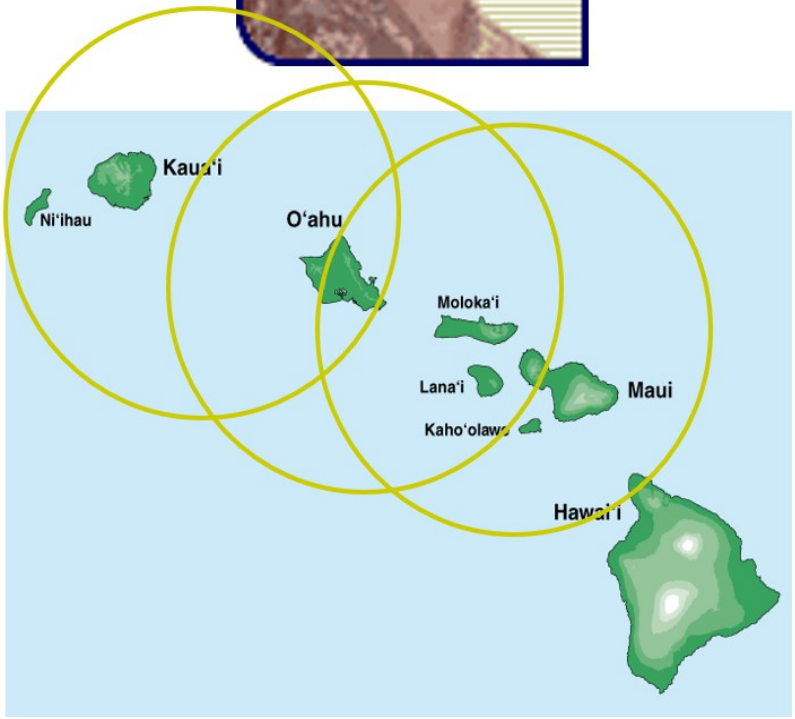
- quando un nodo trasmette un paccheto
  - non si coordina con gli altri nodi
- se nello stesso tempo accedono al mezzo di comunicazione due o più nodi, si verifica una collisione
  - i dati vengono persi
- un Random access MAC protocol specifica:
  - come individuare le collisioni
  - come effettuare il recovery dalle collisioni
  - Esempi:
    - ALOHA/ Slotted ALOHA
    - CSMA, CSMA/CD, CSMA/CA (per reti wireless)

IL PROGETTO ALOHANET



- utilizzata una comunicazione radio in entrambe le direzioni
- canale condiviso
- la rete satellitare connessa ad ARPANET
  - precursore di Internet
- perchè studiarla?
  - idea semplice che ispira i protocolli WIFI di oggi, quasi 50 anni dopo
  - ispirò Bob Metcalfe per la creazione di Ethernet,
    - meccanismo di collision detection isirato proprio da Aloha

IL PROGETTO ALOHANET



- Norm Abramson lasciò Stanford nel 1970 e si trasferì alle Hawaii (surfing?)
- obiettivo: connetere un insieme di computer dislocati tra le isole dell'arcipelago delle Hawaii
- switch su un satellite fornisce la connettività tra le isole
- ogni pacchetto
  - deve essere diretto allo switch mediante un uplink
  - dallo switch alla destinazione finale mediante un downlink

ALOHA: PRINCIPI DI FUNZIONAMENTO

- il canale wireless uplink è condiviso da più nodi e la trasmissione risulta valida se al massimo un nodo trasmette, in ogni istante.
- la trasmissione da parte di più di un pacchetto nello stesso intervallo genera una collisione
- gli utenti rilevano la collisione dalla mancata ricezione di un ACK
- scopo del protocollo è quello di coordinare le trasmissioni degli utenti in modo da minimizzare la probabilità di una collisione

SLOTTED ALOHA

alcune ipotesi

- il tempo è diviso in slot discreti di lunghezza τ
- ogni pacchetto può essere trasmesso in un solo slot ed ogni nodo inizia a spedire il pacchetto all'inizio dello slot
- si conosce il numero N di utenti che possono trasmettere contemporaneamente
- i pacchetti vengono spediti in modo casuale.
- se uno o più nodi spediscono il pacchetto nello stesso time slot si verifica una collisione e nessuno dei pacchetti è ricevuto con successo
- Il mittente può riconoscere che la trasmissione del pacchetto ha generato una collisione ed, in questo caso, può ritrasmettere il pacchetto.
- nessuna coppia di nodi che usa il canale condiviso può percepire se l'altro nodo sta trasmettendo sullo stesso canale

SLOTTED ALOHA

Specifica del protocollo:

- se un nodo ha un pacchetto da spedire lo spedisce con una probabilità fissa p (non trasmette con probabilità 1-p)
- scopo del protocollo: stabilire il valore corretto di p.

ALOHA SLOT PER SLOT

Success (S), Collision (C), Empty (E) slots

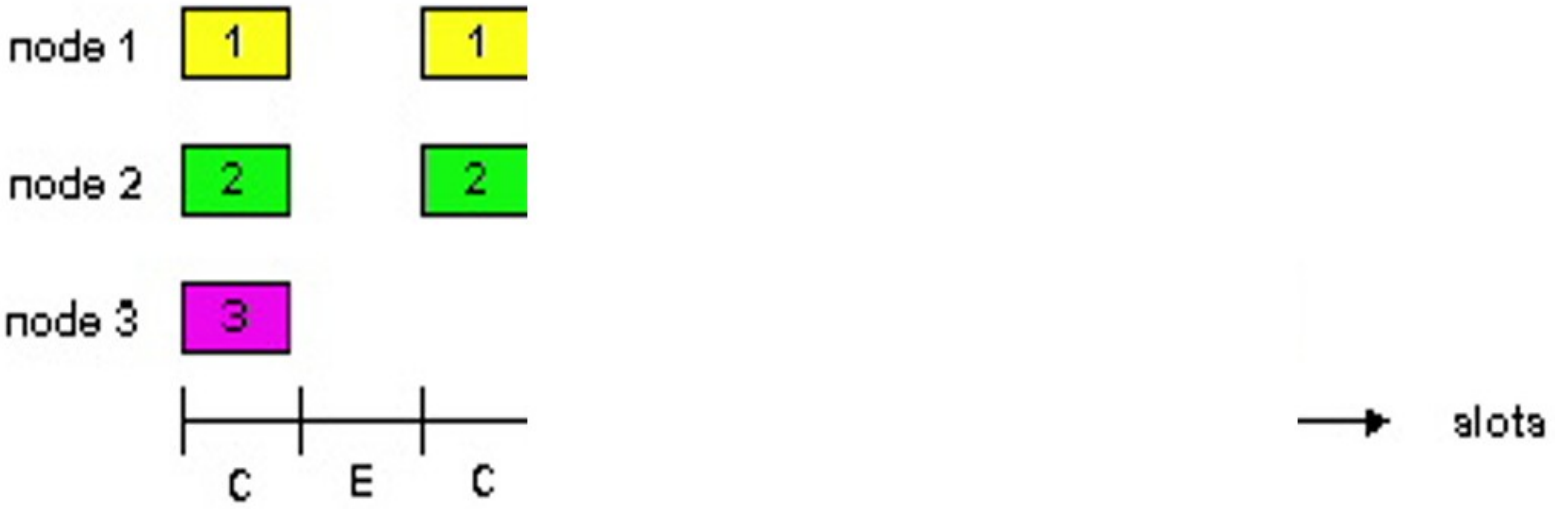
ALOHA SLOT PER SLOT

Success (S), Collision (C), Empty (E) slots

ALOHA SLOT PER SLOT

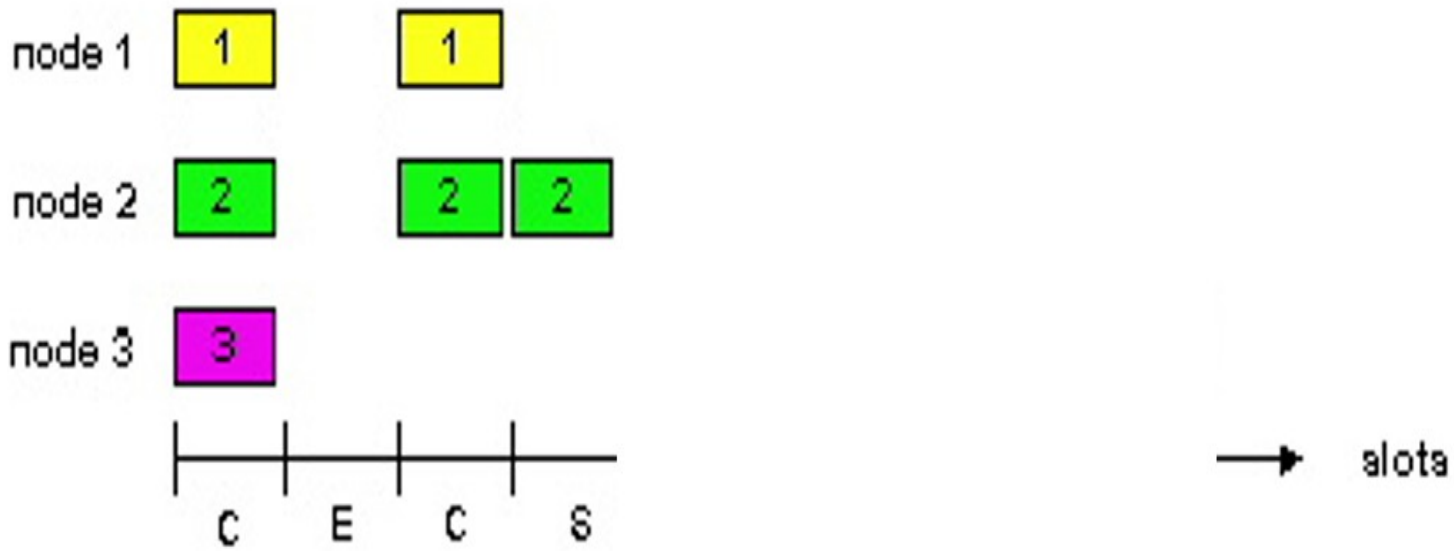
Success (S), Collision (C), Empty (E) slots

ALOHA SLOT PER SLOT



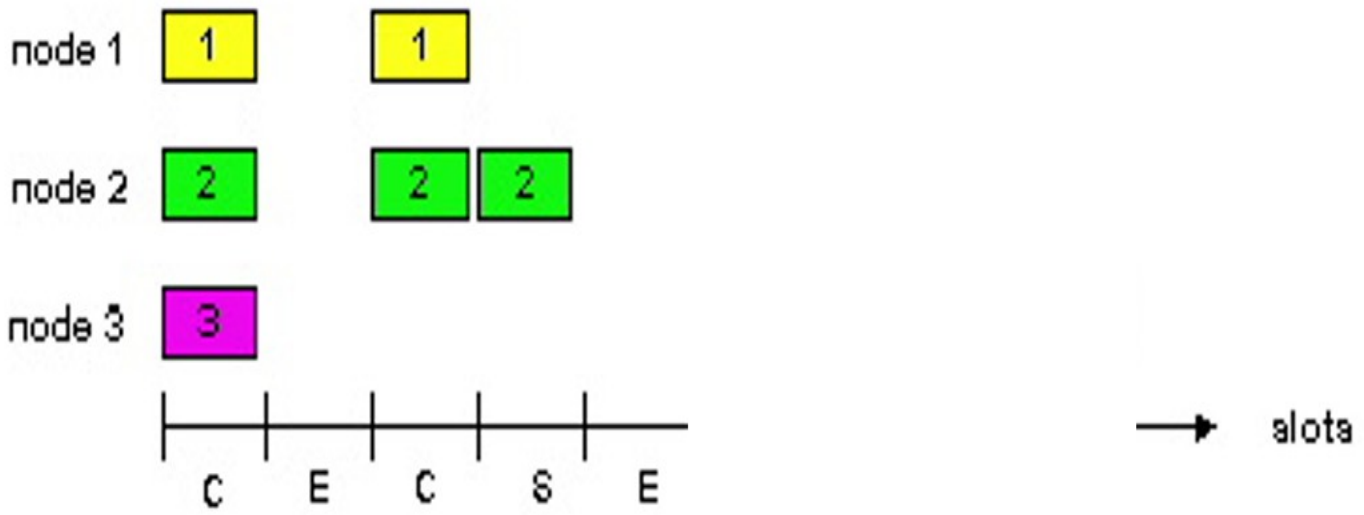
Success (S), Collision (C), Empty (E) slots

ALOHA SLOT PER SLOT



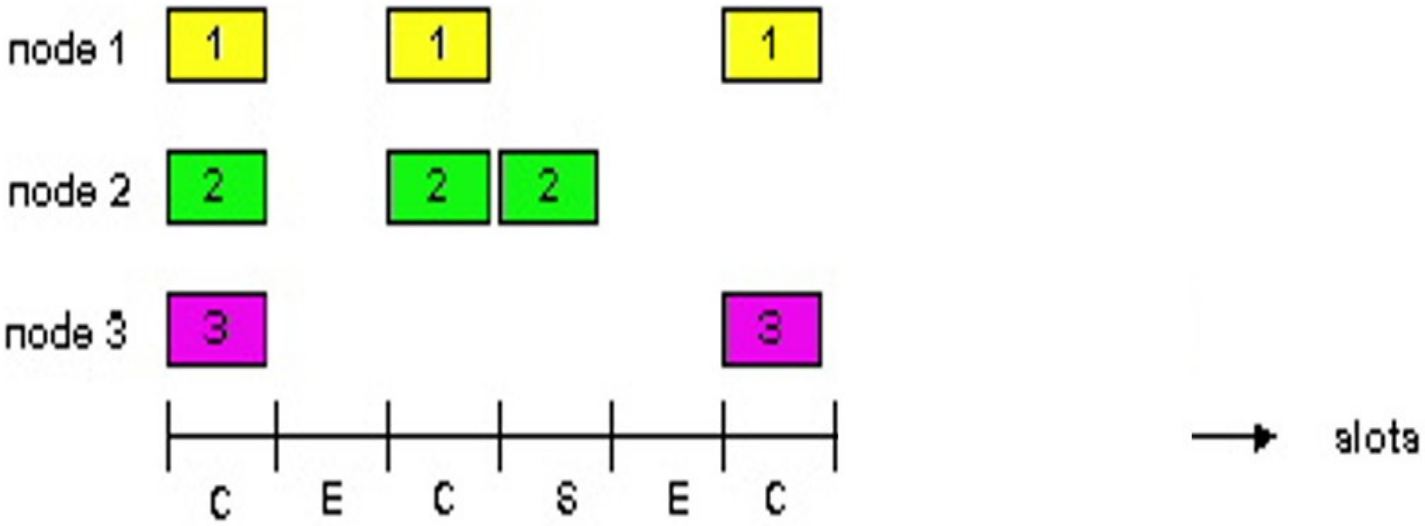
Success (S), Collision (C), Empty (E) slots

ALOHA SLOT PER SLOT



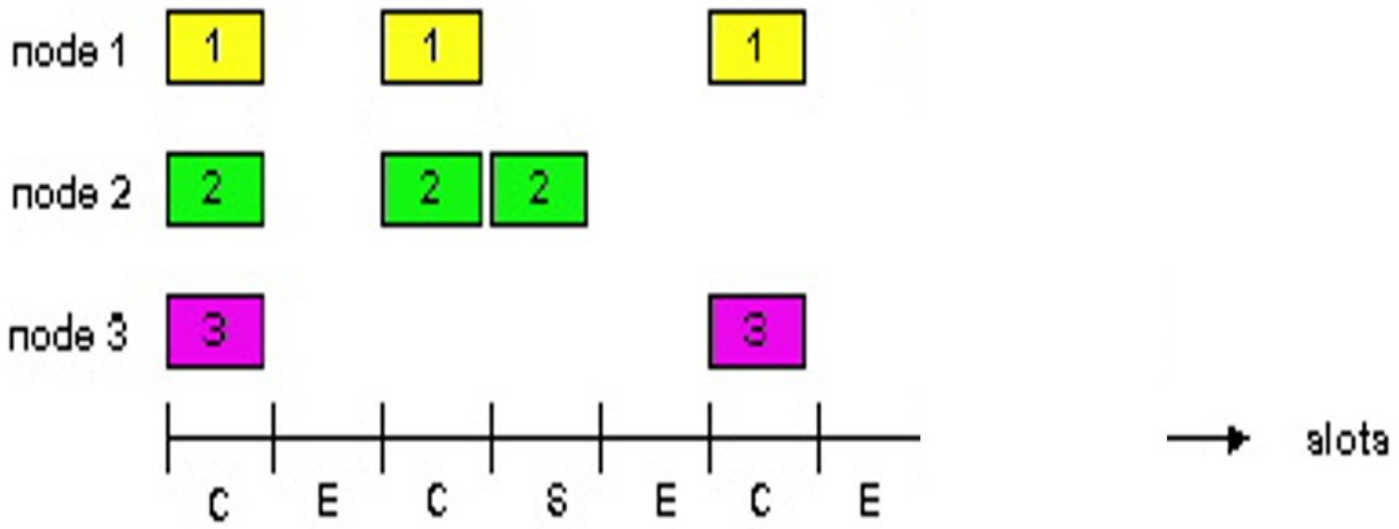
Success (S), Collision (C), Empty (E) slots

ALOHA SLOT PER SLOT



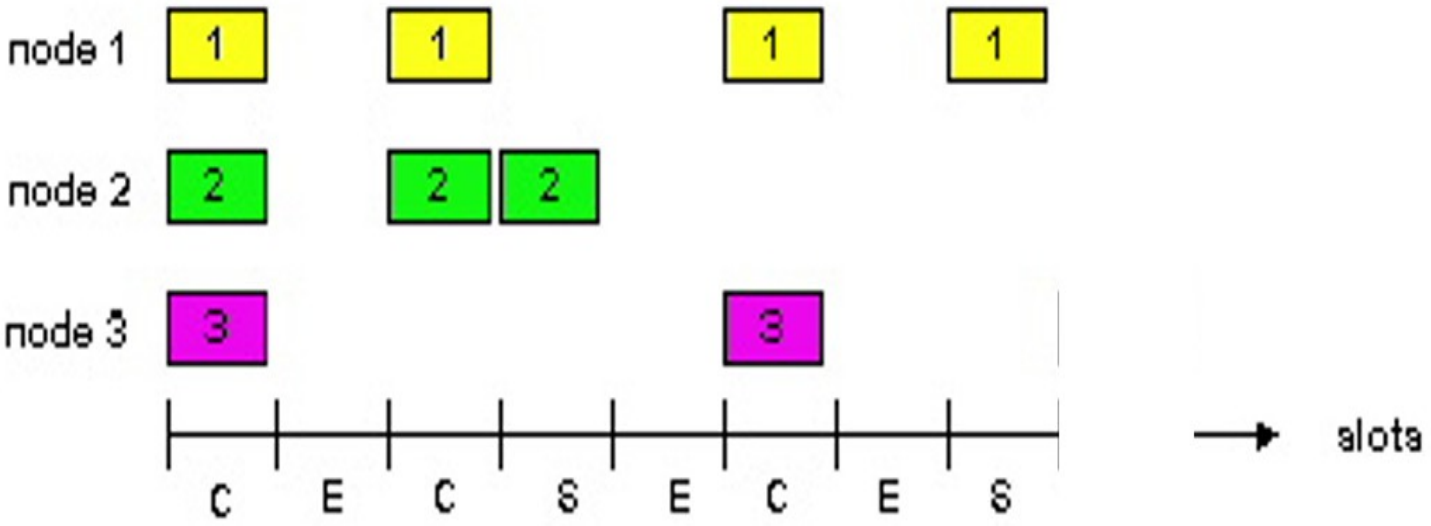
Success (S), Collision (C), Empty (E) slots

ALOHA SLOT PER SLOT



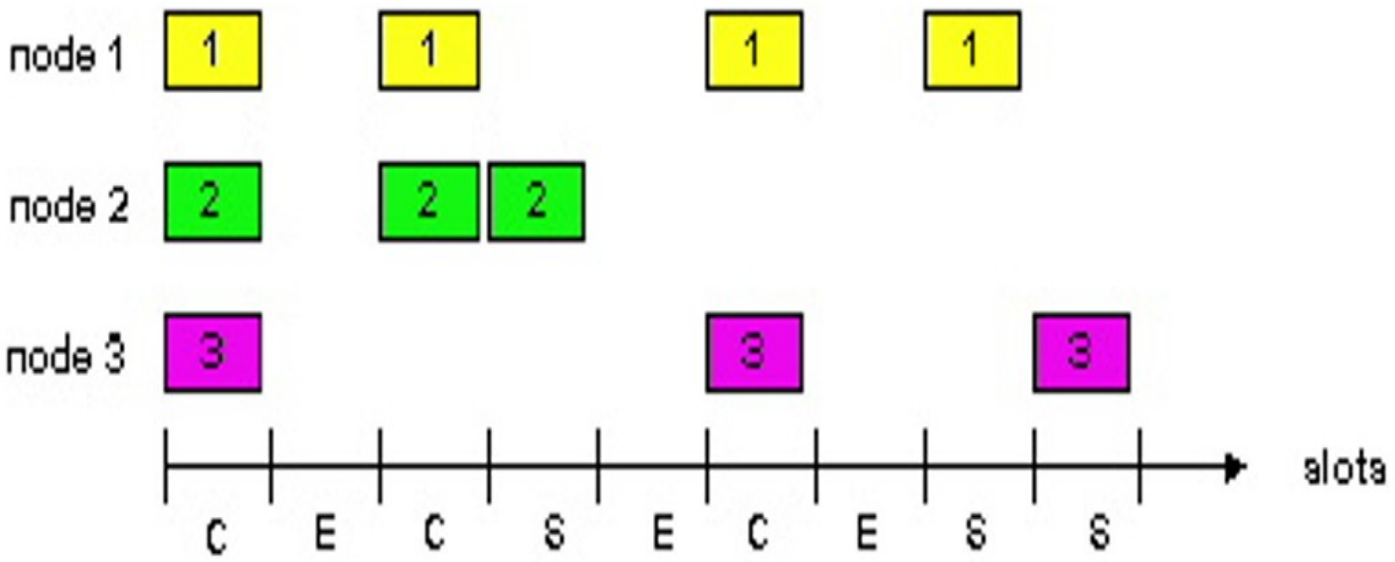
Success (S), Collision (C), Empty (E) slots

ALOHA SLOT PER SLOT



Success (S), Collision (C), Empty (E) slots

POINT TO POINT E BROADCAST MEDIA



Success (S), Collision (C), Empty (E) slots

SLOTTED ALOHA: ANALISI

- supponiamo che N nodi debbano inviare un pacchetto sul canale condiviso
  - ogni nodo trasmette con probabilità uguale a p
- probabilità che:
  - un singolo nodo i riesca a trasmettere con successo (senza collisioni) è

$$S_i = p \times (1-p)^{(N-1)}$$

    - la probabilità che un nodo specifico invii i dati in un time slot è p
    - affinchè riesca a trasmettere con successo, tutti gli altri nodi non devono trasmettere
  - un qualsiasi nodo riesca a trasmettere con successo (senza collisioi) è

$$S = N \times p \times (1-p)^{(N-1)}$$

    - il nodo che trasmette può essere scelto in N modi diversi
    - S= throughput: numero medio di trasmissioni con successo in uno slot

SLOTTED ALOHA: ANALISI

- al variare di p, quale è il valore massimo di $S = Np(1-p)^{N-1}$
- per calcolare il valore massimo della espressione precedente al variare del valore di p, occorre calcolare la derivata e porla = 0.

$$\begin{aligned} N((1-p)^{N-1} - p(N-1)(1-p)^{N-2}) &= 0 \\ (1-p)^{N-2}((1-p) - p(N-1)) &= 0 \\ \text{escludiamo la soluzione di } (1-p)^{N-2} &= 0 \\ \text{rimane } (1-p) - p(N-1) &= 0 \\ 1 - p - Np + p &= 0 \\ p &= \frac{1}{N} \end{aligned}$$

- probabilità che un qualsiasi utente trasmetta senza collisioni in un certo time slot assumendo di utilizzare il valore ottimo di p?
  - sostituiamo nelle espressione precedente $p = \frac{1}{N}$
  - otteniamo

$$(1 - \frac{1}{N})^{N-1}$$

SLOTTED ALOHA: ANALISI

$$\lim_{N\to\infty}(1-\frac{1}{N})^{N-1} = \frac{1}{e}$$

- quale è il valore che massimizza la probabilità di successo?
  - per p fissato, S $\to$0 all'aumentare di N
  - ma se p = 1/N, allora S $\to$ 1/e = 0.37 all'aumentare di N
- massima efficienza poco più di 1/3!

SLOTTED ALOHA: ANALISI

- Sia G, il traffico, ovvero il numero medio di trasmissioni sul canale, datoda:

$$G = Np$$

  - sostituendo nella formula del throughput p=G/N, si ha:

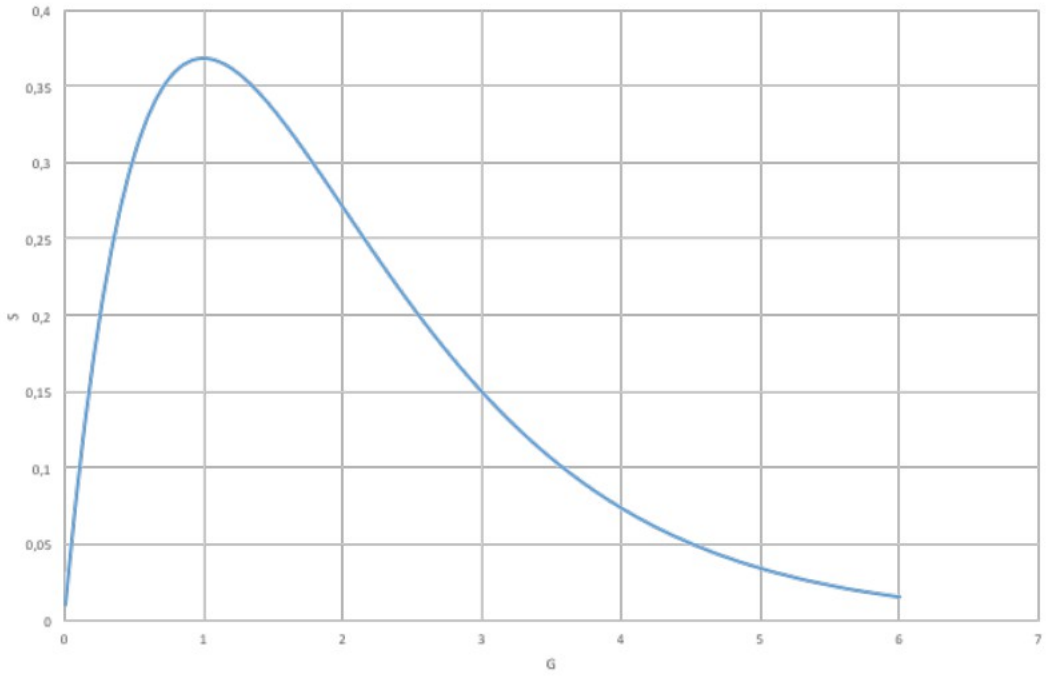
$$G = (1 - \frac{G}{N})^{N-1}$$

- questa formula dà il numero medio di successi in funzione del numero medio di trasmissioni
- è dunque la frazione di slot utilizzati proficuamente

SLOTTED ALOHA: ANALISI

- Il limite per N che tende ad infinito del throughput, in funzione di G

$$S = G \times e^{-G}$$



Massimo in

$G = 1$

$S = 1/e \cong 0.37$

ALOHA PURO : ANALISI

ALOHA (niente slot) è molto simile

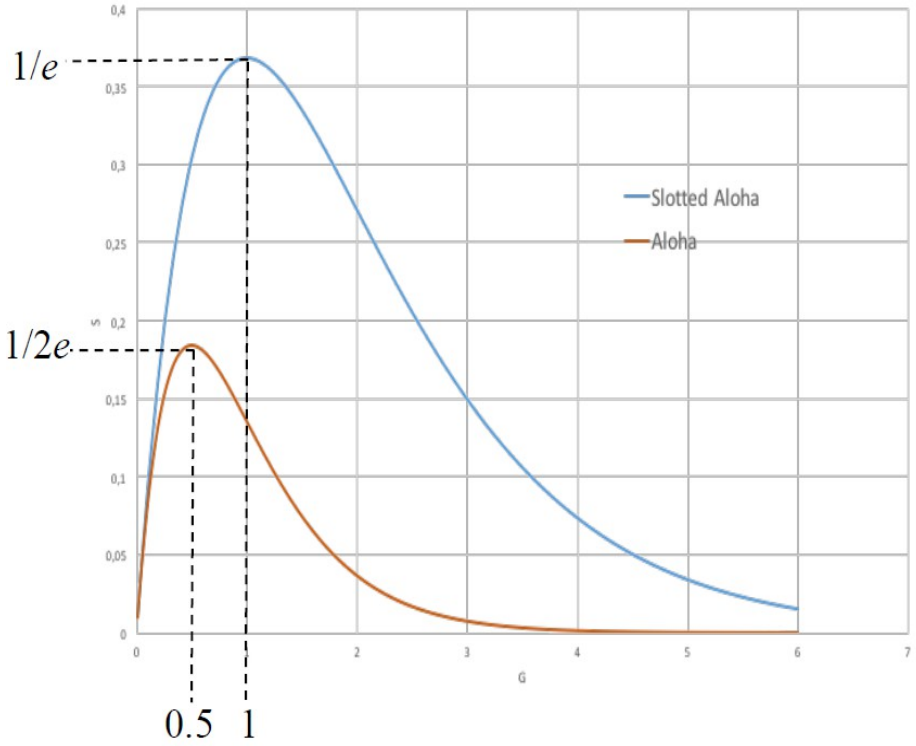
- possibile trasmettere in un istante qualsiasi
- senza slot la collisione è più probabile
- minore efficienza

$$S = Ge^{-2G}$$

Massimo in

$G = 0.5$

$S = 1/2e \cong 0.18$



CSMA: CARRIER SENSE MULTIPLE ACCESS

- fino ad ora, abbiamo assunto che nessuna coppia di nodi che utilizzi il canale condiviso possa capire se l'altro nodo sta trasmettendo sulla linea condivisa
- questa assunzione è:
  - vera per reti satellitari, come Aloha
  - non vera per reti cablate, come Ethernet
  - può essere vera o meno per reti wireless (hidden terminals)
- la capacità di "ascoltare" il canale, prima di trasmettere può essere utilizzata per ridurre il numero di collisioni e migliorarne l'utilizzazione
- carrier sense "percepire il canale":
  - un nodo, prima di trasmettere, "ascolta" il canale per analizzare se il livello il voltaggio o il livello del segnale è più alto che nel caso in cui il canale non sia utilizzato
  - se il canale è occupato, il nodo ritarda la sua trasmissione fino a che non trova il canale libero

CSMA: CARATTERISTICHE

- "Ascolta prima di parlare e mentre parli"
  - rivela le collisioni ed interrompe la trasmissione
  - un nodo ascolta il canale prima di trasmettere
  - dopo l'inizio della trasmissione il nodo continua ad ascoltare il canale per rivelare le collisioni
  - se viene rivelata una collisione, tutti i nodi coinvolti interrompono la trasmissione e rischedulano dopo un intervallo di backoff
- nel protocollo CSMA, una collisione comporta un periodo di inutilizzazione del canale uguale a al tempo di trasmissione di una frame
- il protocollo CSMA-CD riduce la durata delle collisioni e quindi aumenta l'efficienza

CSMA/CD

- CSMA/CD: carrier sensing/Collision Detection
  - individuazione veloce di collisioni
  - veloce abort delle trasmissioni che hanno dato origine a collisione, riduzione dello spreco di banda e di tempo
- collision detection semplice per wired broadcast LAN
  - confronto tra il segnale spedito e quello ricevuto
- sulle reti wireless è sostanzialmente impossibile rilevare un segnale "aggiuntivo" rispetto a quello trasmesso
- per reti wireless: CSMA/CA (Collision Avoidance)

CARRIER SENSE ED ETHERNET

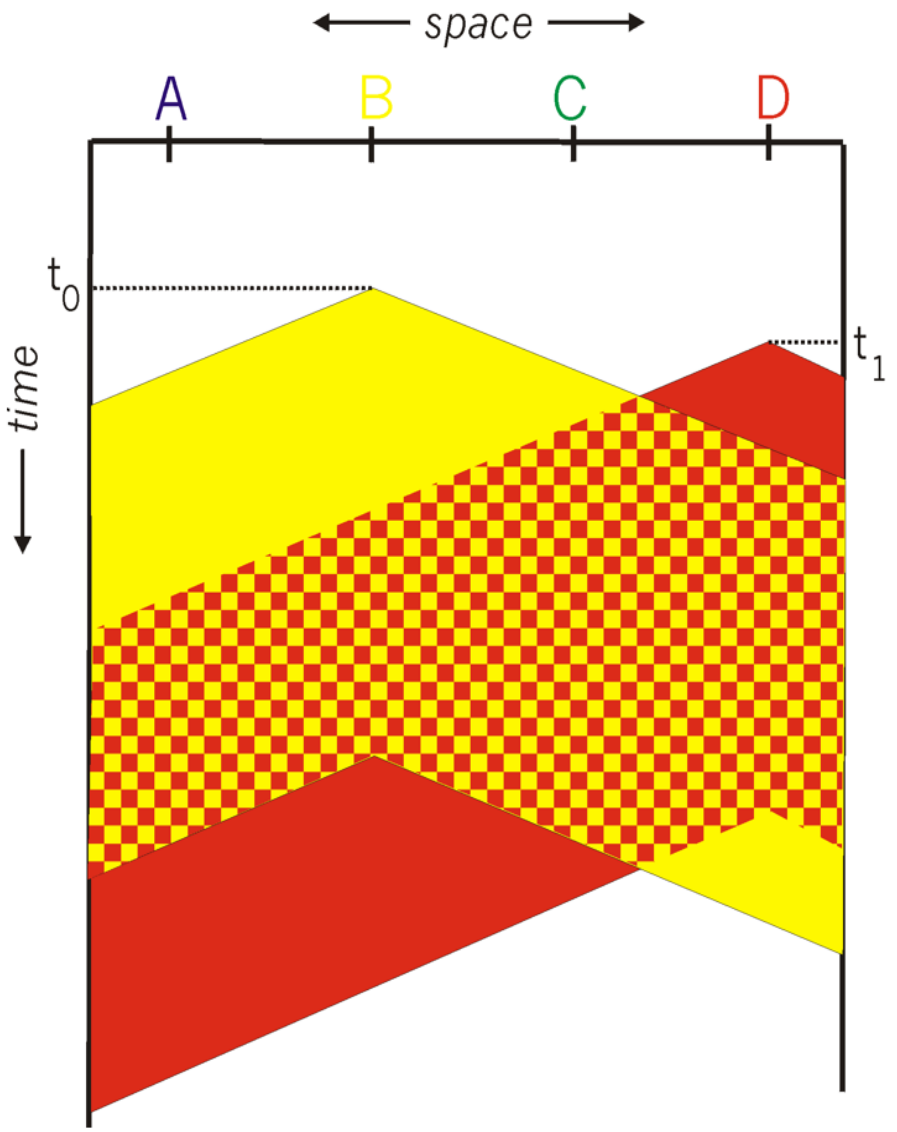
- prima versione di Ethernet
  - una singola linea condivisa (bus)
  - diversi nodi collegati, i nodi inviano pacchetti su questa linea
- ultime versioni di Ethernet: switched base Ethernet
  - utilizzano uno switch, a cui sono collegati i nodi attraverso cavi diversi
  - A può inviare un pacchetto a B e simultaneamente C può inviare un pacchetto a D, se lo switch lo consente
  - una coppia alla volta: solo una coppia sender/receiver può comunicare in ogni istante di tempo
  - la scrittura di più pacchetti nel bus causa la collisione dei pacchetti come in Aloha, i pacchetti interferiscono uno co l'altro a livello di voltaggio elettrico
  - i pacchetti non possono essere ricostruiti

CARRIER SENSE ED ETHERNET

- bus-based Ethernet: un buon esempio di shared communication medium simile ad ALHOA, ma con la capacità aggiuntiva di individuare la trasmissione degli altri utenti
- utilizza un MAC protocol chiamato CSMA/CD (Carrier Sense Multiple Access with Collision Detection).
- prima di trasmettere un pacchetto, un utente connesso ad Ethernet, verifica se il mezzo è libero oppure occupato nella trasmissione di altri pacchetti
  - se è occupato, il nodo continua ad effettuare il "sensing" del canale finchè verifica che il canale è libero
  - quando il canale è libero, il nodo trasmette il primo bit del pacchetto e verifica se questo bit ha provocato la collisione con il pacchetto spedito da un altro utente
  - se rileva una collisione, il nodo "si tira indietro", e non tenta di trasmettere il pacchetto per un intervallo di tempo scelto casualmente

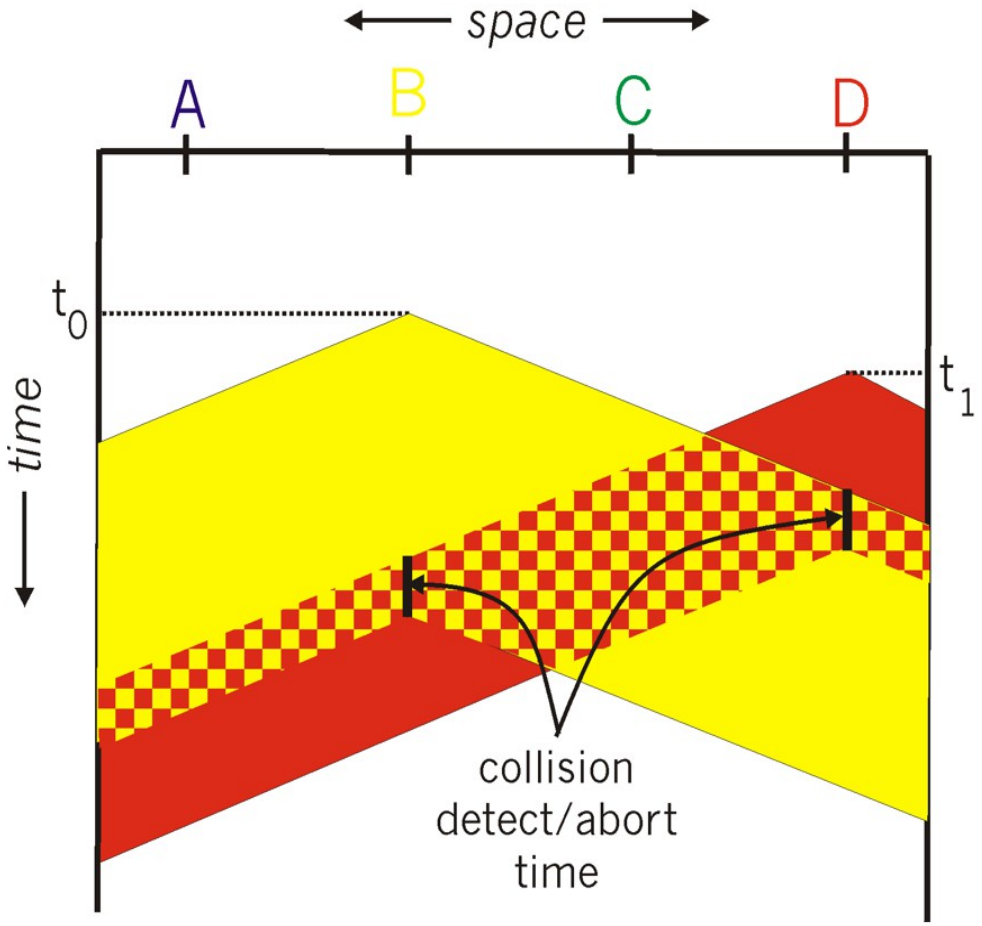
CSMA: COLLISIONI

- questo elimina completamente le collisioni?
  - no, a causa del ritardo di propagazione diverso da 0.
- CSMA riduce, ma non elimina le collisioni!



CSMA/CD: COLLISIONI

- **B** e **D** possono individuare la collisione
- affinchè questo funzioni, sono necessarie restrizioni sulla:
  - dimensione minima dei pacchetti
  - massima distanza tra i nodi
- Perchè questo è necessario?



LIMITI SU CSMA/CD

- la latenza dipende dalla lunghezza del link fisico
  - tempo per propagare il pacchetto da un capo all'altro del link (latenza massima)
- supponiamo che A invii un pacchetto al tempo t
  - B osserva una linea libera fino al tempo t+d
    - ….quindi può iniziare ad inviare un pacchetto..
  - nel caso pessimo, A rileva la collisione fino al tempo t+2d

LIMITI SU CSMA/CD

- A deve aspettare un tempo 2d per individuare la collisione
- per tutto questo periodo A deve continuare a monitorare il canale
  - ...con un occhio alle possibili collisioni
  - motivo: la stazione di trasmissione, una volta che l'intero frame è stato inviato, non ne tiene copia e non controlla più il mezzo trasmissivo per rilevare eventuali collisioni
  - vincolo sulla dimensione del frame

CSMA/CD: UN ESEMPIO

- una rete che utilizza il CSMA/CD ha una ampiezza di banda di 10 Mbps. Se il tempo di propagazione massimo (compresi i ritardi nei dispositivi) è 25,6 μsec, quale è la dimensione minima del frame?
- Il tempo di trasmissione minima del frame è $T_{fr} = 2 \times T_p = 51{,}2$ μsec
- nel peggiore dei casi, la stazione deve trasmettere per un periodo di 51,2 μsec per rilavare la collisione
- la dimensione minima del frame è quindi 10 Mbps × 51,2 μsec = 512 bit o 64 bytes
- questa è proprio la dimensione del frame nell' Ethernet standard.

LIMITI SU CSMA/CD

- tempo perso nelle collisioni
  - proporzionale alla distanza d
- tempo necessario per trasmettere un pacchetto
  - lunghezza del pacchetto p diviso la banda b
- stima approssimativa dell'efficienza (K costante)

$$E \sim \frac{\frac{p}{b}}{\frac{p}{b} + Kd}$$

- nota:
  - per pacchetti di grosse dimensioni, e piccole distanze, E ~ 1
  - all'aumentare della banda, E diminuisce
  - ragione per cui tutte le LAN ad alta banda sono attualmente switched LAN

CONCLUSIONI

- Carrier sense
  - "Listen before speaking, and don't interrupt"
  - controllare se qualche altra stazione sta inviando dei dati
  - ….ed attendere fino a l'altra stazione non ha terminato la trasmissione dei dati
- Collision Detection
  - "If someone else starts talking at the same time, stop"
    - assicurarsi che tutti conoscano che c'è una collisione!
  - determinare se due nodi stanno trasmettendo nello stesso istante
    - ….controllando sei dati sulla linea sono corrotti.
- Randomness
  - "non riniziare a parlare immediatamente"
  - aspettare un intervallo di tempo casuale prima di riprovare a trasmettere

CONCLUSIONI: CANALI CONDIVISI

Cosa si può fare con un canale condiviso ?

- suddivisione del canale per: tempo, frequenza, codice.
  - TDM, FDM
- accesso casuale
  - ALOHA, Slotted ALOHA, CSMA, CSMA/CD
  - rilevamento delle collisioni: facile in alcune tecnologie (cablate), difficile in altre (wireless)
  - CSMA/CD usato in Ethernet
  - CSMA/CA (da vedere) usato in 802.11
- ad accesso controllato
  - polling con un nodo principale; a passaggio di token
  - Bluetooth, FDDI, IBM Token Ring

MAC ADDRESSES

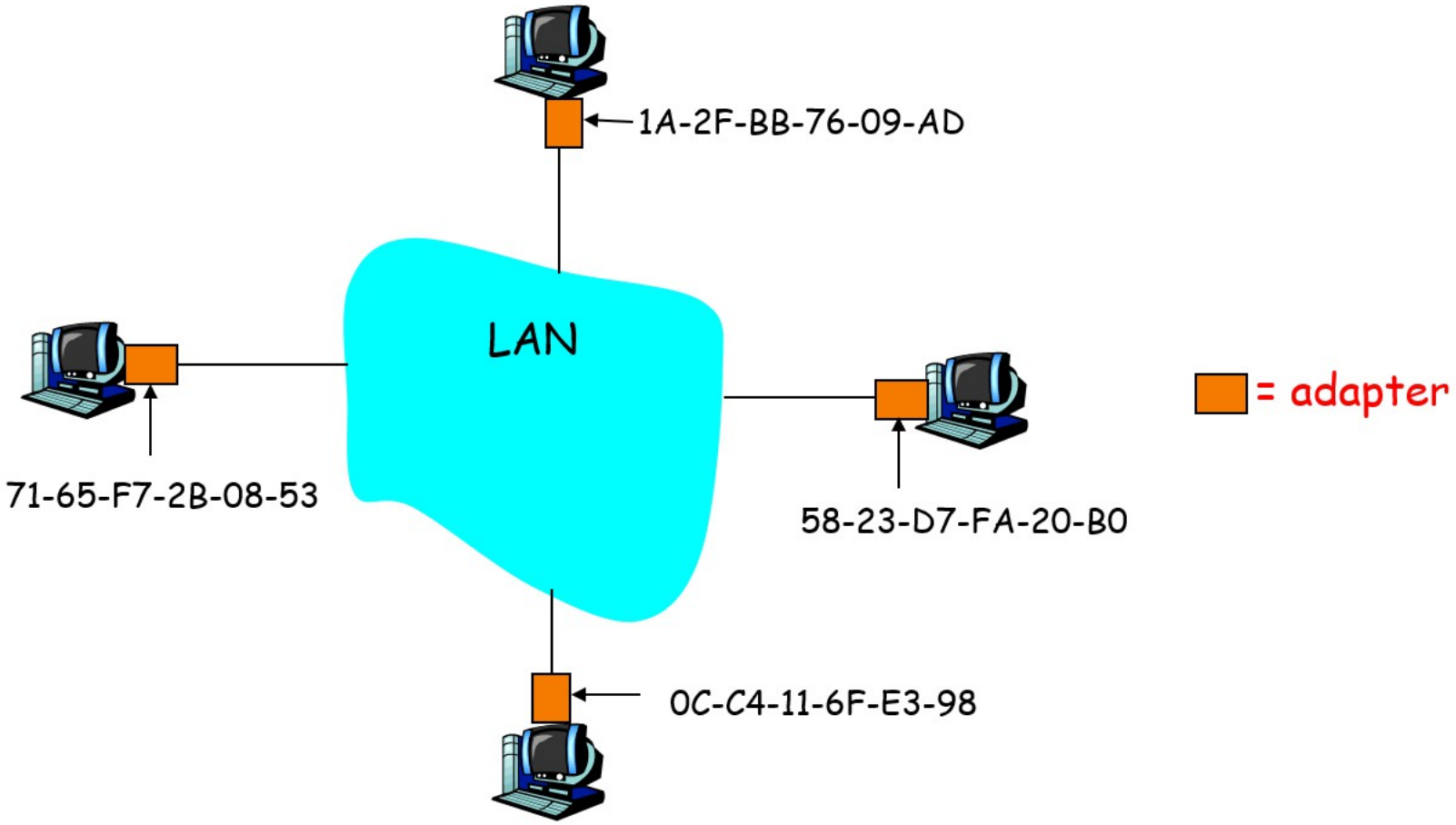
- MAC address
  - indirizzo numerico associato ad un adattatore di rete
  - spazio dei nomi piatto di 48 bits (esempio, 00-15-C5-49-04-A9 in HEX)
  - unico, hard-coded bell'adattatore, quando esso è costruito
- allocazione gerarchica
  - Blocchi: assegnati ai costruttori (esempio, Dell) da IEEE
    - primi 24 bits (esempio, 00-15-C5-**-**-**)
  - Adapter: assegnato dal costruttore e prelevato dal suo blocco di indirizzi
    - ultimi 24 bits
- Indirizzo di Broadcast (FF-FF-FF-FF-FF-FF)
  - per inviare a tutti gli adattatori di una rete

MAC ADDRESS ED IP ADDRESS

- Indirizzo MAC (usato a livello link)
  - Hard-coded nella memoria read-only quando è costruito
  - come un codice fiscale per l'adattatore
  - spazio di indirizzi flat di 48 bits (e.g., 00-0E-9B-6E-49-76)
  - portabile, rimane il solito quandol'host si muove tra reti diverse
  - usato per trasportare pacchetti tra interfacce della stessa rete

- Indirizzi IP
  - configurato, oppure definito automaticamente
  - come un indirizzo di posta
  - spazio di nomi gerarchico di 32 bits (e.g., 12.178.66.9)
  - non portabile e dipende dalla rete a cui l'host è connesso
  - usato per trasporare il pacchetto verso una sottorete Ip

MAC ADDRESS


1A-2F-BB-76-09-AD
LAN
71-65-F7-2B-08-53
58-23-D7-FA-20-B0
= adapter
0C-C4-11-6F-E3-98

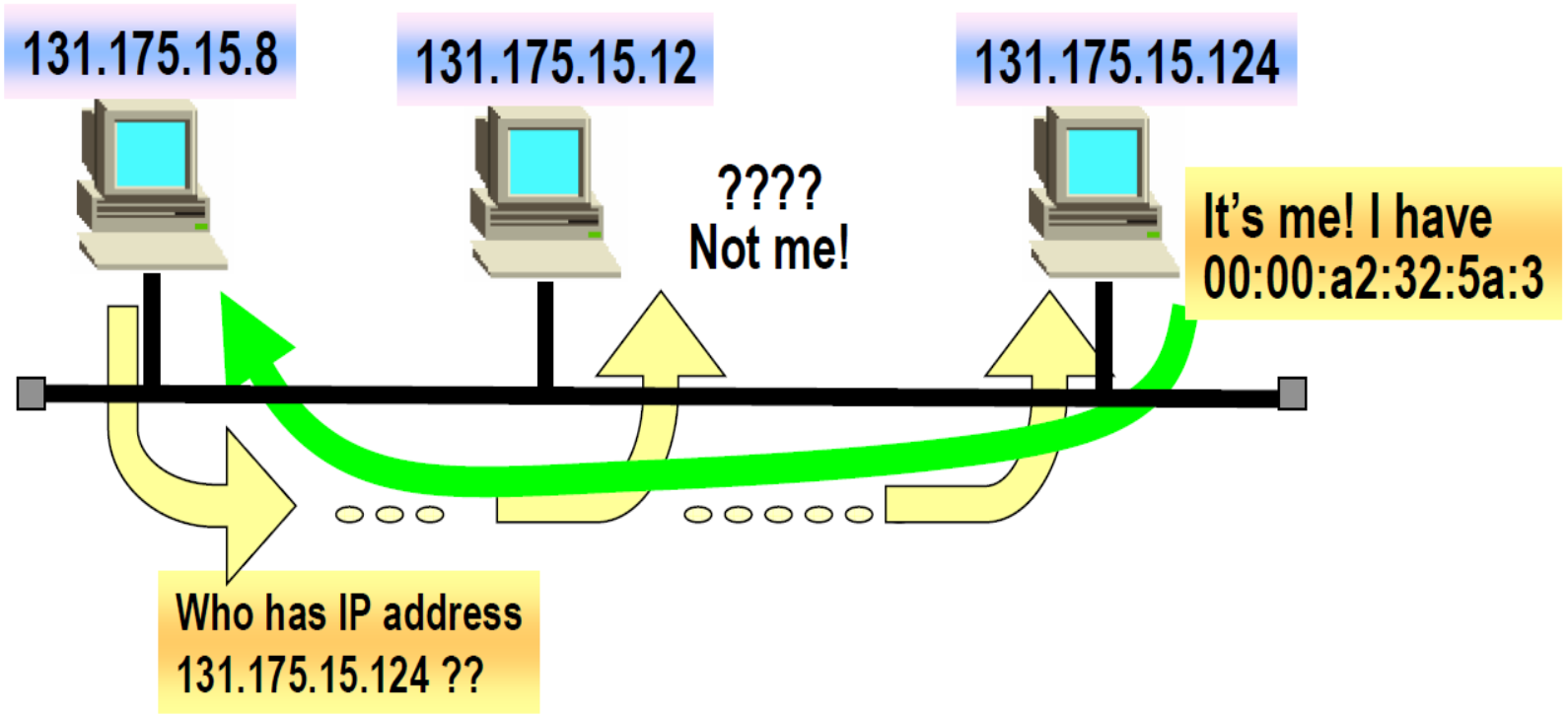
CHI SEI TU? SCOPRIRE IL RICEVENTE

- Address Resolution Protocol (ARP)
  - broadcast "chi ha l'indirizzo IP 1.2.3.6?"
  - risposta "0C-C4-11-6F-E3-98 ha l'indirizzo IP 1.2.3.6!"

ADDRESS RESOLUTION PROTOCOL (ARP)

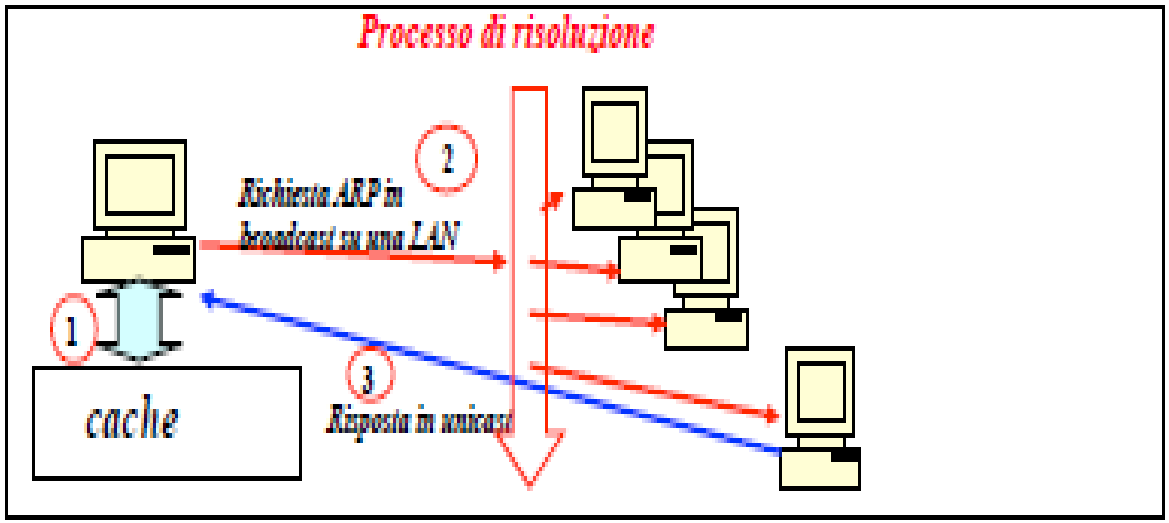
- ogni passo di routing di un pacchetto X ha due possibili risultati:
  - sei arrivato alla destinazione finale: spedisci all'host X
  - non sei arrivato alla destinazione finale: vai tramite l'interfaccia Y del router
- in entrambe i casi si utilizza l'indirizzo IP di un host della rete locale
- come inviare questo indirizzo IP ad un adattatore di una interfaccia di rete
  - gli adattatori sono capaci solo di interpretare gli indirizzi MAC
- necessario un meccanismo che traduca l'indirizzo IP del destinatario nell'indirizzo MAC
- il protocollo ARP si occupa di
  - tradurre un indirizzo IP (indirizzo logico) del destinatario in indirizzo MAC (indirizzo fisico)
  - per poter costruire un frame a livello 2 in cui incapsulare un datagram IP inviato all'indirizzo fisico del destinatario.

ADDRESS RESOLUTION PROTOCOL (ARP)



- il mittente manda in broadcasts: "chi ha l'indirizzo IP 1.2.3.156?"
- il ricevente risponde: "l'indirizzo MAC è 58-23-D7-FA-20-B0"
  - successivamente il pacchetto può essere incapsulato in un frame con quell'indirizzo MAC

ADDRESS RESOLUTION PROTOCOL (ARP)

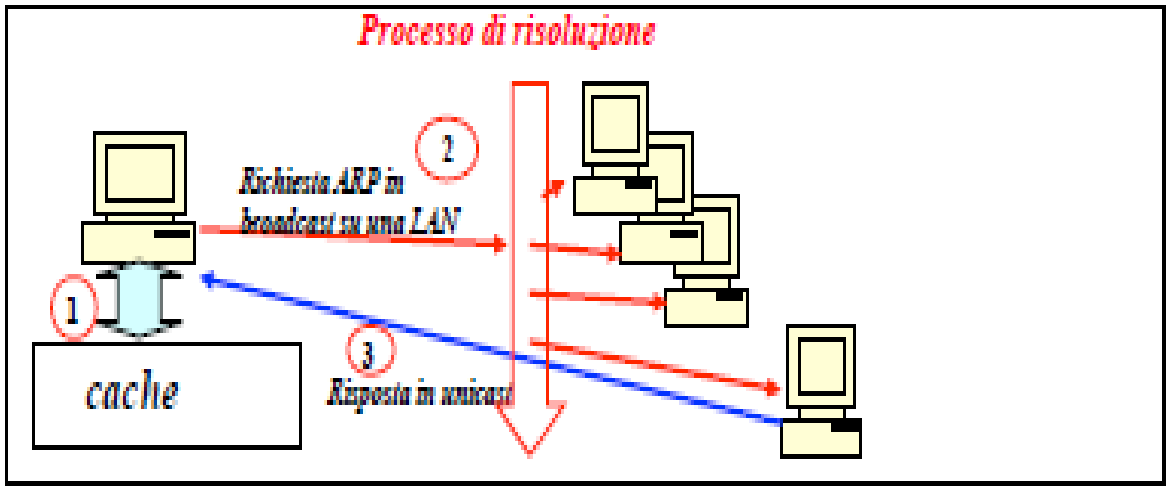


1. Il MAC del destinatario viene cercato nella cache.

2. Se il MAC non è nella cache, si cerca il destinatario con un messaggio ARP con l'indirizzo IP del destinatario in broadcast sulla rete.

3. Il destinatario riceve la richiesta ARP con il proprio indirizzo IP e restituisce *in* unicast al mittente (del quale conosce l'IP ed il MAC) il proprio indirizzo MAC.

ADDRESS RESOLUTION PROTOCOL (ARP)



4. Il mittente memorizza nella propria cache una tabella ARP con le associazioni IP-MAC che conosce
   - tabella ARP mantenuta da ogni nodo

     coppia <IP address, MAC address>
5. Se l'indirizzo IP del destinatario è su un'altra rete, il processo si ripete considerando mittente e ricevente i router delle rispettive reti.

IDEE CHIAVE DI ARP (ED ANCHE DI DHCP)

- broadcasting: usare il broadcast per ottenere l'informazione
  - scalabile a causa della dimensione limitata del messaggio
- caching: ricordare il passato per un periodo limiata
  - memorizza l'informazione che hai appreso per limitare l'overhead
  - ricordati il tuo indirizzo e gli indirizzi degli altri host
- soft state: dopo un pò dimenticati del passato
  - associa un time-to-live alla informazione
  - … e rinfresca o scarta l'informazione
  - proprietà chiave per la robustezza