Reti di Calcolatori
AA 2013/2014

UNIVERSITÀ DEGLI STUDI DI TRENTO

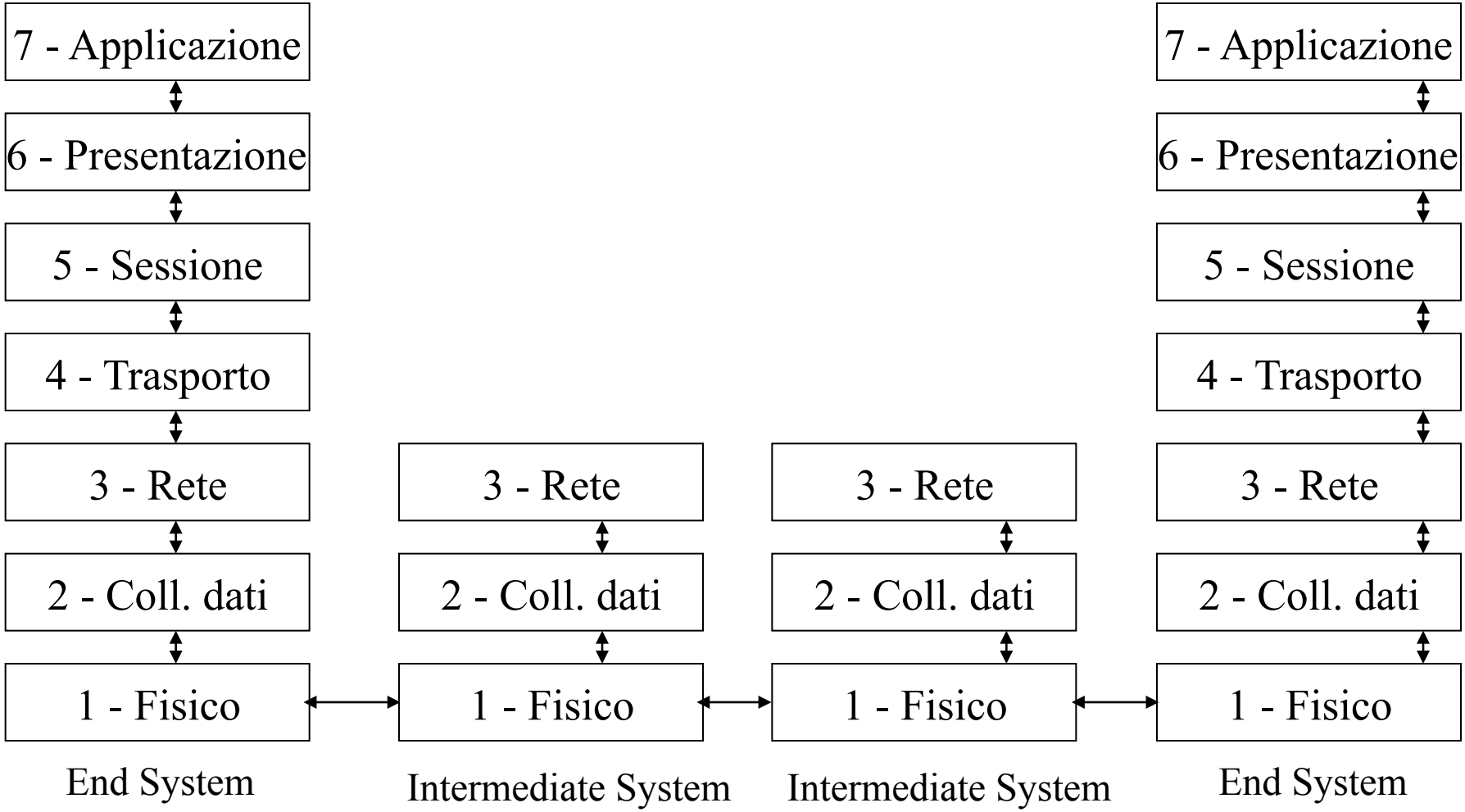
http://disi.unitn.it/locigno/index.php/teaching-duties/computer-networks

Livello 2 OSI: Data Link e MAC. Standard per LAN, Ethernet, LAN Estese e cenni ad altre reti di livello 2

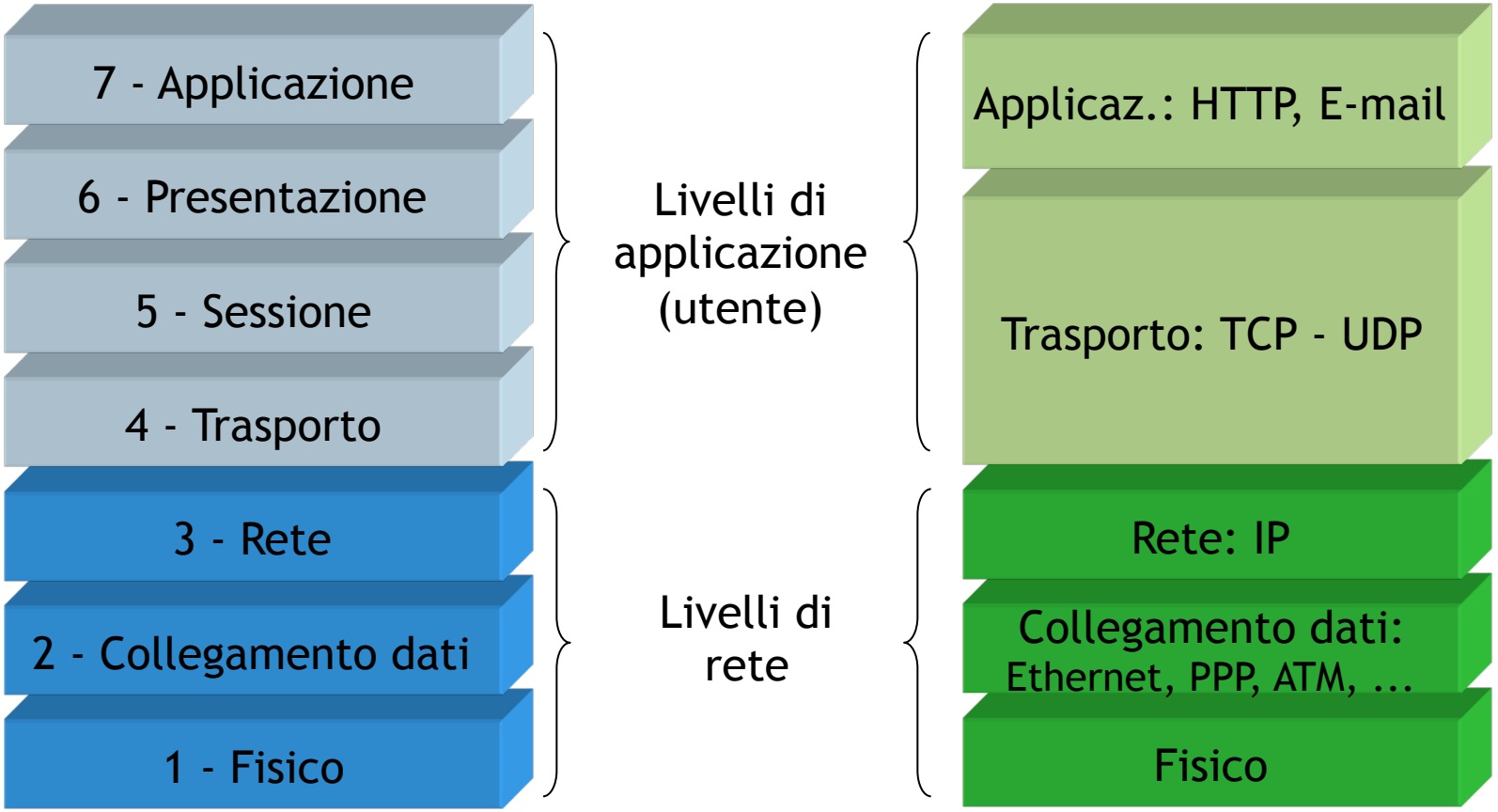
Renato Lo Cigno

Copyright

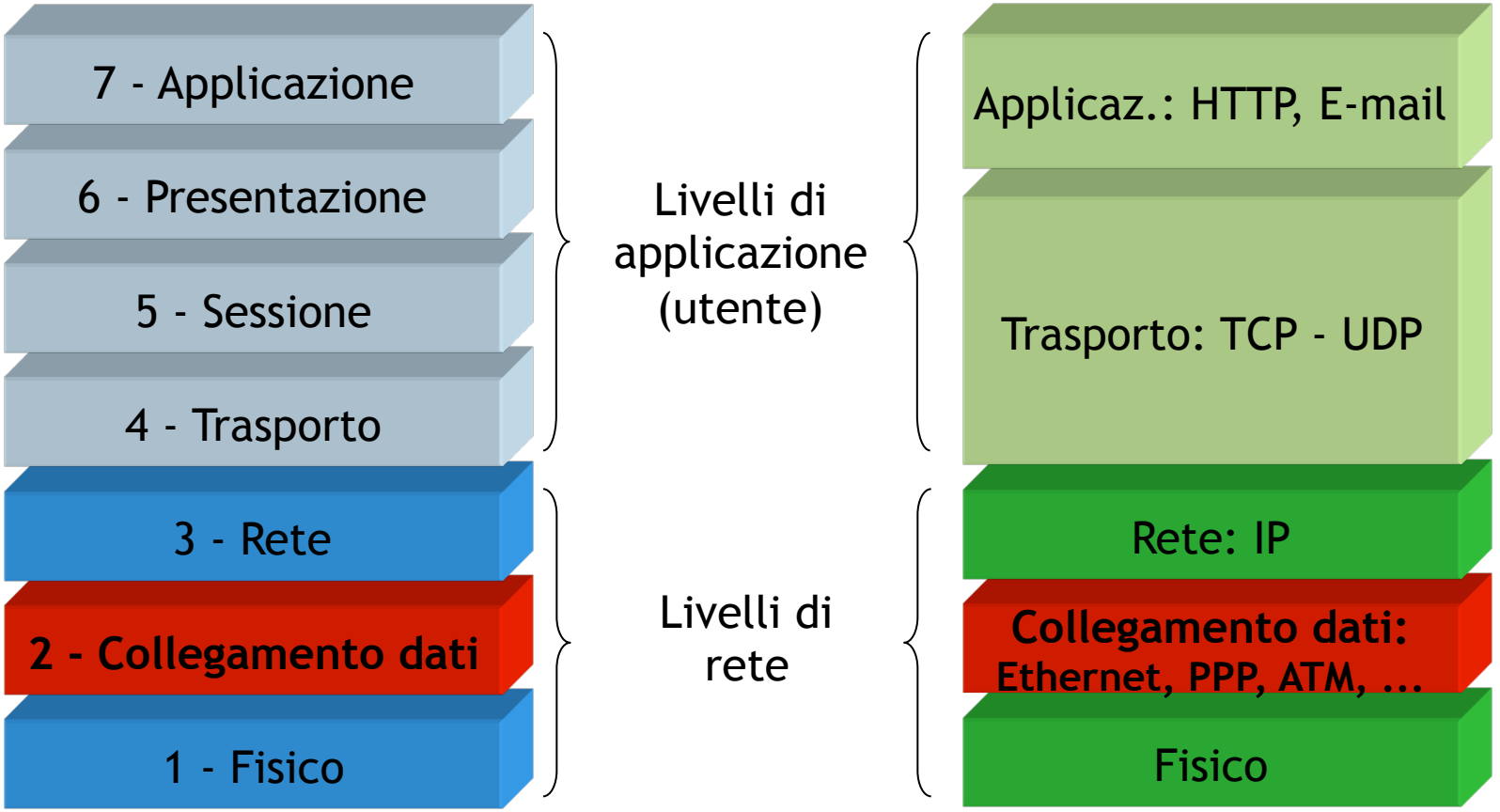
Modello a strati



Stack OSI... ...e Stack TCP/IP



Livello Data Link



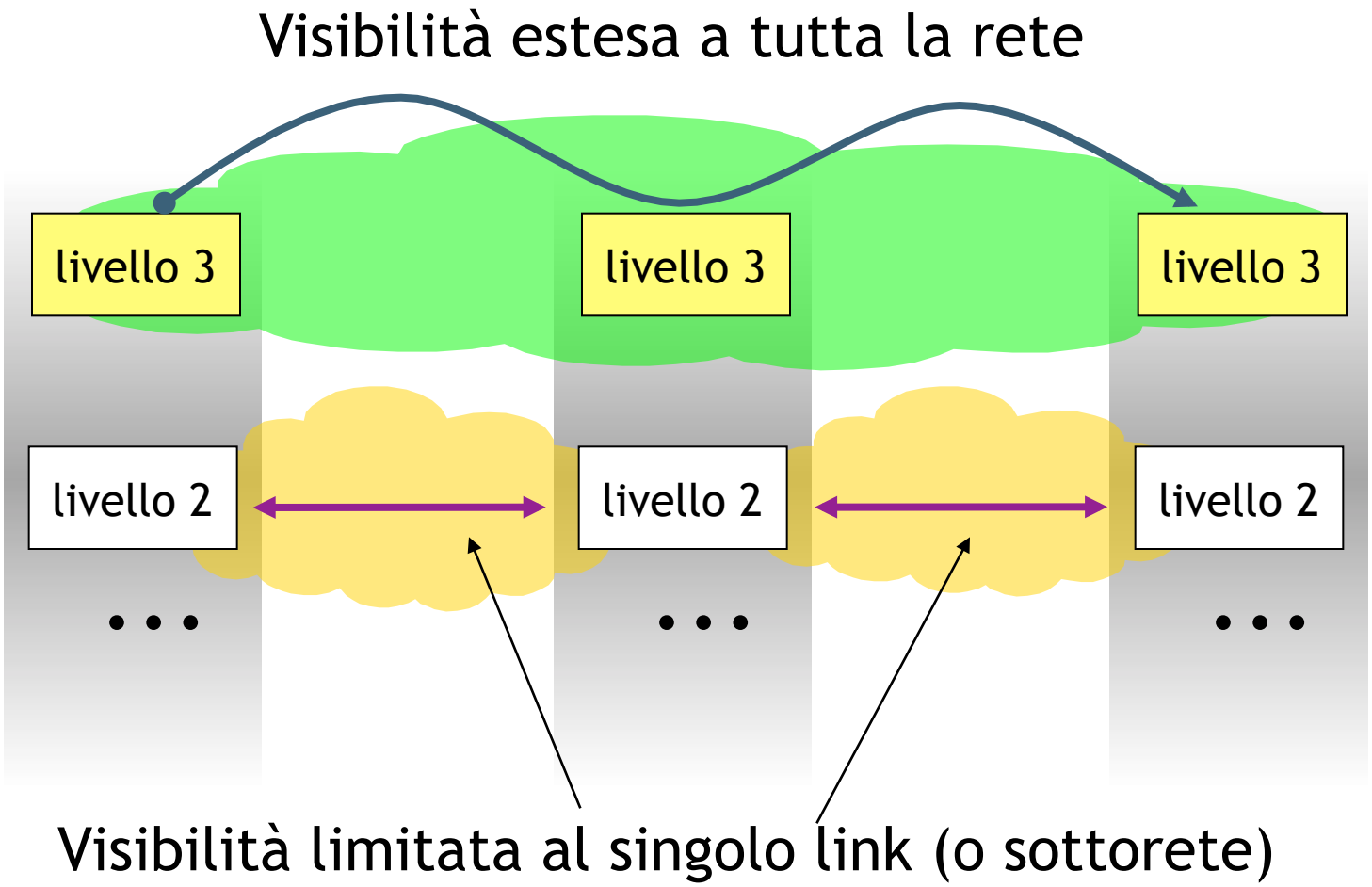
Livello Data Link

- 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 riscontro (ACK)
  - 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



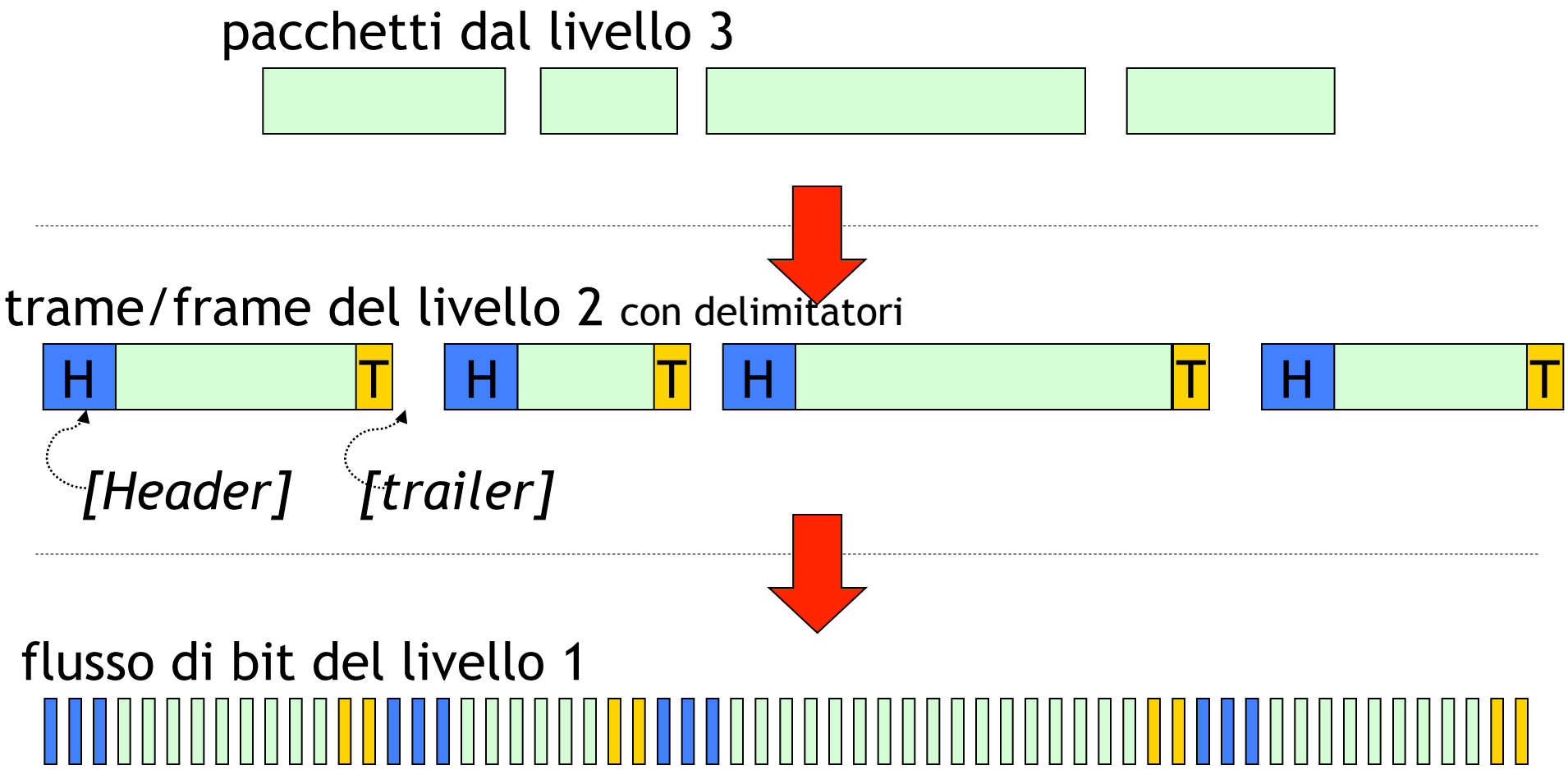
Funzioni di competenza del livello 2

- 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

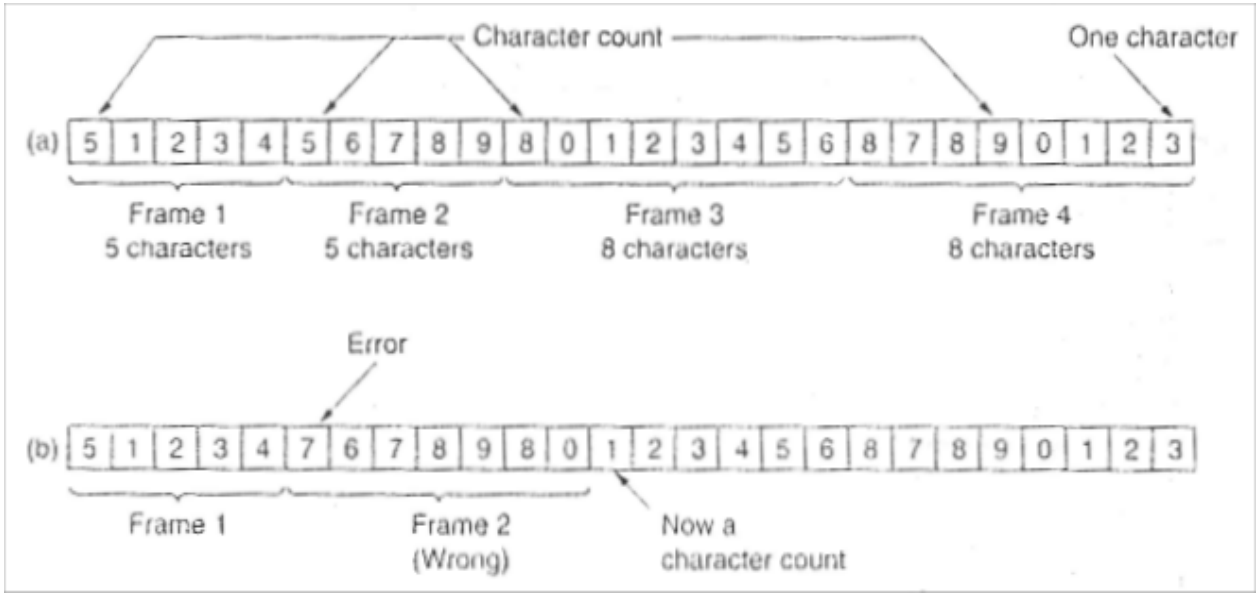

pacchetti dal livello 3
trame/frame del livello 2 con delimitatori
H
T
H
T
H
T
H
T
[Header]
[trailer]
flusso di bit del livello 1

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. Character stuffing
    3. Starting and ending flags (bit stuffing)
    4. Physical layer coding violations

Framing: Character Count

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



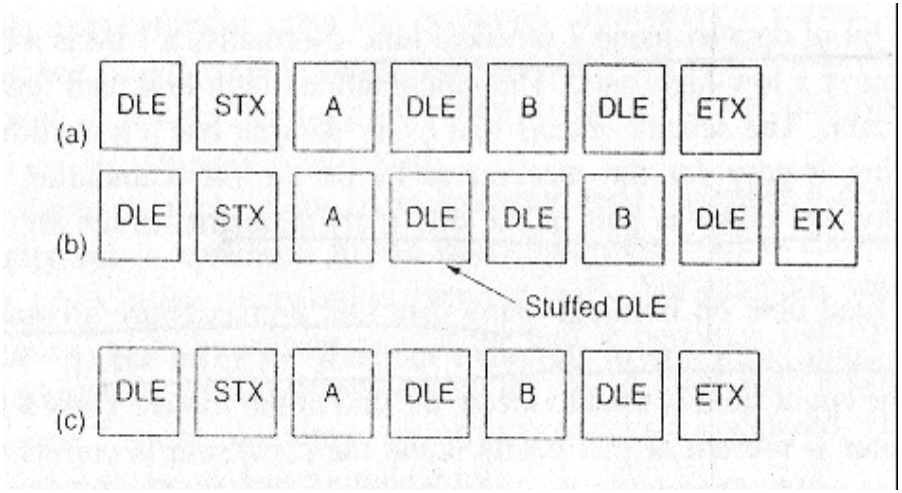
(fonte A.Tanenbaum, Computr Networks)

Framing: Character stuffing (1)

- Ogni trama inizia e termina con una sequenza di caratteri ASCII ben definita
  - DLE (Data Link Escape) + STX (Start of TeXt)
  - DLE (Data Link Escape) + ETX (End of TeXt)
- Se nella trasmissione di dati binari, una sottosequenza di bit corrisponde ai caratteri speciali...

- ...la sorgente duplica il carattere DLE
  - **character stuffing**

Framing: Character Stuffing (2)



(fonte A.Tanenbaum, Computr Networks)

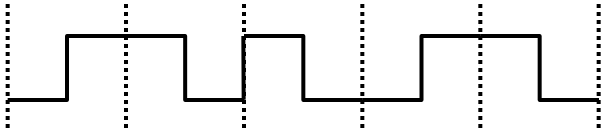
- Svantaggio principale: soluzione legata al modulo base dei caratteri ad 8 bit e alla codifica ASCII

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**
- In trasmissione se la sorgente incontra 5 bit "1" consecutivi, aggiunge uno "0" (indipendentemente dal bit che segue)
  - **bit stuffing**
  - es. la sequenza "01111110" è trasmessa come "011111010"
- Il ricevitore quando riceve 5 "1" consecutivi elimina sempre lo 0 che segue, ripristinando la sequenza originale

Framing: Physical medium coding violations

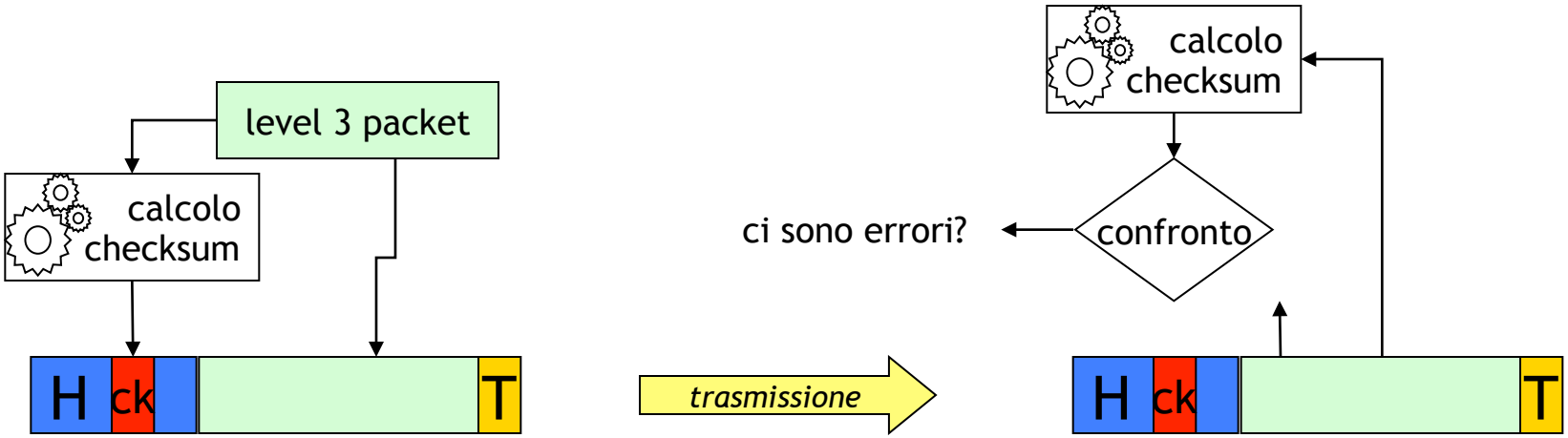
- E' una tecnica basata su sistemi che utilizzano ridondanza a livello fisico
  - es. ogni bit di informazione viene trasmesso utilizzando una combinazione di due bit a livello fisico
    - '1' ⇨ '10'
    - '0' ⇨ '01'

"01101" ⇨ 

  - determinate combinazioni non sono quindi usate per i dati e possono essere quindi utilizzate per il framing
    - '00' e '11'

Rilevazione dell'errore

- Il livello fisico offre un canale di trasmissione **con 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

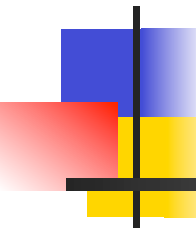


Controllo di flusso (v. Prot. a Finestra)

- 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
- I feedback possono essere
  - nei servizi con riscontro, gli ack stessi
  - nei servizi senza riscontro, dei pacchetti appositi

Correzione errori

- Spesso assente nelle reti locali (ma presente invece nelle reti wireless LAN)
- Presente nelle reti tradizionali di tipo geografico
- Come a livello trasporto basato su protocolli a finestra
  - normalmente stop&wait
  - sul singolo canale non ho problemi di ritardo variabile
- Ritrasmissione dell'intera trama, controllo basato su CRC

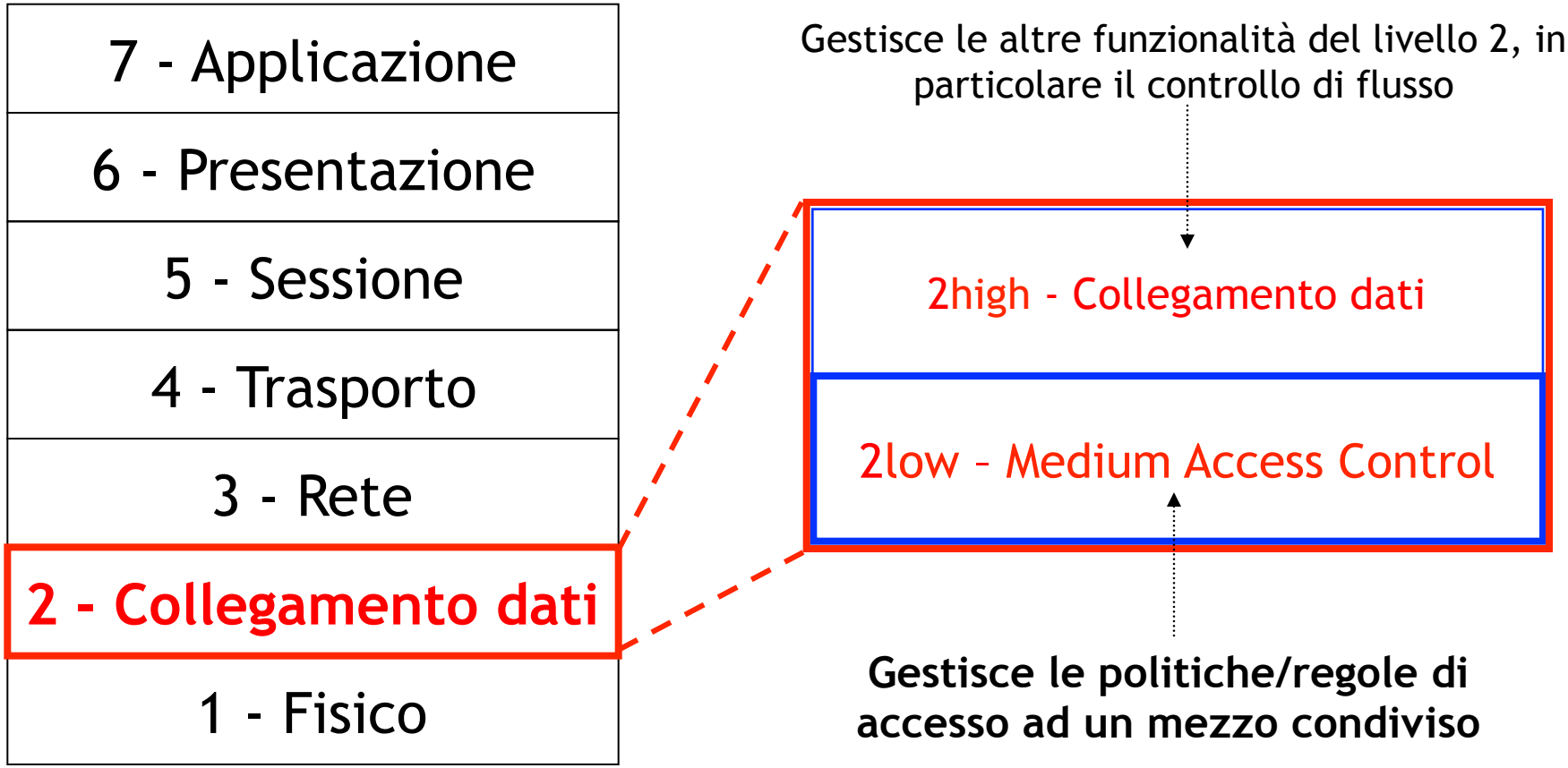


Il sotto-livello MAC

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

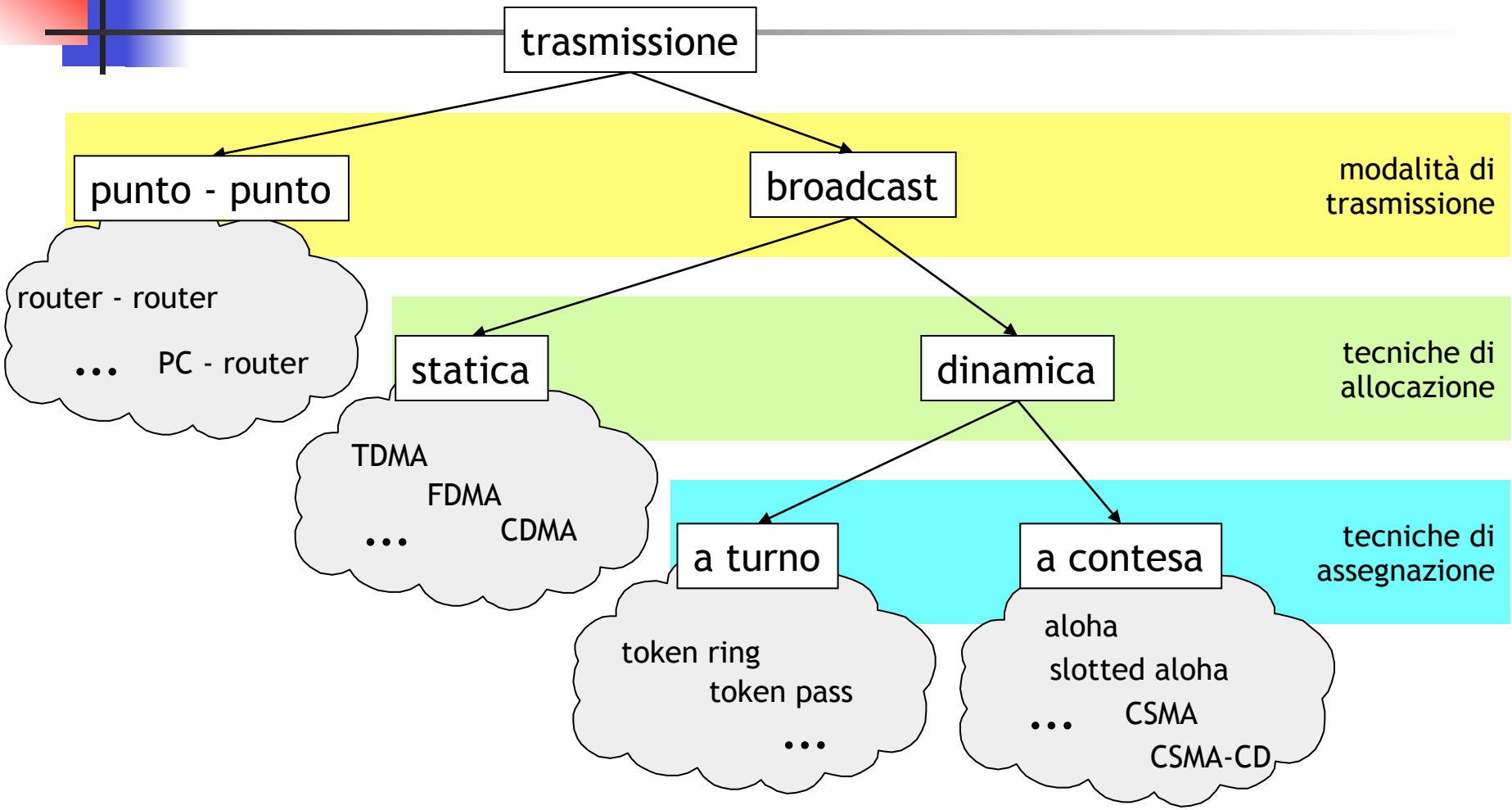
Allocazione statica

- Soluzioni "tradizionali"
  - Frequency Division Multiple Access (FDMA)
  - Time Division Multiple Access (TDMA)
  - Code Division Multiple Access (CDMA)
- 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

Single channel assumption

- unico canale per tutte le comunicazioni

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

Collision assumption

- due trame contemporaneamente presenti sul canale generano collisione
- non sono presenti altre forme di errore

Tempo...

- continuo: la trasmissione della trama può iniziare in qualunque istante
- *slotted*: la trasmissione della trama può iniziare solo in istanti discreti

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

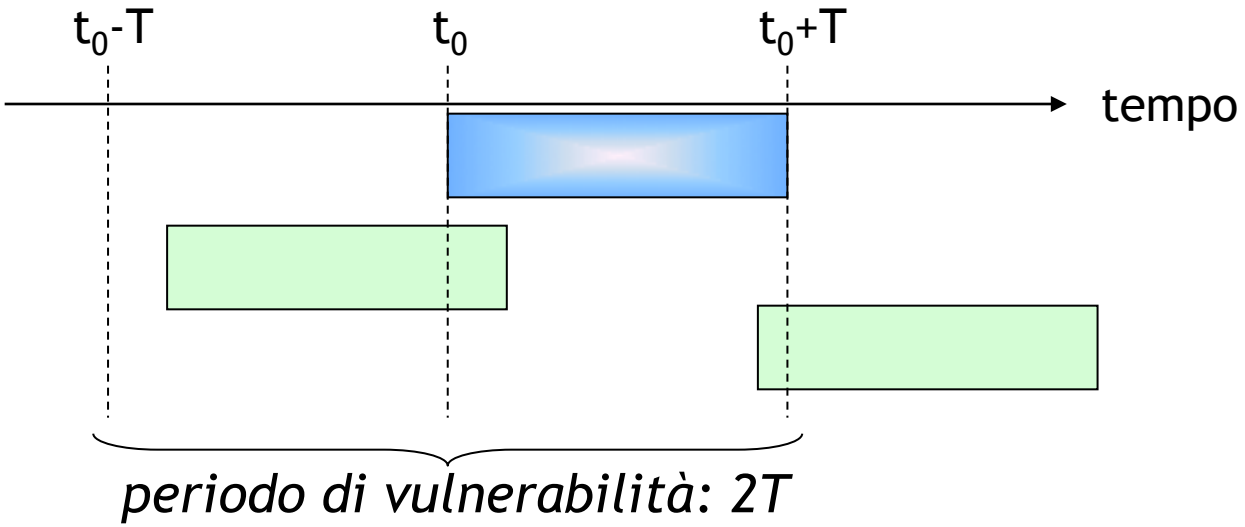
- In letteratura sono disponibili molti algoritmi di accesso multiplo al mezzo condiviso con contesa
- Principali algoritmi (utilizzati dai protocolli):
  - ALOHA
    - Pure ALOHA
    - Slotted ALOHA
  - Carrier Sense Multiple Access Protocols
    - CSMA
    - CSMA-CD (Collision Detection: con rilevazione della collisione)
    - CSMA-CA (Collision Avoidance: con tecniche per ridurre la probabilità di 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)*
  - se il canale è cablato la sorgente ascolta il canale per rilevare **collisioni**, se wireless il ricevitore invia esplicitamene un ACK di ricezione
  - **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)

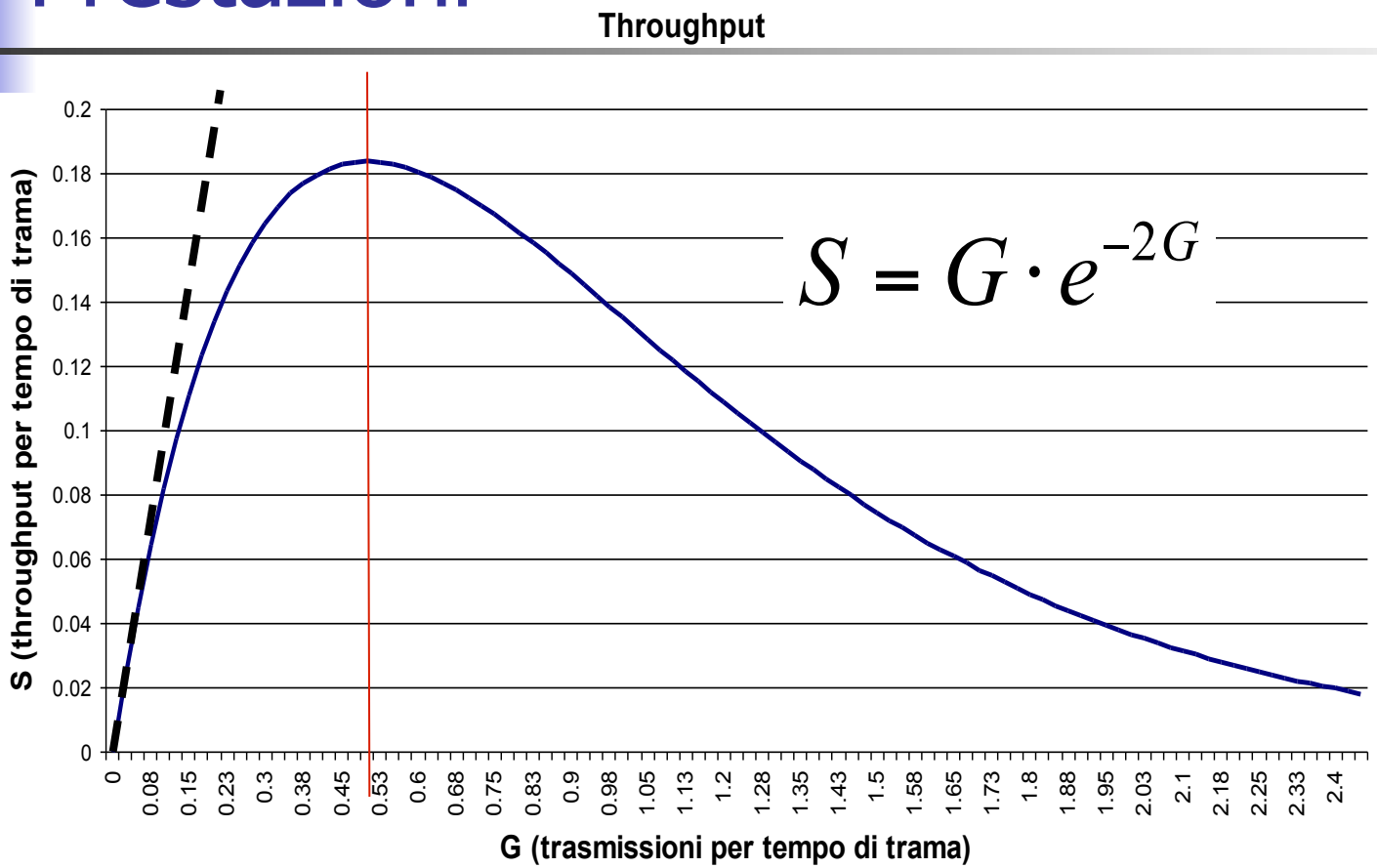
    → S = G*P[0 trasmissioni per 2T], ovvero

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

G = numero medio di trame trasmesse nel tempo di trama

S = numero medio di trame trasmesse con successo (throughput)

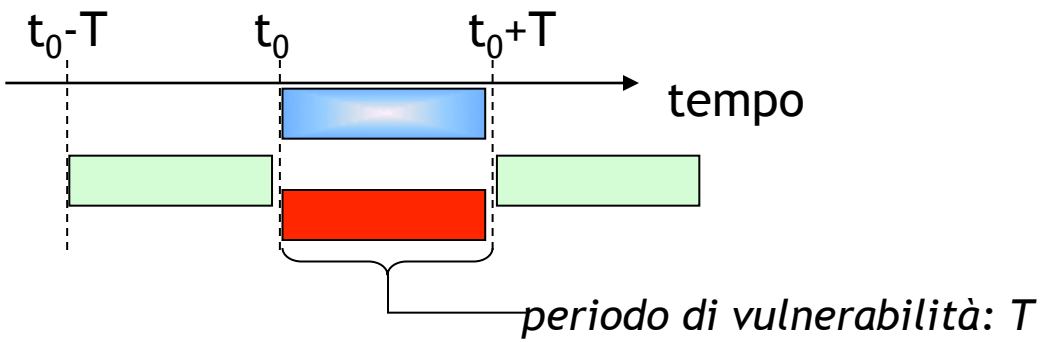
Prestazioni



- ALOHA permette al massimo di sfruttare il 19% del tempo, il massimo si ha quando il traffico offerto è 0.5 volte la capacità del canale. **Protocollo instabile!!**

Slotted ALOHA

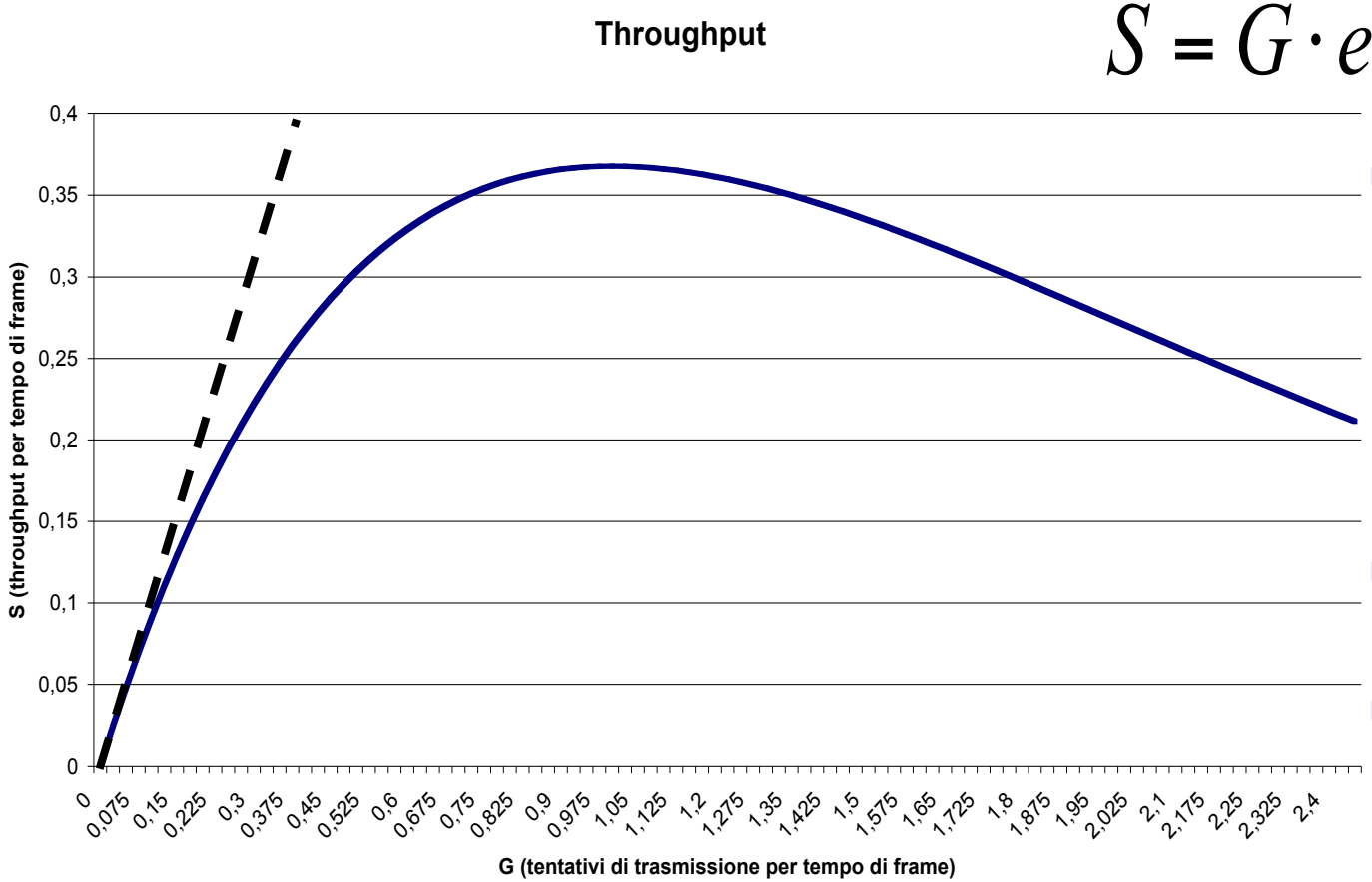
- Proposto nel 1972 da Roberts per migliorare la capacità di Pure ALOHA
- Basato su ipotesi di *slotted time* (tempo suddiviso ad intervalli discreti)
- Algoritmo:
  - Pure ALOHA
  - la trasmissione di una trama può iniziare solo ad intervalli discreti
  - necessaria sincronizzazione tra stazioni
- Periodo 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 a carico 1
- Il protocollo è instabile!!
- Bisogna distribuire un sincronismo

Carrier Sense Multiple Access (CSMA)

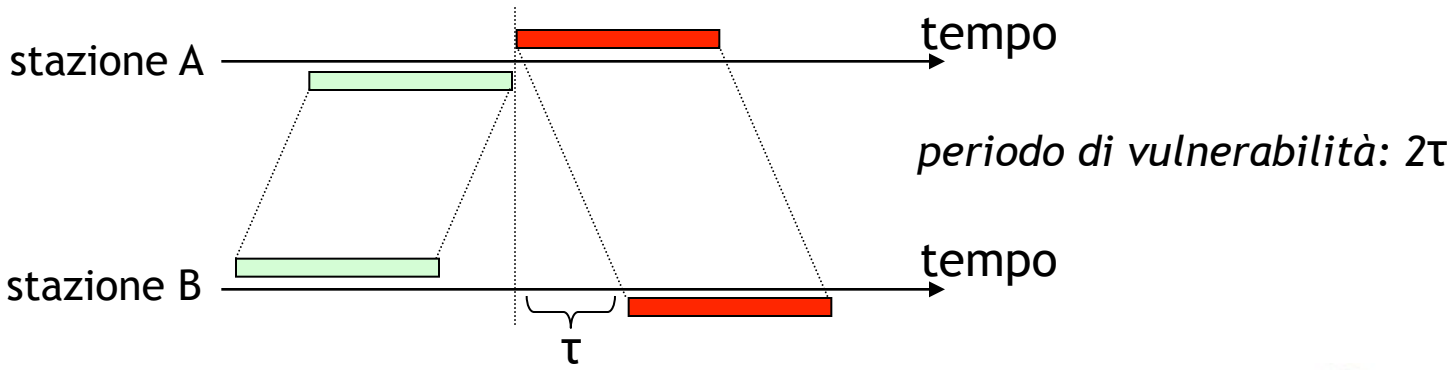
- Ambito LAN: le stazioni possono monitorare lo stato del canale di trasmissione (ritardi bassi)
- Le stazioni sono in grado di "ascoltare" il canale *prima di iniziare a trasmettere* per verificare se c'è una trasmissione in corso
- Algoritmo
  - se il canale è libero, si trasmette
  - se è occupato, sono possibili diverse varianti
    - non-persistent (0-persistent)
      - rimanda la trasmissione ad un nuovo istante >> tempo di trasmissione, scelto in modo casuale
    - persistent (1-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

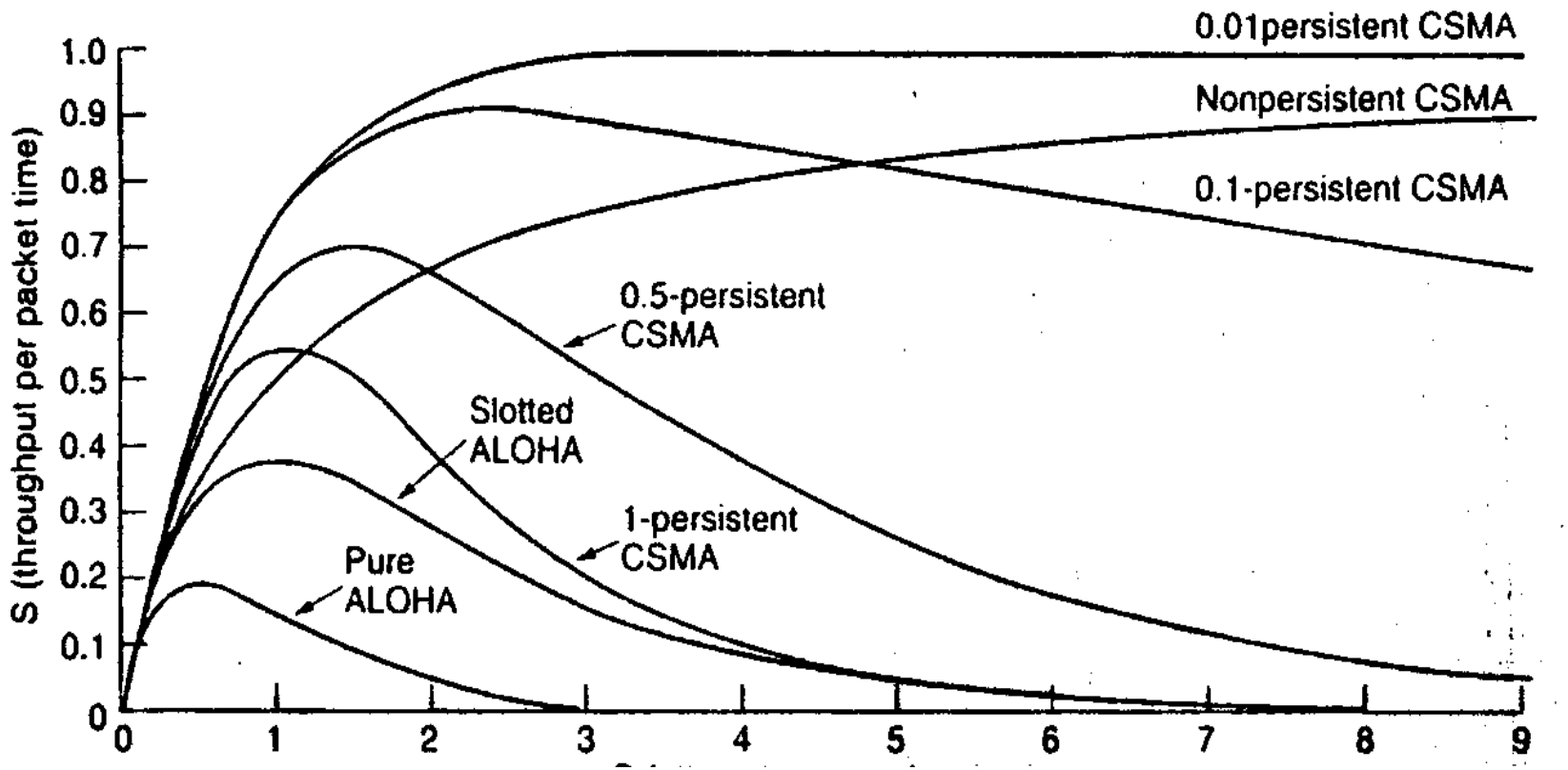
- Il tempo viene suddiviso in intervalli
  - la lunghezza degli intervalli è uguale al periodo di vulnerabilità
    - *round trip propagation delay* 2τ
- Algoritmo
  1. ascolta il canale
     - se il canale è libero **si trasmette**;
     - se è occupato, si attende che il canale diventi libero
       - quando 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 >> del tempo di trasmissione T e si torna al punto 1
  2. se c'è collisione
     - si attende un tempo casuale (>>T) 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 → 2 τ
- 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

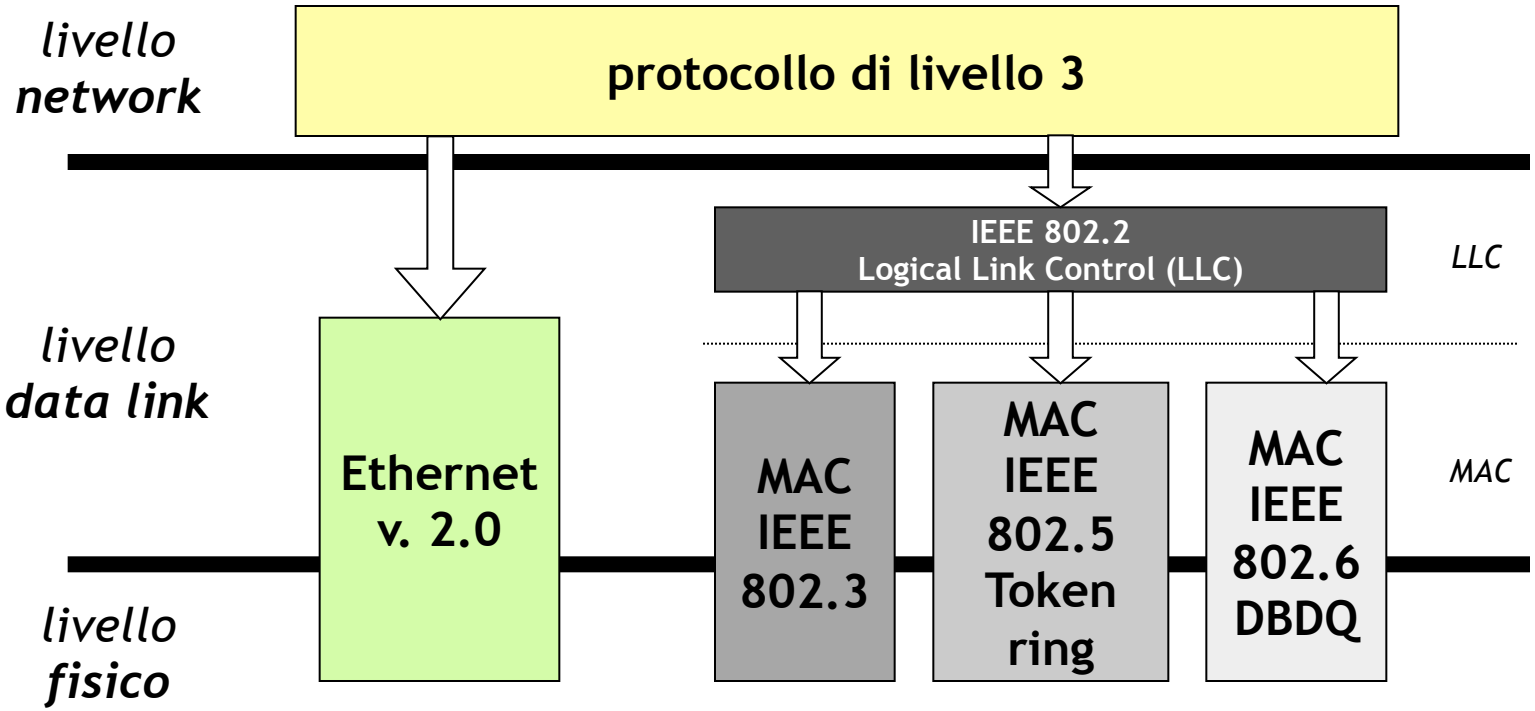
Le LAN sotto IP

- L'elemento unificante è il protocollo di Rete
  - il livello 3 ha la visibilità globale della rete e della sua topologia
- 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 backbone (non le vediamo)
    - Frame Relay
    - ATM
    - SDH
    - Carrier Ethernet
    - IP over Optical

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

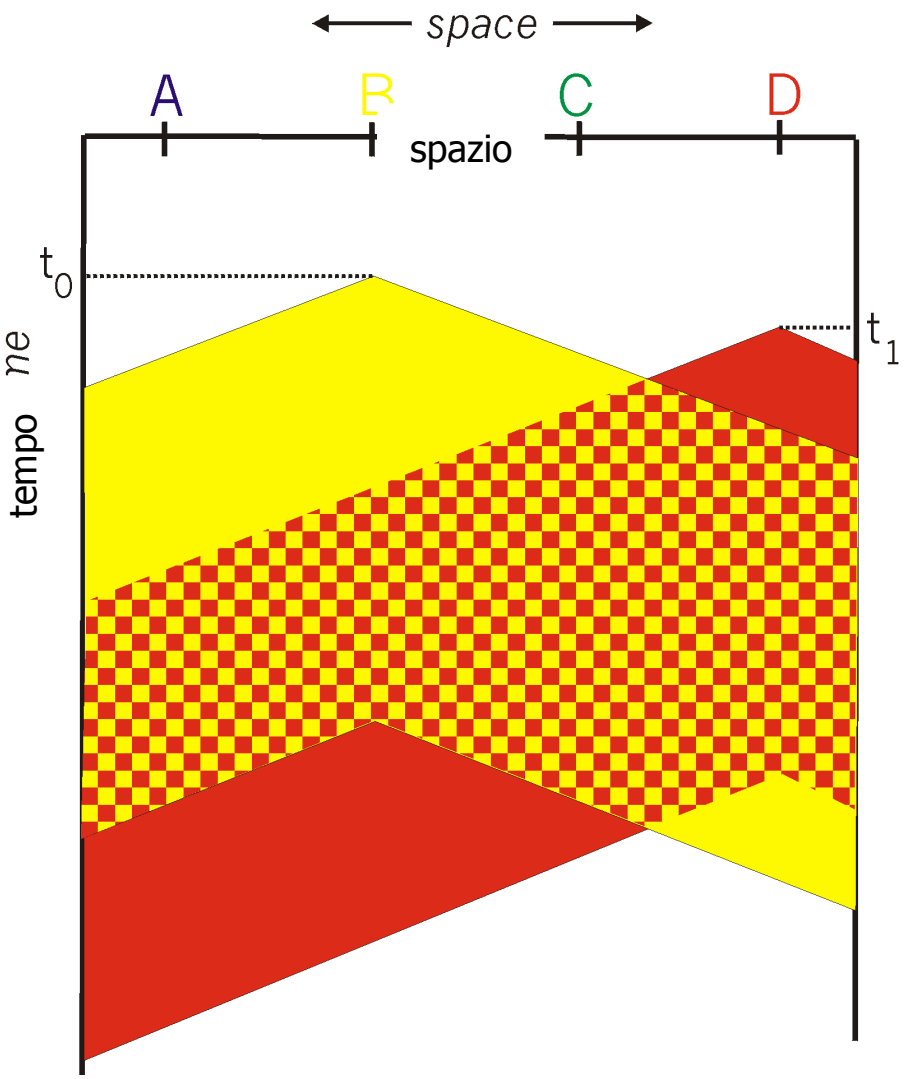


Ethernet e Standard IEEE 802.3
Algoritmi implementati

- 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

CSMA: collisioni?

- Si verificano a causa dei ritardi di propagazione e sono inevitabili
- Collisione: spreco completamente tempo di trasmissione pacchetto
- Note:
  - la distanza (ritardo di propagazione) gioca ruolo fondamentale nella probabilità di collisione
  - con pacchetti di grandi dimensioni, a parità di traffico trasmesso, riduco il numero di contese, e quindi di collisioni



Prestazione CSMA

- Dipendenti da rapporto tra dimensione della rete e dimensione del pacchetto
- Lo 'spreco' di risorse è legato al rapporto tra il tempo di propagazione tp e il tempo di trasmissione del pacchetto Ttx

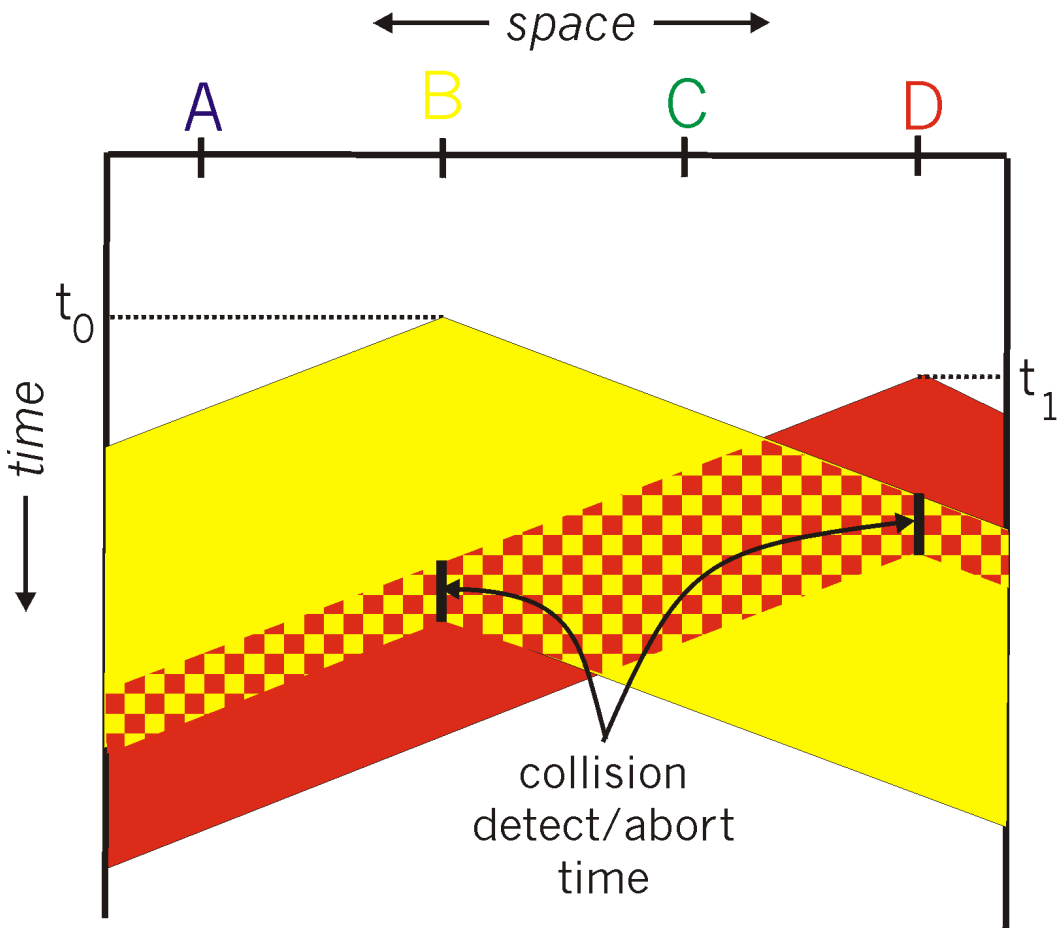
$$a = \frac{t_p}{T_{TX}}$$

CSMA/CD (Collision Detection)

- Vantaggi di CSMA/CD su CSMA:
  - se mi accorgo (in fretta) delle collisioni sospendo la trasmissione del pacchetto
  - riduco lo spreco dovuto ad una trasmissione inutile
- Collision detection:
  - facile nelle LAN cablate: misuro potenza segnale, confronto segnale ricevuto e trasmesso
  - difficile in LAN wireless: half duplex (quando trasmetto ricevitore disattivo)

CSMA/CD collision detection

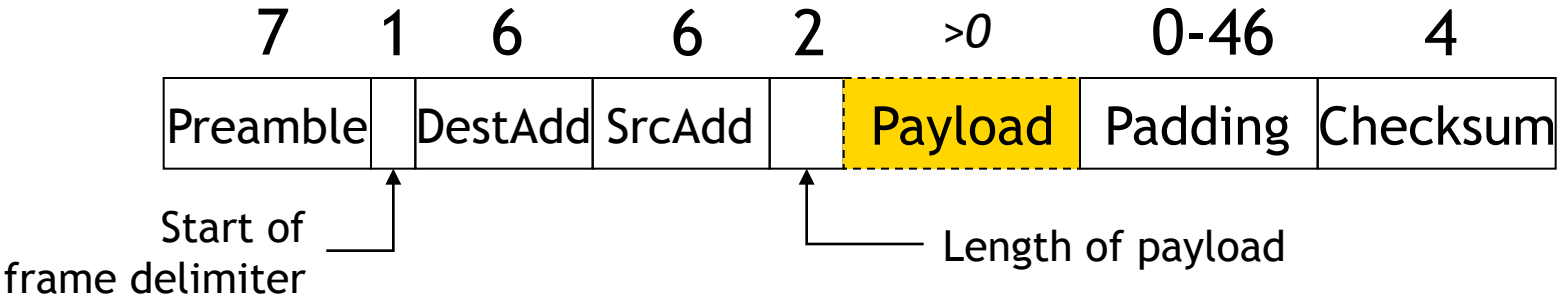
È necessario che il rapporto Ttx/tp sia tale da consentire l'identificazione della collisione e che venga trasmessa una sequenza speciale (dopo aver rilevato la collisione) per consentire a tutti di "capire" che c'è stata una collisione



CSMA/CD: prestazioni (1)

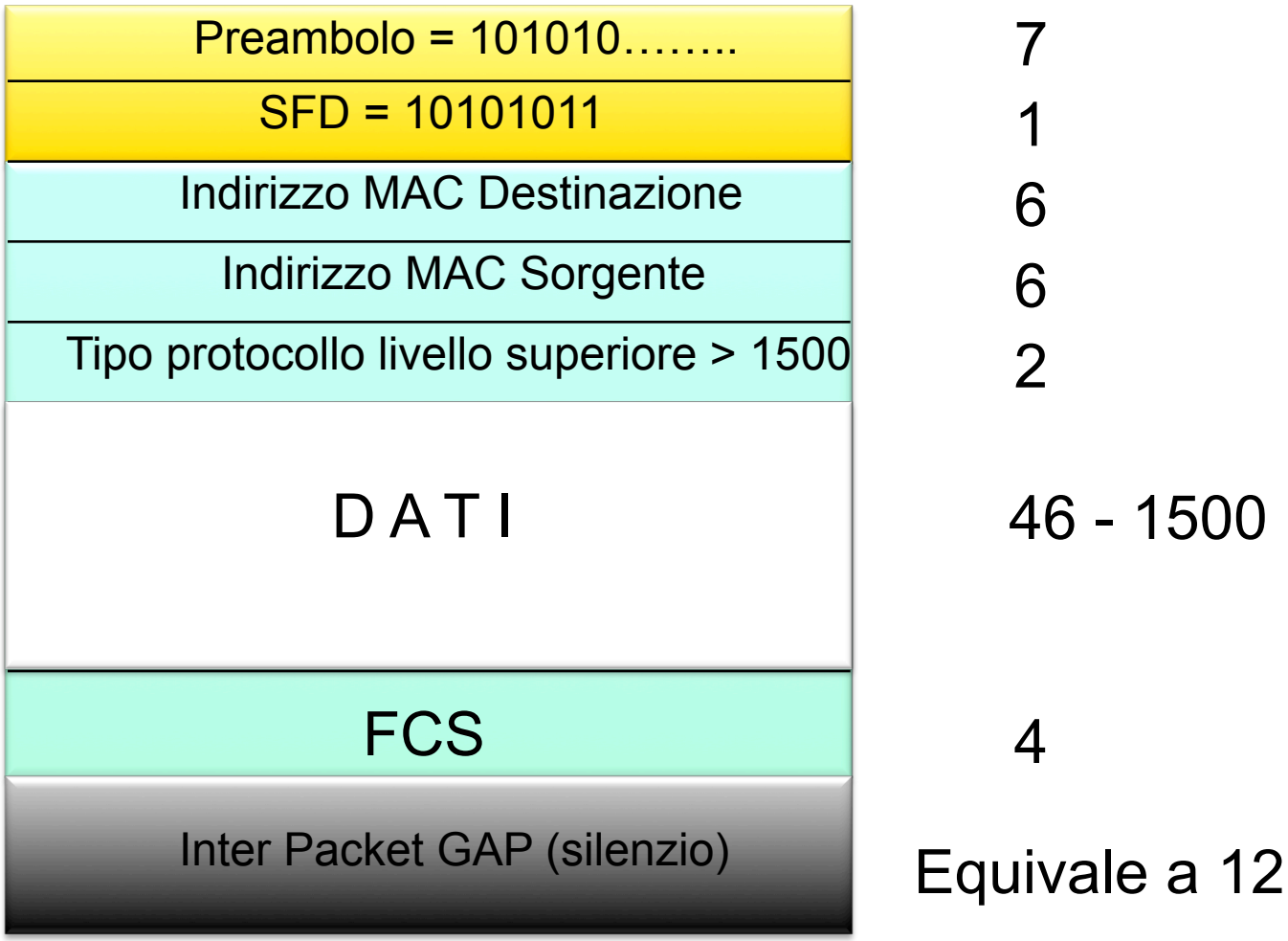
- Si hanno prestazioni migliori
  - su reti piccole: riduco periodo di vulnerabilità (pari al ritardo di propagazione sul canale)
  - su reti piccole rispetto alla dimensione del pacchetto *(*parametro *'a'* piccolo)*:* collisione rilevata prima, riduco lo spreco
  - con velocità di trasmissione bassa: pochi bit trasmessi quando rilevo collisione

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

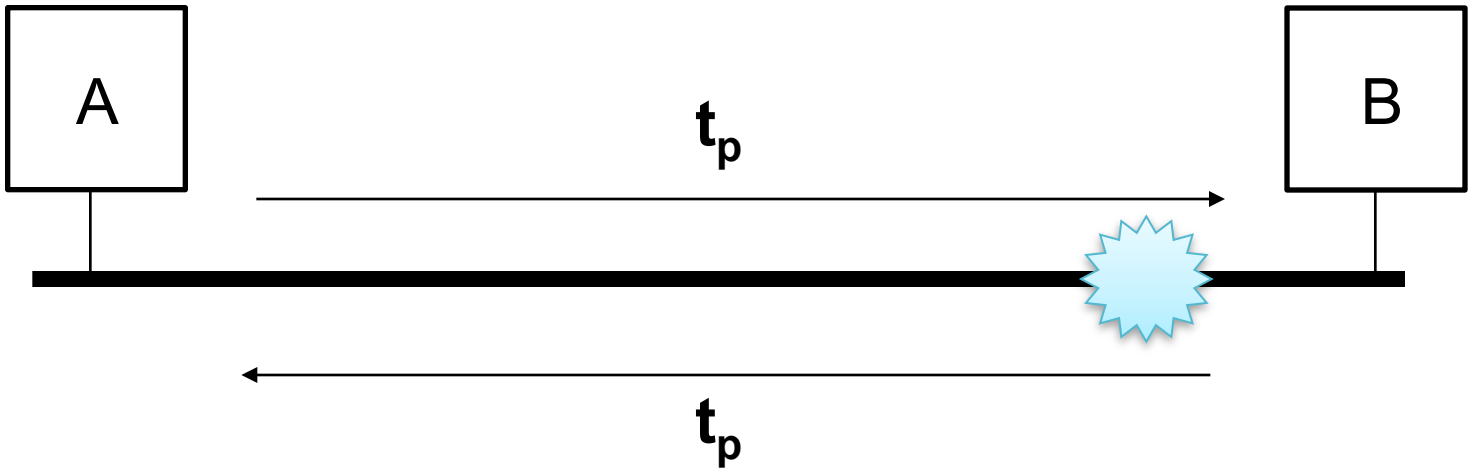
Ethernet: formato di trama



Round Trip Delay

- È il tempo necessario, nel caso peggiore, al segnale inviato da una stazione per arrivare all'altro estremo del cavo e a tornare indietro

$$\text{Round Trip Delay} = 2\ t_p$$



Ethernet: parametri di progetto

- Il tempo di trasmissione di una trama non può essere inferiore al RTD
- La velocità del mezzo trasmissivo e le dimensioni della rete determinano quindi la lunghezza minima della trama
- La lunghezza di trama dipende anche dall'IPG (Inter-Packet Gap), che segnala la fine trama
- Diametro del Collision Domain

Collision Domain

- Il collision domain è quella porzione di rete Ethernet in cui, se due stazioni trasmettono simultaneamente, le due trame collidono
  - spezzoni di rete connessi da repeater sono nello stesso collision domain
  - spezzoni di rete connessi da dispositivi di tipo store and forward (bridge, switch o router) sono in collision domain diversi

Diametro di un Collision Domain

- Con il termine diametro di un collision domain si indica la distanza massima tra ogni possibile coppia di stazioni
- Il diametro massimo di un collision domain a 10Mbit/s è di 2800m e dipende da:
  - lunghezza massima dei cavi (attenuazione del segnale che induce uso di repeater, con ritardo aggiuntivo)
  - ritardo di propagazione (round trip delay)

Caratteristiche MAC Ethernet

- Per garantire buone prestazioni (collisioni ridotte) non bisogna caricare troppo la rete
- Protocollo semplice e totalmente distribuito
- Non avendo un ritardo massimo non è adatto ad applicazioni real-time
- Ritardi di accesso piccoli a basso carico
- Standard per LAN più diffuso quindi ampia disponibilità di componenti di basso costo
- Non esistono conferme di avvenuta ricezione
- Non gestisce priorità

Ethernet: livello fisico

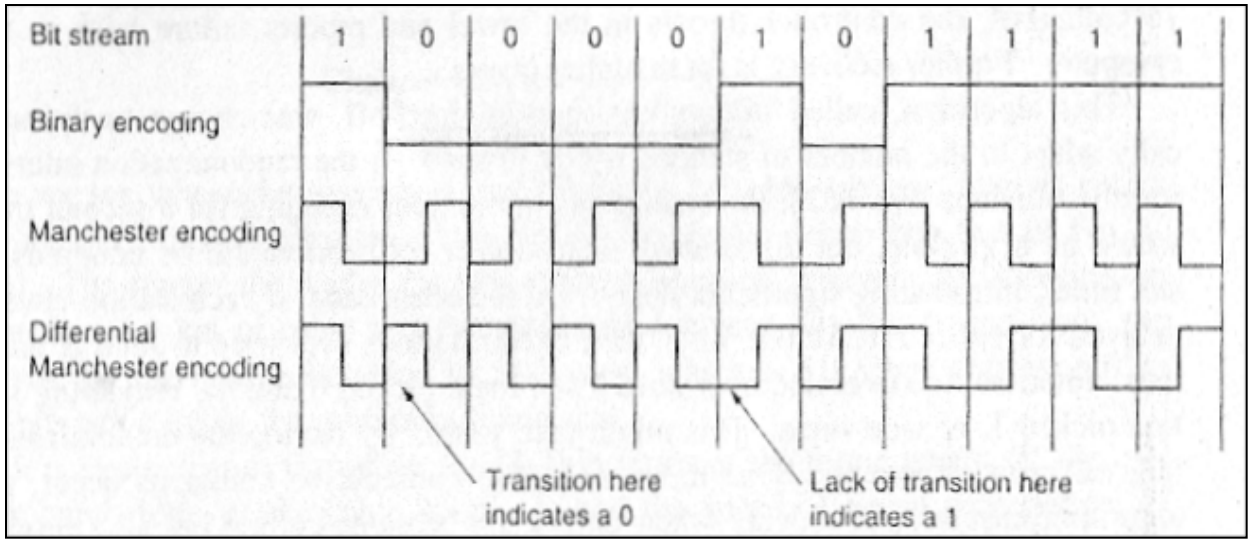
- Velocità trasmissione: 10 Mb/s (bit time = 0.1μs)
- Codifica Manchester (20Mbit/s di clock per facilitare recupero sincronismo in rete asincrona)
- Stazioni: max 1024 (2^{10})
- Mezzi trasmissivi:
  - 10 BASE 5: cavo coassiale spesso RG213
  - 10 BASE 2: cavo coassiale sottile RG58
  - 10 BASE T: doppino UTP da 100 Ohm
  - 10 BASE FL, 10 BASE FB, 10 BASE FP: fibra ottica multimodale

Ethernet: livello fisico

- Topologie:
  - bus o albero di bus: 10 BASE 5, 10 BASE 2
  - stella: 10 BASE T, 10 BASE FB, 10 BASE FP
- Possono essere utilizzati repeater
  - decodificano e ricodificano Manchester
  - rilevano collisione e la inoltrano su tutte le porte
  - rigenerano preambolo (802.3)
  - isolano segmenti di rete se si verificano 30 collisioni consecutive
  - possono ridurre preambolo e non modificare inter-packet gap o viceversa

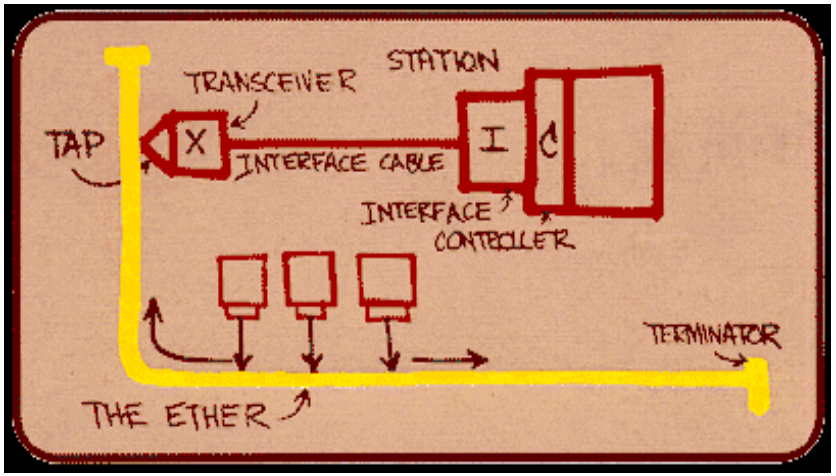
Codifica Manchester

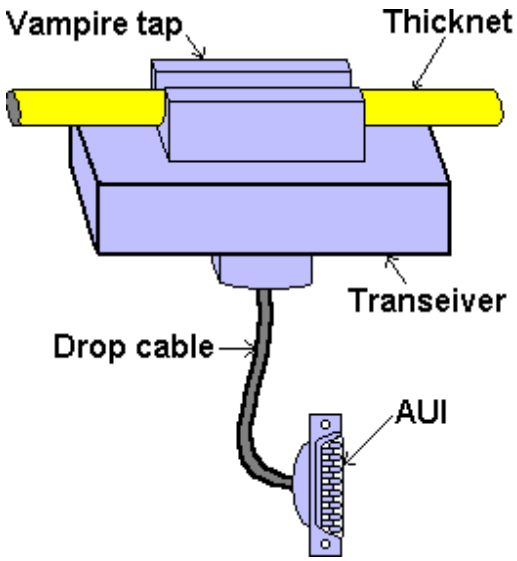
- Tradizionale
  - ogni periodo di bit è suddiviso in due sottoperiodi
    - "0" ⇨ basso,alto
    - "1" ⇨ alto basso
- Differenziale
  - ogni periodo di bit è diviso in 2 sottoperiodi
    - "1" assenza di transizione all'inizio del periodo di bit
    - "0" transizione all'inizio del periodo di bit



10 BASE 5

- Cavo coassiale spesso
  - stazioni collegate con transceiver cable
    e connessione a vampiro su cavo coassiale
- Su transceiver cable ho segnali tx, rx e collisione rivelata (e alimentazione)
- Topologia a bus, oppure a bus interconnessi a 10 Mb/s
- Lunghezza massima segmento coassiale 500 m (max 100 stazioni)
- Lunghezza massima transceiver cable 50 m
- Max 2 ripetitori tra due stazioni



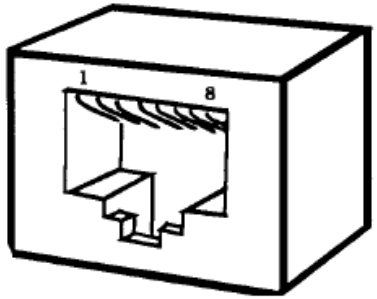


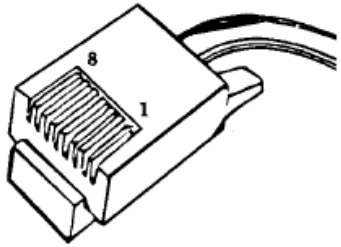
10 BASE 2

- Cavo coassiale sottile
  - stazioni connesse direttamente al cavo con connettore a T
- Transceiver incorporato nella scheda
- Lungh max segmento coassiale 185 m (max 30 stazioni)
- Stesse configurazioni di 10BASE 5 fino a 2800 m max
- Max 4 ripetitori tra due stazioni

10 BASE T

- Doppino UTP (Unshielded Twisted Pair)
- Collegamento punto punto tra stazioni e repeater (hub)
- Adatto a cablaggi strutturati
- Lunghezza massima del cavo 100 m
- Connettori RJ45 ad 8 fili (simile al telefono)





Ethernet: ritrasmissioni

- Slot time = 512 bit time (51.2 μs)
  - unità base di attesa prima di una ritrasmissione (pari ad un pacchetto di dimensione minima)
- In caso di n-esima collisione di un pacchetto, si ritrasmette dopo ritardo casuale estratto tra 0 e 2^k-1slot time, con k=min(n, 10)
- Backoff limit = 10
  - Numero di tentativi oltre al quale non aumenta più il valor medio del back-off
- Attempt limit n=16
  - Massimo numero di tentativi di ritrasmissione

Ethernet: parametri e temporizzazioni

- Inter Packet Gap = 9.6 μs
  - Distanza minima tra due pacchetti
- Jam size = da 32 a 48 bit
  - Lunghezza della sequenza di jamming
- Max frame size = 1518 ottetti
  - Lunghezza massima del pacchetto (esclude preambolo e interpacket gap)
- Min frame size = 64 ottetti (512 bit)
  - Lunghezza minima del pacchetto
- Addresssize = 48 bit
  - Lunghezza indirizzi MAC

Ethernet: parametri e temporizzazioni

- Pacchetto minimo 512 bit, ovvero 51.2 μs
- Round trip delay massimo ammesso dallo standard: 45 μs
- Si rispetta la condizione che il ritardo di propagazione non eccede la minima durata del pacchetto per garantire il rilevamento delle collisioni

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
  - ormai disponibile anche a 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)

Fast Ethernet

- Mantiene inalterato l'algoritmo CSMA-CD realizzato con 10Base-T e la dimensione dei pacchetti
- Tre standard per mezzi fisici (doppino su 4 coppie, doppino su 2 coppie, fibra)
- Trasmissione codifica 4B5B (di fatto si trasmettono 5 bit sul canale ogni 4 bit di informazione: la velocità effettiva sul canale è 125 Mbit/s)
- Riduce le dimensioni della rete
- La massima distanza tra due stazioni (collision domain) scende a 210m
- Interoperabilità con Ethernet 10Base-T

Gigabit Ethernet

- Uso formato di trama 802.3
- Operazioni half duplex e full duplex, ma usato in pratica solo in full duplex
  - si perdono vincoli legati a collision domain
  - CSMA/CD non utilizzato
- Controllo di flusso (definizione di master/slave)
- Backward compatibility con mezzi fisici già installati
- Aumenta di un fattore 10 dimensione minima di pacchetto con padding di caratteri speciali per consentire l'uso di CSMA/CD se necessario
- Definizione di Jumbo Frames per aumentare throughput massimo
  - Serve anche a consentire l'annidamento di protocolli e il tunneling.

Modifiche al protocollo

- Slot portato da 64 a 512 bytes (se ho pacchetti piccoli le prestazioni sono basse)
- Collision domain di 200 m
- Solo topologie a stella
- Consente la tecnica ”frame bursting” (o Jumbo Frames) per mantenere il controllo del canale fino ad un massimo di 8192 bytes (l’estensione della lunghezza minima del pacchetto è necessaria solo per il primo pacchetto)

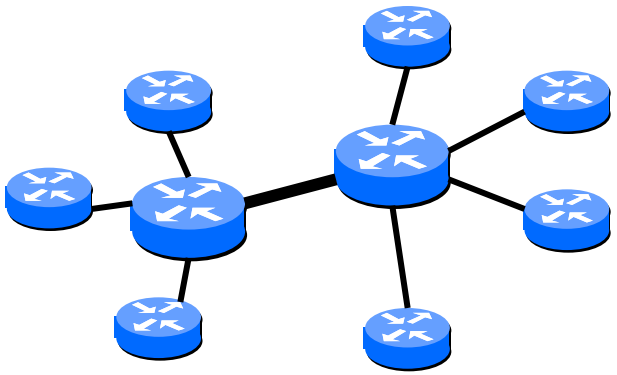
10 Gigabit Ethernet

- Il comitato IEEE 802.3 ha standardizzato 10, 40 e 100 Gbit/s Ethernet
- Solo la modalità full duplex, senza CSMA-CD
- Soluzioni proposte:
  - Seriale, con framing Ethernet, su distanze da LAN fino a 40 Km
    - 65 m su fibra multimodo (MMF)
    - 300 m su MMF installata
    - 2 km su fibra monomodo (SMF)
    - 10 km su SMF
    - 40 km su SMF
  - Seriale, su SONET, per distanze maggiori di 40 Km
- Per maggiori informazioni:
  - www.10gea.org
  - www.ieee802.org

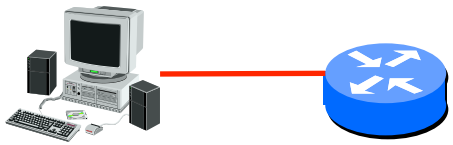
PPP: caratteristiche

- Point-to-Point Protocol: 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"

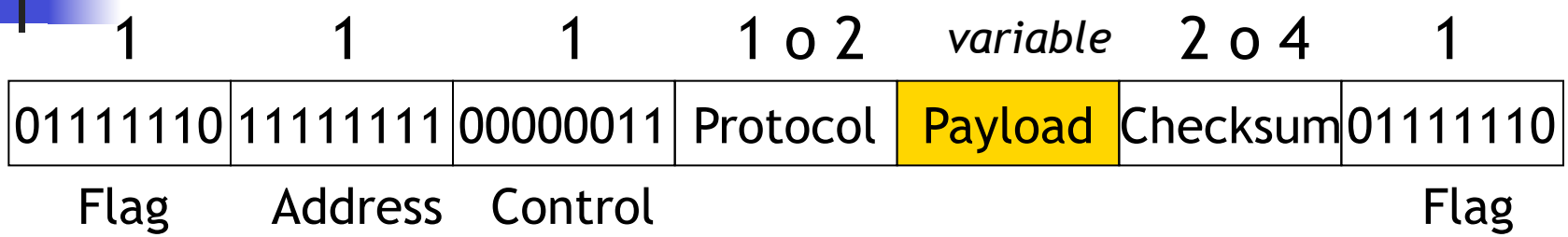
collegamento punto-punto tra router



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



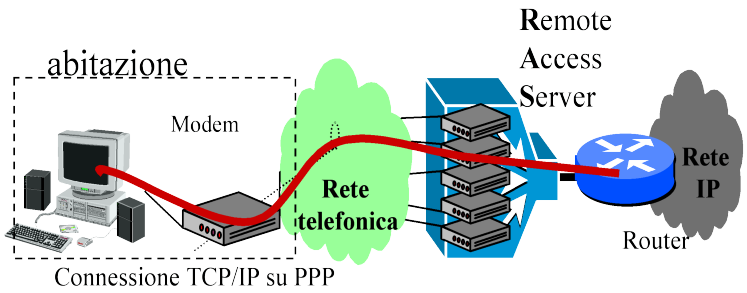
PPP: Formato della trama

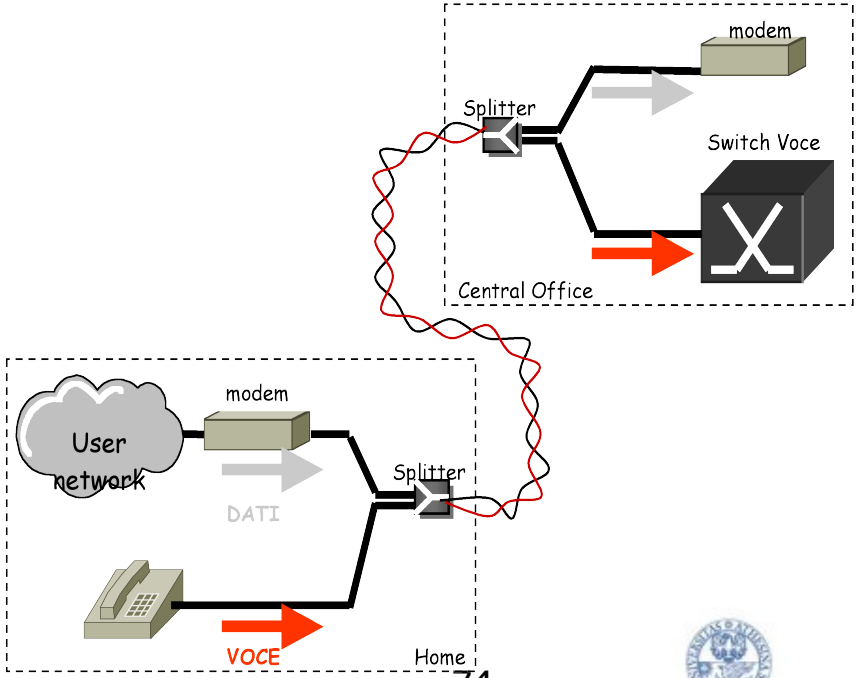


- Flag (1 byte)
  - identifica inizio e fine della trama ("01111110")
- Address (1 byte)
  - utilizzato in configurazione "tutti gli host"
- Control (1 byte)
  - valore predefinito "00000011" ⇨ *unnumbered*
  - di default non fornisce un servizio affidabile: richiesta di ritrasmissione e rimozione replicazioni 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

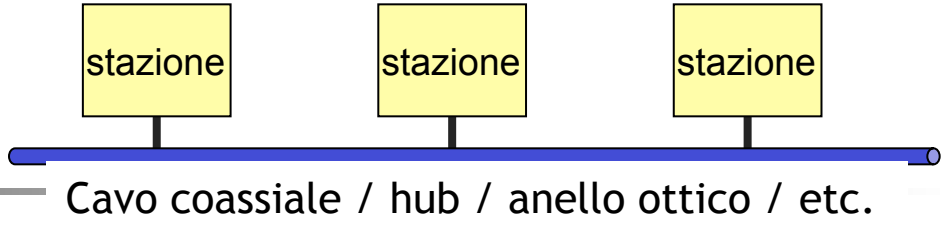
- Modem (es.: V.90)
  - utilizza la banda telefonica per inviare i segnali
  - ha limite estremo superiore 56 Kbps
- xDSL (Digital Subscriber Line)
  - famiglie di tecnologie che permette di utilizzare la banda disponibile del doppino telefonico
  - si possono distinguere in sistemi simmetrici e asimmetrici
  - 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





LAN estese

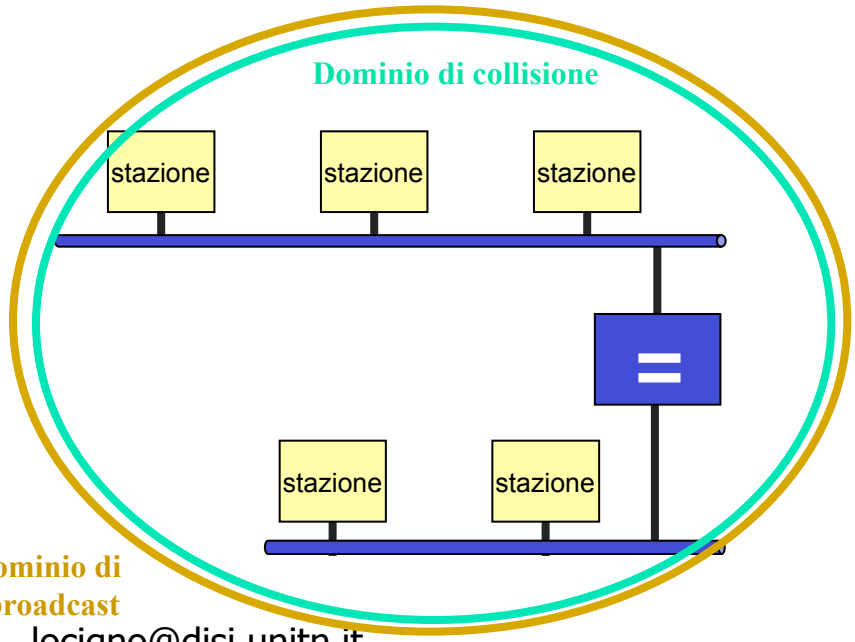
Introduzione

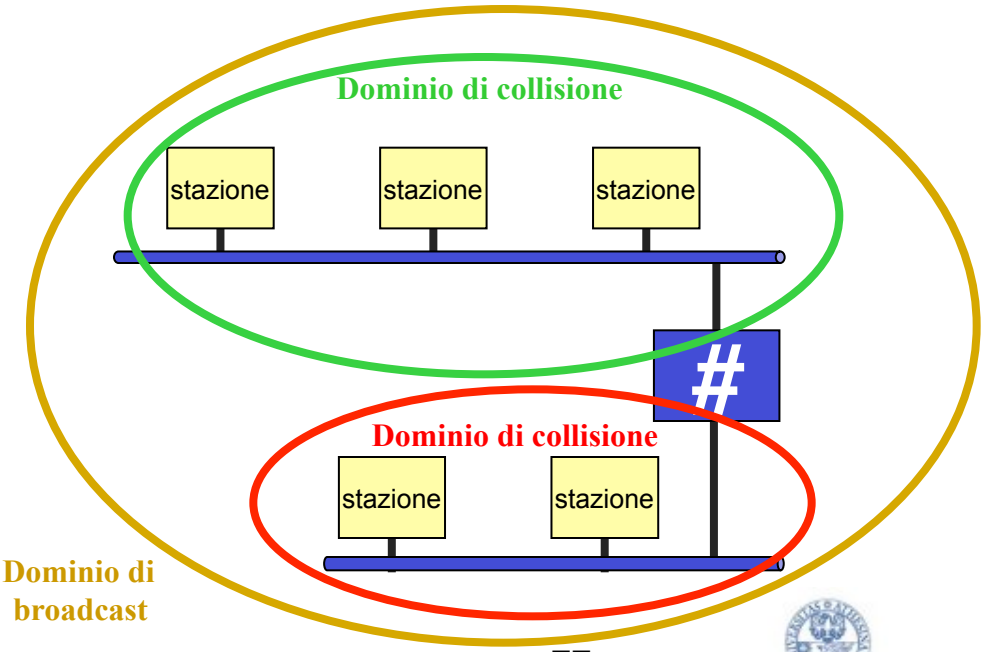


- La scelta di utilizzare mezzi condivisi per l'accesso al canale di trasmissione è stata fatta sia per necessità (ad es. trasmissioni wireless) sia motivi economici
- Grazie proprio agli aspetti economici, tale tecnologia è stata utilizzata e si è diffusa particolarmente nelle *reti locali* (Local Area 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

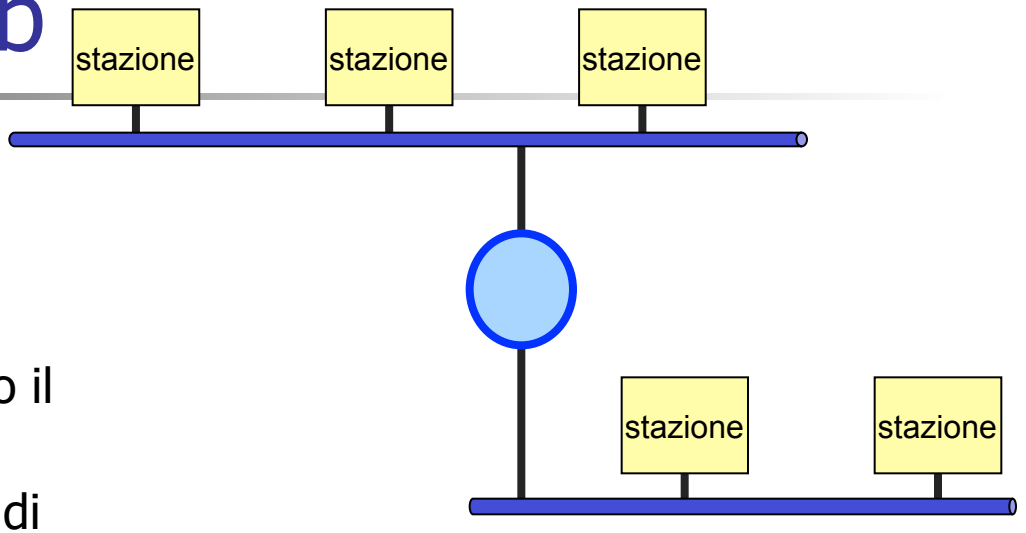
Dominio di collisione – Dominio di broadcast

- 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

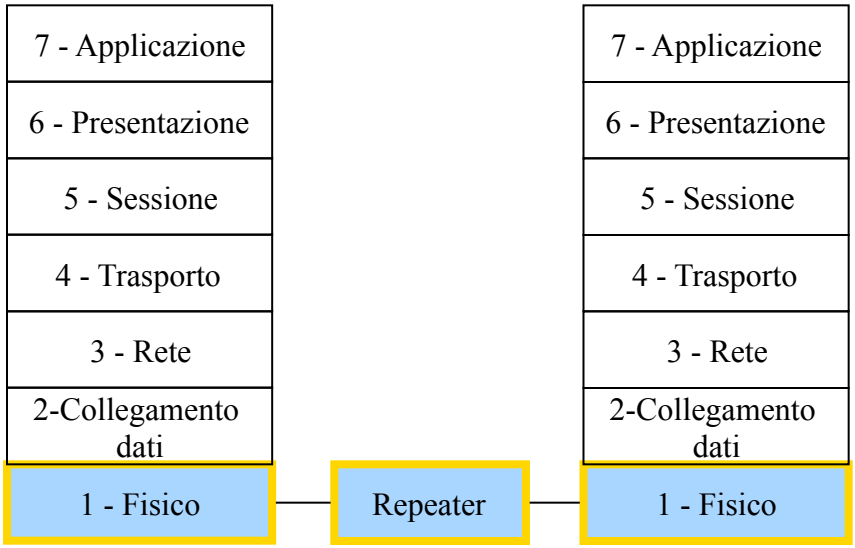




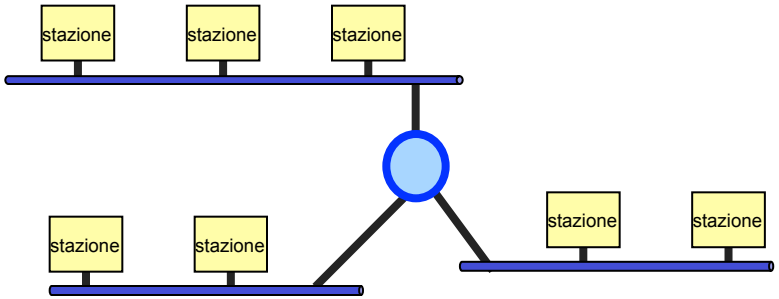
Repeater e Hub

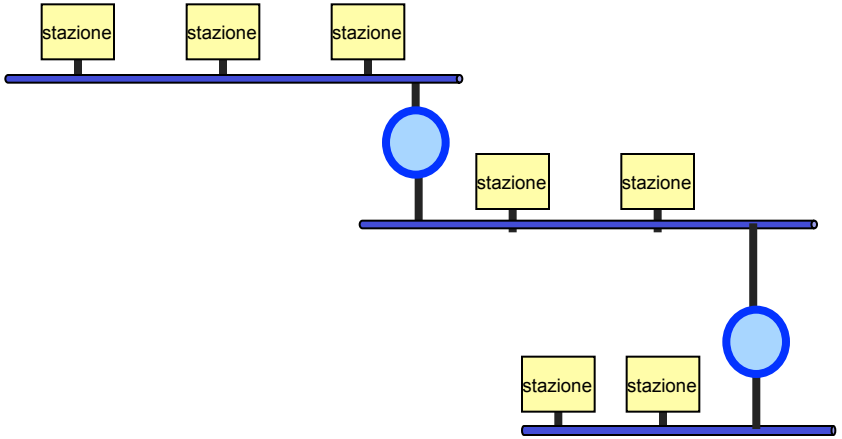


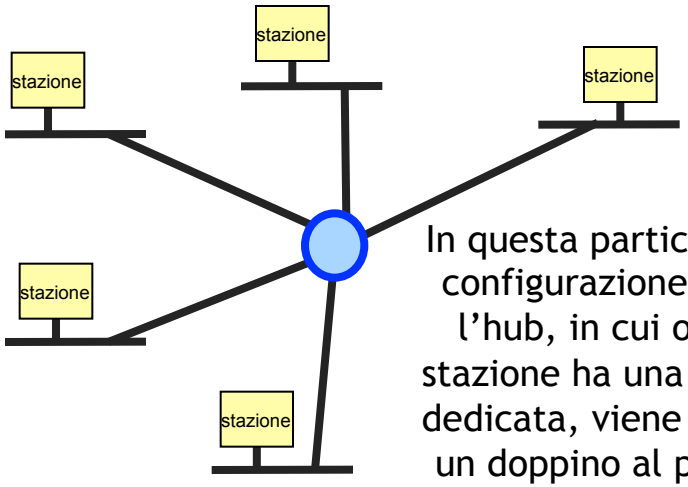
- Interviene solo a livello fisico ISO/ OSI
- Replica le trame in arrivo da un segmento ad un altro, amplificando il segnale
- I repeater possono connettere più di due segmenti
  - in questo caso di parla di ***Hub***
    - copia le trame che riceve su una porta su tutte le altre porte
  - il segnale 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



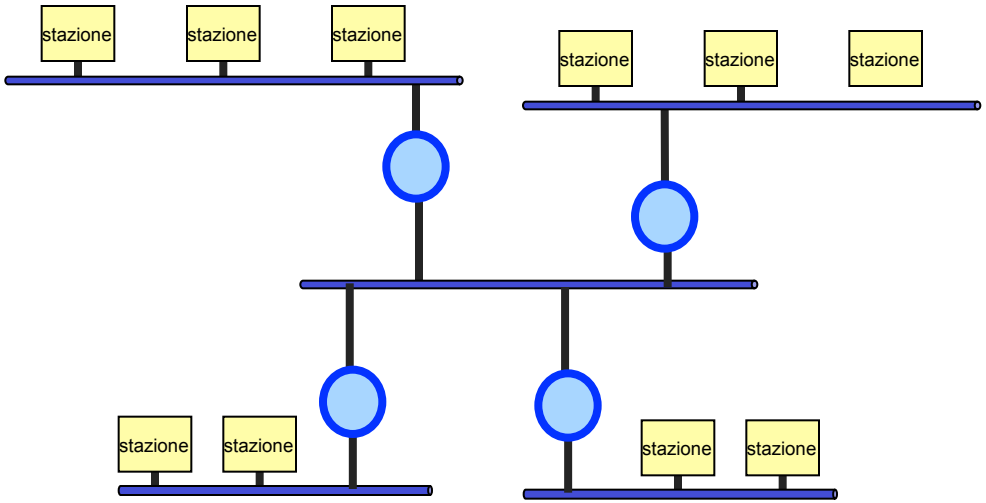
Alcune possibili combinazioni



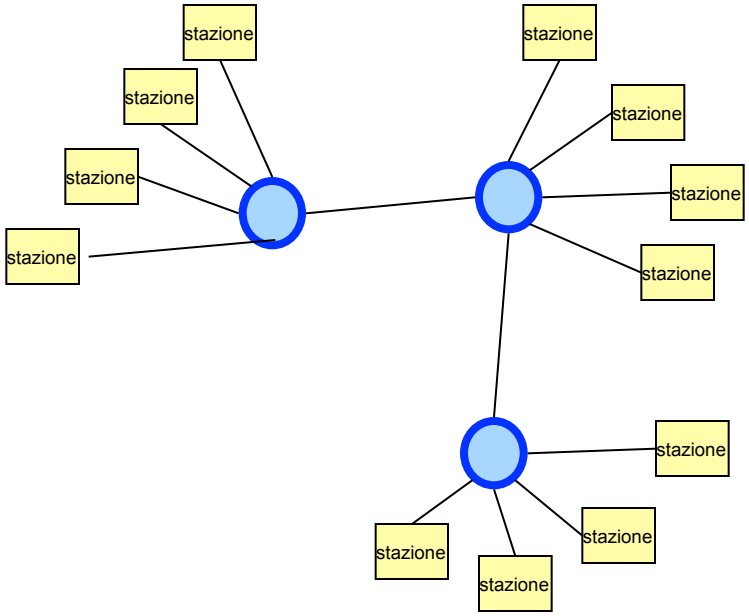


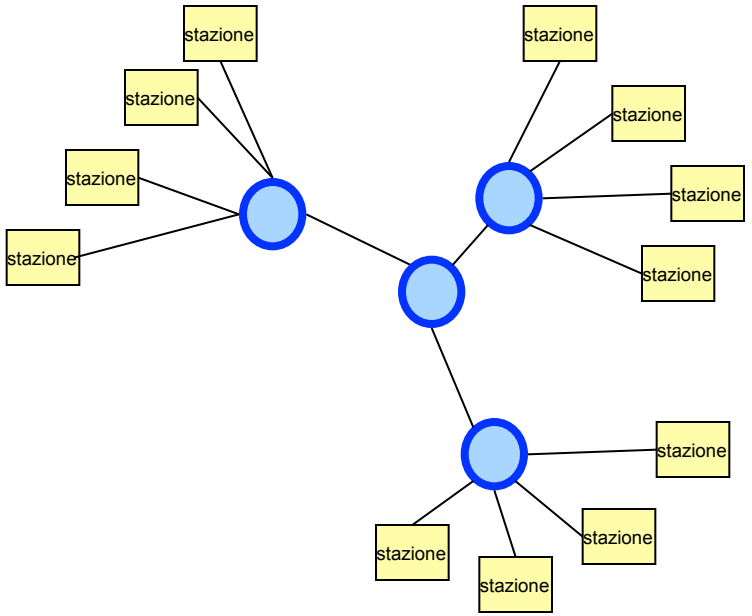


In questa particolare configurazione con l'hub, in cui ogni stazione ha una porta dedicata, viene usato un doppino al posto del cavo coassiale



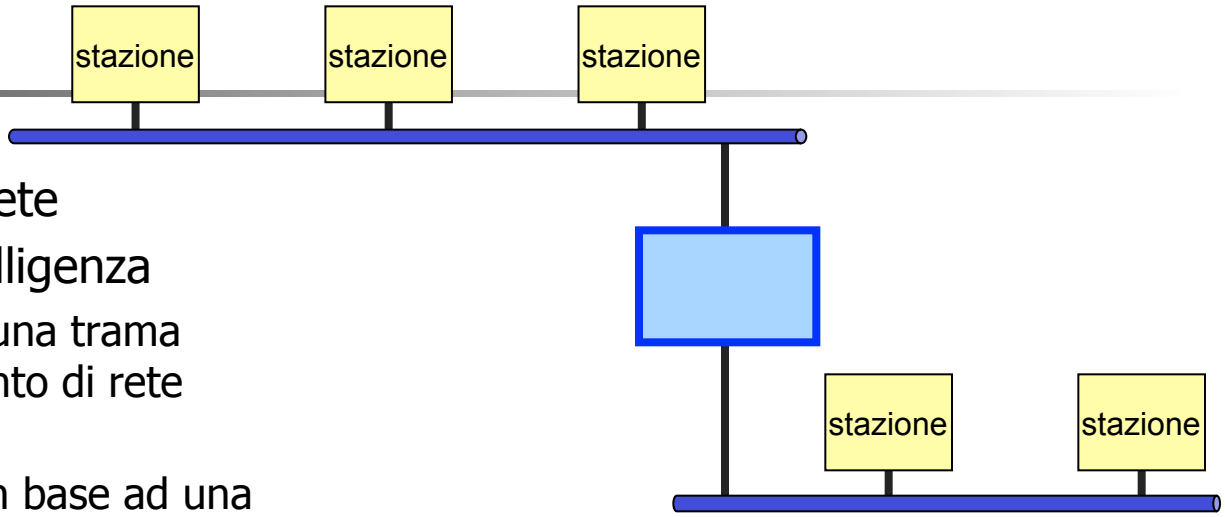
e ancora...



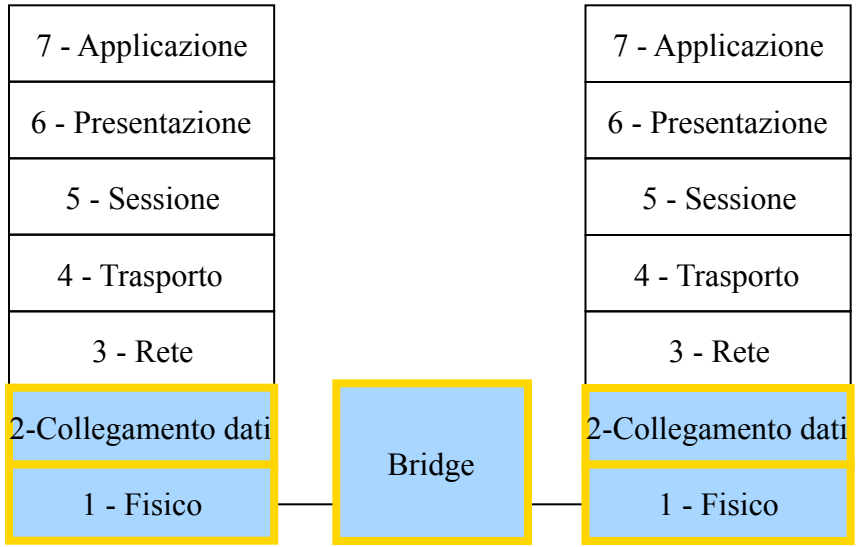


- Il problema legato a questo tipo di configurazioni è l'eccessiva estensione del dominio di collisione
  - con i repeater è come se tutte le stazioni condividessero lo stesso mezzo fisico

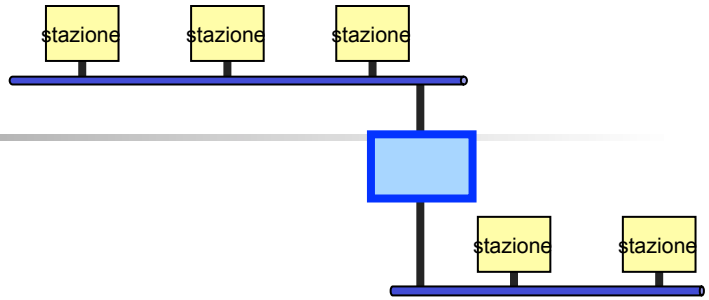
Bridge

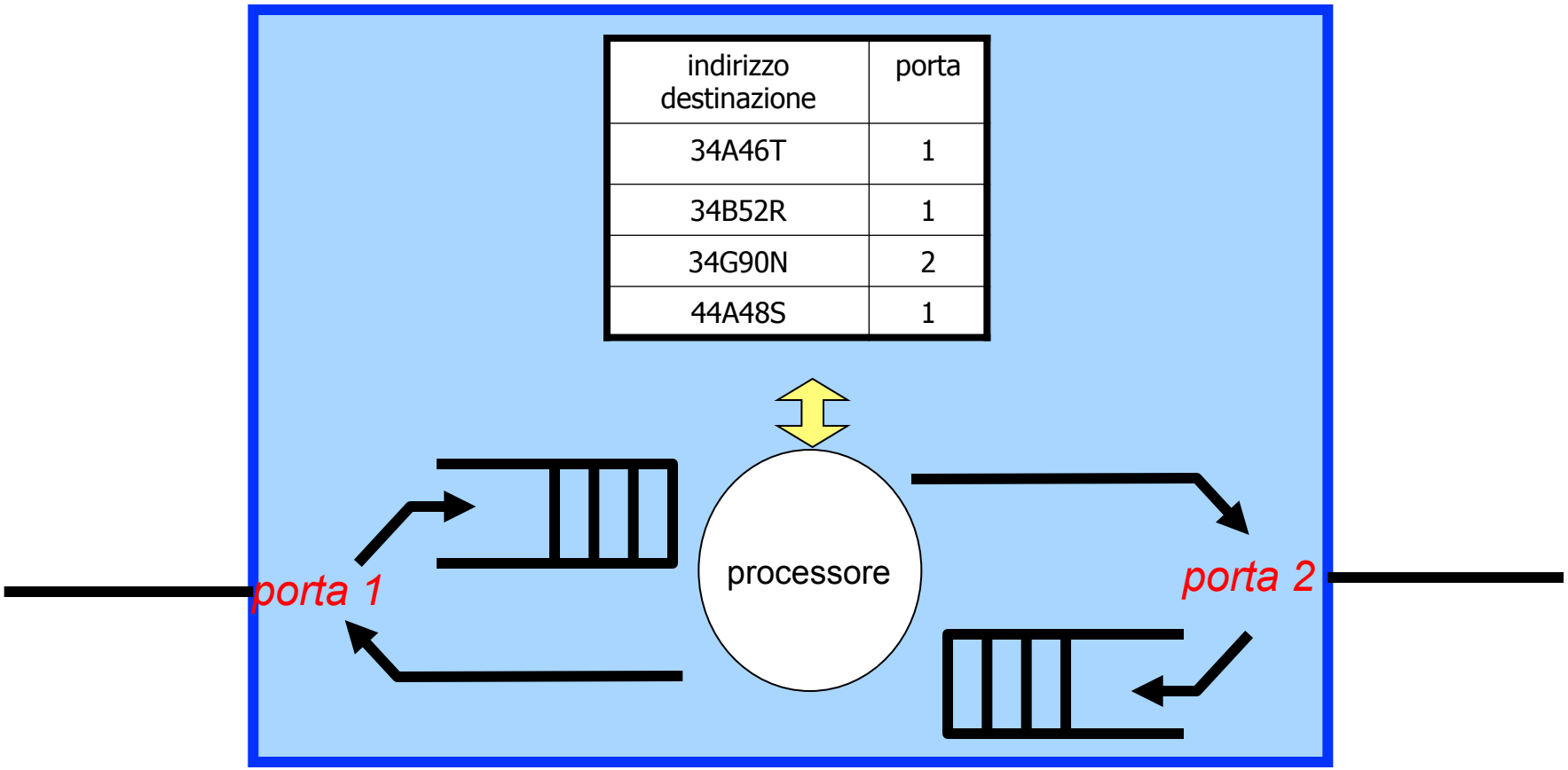


- Collega 2 segmenti di rete
- Apparato dotato di intelligenza
  - seleziona se ripetere una trama generata da un semento di rete sull'altro segmento
  - la selezione avviene in base ad una tabella che esso mantiene
  - in tale tabella c'è scritto quali stazioni fanno parte di ciascun segmento di rete
  - 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



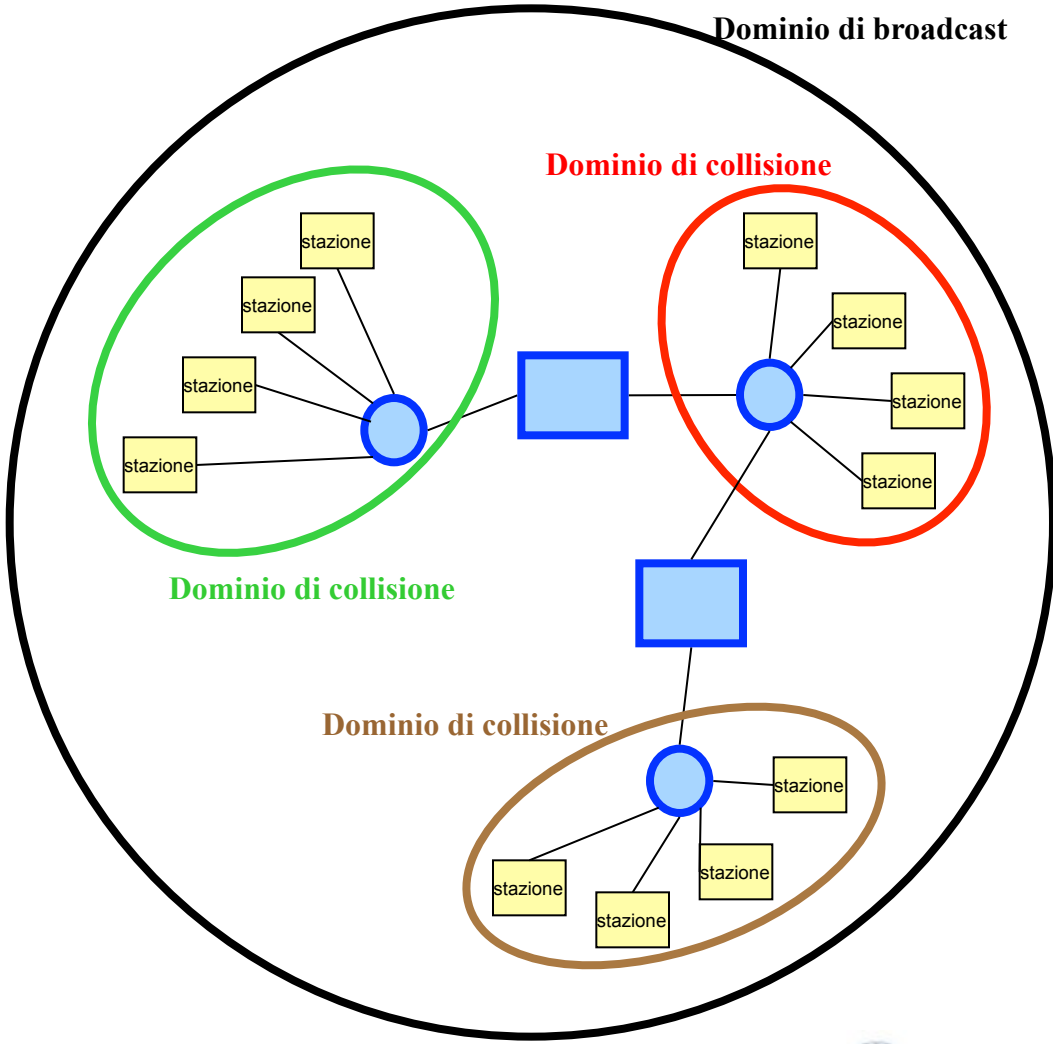
Schema di un bridge





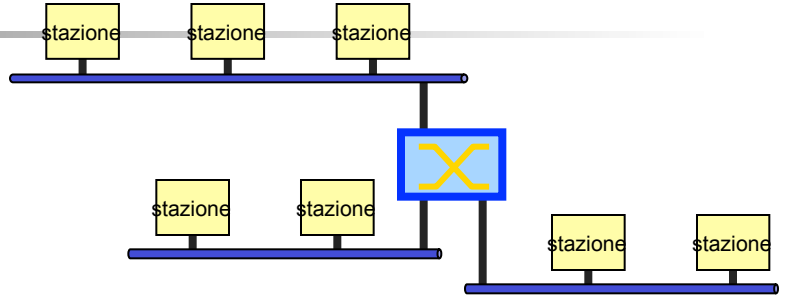
Bridge: esempio di configurazione

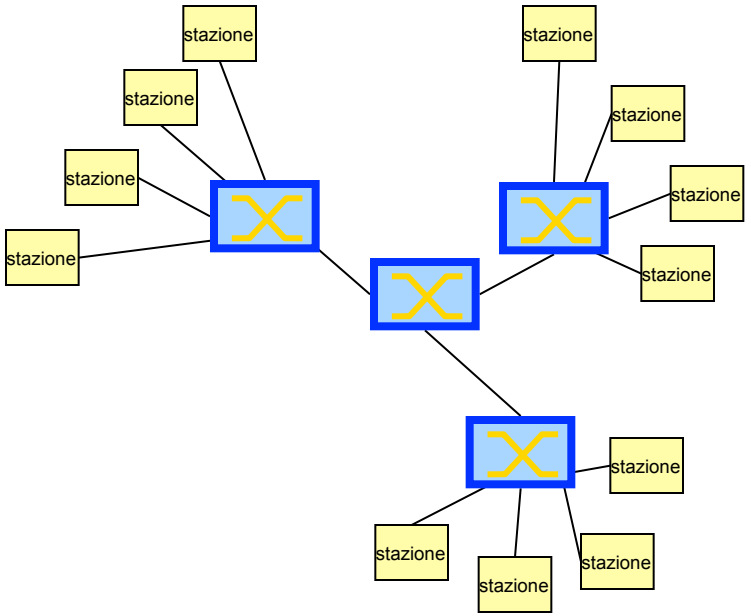
- Spezza il dominio di collisione, ovvero ciascun segmento di rete è conteso solo da chi è attestato sull'hub
- Gli hub vedono il bridge come una stazione qualsiasi che genera trame
- La trama è propagata dal bridge solo se il destinatario è attestato su un hub diverso da quello di origine
- Il concetto 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



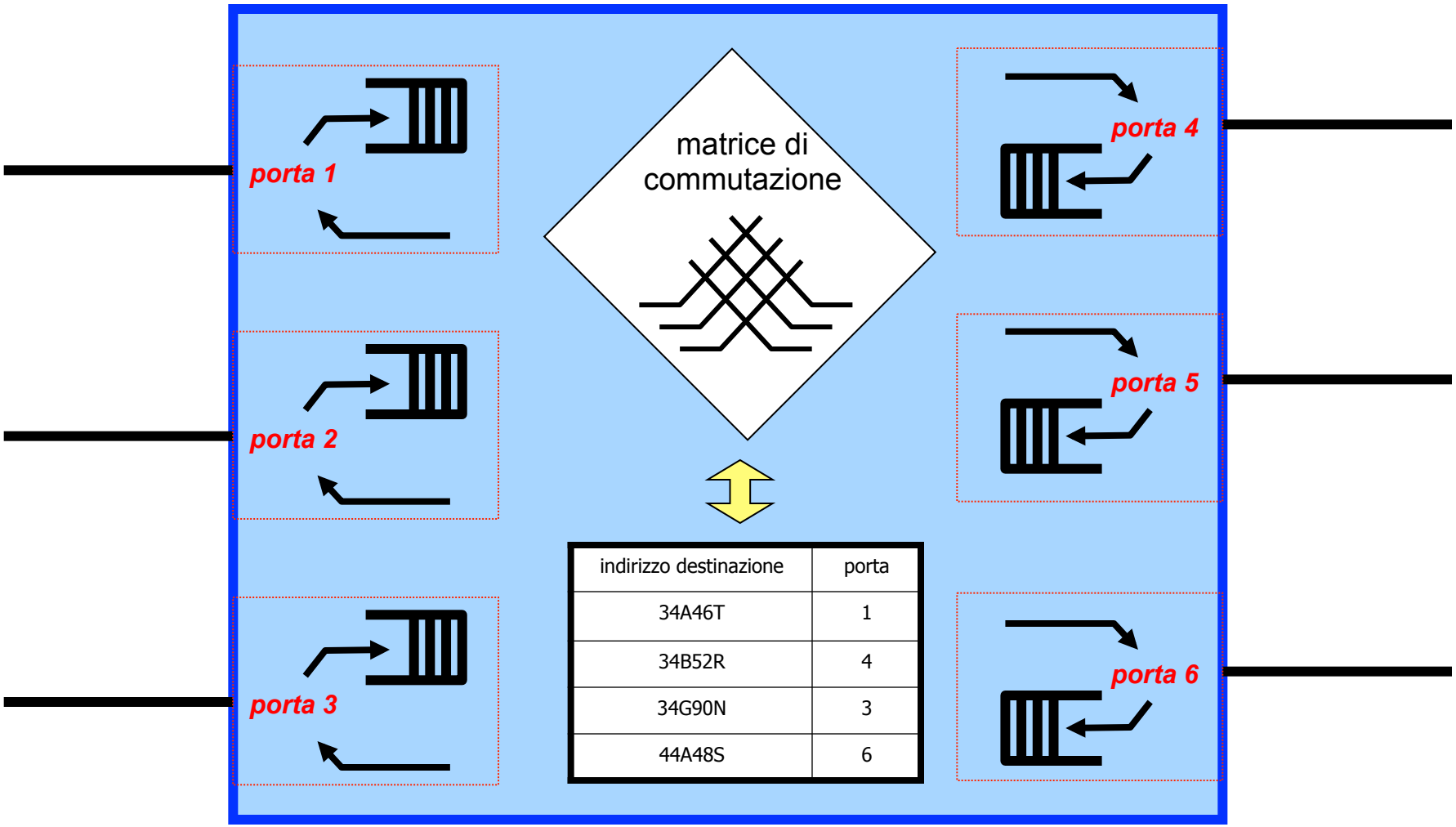
Evoluzione: Layer 2 Switch

- 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



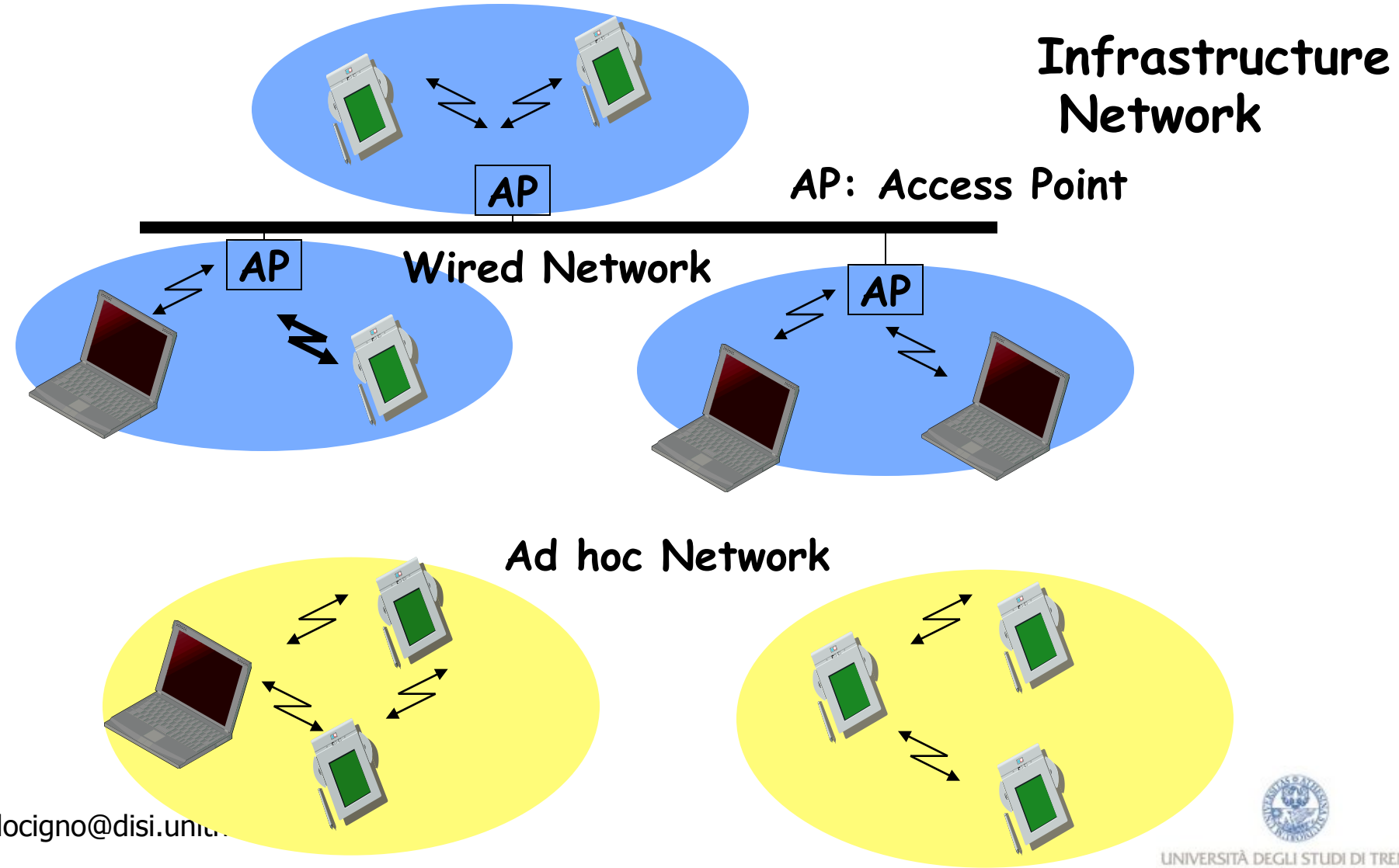


Schema di uno switch

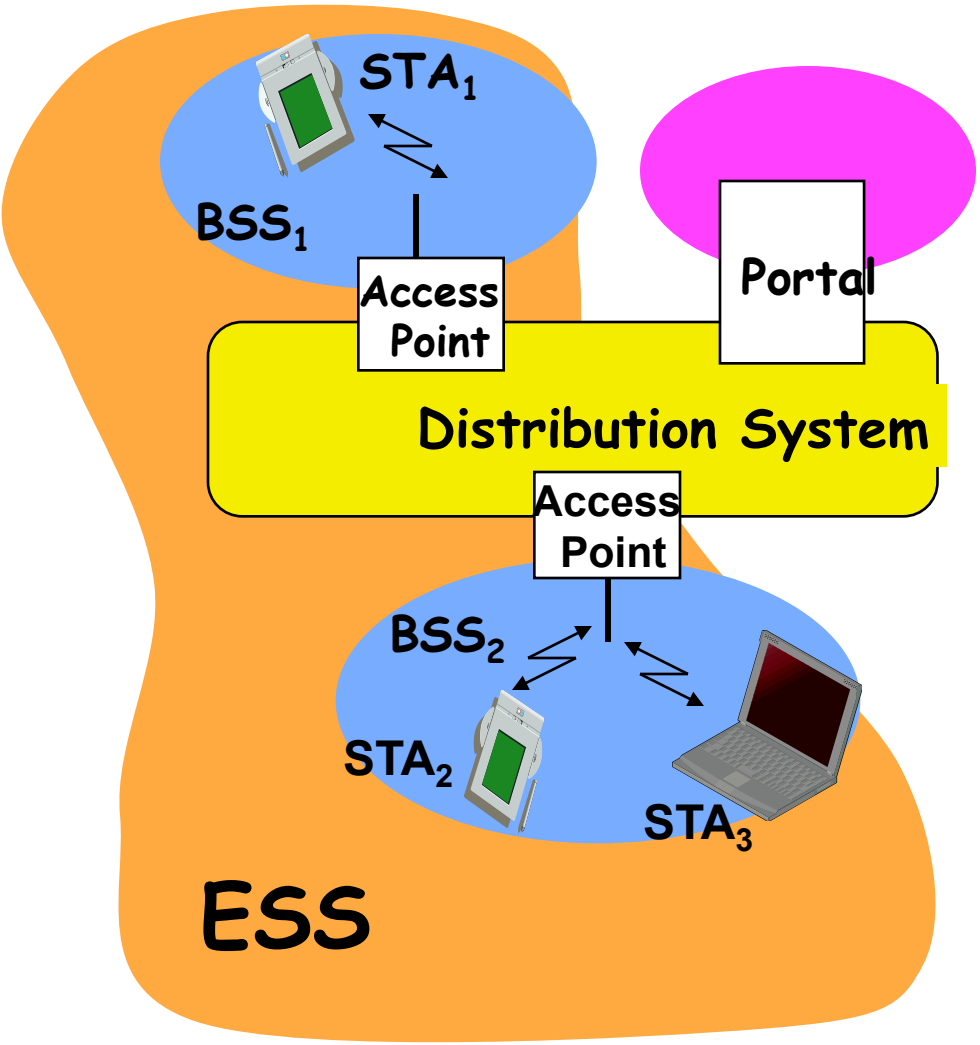


indirizzo destinazione	porta
34A46T	1
34B52R	4
34G90N	3
44A48S	6

WIRELESS LANs Architecture



Reference Architecture of Wireless LANs



- Station (STA)
  - Terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - Group of stations using the same radio frequency
- Access Point
  - Station integrated into the wireless LAN and the distribution system
- Portal
  - Bridge to other (wired) networks
- Distribution System
  - Interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

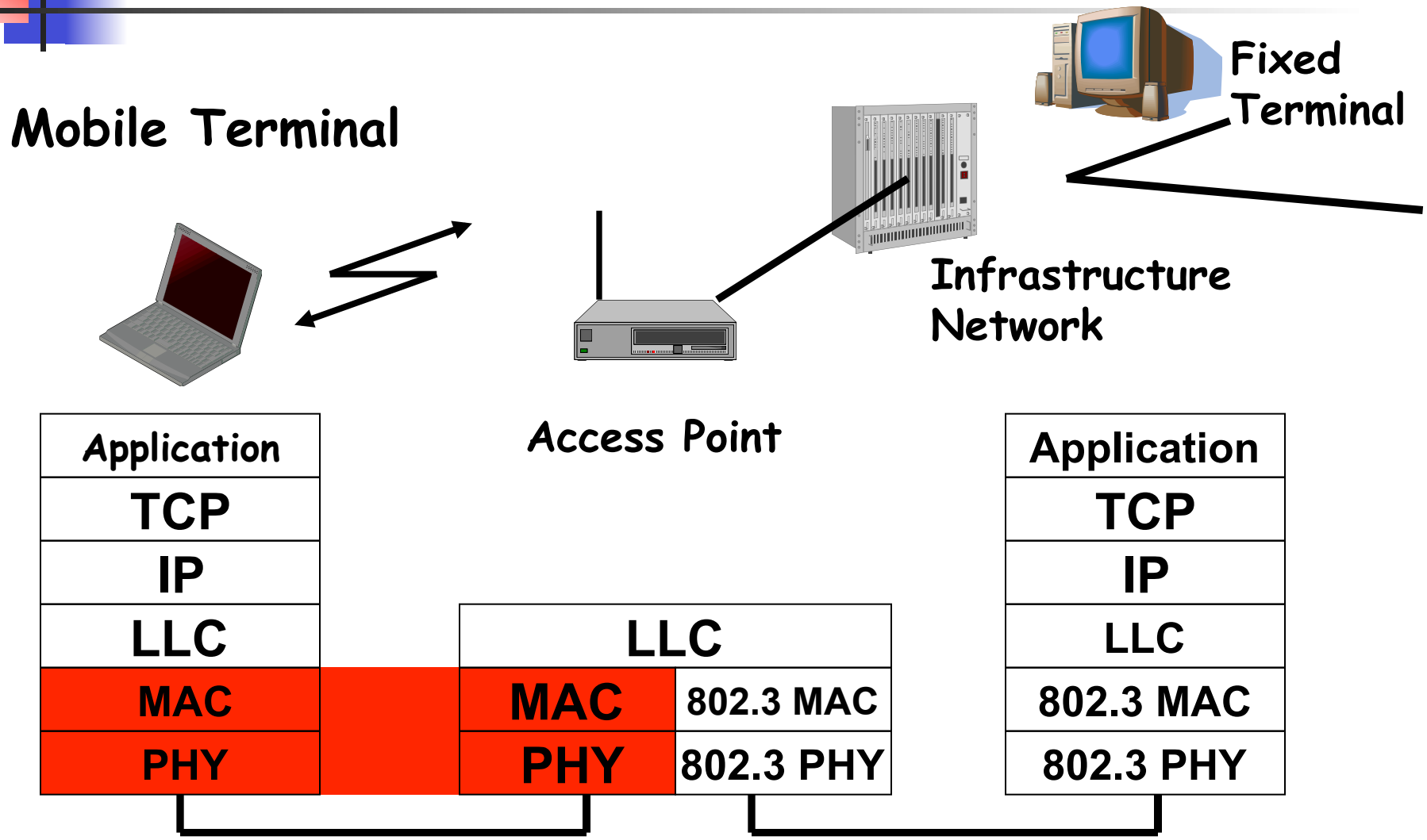
Reference Architecture

- Basic Service Set (BSS) consists of some number of stations with the same MAC protocol and competing for access to the same shared medium.
- A BSS may be isolated or it may connect to a backbone distribution system through an access point
- AP functions as a bridge.
- The MAC protocol may be fully distributed or controlled by a central coordination function housed in the AP.

Reference Architecture

- Basic Service Set (BSS) <-> CELL
- Extended Service Set (ESS) consists of two or more BSSs interconnected by a distribution system.
- Distribution System → a wired backbone LAN.
- ESS appears as a single logical LAN to the logical link control (LLC) level.

Protocol Architecture



Family of Wireless LAN (WLAN) Standards 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)
- ..... It is a live and evolving standard

802.11 Technologies Comparison

	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

802.11n Space diversity

- Exploit multiple Tx and Rx antennas with a reasonable independent transmission path combining the different signals
- Enhancing 802.11a and supporting up to 4 parallel channels arrives at 600 (150 X 4) Mbit/s at PHY layer