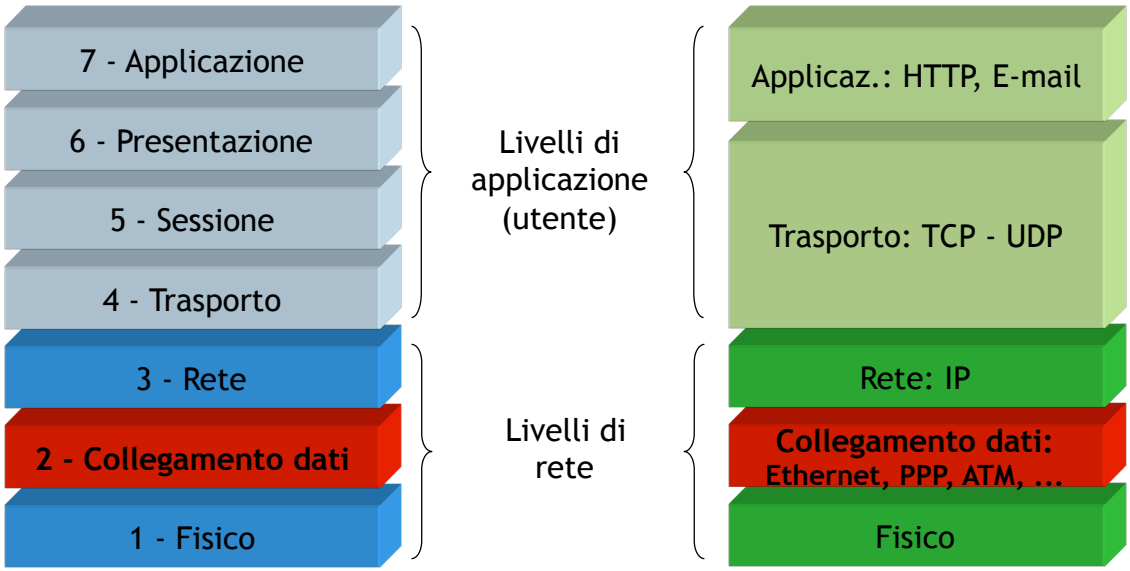
Reti di Calcolatori

Il livello Data Link

Università degli studi di Verona
Dipartimento di Informatica

Docente: Damiano Carra

Livello Data Link



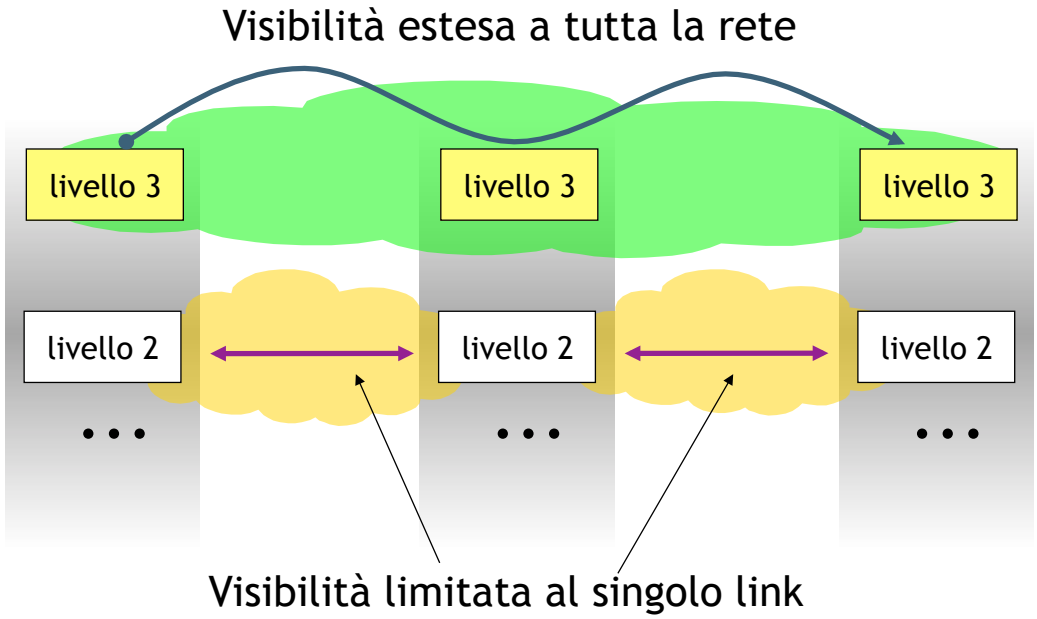
Livello Data Link

- Obiettivo principale: fornire al livello di rete di due macchine adiacenti un ***canale di comunicazione*** il più possibile affidabile.
  - macchine adiacenti → fisicamente connesse da un canale di comunicazione (es. un cavo coassiale, doppino telefonico)
  - canale di comunicazione → "tubo digitale", ovvero i bit sono ricevuti nello stesso ordine in cui sono inviati
- Per compiere questo obiettivo, come tutti i livelli OSI, il livello 2 offre dei servizi al livello superiore (livello di rete) e svolge una serie di funzioni
- Problematiche: il canale fisico non è ideale
  - errori di trasmissione tra sorgente e destinazione
  - necessità di dover gestire la velocità di trasmissione dei dati
  - ritardo di propagazione non nullo

Tipologia di servizi offerti al livello superiore

- Servizio connectionless senza acknowledge
  - non viene attivata nessuna connessione
  - invio delle trame senza attendere alcun *feedback* dalla destinazione
    - Se una trama viene persa non ci sono tentativi per recuperarla, il compito viene lasciato ai livelli superiori
  - ***la maggior parte delle LAN utilizzano questa tipologia di servizio***
- Servizio connectionless con acknowledge
  - non viene attivata nessuna connessione
  - ogni trama inviata viene "riscontrata" in modo individuale
- Servizio connection-oriented con acknowledge
  - viene attivata una connessione e, al termine del trasferimento, essa viene abbattuta
  - ogni trama inviata viene "riscontrata" in modo individuale

Visibilità della rete del livello 2



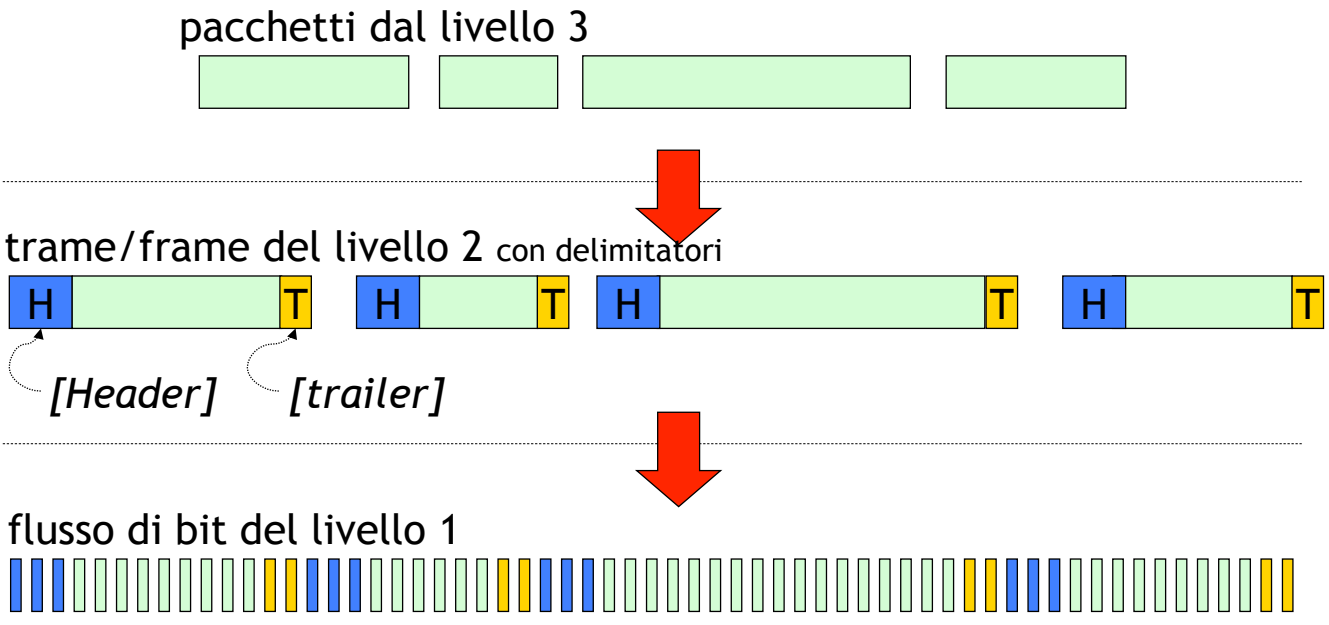
Funzioni di competenza del livello 2

- Le principali funzioni svolte dal livello 2 sono:
  - framing
    - delimitazione delle trame
  - rilevazione/gestione errori
    - controlla se la trama contiene errori ed eventualmente gestisce il recupero
  - controllo di flusso
    - gestisce la velocità di trasmissione

Framing

- Il livello 2 riceve dal livello superiore (rete) dei pacchetti
- Considerando che:
  - la lunghezza dei pacchetti (di livello 3) e delle corrispondenti trame (livello 2) è variabile
  - i sistemi non sono sincronizzati tra loro, ovvero non hanno un orologio comune che segna la stessa ora per tutti
  - il livello 1 tratta solo bit, e quindi non è in grado di distinguere se un bit appartiene ad una trama o a quella successiva
- ... nasce il problema della ***delimitazione delle trame***
- La funzionalità di *framing* (frame = trama) è dunque di rendere distinguibile una trama dall'altra attraverso l'utilizzo di opportuni codici all'inizio e alla fine della trama stessa

Esempio

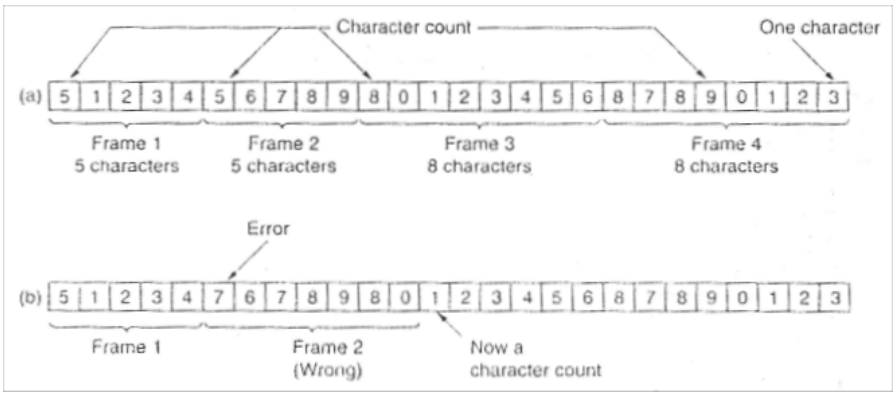


Modalità di Framing

- Esistono diverse tecniche per implementare il framing:
  - inserire intervalli temporali fra trame consecutive
    - problema: per natura intrinseca le reti di telecomunicazione non danno garanzie sul rispetto delle caratteristiche temporali delle informazioni trasmesse
    - gli intervalli inseriti potrebbero essere espansi o ridotti generando problemi di ricezione
  - marcare inizio e termine di ogni trama
    1. Character count
    2. Starting and ending flags (bit stuffing)

Framing: Character Count

- Un campo nell'header del frame indica il numero di 'caratteri' nel frame stesso



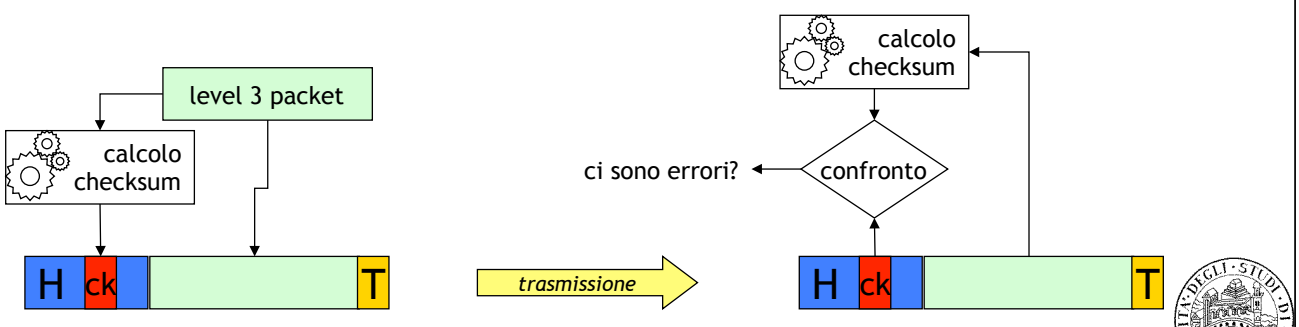
(fonte A.Tanenbaum, Computr Networks)

Framing: Bit Stuffing

- Ogni trama può includere un numero arbitrario di bit
- Ogni trama inizia e termina con uno speciale pattern di bit, 01111110, chiamato **byte di flag**
- Problema: come comportarsi se la trama contiene al suo interno il pattern di bit usato per il byte di flag?
- Soluzione:
  - Se la sorgente incontra 5 bit "1" consecutivi, aggiunge uno "0"
    - **bit stuffing**
    - es. la sequenza "011111x" è trasmessa come "0111110x", dove "x" e' il bit successivo, puo' essere sia "0" che "1"
  - Se la destinazione incontra 5 bit "1" consecutivi, toglie uno "0"
    - es. la sequenza "0111110x" è modificata in "011111x"

Rilevazione dell'errore

- Il livello fisico offre un canale di trasmissione ***non privo di errori***
  - errori sul singolo bit
  - replicazione di bit
  - perdita di bit
- Per la rilevazione di tali errori, nell'header di ogni trama il livello 2 inserisce un campo denominato **checksum**
  - il checksum è il risultato di un calcolo fatto utilizzando i bit della trama
  - la destinazione ripete il calcolo e confronta il risultato con il checksum: se coincide la trama è corretta



Gestione del flusso

- Problema: la sorgente trasmette le trame ad una velocità superiore di quella che la destinazione utilizza per accettare l'informazione
  - conseguenza: congestione del nodo destinazione
- Soluzione: implementare il **controllo di flusso**
- Il controllo della velocità di trasmissione della sorgente è basato su feedback inviati alla sorgente dalla destinazione indicando
  - di bloccare la trasmissione fino a comando successivo
  - la quantità di informazione che la destinazione è ancora in grado di gestire

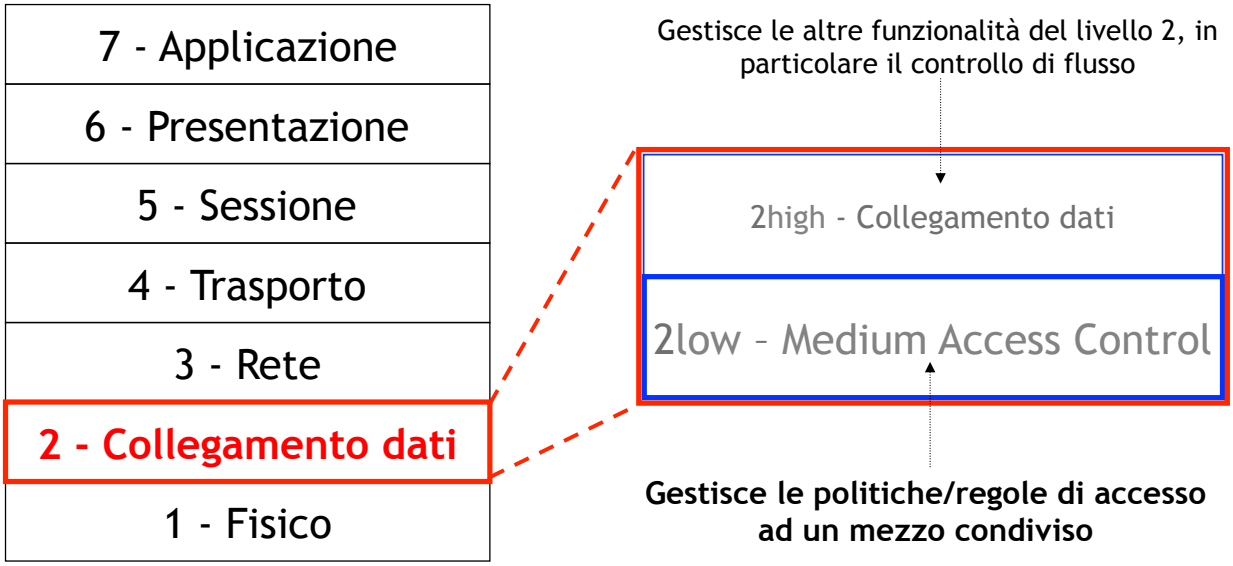
- Nelle reti TCP/IP il controllo di flusso e il recupero degli errori è demandato ai livelli superiori

Il sotto-livello MAC

Introduzione di un nuovo sotto-livello

- Abbiamo visto che il livello 2 gestisce un insieme di problematiche svolgendo le funzioni di framing, rivelazione degli errori, controllo di flusso
- Bisogna considerare però che il livello 2 ha a che fare con il livello 1, ovvero il livello fisico (direttamente collegato al mezzo fisico)
- Il mezzo fisico può essere:
  - dedicato (reti punto-punto)
  - condiviso (reti broadcast)
- Se il mezzo fisico è condiviso, nascono una serie di problematiche relative all'accesso a tale mezzo
  - selezione dell'host che ha il diritto di trasmettere sul mezzo condiviso
  - situazione di competizione per la risorsa trasmissiva
- Viene introdotto un sotto-livello al livello 2 che gestisce queste problematiche
  - **MAC (Medium Access Control)**

Livello MAC



NOTA: anche se in linea di principio il livello MAC gestisce *l'accesso al mezzo* e il livello "high" gestisce le altre funzionalità, nella pratica il livello MAC gestisce anche il framing e il controllo di errore, mentre il livello 2 "high" si occupa del *controllo di flusso*. Nello stack TCP/IP ove il livello 2 non fa controllo di flusso, il livello 2 "high" è completamente assente o, se c'è, non svolge nessuna funzione

Definizione del problema

- Per mezzo ***condiviso*** si intende che un unico canale trasmissivo può essere usato da più sorgenti
  - esempio: stanza piena di persone che vogliono parlare tra di loro
    - se tutti parlano contemporaneamente, non potrà esserci scambio di informazione
    - l'opposto è avere un mezzo dedicato per ogni coppia di persone che vuole parlare (ad esempio un tubo o una coppia di walkie-talkie)
- E' necessario definire una serie di regole per poter utilizzare il mezzo (tecniche di allocazione del canale)
  - se due sorgenti parlano contemporaneamente vi sarà collisione è l'informazione andrà persa

Tecniche di allocazione del canale

- Esistono due categorie in cui rientrano le tecniche di allocazione del canale trasmissivo
  - allocazione statica
    - il mezzo trasmissivo viene "partizionato" e ogni porzione viene data alle diverse sorgenti
    - il partizionamento può avvenire in base:
      - al tempo: ogni sorgente ha a disposizione il mezzo per un determinato periodo
      - alla frequenza: ogni sorgente ha a disposizione una determinata frequenza (si pensi alle stazioni radiofoniche ove il canale trasmissivo è l'aria...)
  - allocazione dinamica
    - il canale viene assegnato di volta in volta a chi ne fa richiesta e può essere utilizzato una volta che questi ha finito di usarlo e lo libera

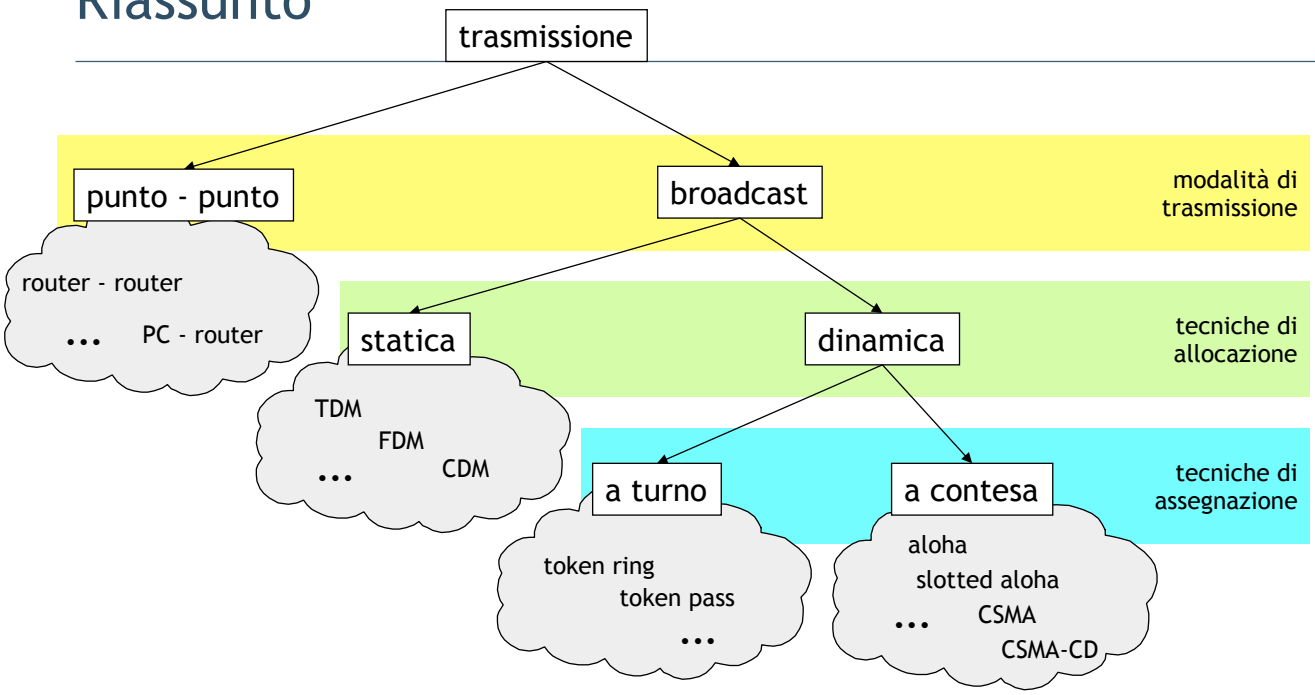
Allocazione statica

- Soluzioni “tradizionali”
  - Frequency Division Multiplexing
  - Time Division Multiplexing
- Buona efficienza in situazioni di ***pochi utenti con molto carico costante nel tempo***
- Meccanismi di semplice implementazione (FDM)
- Tuttavia...
  - molti utenti
  - traffico discontinuo
- ...generano una scarsa efficienza di utilizzo delle risorse trasmissive
  - le risorse dedicate agli utenti “momentaneamente silenziosi” sono perse

Allocazione dinamica

- Il canale trasmissivo può essere assegnato:
  - a turno
    - viene distribuito il “permesso” di trasmettere; la durata viene decisa dalla sorgente
  - a contesa
    - ciascuna sorgente prova a trasmettere indipendentemente dalle altre
- Nel primo caso si presuppone la presenza di meccanismi per l’assegnazione del permesso di trasmettere
  - overhead di gestione
- Nel secondo caso non sono previsti meccanismi particolari
  - sorgente e destinazione sono il più semplici possibile
- I protocolli che gestiscono la trasmissione a contesa sono generalmente i più utilizzati

Riassunto



In generale: se le risorse sono scarse rispetto alle esigenze delle stazioni (tante stazioni con molti dati), un accesso statico (*multiplazione*) è preferibile; viceversa, ovvero con tante risorse rispetto alle necessità delle stazioni e traffico generato discontinuo, l'allocazione dinamica (*accesso multiplo*) risulta più efficiente

Allocazione dinamica con contesa: ipotesi

- Analizziamo in dettaglio le prestazioni ottenibili da protocolli (protocollo: insieme di regole...) progettati per gestire l'allocazione dinamica del canale con contesa della risorsa. Seguono una serie di ipotesi per semplificare il problema

1. **Single channel assumption**
   - unico canale per tutte le comunicazioni
2. **Station model**
   - *N* stazioni indipendenti ognuna delle quali è sorgente di trame di livello 2
   - le trame sono generate secondo la distribuzione di Poisson con media **S**
   - la lunghezza delle trame è fissa, ovvero il tempo di trasmissione è costante e pari a **T** (tempo di trama)
   - una volta generata una trama, la stazione è bloccata fino al momento di corretta trasmissione
3. **Collision assumption**
   - due trame contemporaneamente presenti sul canale generano collisione
   - non sono presenti altre forme di errore
4. **Tempo...**
   - continuo: la trasmissione della trama può iniziare in qualunque istante
   - *slotted*: la trasmissione della trama può iniziare solo in istanti discreti
5. **Ascolto del canale...**
   - *carrier sense*: le stazioni sono in grado di verificare se il canale è in uso prima di iniziare la trasmissione di una trama (questo equivale a dire che il tempo di propagazione t è =< T)

Protocolli di accesso multiplo

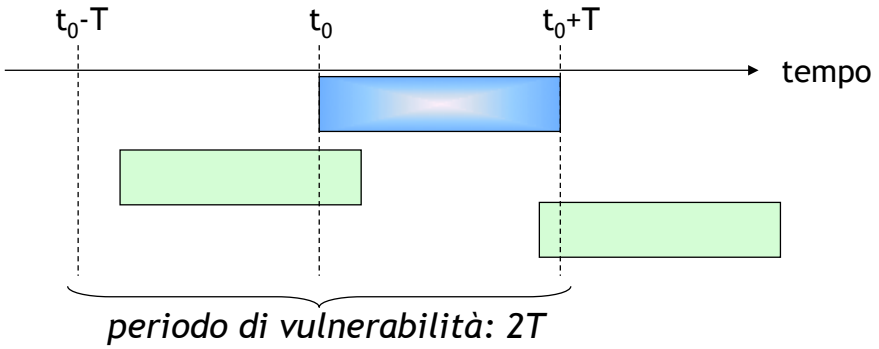
- In letteratura sono disponibili molti algoritmi di accesso multiplo al mezzo condiviso con contesa
- Principali algoritmi (utilizzati dai protocolli):
  - ALOHA
    - Pure ALOHA
    - Slotted ALOHA
  - Carrier Sense Multiple Access Protocols
    - CSMA
    - CSMA-CD (con rilevazione della collisione)

Pure ALOHA

- Definito nel 1970 da N. Abramson all'università delle Hawaii
- Algoritmo:
  - una sorgente può trasmettere una trama ogniqualvolta vi sono dati da inviare *(continuous time)*
  - la sorgente rileva, ascoltando il canale, l'eventuale collisione
  - collisione ⇨ la sorgente aspetta un tempo casuale e ritrasmette la trama
    - un tempo deterministico porterebbe ad una situazione di collisione all'infinito

Periodo di vulnerabilità

- Si definisce "periodo di vulnerabilità" l'intervallo di tempo in cui può avvenire una collisione che invalida una trasmissione
- Detto T il tempo di trama e t_0 l'inizio della trasmissione da parte di una sorgente, il periodo di vulnerabilità è pari al doppio del tempo di trama
  - nel momento in cui inizia a trasmettere (t_0), nessuna altra sorgente deve aver iniziato la trasmissione dopo l'istante di tempo t_0 -T e nessuna altra sorgente deve iniziare la trasmissione fino a t_0 +T



Prestazioni

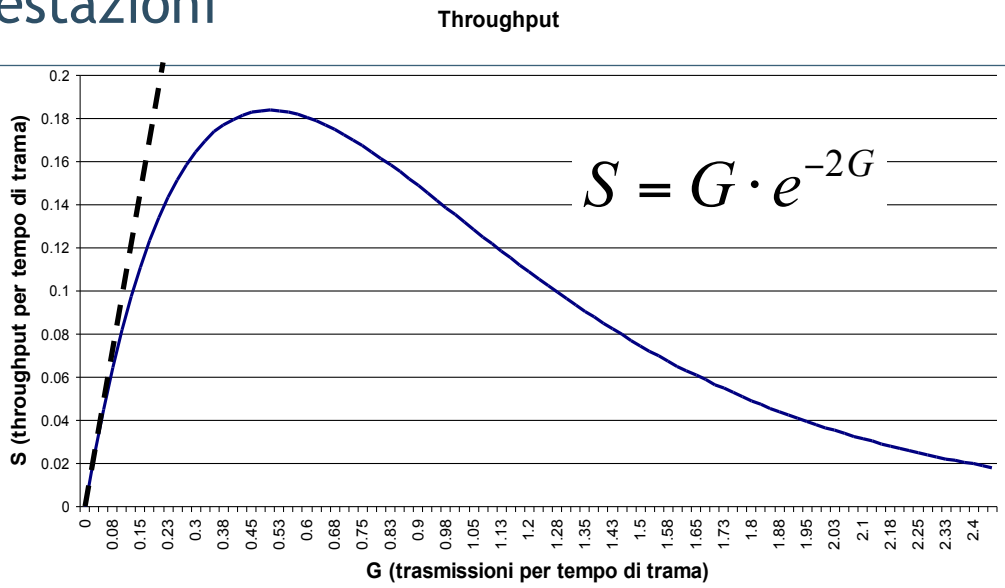
- Ipotesi
  - trame di lunghezza fissa
  - tempo di trama: tempo necessario per trasmettere una trama
  - popolazione ∞ che accede ad un mezzo condiviso
- Traffico generato (numero di trame per tempo di trama) segue la distribuzione di Poisson con media G
  - G ingloba anche il numero di ri-trasmissioni dovuto a collisioni
- Il throughput reale è dato da
  - numero medio di trasmissioni * probabilità che non ci siano trasmissioni per tutto il periodo di vulnerabilità (2 tempi di trama consecutivi)

    → S = G*P[0 trasmissioni per 2T], ovvero

$$S = G \cdot e^{-2G}$$

G = numero medio di trame trasmesse nel tempo di trama
S = numero medio di trame trasmesse con successo (throughput)

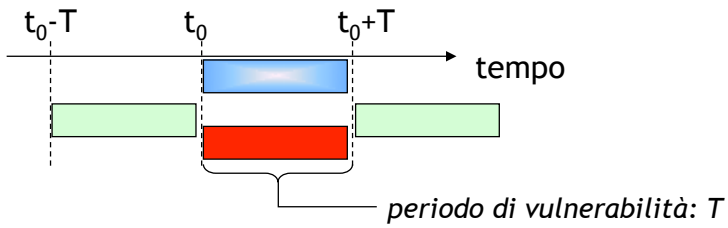
Prestazioni



- ALOHA permette al massimo di sfruttare il 19% degli slot liberi (nel caso in cui mediamente vengono generati 0.5 trasmissioni per tempo di trama)

Slotted ALOHA

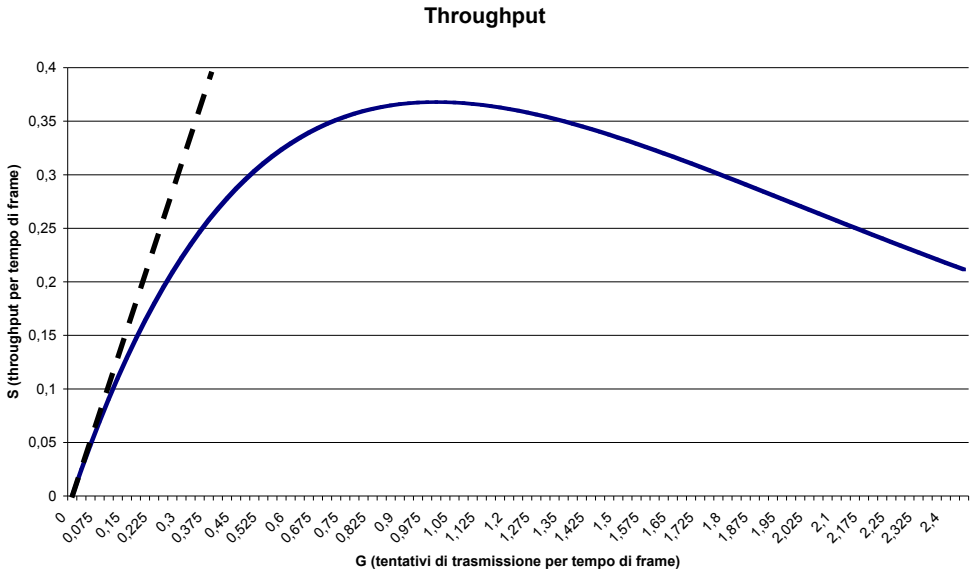
- Proposto nel 1972 da Roberts per duplicare la capacità di Pure ALOHA
- Basato su ipotesi di *slotted time* (tempo suddiviso ad intervalli discreti)
- Algoritmo:
  - Pure ALOHA
  - la trasmissione di una trama può iniziare solo ad intervalli discreti
  - necessaria sincronizzazione tra stazioni
- Periodo di vulnerabilità: T (tempo di trama)



Prestazioni

- Il periodo di vulnerabilità è dimezzato, quindi il throughput reale è dato da

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



- Slotted ALOHA permette al massimo di sfruttare il 37% degli slot liberi (nel caso in cui mediamente viene generata 1 trasmissione per tempo di trama)

Carrier Sense Multiple Access (CSMA)

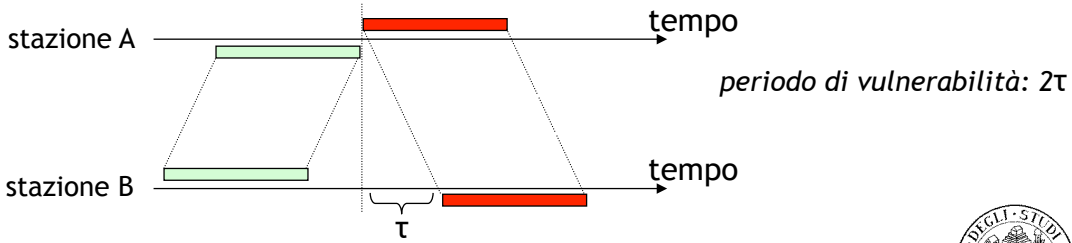
- Ambito LAN: le stazioni possono monitorare lo stato del canale di trasmissione (ritardi bassi)
- Le stazioni sono in grado di "ascoltare" il canale *prima di iniziare a trasmettere* per verificare se c'è una trasmissione in corso
- Algoritmo
  - se il canale è libero, si trasmette
  - se è occupato, sono possibili diverse varianti
    - non-persistent
      - rimanda la trasmissione ad un nuovo istante, scelto in modo casuale
    - persistent
      - nel momento in cui si libera il canale, la stazione inizia a trasmettere
  - se c'è collisione, come in ALOHA, si attende un tempo casuale e poi si cerca di ritrasmettere

CSMA: modalità p-persistent

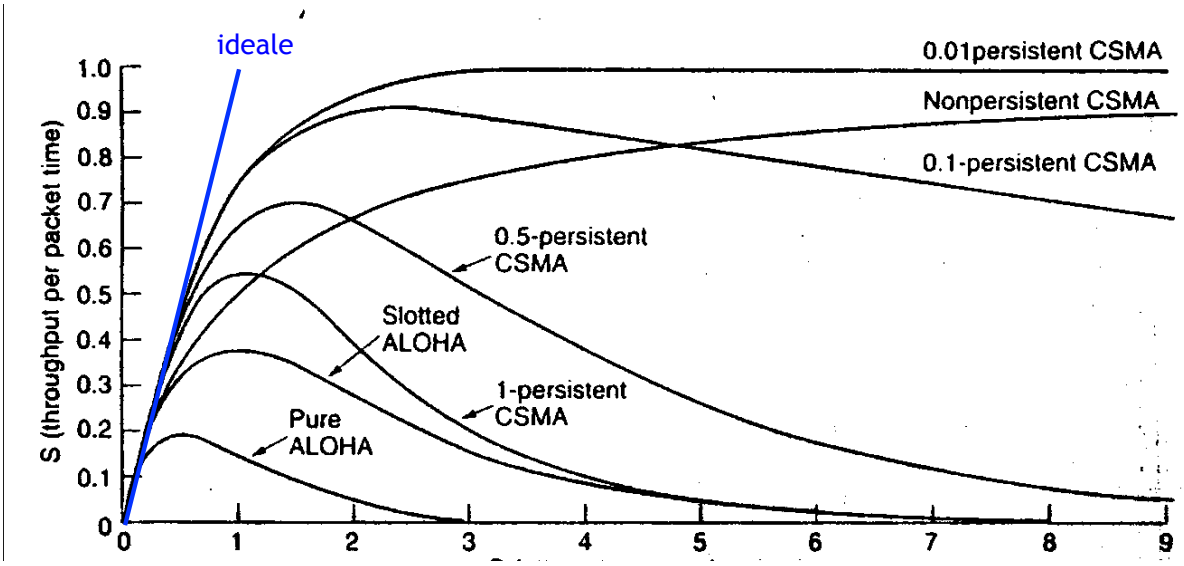
- Il tempo viene suddiviso in intervalli
  - la lunghezza degli intervalli è uguale alal periodo di vulnerabilità
    - *round trip propagation delay* 2τ
- Algoritmo
  1. ascolta il canale
     - se il canale è libero
       - si trasmette con probabilità p;
       - se si è deciso di trasmettere, si passa al punto 2
       - se non si è deciso di trasmettere, si attende un intervallo di tempo e si torna al punto 1
     - se è occupato, si attende un intervallo di tempo e si torna al punto 1
  2. se c'è collisione
     - si attende un tempo casuale e poi si torna al punto 1

Periodo di vulnerabilità

- In questo caso il periodo di vulnerabilità è legato al ritardo di propagazione del segnale (τ)
  - se una stazione ha iniziato a trasmettere, ma il suo segnale non è ancora arrivato a tutte le stazioni, qualcun altro potrebbe iniziare la trasmissione
  - periodo di vulnerabilità → 2τ
- A seconda del ritardo di propagazione, se questi risulta paragonabile al tempo si trama o meno, si hanno prestazioni differenti
- In generale, il CSMA viene usato in reti in cui il ritardo di propagazione τ è << di T (tempo di trama)



Confronto efficienza algoritmi



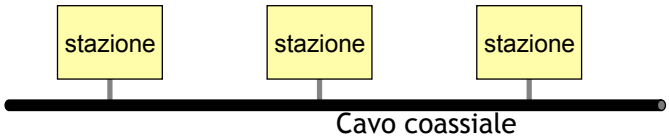
(fonte: A. Tanenbaum, Computer Networks)

CSMA con Collision Detection (CSMA-CD)

- Miglioramento
  - se la stazione che sta trasmettendo rileva la collisione, interrompe immediatamente
- In questo modo, una volta rilevata collisione, non si spreca tempo a trasmettere trame già corrotte
- Inoltre, per far sentire a tutte le stazioni che vi è stata collisione, si trasmette una particolare sequenza, detta di jamming

LAN estese

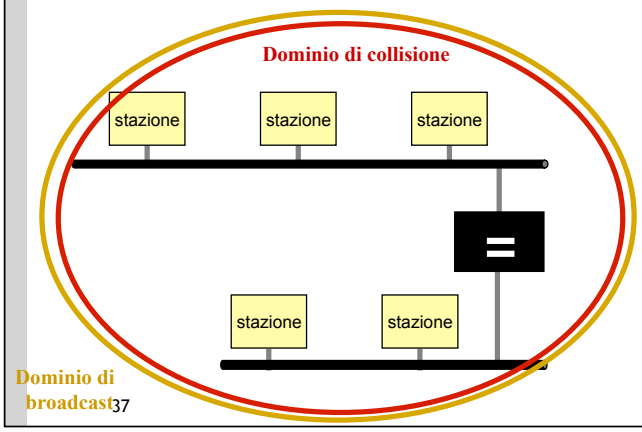
Introduzione

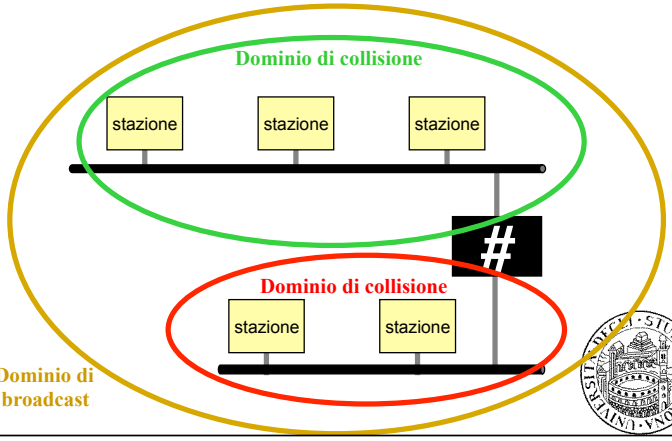


- La scelta di utilizzare mezzi condivisi per l'accesso al canale di trasmissione è stata fatta sia per necessità (ad es. trasmissioni wireless) sia motivi economici
- Grazie proprio agli aspetti economici, tale tecnologia è stata utilizzata e si è diffusa particolarmente nelle *reti locali* (Local Area Networks, LAN)
- La rappresentazione tipica di una LAN è una serie di stazioni (PC) connesse ad un segmento di cavo (bus)
- Poiché il segmento non può essere troppo lungo...
  - attenuazione del segnale
  - disposizione spaziale delle stazioni all'interno di un edificio (ad es.: su più piani)
- ... nasce il problema di come estendere le LAN
- Esistono 3 tipi di apparati, in ordine crescente di complessità:
  - Repeater o Hub
  - Bridge
  - Switch

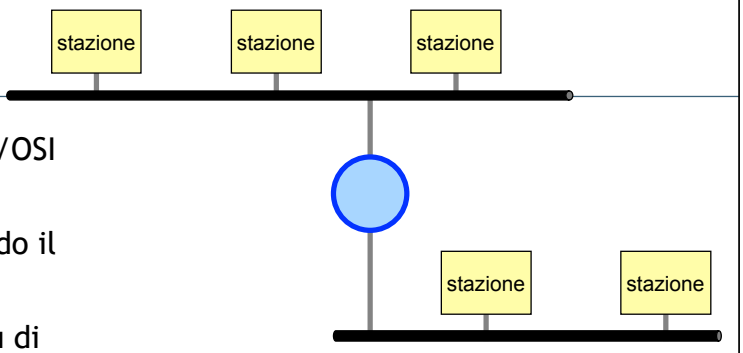
Dominio di collisione – Dominio di broadcast

- Dominio di collisione
  - parte di rete per cui, se due stazioni trasmettono dati contemporaneamente, il segnale ricevuto dalle stazioni risulta danneggiato
- Dominio di broadcast (detto anche *Segmento data-link)*
  - parte di rete raggiunta da una trama con indirizzo broadcast (a livello 2)
- Stazioni appartenenti alla medesima rete di livello 2 condividono lo stesso dominio di broadcast
  - gli apparati che estendo le LAN possono solo influire sul dominio di collisione

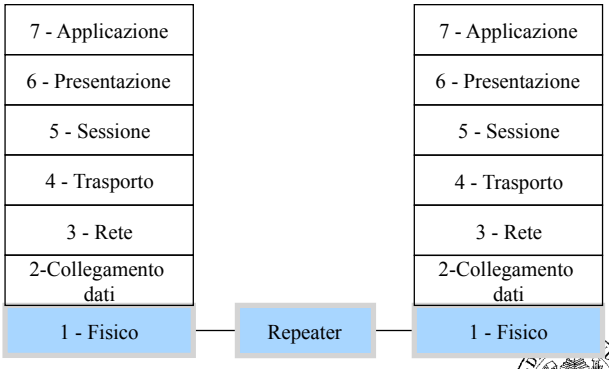




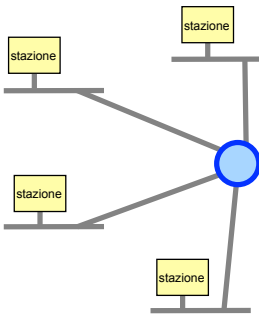
Repeater e Hub



- Interviene solo a livello fisico ISO/OSI
- Replica le trame in arrivo da un segmento ad un altro, amplificando il segnale
- I repeater possono connettere più di due segmenti
  - in questo caso di parla di ***Hub***
    - copia le trame che riceve su una porta su tutte le altre porte
  - il segnale trasmesso da una stazione viene propagato a tutte le uscite
- Non ci possono essere più di 4 repeater in cascata tra due stazioni
- Il dominio di collisione coincide con il dominio di broadcast



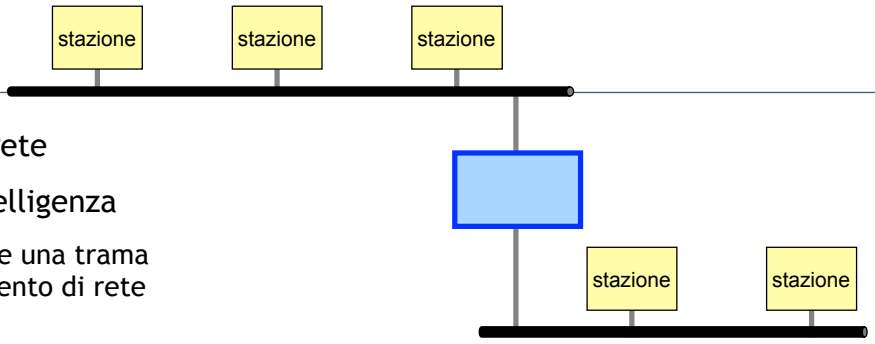
Possibile configurazione



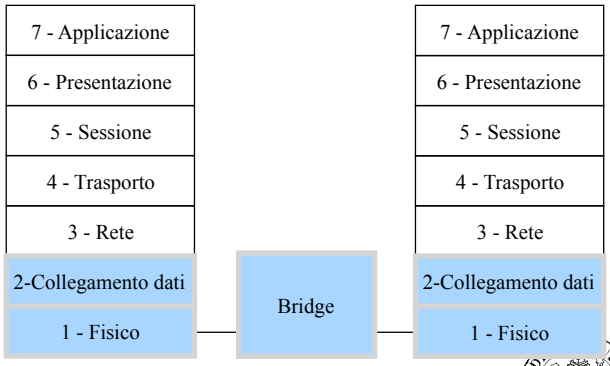
In questa particolare configurazione con l'hub, in cui ogni stazione ha una porta dedicata, viene usato un doppino al posto del cavo coassiale

- Il problema legato a questo tipo di configurazioni è l'eccessiva estensione del dominio di collisione
  - con i repeater è come se tutte le stazioni condividessero lo stesso mezzo fisico

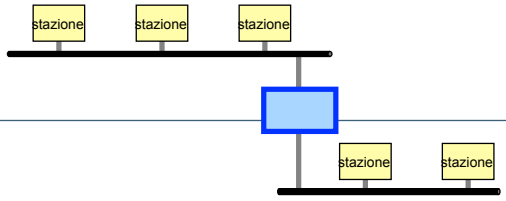
Bridge

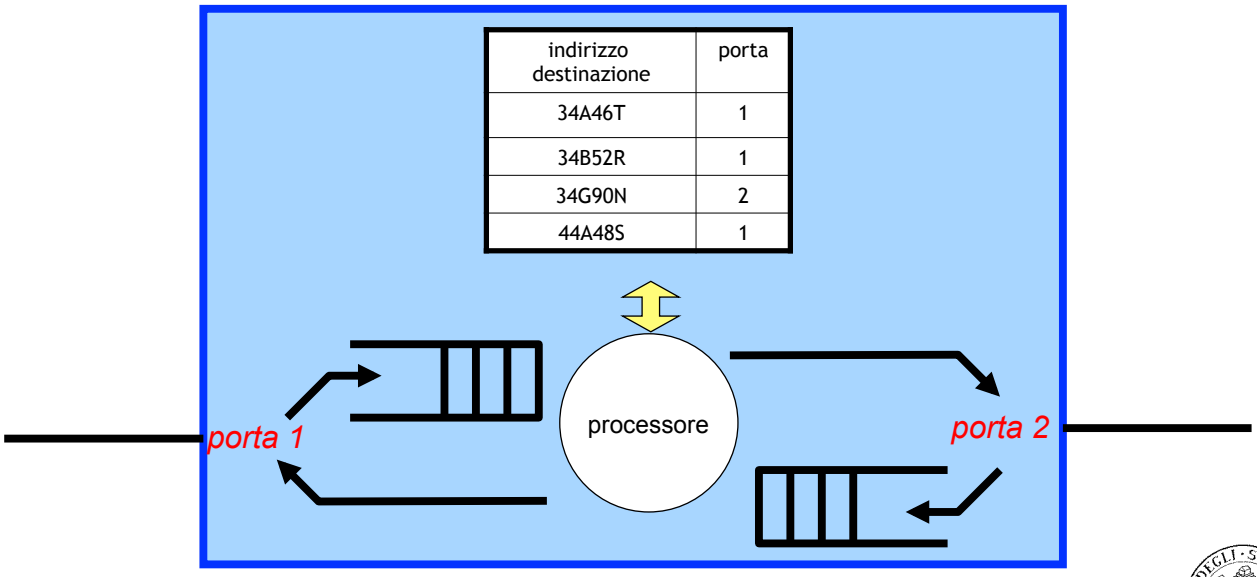


- Collega 2 segmenti di rete
- Apparato dotato di intelligenza
  - seleziona se ripetere una trama generata da un semento di rete sull'altro segmento
  - la selezione avviene in base ad una tabella che esso mantiene
  - in tale tabella c'è scritto quali stazioni fanno parte di ciascun segmento di rete
  - quando viene generata una trama, il bridge legge l'indirizzo di destinazione e in base alla propria tabella decide se propagare la trama nell'altro segmento di rete
- Spezza il dominio di collisione



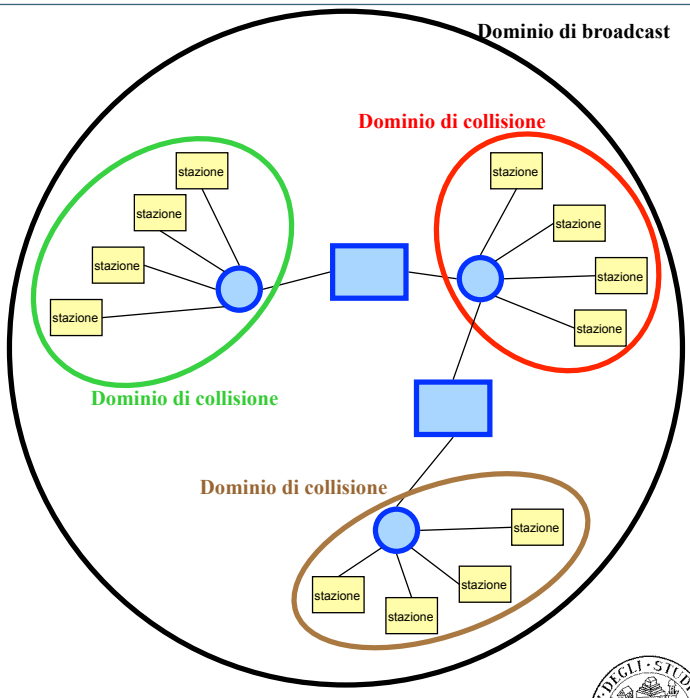
Schema di un bridge





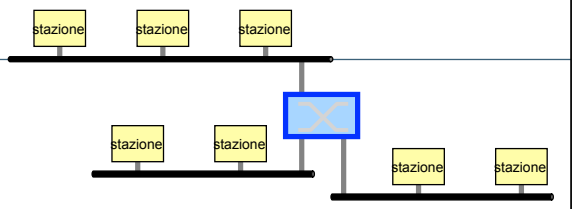
Bridge: esempio di configurazione

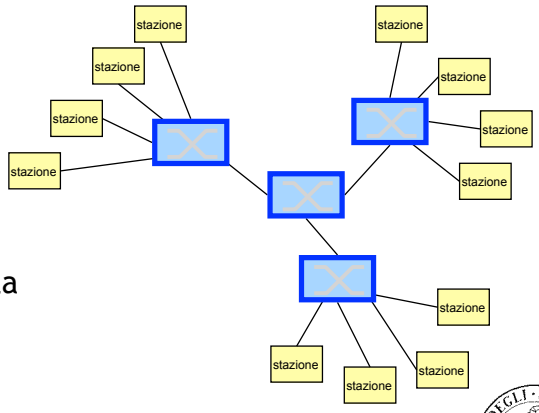
- Spezza il dominio di collisione, ovvero ciascun segmento di rete è conteso solo da chi è attestato sull'hub
- Gli hub vedono il bridge come una stazione qualsiasi che genera trame
- La trama è propagata dal bridge solo se il destinatario è attestato su un hub diverso da quello di origine
- Il concetto di *segmento data-link* viene preservato: ogni frame indirizzata ad un indirizzo broadcast di livello 2 viene ricevuta da tutti i nodi del segmento, anche se separati da diversi bridge



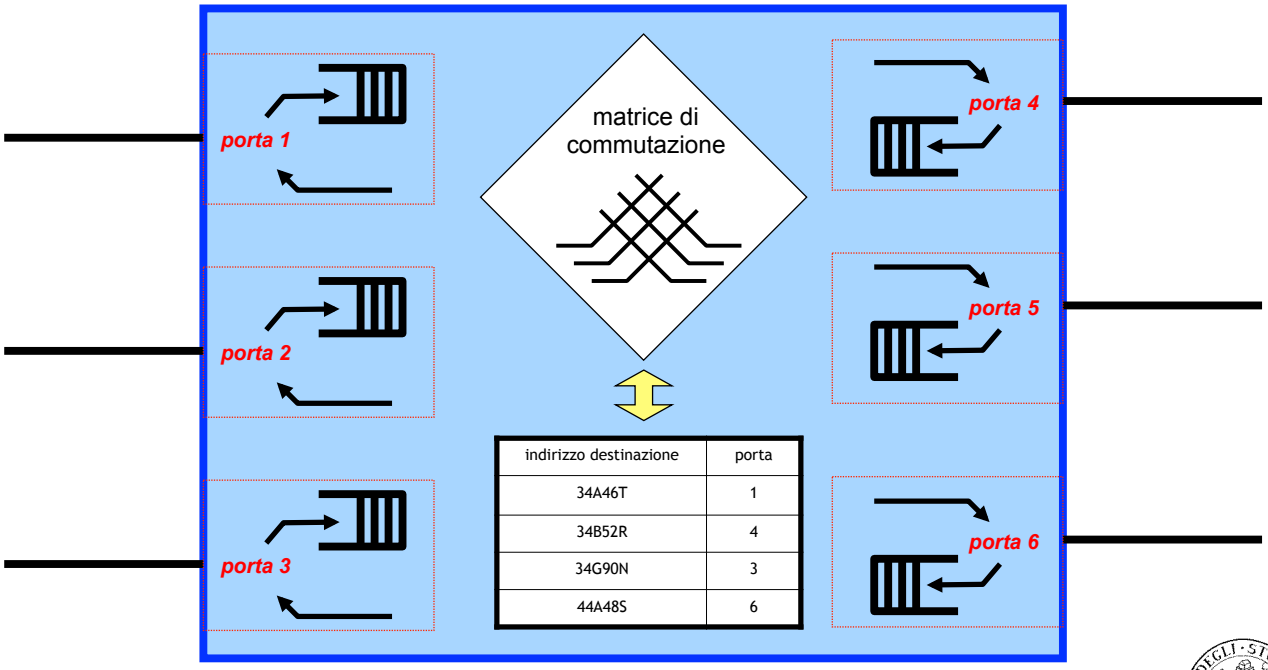
Evoluzione: Layer 2 Switch

- Il bridge ha solo 2 porte
- Lo switch è un bridge multiporta
  - mantiene una tabella in cui sono associati indirizzi di livello 2 e segmenti di rete di appartenenza
- Spesso ogni porta è connessa ad un'unica stazione (invece che ad un segmento di rete)
  - realizza un accesso dedicato per ogni nodo
  - elimina le collisioni e dunque aumenta la capacità
  - supporta conversazioni multiple contemporanee



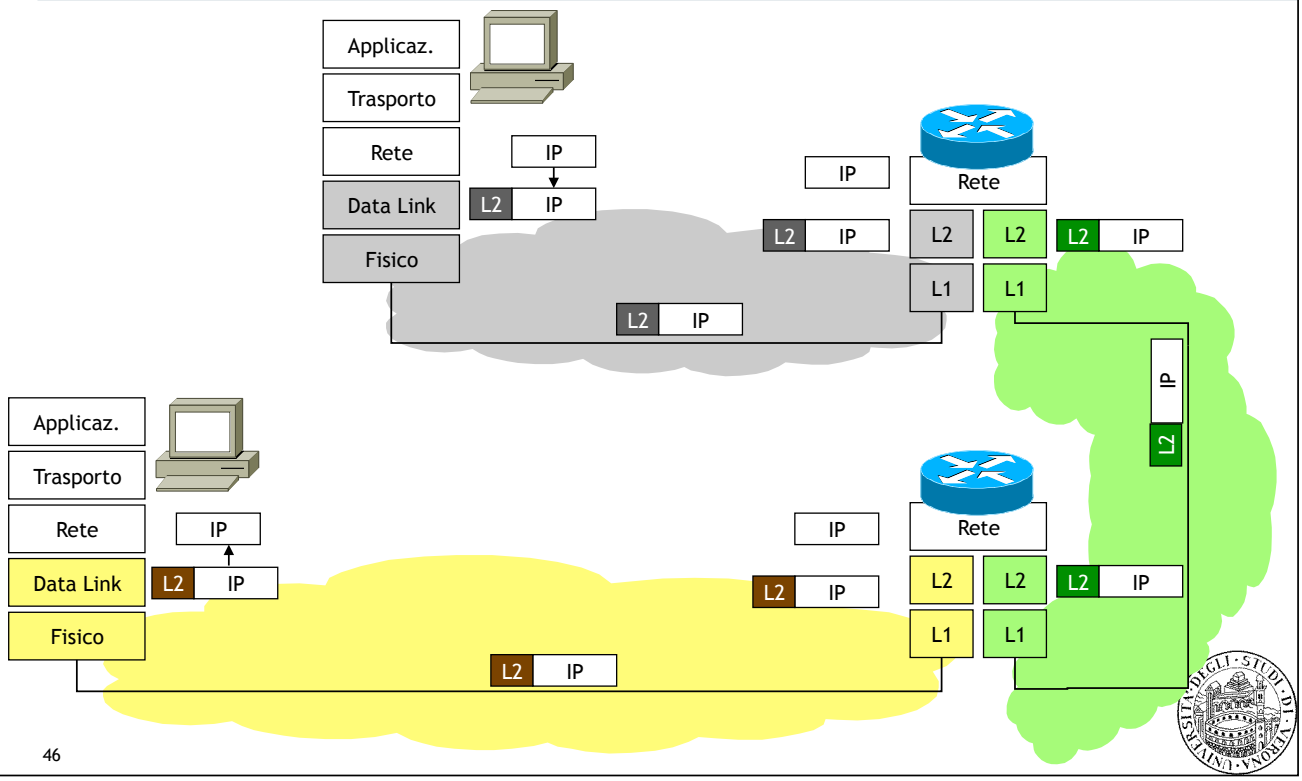


Schema di uno switch



Protocolli di livello 2 (incapsulamento di IP)

Visione d'insieme



Introduzione

- Il livello 2 svolge una serie di funzionalità che consentono il trasferimento hop-by-hop
  - funzionalità del livello 2
    - framing, rilevazione errori, controllo flusso
  - in caso di mezzo condiviso, è necessaria la presenza di un sotto livello di accesso al mezzo
- Le funzionalità sono implementate dai protocolli di livello 2
  - insieme di regole e formato dei messaggi che regolano la comunicazione tra entità peer
- Ogni hop può avere un protocollo di livello 2 che può essere differente dall'hop successivo

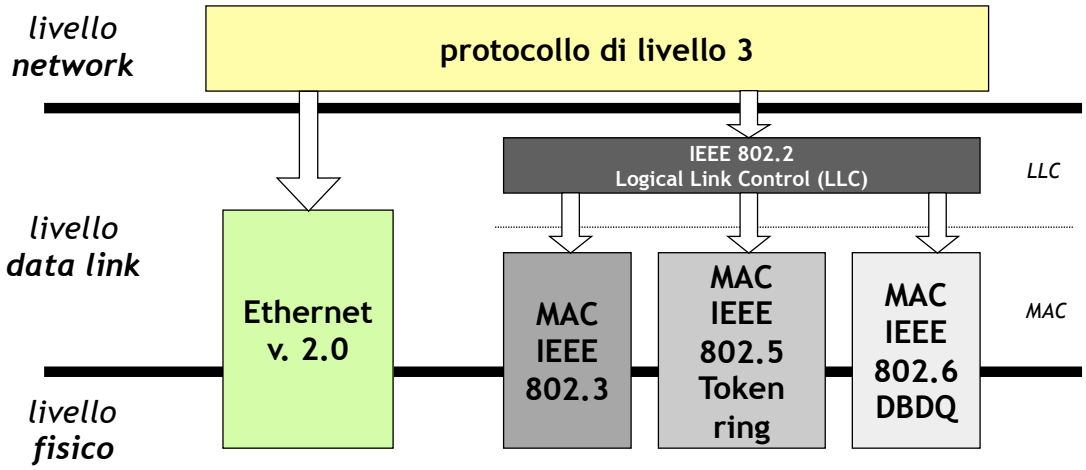
Introduzione

- L'elemento unificante è il protocollo di Rete
  - il livello 3 ha visibilità end-to-end
- Esistono dunque diverse modalità di incapsulamento dei pacchetti IP
  - ovvero esistono diversi protocolli di livello 2
- Alcuni modalità di incapsulamento dei pacchetti IP
  - soluzioni utilizzate prevalentemente per l'accesso
    - ethernet e IEEE 802.3
    - PPP
      - PPP con modem
      - PPP con ADSL
  - soluzioni utilizzate prevalentemente per il backbone
    - Frame Relay
    - ATM
    - soluzioni su SDH

Ethernet e Standard IEEE 802.3
Caratteristiche e prestazioni

- Ambito di utilizzo
  - reti locali (LAN)
    - uffici, campus universitari, ...
- Tecnologia economica
  - facilità di installazione e manutenzione
- Si interfaccia direttamente e gestisce il livello fisico
- Sopporta un carico medio del 30% (3 Mb/s) con picchi del 60% (6 Mb/s)
- Sotto carico medio
  - Il 2-3% dei pacchetti ha una sola collisione
  - Qualche pacchetto su 10,000 ha più di una collisione
- Principale differenza tra Ethernet e 802.3
  - 802.3 definisce un'intera famiglia di sistemi CSMA/CD con velocità 1-10Mbps
  - Ethernet è solamente a 10Mbps

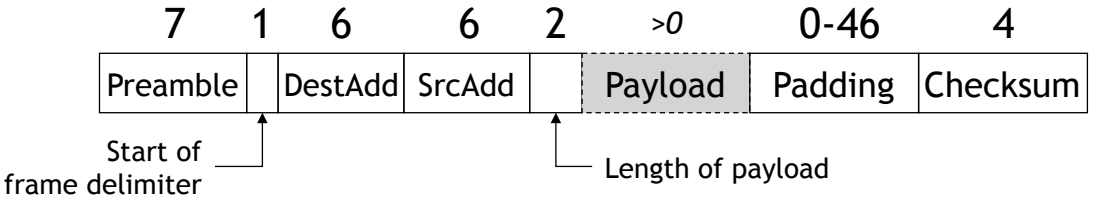
Ethernet e Standard IEEE 802.3
Posizionamento nello stack



Ethernet e Standard IEEE 802.3
Algoritmi implementati

- Gli standard Ethernet e 802.3 implementano un livello MAC di tipo CSMA/CD *1-persistent*
- In caso di collisione, l'istante in cui ritrasmettere viene calcolato utilizzando un algoritmo di **binary exponential backoff**
  - dopo *i* collisioni, l'host attende prima di ri-iniziare la procedura di trasmissione un tempo casuale nell'intervallo [0, 1, ..., 2^i-1]
  - vincoli
    - dopo 10 collisioni il tempo di attesa è limitato all'intervallo [0, 1, ..., 1023]
    - dopo 16 collisioni viene riportata una *failure* al sistema operativo

Ethernet e Standard IEEE 802.3
Formato della trama



- Preambolo (7 byte)
  - sequenza di byte "10101010" utilizzata per sincronizzare il ricevitore
- Start of frame (1 byte)
  - flag di inizio della trama "10101011"
- Addresses (6 byte)
  - indirizzi destinazione e sorgente della trama
- Length (2 byte)
  - lunghezza in byte della trama (0-1500)
  - se > 1500 indica Protocol Type
- Payload
  - informazione trasmessa
- Checksum
  - codice per rilevazione di errore

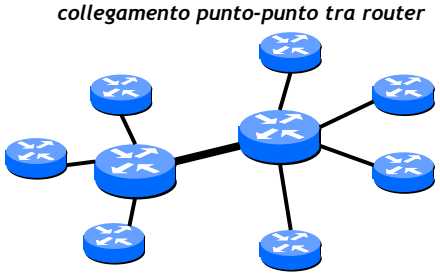
Ethernet e Standard IEEE 802.3
Evoluzione di Ethernet

- Fast Ethernet
  - Ethernet a velocità di 100Mbps
- Gigabit Ethernet
  - formato e dimensione dei pacchetti uguale a Ethernet/802.3
  - velocità di 1 Gbps (in corso di standardizzazione anche 10 Gbps)
  - Offre i vantaggio tipici di Ethernet:
    - Semplicità di accesso al mezzo CSMA/CD
    - Alta scalabilità tra le diverse velocità di trasmissione
  - Permette di velocizzare le moltissime LAN Ethernet e FastEthernet già presenti con costi contenuti tramite sostituzione apparati di rete (Hub, Switch, interfacce)

PPP
Caratterisitiche

- E' un protocollo di livello 2 utilizzato sia nell'accesso e che nel backbone
- Caratteristiche principali:
  - character oriented
  - character stuffing per il framing
  - identificazione degli errori
  - supporta vari protocolli di livello superiore (rete)
  - negoziazione dinamica degli indirizzi IP
  - autenticazione del "chiamante"

collegamento punto-punto tra router



collegamento punto-punto dial-up tra un PC e un router

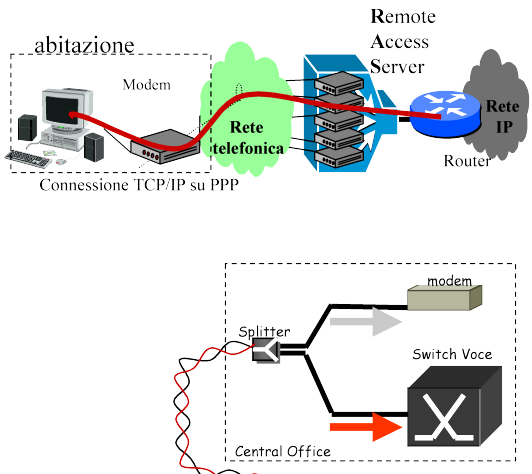
PPP
Formato della trama

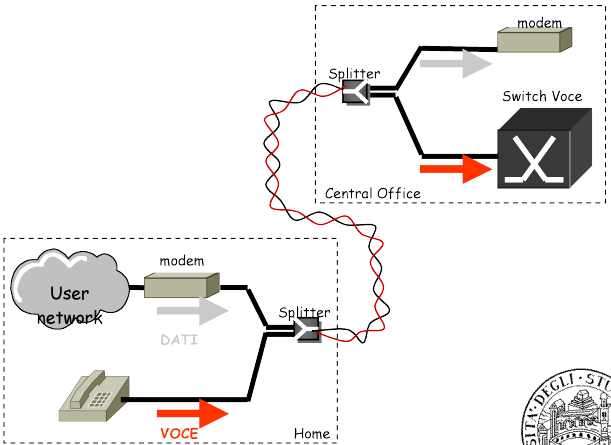
1	1	1	1 o 2	*variable*	2 o 4	1
01111110	11111111	00000011	Protocol	Payload	Checksum	01111110
Flag	Address	Control				Flag

- Flag (1 byte)
  - identifica inizio e fine della trama ("01111110")
- Address (1 byte)
  - utilizzato in configurazione "tutti gli host"
- Control (1 byte)
  - valore predefinito "00000011" ⇨ *unnumbered*
  - di default non fornisce un servizio affidabile: richiesta di ritrasmissione e rimozione replicazioni sono lasciate ai livelli superiori
    - è disponibile un'estensione per reti con alto BER (wireless) ad un servizio connection oriented (RFC1663)
- Protocol (1 o 2 byte)
  - identifica il tipo di livello di frame (LCP, NCP, IP, IPX, ...)
- Payload (>0 byte)
  - informazione trasmessa
- Checksum (2 o 4 byte)
  - identificazione dell'errore

PPP
accesso con modem e ADSL

- Modem (es.: V.90)
  - utilizza la banda telefonica per inviare i segnali
  - ha limite estremo superiore 56 Kbps
- xDSL (Digital Subscriber Line)
  - famiglie di tecnologie che permette di utilizzare la banda disponibile del doppino telefonico
  - si possono distinguere in sistemi simmetrici e asimmetrici
    - es: ADSL
      - Sistema asimmetrico su singola coppia
      - Rate adaptive:
        - 640 – 8200 kb/s downstream
        - Fino a 512 kb/s upstream
      - Strato di trasporto di livello 2: PPP su ATM
      - Distanze: a seconda del bit-rate





Protocolli di supporto: Address Resolution Protocol (ARP)

Risoluzione degli indirizzi

- Per il forwarding, e' necessario eseguire una "traduzione" :
  - il forwarding utilizza gli indirizzi IP
  - una trama deve contenere l'indirizzo MAC (livello data link) del "next hop"
  - Quindi il livello IP deve tradurre l'indirizzo IP del next-hop nel corrispondente indirizzo MAC
- Il principio generale e' :
  - Gli indirizzi IP sono un' astrazione
    - gestiti da software
  - La rete non sa come localizzare un host dal suo indirizzo IP
    - l'indirzzo di next-hop deve essere tradotto nel corrispondente indirizzo fisico MAC

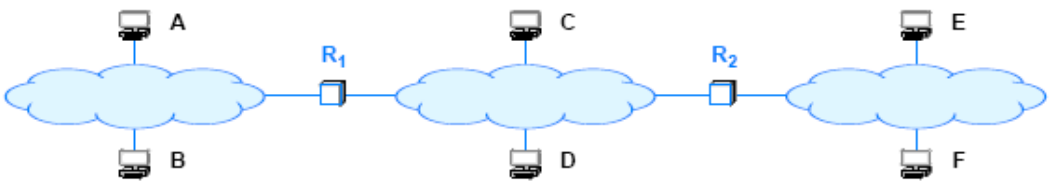
Risoluzione degli indirizzi

- L'associazione tra un indirizzo IP di un host e il suo corrispondente indirizzo hardware e' nota come "risoluzione degli indirizzi"

- La risoluzione degli indirizzi avviene localmente
  - semplice nel caso di connessioni Point-to-Point
  - piu' complicata nel caso di mezzi condivisi (ad es., Ethernet)
    - serve un protocollo specifico

Risoluzione degli indirizzi

- Un host puo' risolvere l'indirizzo di un altro host solo se entrambi sono connessi alla medesima rete fisica
  - Consegna diretta
  - Un host non e' in grado di risolvere un indirizzo di un host connesso ad un'altra rete
  - Quindi la risoluzione degli indirizzi avviene sempre all'interno di una rete



Risoluzione degli indirizzi

- Come puo' un host sapere se l'indirizzo da risolvere appartiene alla stessa rete fisica?
  - l'indirizzo IP da risolvere (di destinazione) deve avere lo stesso prefisso (NetID) dell'host sorgente (che deve risolvere l'indirizzo)
- Cosa succede se l'indirizzo non e' locale (non appartiene alla stessa rete)?
  - Consegna indiretta
  - Invia il pacchetto al router che provvedera' all'invio verso la rete di destinazione

Address Resolution Protocol (ARP)

- Quale algoritmo viene utilizzato per la risoluzione?
  - La risposta dipende dal protocollo e dall'hardware coinvolti
    - qui ci focalizziamo sulla risoluzione degl indirizzi IP
- La maggior parte degli hardware e' rappresentato da 802.3 (Ethernet), che ha un MAC address composto da 6 byte (48 bit)
- In Ethernet ➔ Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP)

- Si supponga che B debba risolvere l'indirizzo IP di C
- B invia una richiesta in broadcast che dice:
  - "Ho bisogno dell'indirizzo MAC dell'host con il seguente indirizzo IP: C"
- Il broadcast (limitato) viaggia solo sulla rete locale
- Il messagio ARP di richiesta raggiunge tutti gli host della rete locale
- Quando l'host C riceve la richiesta, risponde direttamente all'host B:
  - "Sono l'host con indirizzo IP C e il mio MAC address e' M"

ARP: formato dei messaggi

- ARP non risolve solo gli indirizzi IP e MAC
  - Lo standard e' generale e specifica i diversi messaggi a seconda dei protocolli coinvolti
- Per questo non e' possibile avere una dimensione prefissata per contenere l'indirizzo hardware di un host
  - Potrebbero essere introdotte nuove tecnologie in futuro con tipologie di indirizzi hardware diverse da quelle di oggi
  - La soluzione sta nell'avere un campo iniziale (di dimensione fissa) che indica la dimensione dell'indirizzo hardware utilizzato
- Ad esempio, se ARP viene usato con Ethernet
  - la lunghezza dell'indirizzo hardware e' di 6 byte

ARP: formato dei messaggi

- Analogamente, per rendere ARP piu' generale, esiste un campo che specifica la dimensione dell'indirizzo di livello rete
- Il protocollo ARP puo' essere dunque usato per la risoluzione di un indirizzo di rete arbitrario (non solo IP) con un indirizzo hardware arbitrario
- Nella pratica, ARP viene utilizzato principalmente per associare indirizzi IP con indirizzi Ethernet (IEEE 802.3) o wireless LAN (IEEE 802.11)

65

ARP: formato dei messaggi

0	8	16	24	31
HARDWARE ADDRESS TYPE		PROTOCOL ADDRESS TYPE		
HADDR LEN	PADDR LEN	OPERATION		
SENDER HADDR (first 4 octets)				
SENDER HADDR (last 2 octets)		SENDER PADDR (first 2 octets)		
SENDER PADDR (last 2 octets)		TARGET HADDR (first 2 octets)		
TARGET HADDR (last 4 octets)				
TARGET PADDR (all 4 octets)				

66

ARP: formato dei messaggi

- HARDWARE ADDRESS TYPE
  - campo da 16-bit che specifica il tipo di indirizzo hardware utilizzato
    - in caso di Ethernet, tale valore e' pari a 1
- PROTOCOL ADDRESS TYPE
  - campo da 16-bit che specifica il tipo di indirizzo del protocollo utilizzato
    - in caso di IP (versione 4) il valore e' 0x0800
- HADDR LEN
  - intero a 8-bit che specifica la dimensione in byte dell'indirizzo hardware
    - in caso di Ethernet, tale valore e' pari a 6
- PADDR LEN
  - intero a 8-bit che specifica la dimensione in byte dell'indirizzo del protocollo
    - in caso di IP (versione 4) il valore e' 4

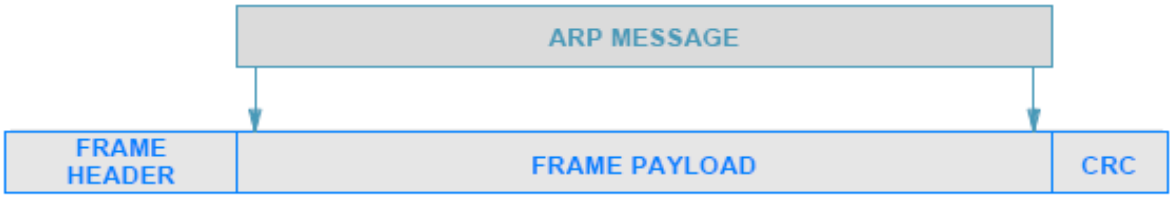
ARP: formato dei messaggi

- OPERATION
  - campo a 16-bit che specifica se il messaggio e' una "Request" (valore pari a 1) o una "Response" (valore pari a 2)
- SENDER HADDR
  - indirizzo hardware della sorgente (lunghezza pari a HADDR LEN)
- SENDER PADDR
  - indirizzo del protocollo della sorgente (lunghezza pari a PADDR LEN)
- TARGET HADDR
  - indirizzo hardware del target (lunghezza pari a HADDR LEN)
- TARGET PADDR
  - indirizzo del protocollo del target (lunghezza pari a PADDR LEN)

ARP: formato dei messaggi

- Un messaggio ARP contiene i campi per due associazioni di indirizzo
  - una per la sorgente
  - l'altro per la destinazione, denominata "target"
- Quando viene inviata una richiesta
  - la sorgente non conosce l'indirizzo hardware della destinazione
    - il campo TARGET HADDR in una richiesta ARP e' formato da zeri
- Quando viene inviata una risposta
  - il target si riferisce all'host che aveva originato la richiesta, e quindi non serve a nulla
    - l'inclusione del campo target deriva da versioni precedenti di ARP ed e' sopravvissuta

Trasporto dei messaggi ARP



- Quando viaggiano su una rete fisica, i messaggi ARP vengono racchiusi in una trama di livello data link
  - ad es., Ethernet
- Il messaggio ARP viene quindi considerato come dei dati trasportati dal livello 2
  - il livello di rete non fa il processing dei messaggi di ARP

Trasporto dei messaggi ARP

- Nell'header della trama esiste un campo "type" che indica il tipo di trama trasportata
  - Per Ethernet il valore 0x806 denota i messaggi ARP
- La sorgente deve assegnare il valore opportuno a tale campo prima di inviare la trama
- Un host deve esaminare sempre il campo "type" di ciascuna trama ricevuta
- Il campo "type" assume lo stesso valore sia che si tratti di richieste ARP che di risposte ARP
  - La destinazione, una volta determinato che si tratta di un messaggio ARP, andra' a vedere il campo OPERATION del messaggio per determinare se si tratta di una richiesta o di una risposta

ARP Caching e Processing dei Messaggi

- Inviare una richiesta ARP per ciascun datagramma e' inefficiente
  - Tre trame attraversano la rete per ciascun datagramma
    - richiesta ARP, risposta ARP, e la trama con i dati
- Nella maggior parte dei casi, la comunicazione tra host avviene usando una sequenza di pacchetti
- Per ridurre il traffico di rete
  - Il software ARP estrae e salva le informazioni delle risposte ARP
    - in modo da poterle utilizzare anche in futuro
  - Il software non mantiene tali informazioni per sempre
    - le mantiene in memoria in una tabella

ARP Caching e Processing dei Messaggi

- ARP gestisce la tabella come una cache
  - un' associazione (tra indirizzo IP e MAC) viene aggiornata quando si riceve una risposta
  - se la tabella ha raggiunto la sua dimensione massima e arriva una nuova informazione, si procede alla rimozione delle informazioni piu' vecchie
  - se un' informazione non e' stata aggiornata per molto tempo, viene rimossa

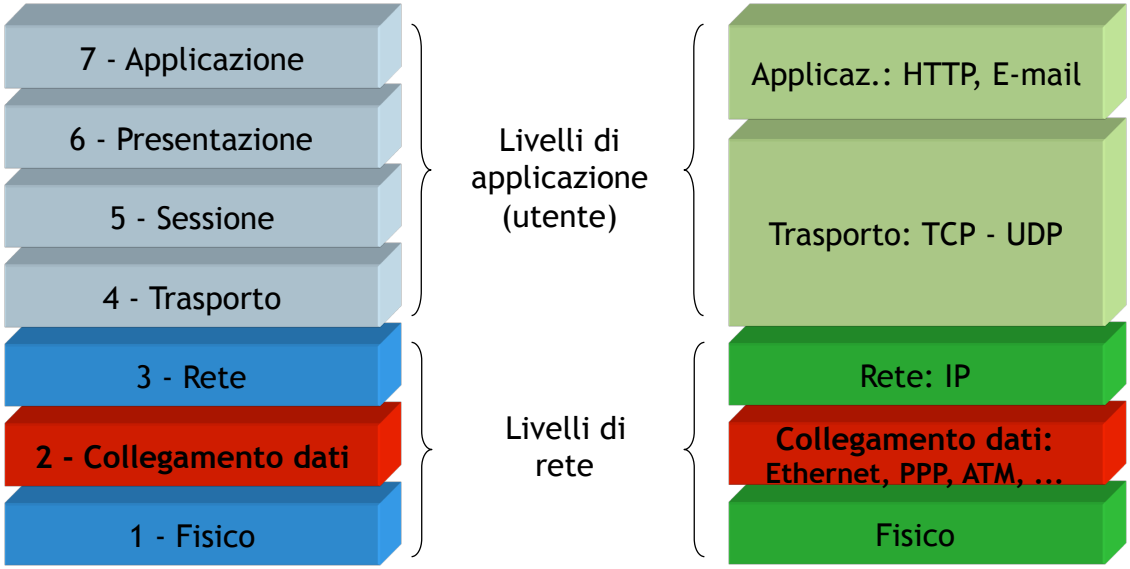
ARP Caching e Processing dei Messaggi

- Prima di inviare una richiesta ARP, si controlla se esiste gia' l' informazione nella cache
- Se l' informazione e' presente:
  - ARP utilizza l' associazione degli indirizzi senza inviare una nuova richiesta
- Se l' informazione non e' presente:
  - ARP manda in broadcast la richiesta
  - aspetta la risposta
  - aggiorna la cache
  - e usa l' informazione ottenuta per l' invio della trama

Reti di Calcolatori

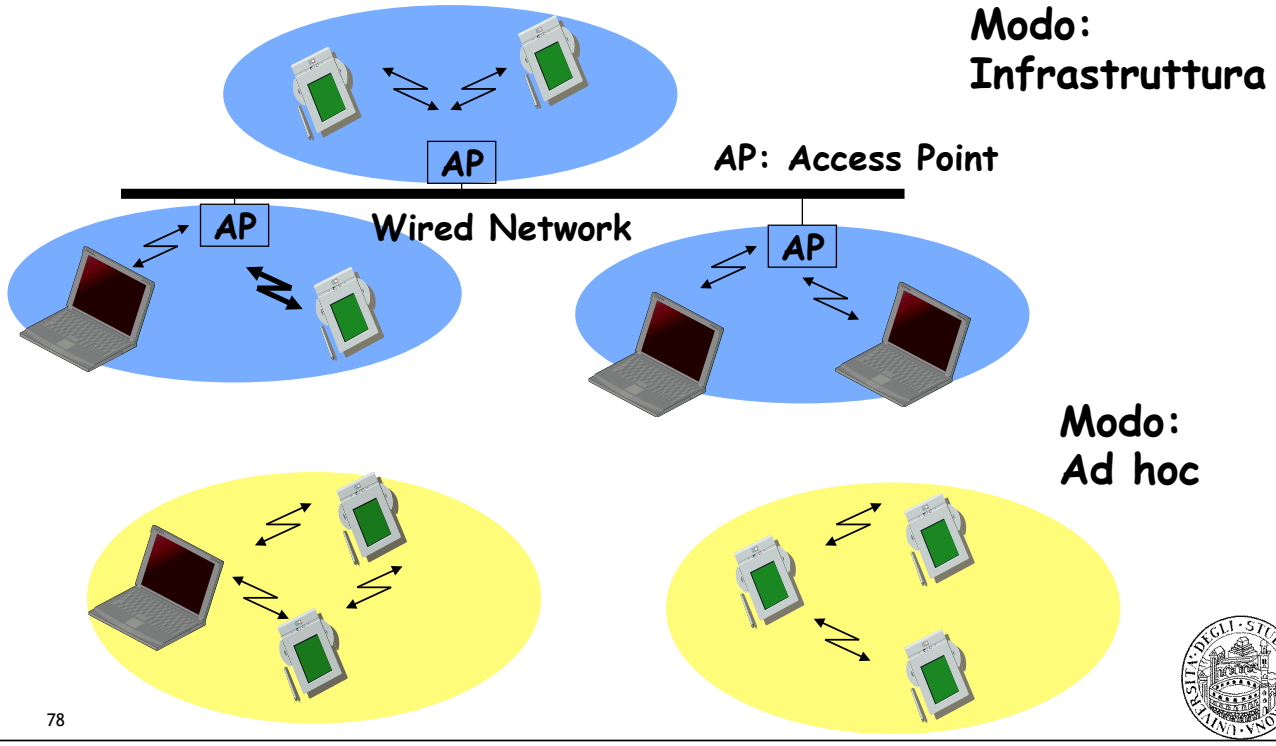
Le reti 802.11

Livello Data Link

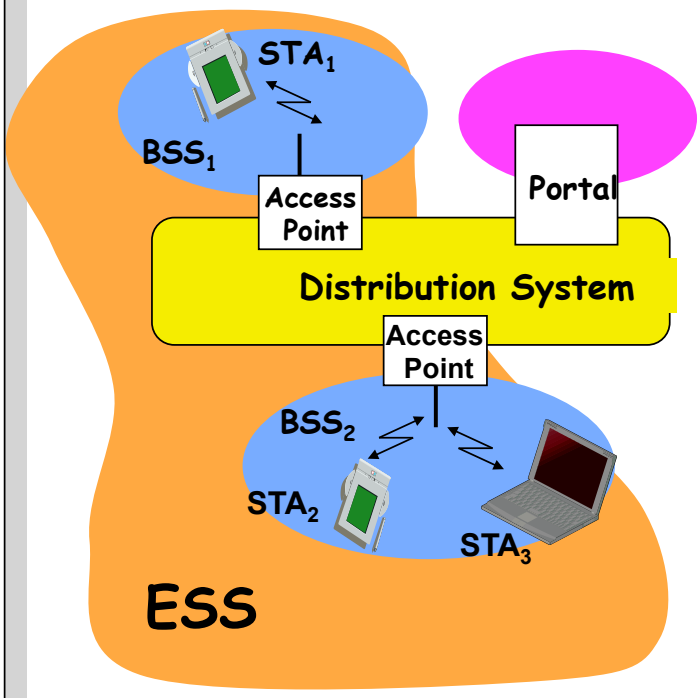


Introduzione

Architettura WIRELESS LAN



Architettura di riferimento delle WLAN



- Station (STA)
  - Terminale con capacita' di accesso al mezzo wireless
- Basic Service Set (BSS)
  - Insieme di terminali che usano le stesse frequenze
- Access Point
  - Stazione integrata sia nella WLAN che nel "Distribution System"
- Portal
  - Bridge verso altre reti (wired)
- Distribution System
  - Rete di interconnesione per formare un' unica rete logica (ESS: Extended Service Set) partendo da diverse BSS

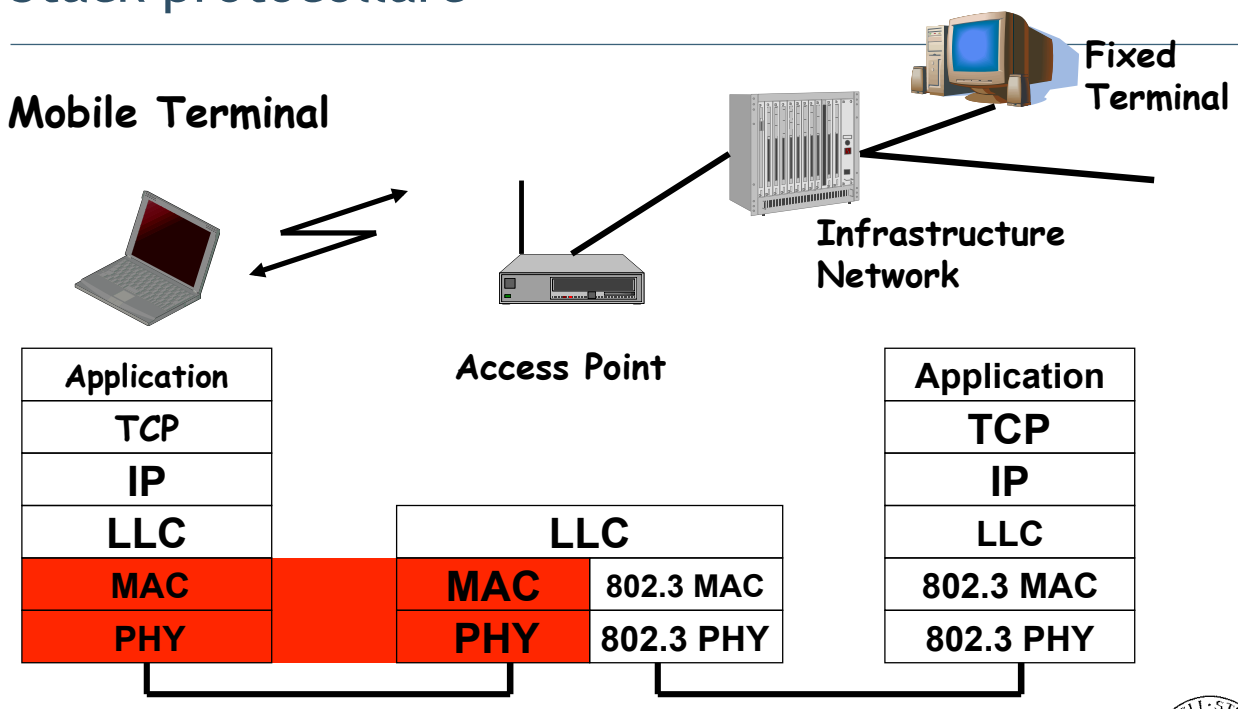
Architettura di riferimento

- Il Basic Service Set (BSS) e' formato da un insieme di terminali con lo stesso protocollo MAC che competono per l' accesso allo stesso mezzo condiviso
- Un BSS puo' essere isolato o puo' essere collegato ad un distribution system attraverso un access point (AP)
- L' AP funziona come bridge
- Il protocollo MAC puo' essere completamente distribuito o controllato da un' entita' centrale che fa da coordinatore (AP)

Architettura di riferimento

- Basic Service Set (BSS) ⇔ CELL
- L'Extended Service Set (ESS) e' formato da due o piu' BSS interconnesse da un distribution system.
- Distribution System ➔ una LAN di backbone (wired)
- Un ESS appare come una sola LAN logica a livello logical link control (LLC)

Stack protocollare



Famiglia degli standard 802.11

- 802.11a - 5GHz- Ratified in 1999
- 802.11b - 11Mb 2.4GHz- ratified in 1999
- 802.11d - Additional Regulatory Domains
- 802.11e - Quality of Service
- 802.11f - Inter-Access Point Protocol (IAPP)
- 802.11g - Higher Data rate (>20mBps) 2.4GHz
- 802.11h - Dynamic Frequency Selection and Transmit Power Control Mechanisms
- 802.11i - Authentication and Security
- 802.11n – Very High Bandwidth (10-20 times more)

802.11: confronto delle tecnologie

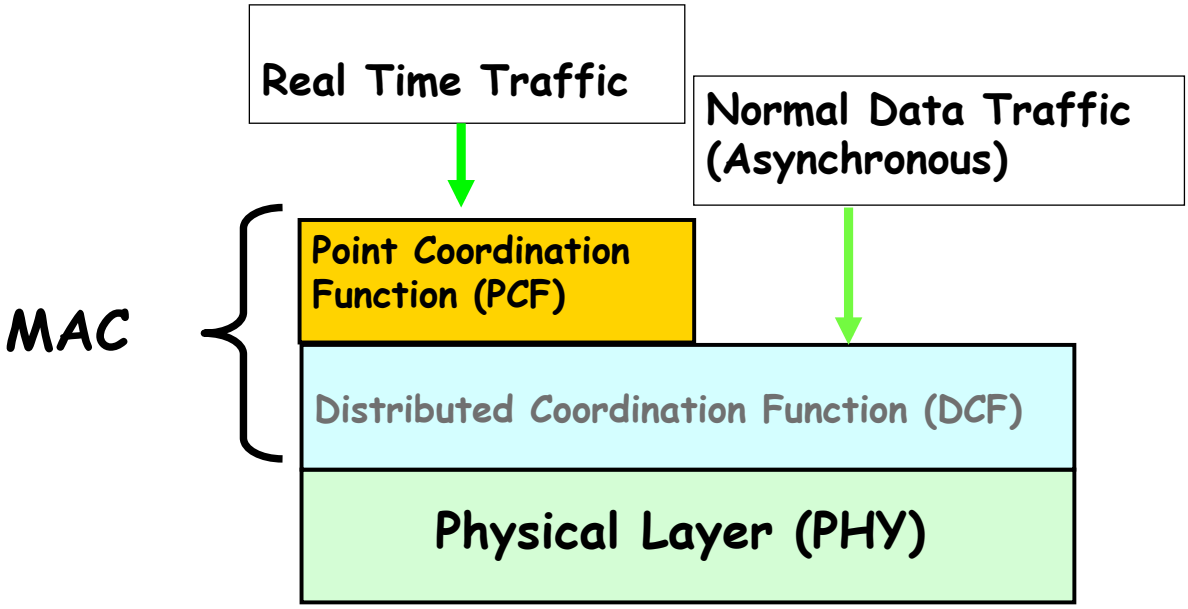
	802.11b	802.11g	802.11a
Max rate (Mbps)	11	54	54
Modulation Type	CCK	CCK, OFDM	OFDM
Data Rates	1, 2, 5.5, 11	1, 2, 5.5. 11, 6, 9, 12, 18, 24, 36, 48, 54	6, 9, 12, 18, 24, 36, 48, 54
Frequency	2.4-2.497GHz	2.4-2.497GHz	~5GHz

Livello MAC - Introduzione

Il livello MAC nelle reti 802.11

- È possibile utilizzare CSMA per le WLAN?
  - Tecnicamente sì, il CSMA è stato pensato per l'accesso ad un mezzo condiviso
- Tuttavia, la risorsa di trasmissione (banda disponibile) è molto preziosa
  - Le collisioni sprecano banda e aumentano il ritardo
- Obiettivo: modificare il CSMA con lo scopo di ridurre la possibilità di collisione
  - CSMA-CA
  - Per spiegarlo, serve introdurre alcuni concetti…

WLANs – 802.11: Architettura protocollare



Distributed Coordination Function (DCF)

- Basata sul protocollo CSMA/CA
- Utilizza un algoritmo per la risoluzione delle contese per fornire accesso a tutti i tipi di traffico
- Il traffico ordinario si appoggia direttamente su DCF

Point Coordination Function (PCF)

- Supporta il traffico Real-Time
- Basato su "polling" controllato da un Centralized Point Coordinator
- Utilizza un algoritmo MAC gestito a livello centralizzato e fornisce un servizio senza contesa del canale
- PCF e' costruito su DCF e sfrutta le funzionalita' di DCF per fornire l'accesso agli utenti

DCF vs PCF

- DCF e PCF possono funzionare allo stesso tempo all'interno della stessa BSS
  - fornendo alternativamente periodi con contesa e senza contesa
- Nel seguito descriveremo solo DCF
  - PCF e' opzionale e poco diffuso
- Prima di entrare nei dettagli di DCF vedremo gli intervalli tra trame

Inter-Frame Spacing (IFS)

Text
~~Time Slot~~

Time slot

- Il tempo e' suddiviso in intervalli, chiamati "slot"
- Uno slot rappresenta l'unita' di tempo del sistema e la sua durata dipende dall'implementazione del livello fisico
  - ad es., 802.11b ➔ 20μs
- le stazioni sono sincronizzate
  - nella modalita' "infrastructure ", con l'AP
  - nella modalita' "ad hoc", tra loro

  ➔ il sistema e' sincrono
- La sincronizzazione e' mantenuta attraverso trame di Beacon

Inter-frame space (IFS)

- Intervallo di tempo tra la trasmissione di trame
  - usato per stabilire dei livelli di priorita' nell'accedere al canale
- Sono stati defini 4 tipi IFS:
  - SIFS: Short IFS
  - PIFS: Point coordination IFS (> SIFS)
  - DIFS: Distributed IFS (> PIFS)
  - EIFS: Extended IFS (> DIFS)
- La durata dipende dall'implementazione fisica

Short IFS (SIFS)

- Usato per separare la trasmissione di trame appartenenti allo stesso "dialogo"
- Corrisponde alla piu' alta priorita'
  - usato per l'invio di pacchetti corrispondenti ad una risposta immediate
  - ACK, CTS, risposte a polling
- La sua durata dipende da
  - Tempo di propagazione sul canale
  - Tempo per passare l'informazione dal livello fisico a livello MAC
  - Tempo di switch tra modalita' TX e RX del trasmettitore radio
- Esempio: 802.11b ➔ 10µs

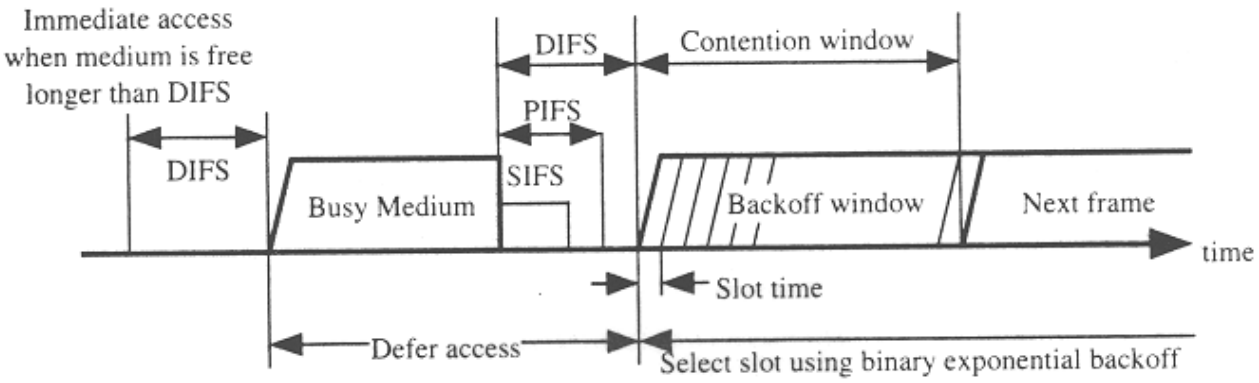
Point Coordination IFS (PIFS)

- Priorita' media, per servizi real-time che usano PCF
- PIFS = SIFS + un time-slot
- Usato dal controller centrale nello schema PCF durante il polling

Distributed IFS (DIFS)

- Piorita' piu' bassa, per il servizio di invio dati asincrono
- DIFS = PIFS + 1 time slot = SIFS + 2 time slot
- Usato dalle trame per l'invio asincrono con ritardo minimo nel caso di contesa del canale

Inter-frame Spaces (IFS)



Livello MAC: DCF con CSMA/CA

CSMA/CA (1)

- Una stazione con dei dati da trasmettere ascolta il canale

1. Se il canale è libero
   - continua a ascoltare per capire se il mezzo rimane libero per un tempo pari a DIFS. In tal caso, la stazione può trasmettere immediatamente
2. Se il canale è occupato
   - (sia perché il mezzo era occupato fin dall'inizio, sia perché è divenuto occupato durante il periodo di attesa pari a DIFS), la stazione continua a monitorare il mezzo fino a quando la trasmissione corrente è finita
3. Quando la trasmissione corrente è finita, la stazione aspetta un altro DIFS
   - Se, dopo l'intervallo DIFS, il canale è di nuovo occupato, si torna al punto 2

CSMA/CA (2)

4. Se il mezzo rimane libero per un intervallo DIFS
   - La stazione estrae un numero casuale di slot uniformemente distribuito all'interno di una **Contention Window** [0, CW-1]
     - contatore di backoff
   - Fintantoché il canale rimane libero, la stazione decrementa il contatore di backoff man mano che il tempo passa
   - Se il contatore arriva a zero, la stazione trasmette
5. Se il canale torna ad essere occupato prima che il contatore arrivi a zero
   - Il contatore viene congelato e si torna al punto 2
   - Tuttavia al punto 4 non verrà estratto un nuovo valore del contatore, ma si userà il valore congelato

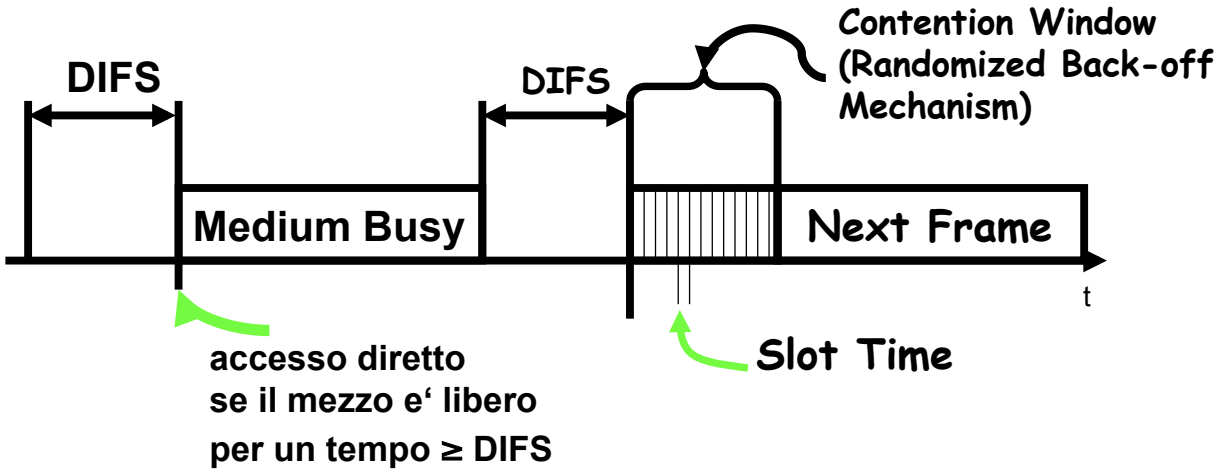
Sul valore di backoff

- Numero intero che corrisponde al numero di time slot
  - variabile casuale uniformemente distribuita tra [0,CW-1]
- CW e' il valore della Contention Window, che viene aggiornato ad ogni tentativo di trasmissione:
  - For i=1, $CW_1=CW_{min}$
  - For i>1, $CW_i=2CW_{i-1}$ con i>1 numero di tentativi consecutivi di trasmissione del pacchetto
  - For any i, $CW_i \leq CW_{max}$
- In definitiva
  - La prima stazione a cui scade il backoff inzia la trasmissione
  - Le altre stazioni percepiscono la trasmissione e bloccano il loro backoff, che fanno ripartire nel successivo periodo di contesa

CSMA/CA collision

- In caso di collisione
  - Raddoppio della CW_{max}
  - La lunghezza del tempo di backoff viene aumentata esponenzialmente nel caso di ritrasmissioni multiple
- Selezione di un nuovo valore della CW (random) tra 0 e il nuovo CW_{max}
- Attesa fino allo scadere del backoff
- […]

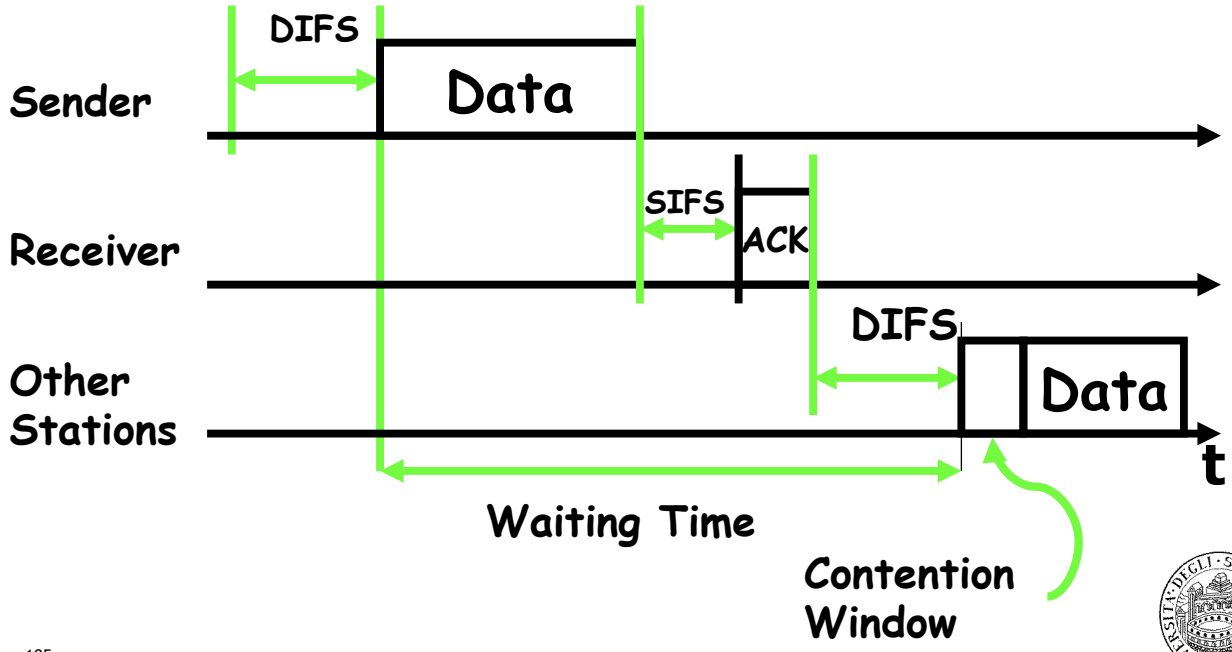
CSMA/CA



CSMA/CA con ACK

- La stazione ricevente manda un ACK immediatamente dopo la ricezione di una trama
  - ovvero aspetta per un tempo pari a SIFS < DIFS (se il pacchetto non ha errori)
- Il ricevente trasmette l'ACK senza ascoltare prima il mezzo
- ATTENZIONE: attualmente la maggior parte delle implementazioni, benche' presente nello standard, non implementa gli ACK a livello data link (funzionalita' lasciata ai livelli superiori, come quello di trasporto)

CSMA/CA con ACK

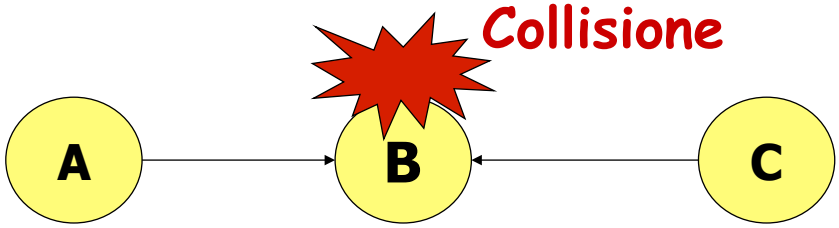


Livello MAC: DCF con RTS/CTS

Il problema del terminale nascosto

- Il segnale generato dalle stazioni (o dall'access point) è percepibile solo fino ad una certa distanza
  - La distanza dipende dalla potenza di emissione del segnale
  - Quando il segnale è troppo debole, non è possibile ricostruirlo
- Ci sono particolari disposizioni spaziali per cui il segnale emesso da una stazione può essere percepito solo da un sottoinsieme di altre stazioni
  - Nasce il problema del terminale nascosto

Problema del terminale nascosto



- A invia una trama a B
- C ascolta il canale
- C non rileva la trasmissione di A (fuori range)
- C invia una trama a B
- I segnali da A e da C si sovrappongono (collisione)

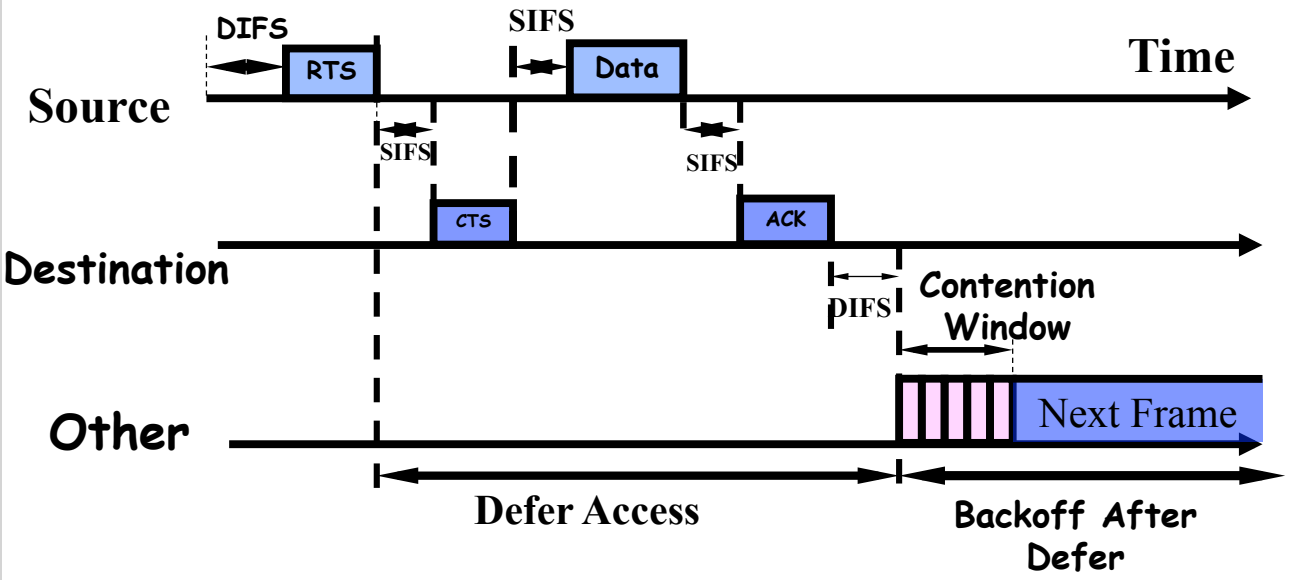
Problema del terminale esposto

- B invia trame ad A
- C vuole parlare con D
- C ascolta il canale e rileva la trasmissione di B
- C non trasmette
  - nonostante possa farlo, visto che questo non disturberebbe la trasmissione tra B e A

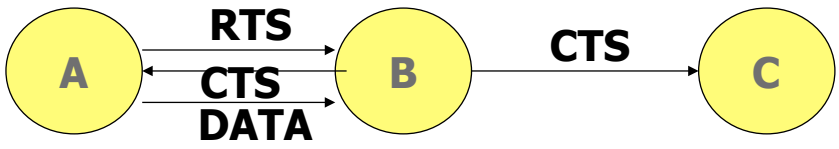
RTS/CTS

- Scopo: risolvere il problema del terminale nascosto
- La sorgente invia una trama RTS (Request To Send) dopo aver percepito il canale libero per un intervallo pari a DIFS
- Il ricevente risponde con una trama CTS (Clear To Send) dopo un intervallo SIFS
- I dati possono essere trasmessi
- RTS/CTS vengono usati per riservare il canale per la trasmissione dei dati, in modo tale che le eventuali collisioni possano avvenire solo tra i messaggi di controllo

RTS/CTS esempio



Problema del terminale nascosto

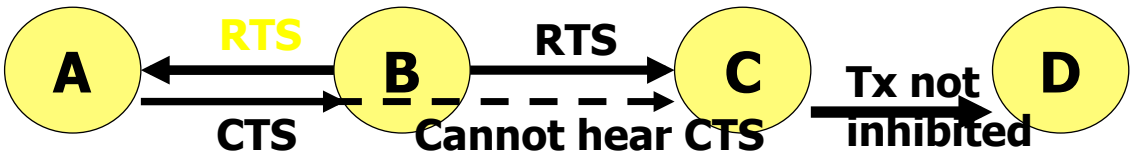


- A invia una trama RTS a B
- B invia una trama CTS (in broracast)
- A e C ricevono la trama CTS
- C blocca la sua trasmissione
- A invia i dati a B con successo

Problema del terminale nascosto

- Come puo' C sapere quanto tempo deve aspettare prima di poter tentare una trasmissione?
- La stazione A include la lunghezza dei dati da trasmettere nella trama RTS
- La stazione B include tale informazione nella trama CTS
- La stazione C, quando ascolta il canale e riceve la trama CTS, riceve anche la durata della trasmissione e calcola per quanto tempo inibire la trasmissione

Terminale esposto



- B invia una trama RTS ad A (percepita anche da C)
- A invia una trama CTS a B
- C non riceve la trama CTS di A (fuori range)
- C assume che non sia raggiungibile
- C non inibisce la trasmissione a D

Network Allocation Vector

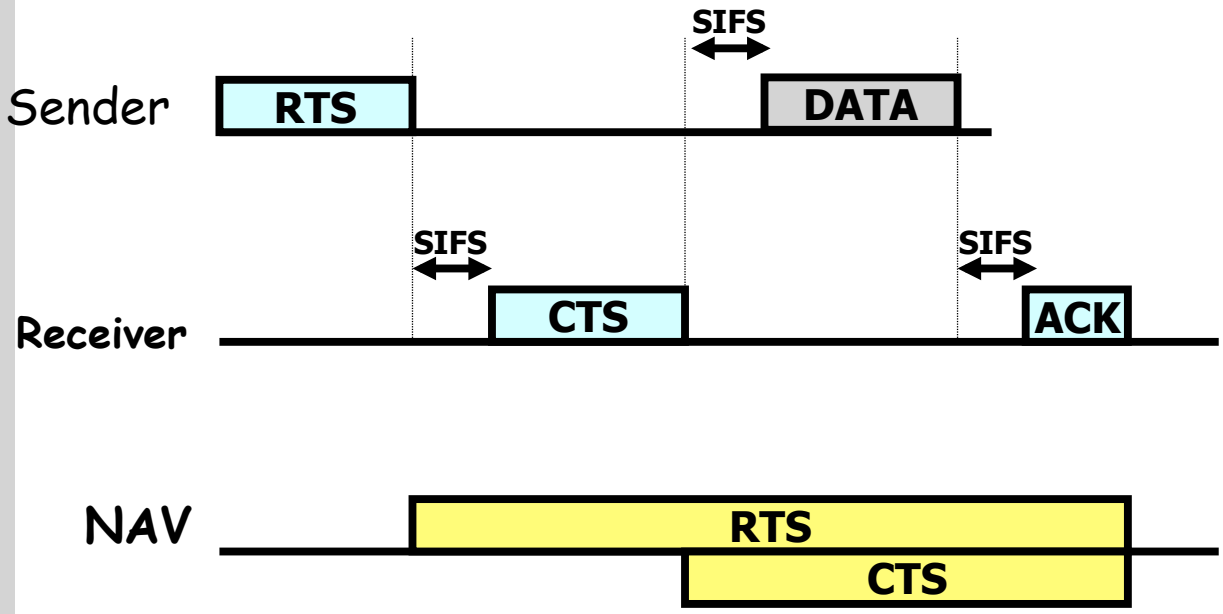
Network Allocation Vector (NAV)

- In 802.11, l'ascolto del canale e' sia fisico che "virtuale"
- Se una delle due funzionalita' indica che il mezzo e' occupato, allora 802.11 considera il canale occupato
- L'ascolto virtuale del canale e' fornito dal NAV (Network Allocation Vector)

Network Allocation Vector (NAV)

- La maggior parte delle trame 802.11 includono il campo di lunghezza della trama
- I nodi che percepiscono le trame, impostano il NAV al tempo in cui si aspettano che il mezzo sia libero
- Se il NAV > 0, il mezzo e' considerato occupato

Esempio con RTS/CTS



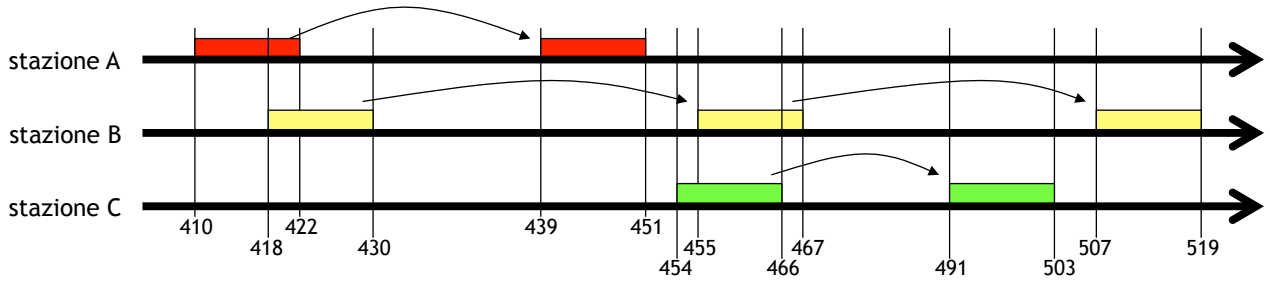
Reti di Calcolatori

Il livello Data Link - Esercizi

Esercizio 1

- 3 stazioni comunicano utilizzando il protocollo ALOHA; si suppone che il tempo di propagazione sia nullo; le caratteristiche del sistema sono:
  - velocità della linea: 2.5 Mbit/s
  - lunghezza delle trame: 30 Kbit (→3.75 Kbyte)
- La stazione A inizia a trasmettere all'istante tA=410 msec;
- La stazione B inizia a trasmettere all'istante tB=418 msec;
- La stazione C inizia a trasmettere all'istante tC=454 msec;
- C'è collisione tra A e B? Per quanto tempo si sovrappongono le trame?
- Si supponga che, dopo la collisione, le stazioni decidono di ritrasmettere Z millisecondi dopo la fine della trasmissione del pacchetto corrotto;
  - Z viene deciso secondo il seguente metodo: si attende un tempo pari a
    - somma delle cifre che compongono l'istante di inizio trasmissione * numero di collisioni consecutive + T (ad esempio, se l'istante è 315 msec, Z = (3+1+5)*#collisioni + T)
- Si determini in quale istante riescono a trasmettere le 3 stazioni

Esercizio 1 – Soluzione

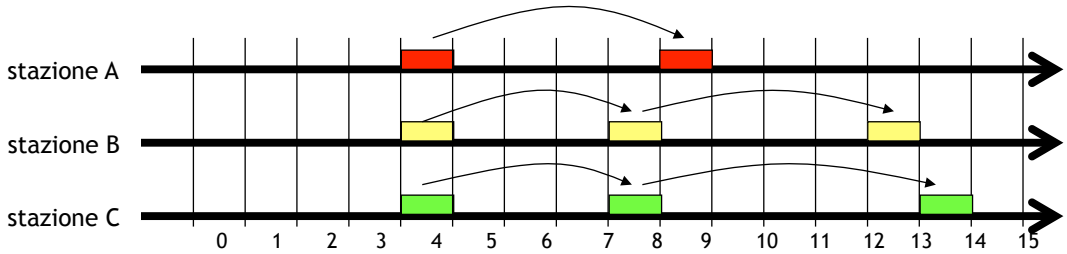


- Tempo di trama T: 30.000 bit / 2.500.000bit/s = 12 msec
- Stazione A
  - prima collisione, Z= (4+1+0)*1+12=17, istante di ritrasmissione=422+17=**439**
- Stazione B
  - prima collisione, Z=(4+1+8)*1+12=25, istante di ritrasmissione=430+25=455
  - seconda collisione, Z=(4+5+5)*2+12=40, istante si ritrasmissione=467+40=**507**
- Stazione C
  - prima collisione, Z= (4+5+4)*1+12=25, istante di ritrasmissione=466+25=**491**

Esercizio 2

- 3 stazioni A, B e C comunicano utilizzando il protocollo Slotted - ALOHA; si suppone che il tempo di propagazione sia nullo; la lunghezza delle trame è fissa e occupa il canale per tutto il tempo di uno slot
- Ad ogni stazione è associato un seme che serve per la generazione dei numeri casuali
  - A → 35; B→ 16; C→22
- Tutte le stazioni iniziano a trasmettere al primo slot
- Si supponga che, dopo la collisione, le stazioni decidono di ritrasmettere Z slot dopo (se Z=1, ritrasmettono lo slot successivo, se =2 dopo 2 slot, ...);
  - Z è il risultato della seguente operazione (viene considerato solo l'intero inferiore) :
    - sqrt(seme associato alla stazione * numero di collisioni consecutive)
    - ad esempio, se il seme è 35 e ci sono gia' state 2 collisioni, Z = sqrt(35*2)= 8
- Si determini in quale slot riescono a trasmettere le 3 stazioni

Esercizio 2 – Soluzione

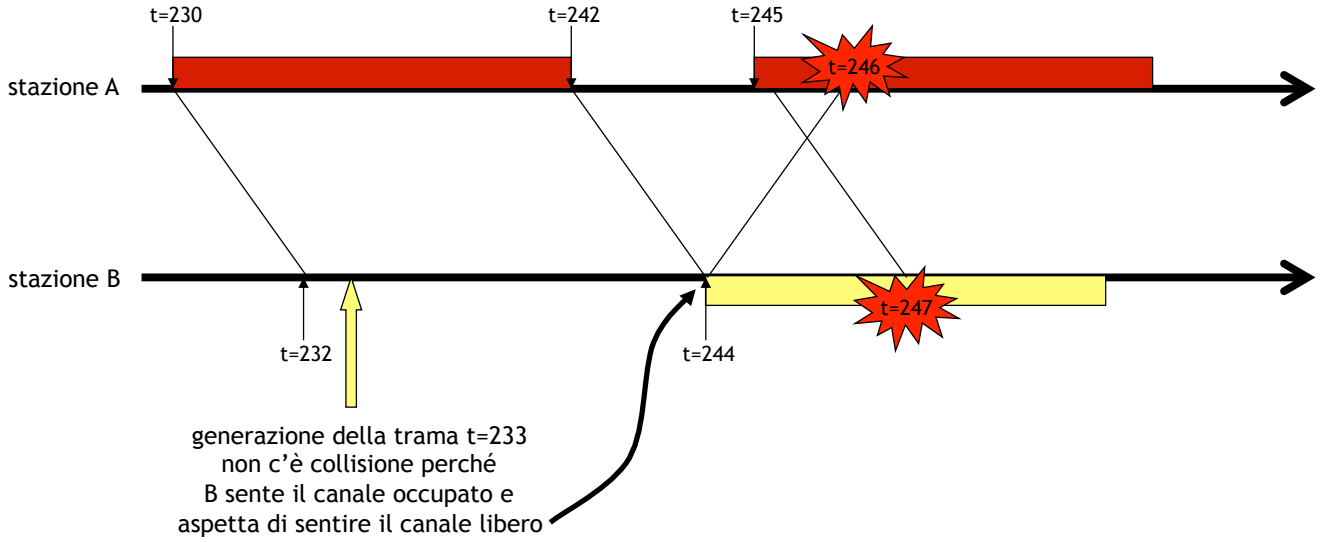


- Stazione A
  - prima collisione, Z= sqrt(35*1)=5, ovvero ritrasmette al quinto slot successivo
- Stazione B
  - prima collisione, Z= sqrt(16*1)=4, ovvero ritrasmette al quarto slot successivo
  - seconda collisione, Z= sqrt(16*2)=5, ovvero ritrasmette al quinto slot successivo
- Stazione C
  - prima collisione, Z= sqrt(22*1)=4, ovvero ritrasmette al quarto slot successivo
  - seconda collisione, Z= sqrt(22*2)=6, ovvero ritrasmette al sesto slot successivo

Esercizio 3

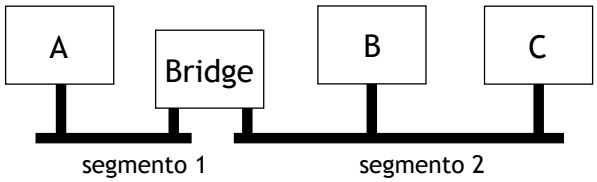
- Due stazioni A e B attestate sullo stesso segmento di rete utilizzano un protocollo CSMA persitent (→ 1-persistent); le caratteristiche del sistema sono:
  - velocità della linea: 2.5 Mbit/s
  - lunghezza delle trame: 30 Kbit (→3.75 Kbyte)
  - ritardo di propagazione: 2 msec
- La stazione A genera 2 pacchetti: uno all'istante tA1=230 msec e uno all'istante tA2=245 msec
- La stazione B genera un pacchetto all'istante tB1=233msec
- Domande:
  - in che istante A si accorge della collisione?
  - e in che istante B si accorge della collisione?

Esercizio 3 – Soluzione



- Tempo di trama T: 30.000 bit / 2.500.000bit/s = 12 msec

Esercizio 4

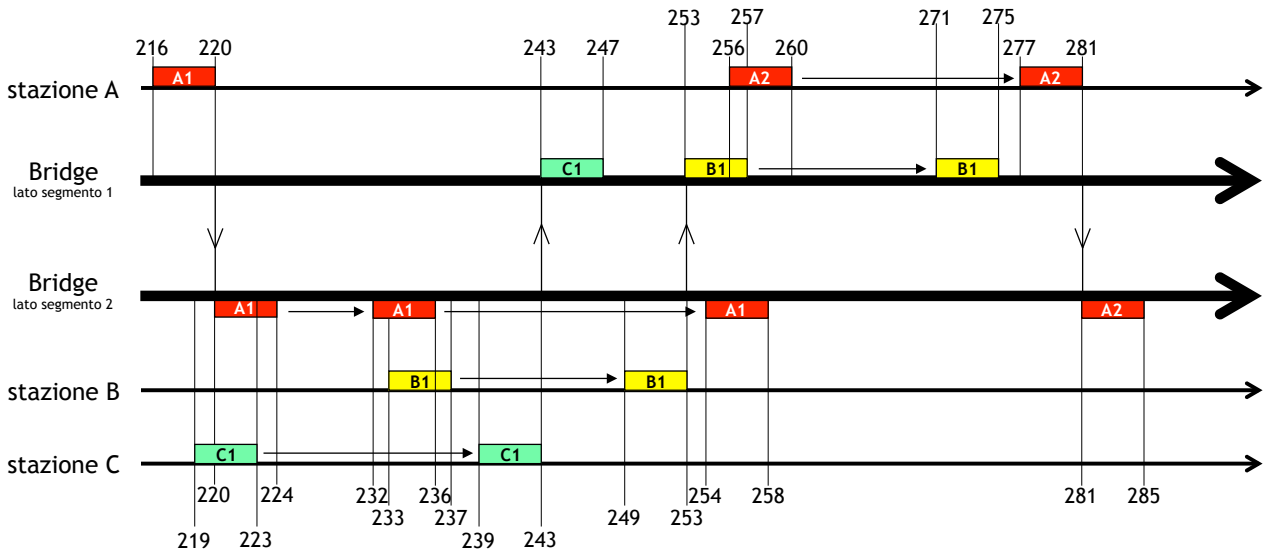


- Configurazione come in figura
- Caratteristiche Bridge
  - memorizza le trame che arrivano da un segmento di rete e le ritrasmette sull'altro segmento di rete; tale comportamento è valido in entrambi i sensi;
  - la capacità di memorizzazione e la capacità di trasmissione è indipendente nei due segmenti (ovvero se arrivano o se devono essere trasmesse due trame contemporaneamente sui due segmenti di rete, il Bridge è in grado di memorizzarle o trasmetterle entrambe);
  - la ritrasmissione sull'altro segmento ha inizio solamente quando la trama è stata memorizzata completamente;
  - nel ricevere e nel trasmettere le trame, utilizza gli stessi protocolli delle altre stazioni;
  - le trame restano in memoria fino a quando la trasmissione sull'altro segmento non è andata a buon fine.

Esercizio 4

- Le stazioni utilizzano il protocollo ALOHA per la trasmissione delle trame; le caratteristiche del sistema sono:
  - velocità delle linee: 1.6 Mbit/s;
  - lunghezza delle trame: 800 byte;
  - ritardo di propagazione su entrambi i segmenti nullo;
- La stazione A genera due trame, A1 e A2, agli istanti tA1=216 msec e tA2=256 msec rispettivamente;
- La stazione B genera una trama, B1, all'istante tB1=233msec;
- La stazione C genera una trama, C1, all'istante tC1=219msec.
- In caso di collisione, si supponga che le stazioni decidono di ritrasmettere Z millisecondi dopo la fine della trasmissione della trama corrotta; il numero Z viene deciso secondo il seguente metodo:
  - si attende un tempo pari a Z = Sc * N + T, dove
    - Sc = somma delle cifre che compongono l'istante di trasmissione
    - N = numero di collisioni subite dalla trama
    - T tempo di trama
- Si determini graficamente le trasmissioni delle diverse trame sui due segmenti distinti

Esercizio 4 – Soluzione



Esercizio 4 – Soluzione

- Tempo di trama T: 800*8 bit / 1,600,000bit/s = 4 msec
- Stazione A
  - prima collisione, Z= (2+5+6)*1+4=17, istante di ritrasmissione=260+17=277
- Bridge lato Stazione A
  - prima collisione, Z= (2+5+3)*1+4=14, istante di ritrasmissione=257+14=271
- Bridge lato Stazioni B e C
  - prima collisione, Z= (2+2+0)*1+4=8, istante di ritrasmissione=224+8=232
  - seconda collisione, Z=(2+3+2)*2+4=18, istante si ritrasmissione=236+18=254
- Stazione B
  - prima collisione, Z=(2+3+3)*1+4=12, istante di ritrasmissione=237+12=249
- Stazione C
  - prima collisione, Z=(2+1+9)*1+4=16, istante di ritrasmissione=223+16=239