

Reti (Computer Networks)

Capitolo 6 Livello data link

Docente: Paolo Casari

TA: Andrea Rosani

Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ IEEE 802 ed Ethernet
- ❑ Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Livello data link

□ Obiettivi

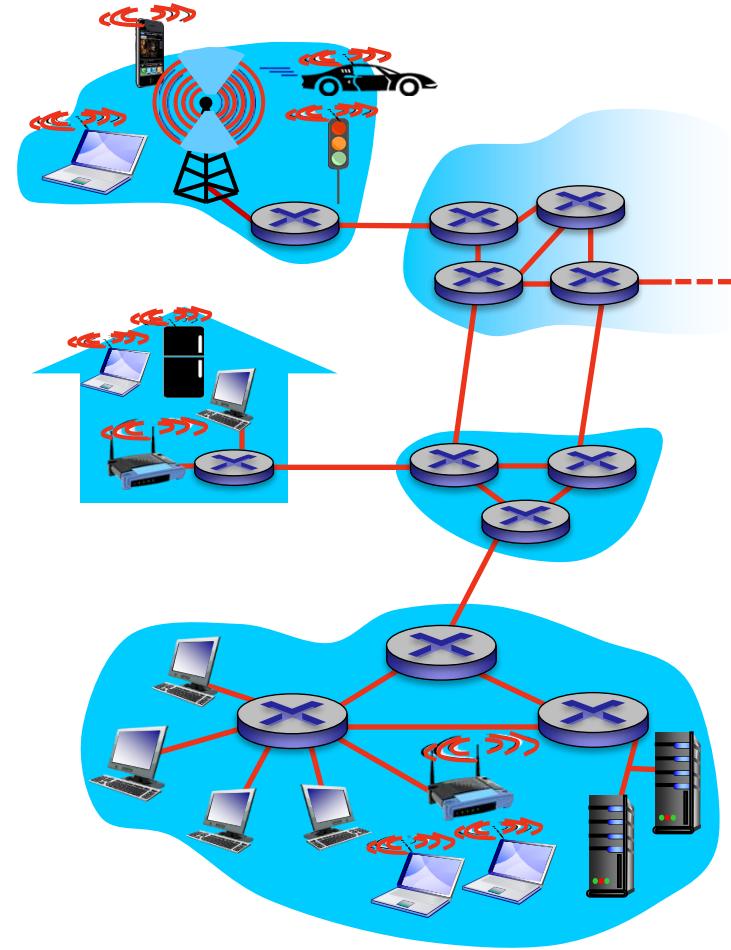
- ❖ Comprendere i principi di base di alcuni servizi di livello data link
 - Rilevamento e correzione di errore
 - Condivisione di un canale di tipo broadcast e accesso multiplo
 - Indirizzamento di livello data link
- ❖ Local area networks: Ethernet e WiFi
- ❖ Implementazione di alcune tecnologie di livello data link

Livello data link: introduzione

Terminologia:

- Host e router: **nodi** (di rete)
- Canale di comunicazione che collega due nodi adiacenti lungo un certo percorso:
collegamenti, o **link**
 - ❖ Link cablati
 - ❖ Link wireless
 - ❖ LANs
- Pacchetto di livello 2: **frame**
 - ❖ Incapsula un datagramma (liv 3)

Il livello data link ha la funzione di trasportare un frame da un nodo a un'altro nodo fisicamente adiacente



Livello data link: contesto

- Un percorso può contenere link di diversi tipi
- Un datagramma trasferito lungo questo percorso attraversa quindi reti con protocolli di livello 2 differenti
 - ❖ Ethernet sul primo link
 - ❖ Frame relay sui link intermedi
 - ❖ 802.11 sull'ultimo link
- Ogni protocollo fornisce servizi diversi
 - ❖ Es. controllo di errore o meno

- Analogia con i sistemi di trasporto
- Viaggio Princeton – Losanna
 - ❖ Limousine: Princeton – JFK
 - ❖ Aereo: JFK – Ginevra
 - ❖ Treno: Ginevra – Losanna
 - Turista = datagramma
 - Porzione del viaggio = link
 - Modalità di viaggio = protocollo di livello data link
 - (Agenzia di viaggio = algoritmo di routing)

Servizi di livello data link

- Creazione di un frame di livello 2, accesso al link
 - ❖ Incapsula un datagramma in un frame, aggiunge header e trailer
 - ❖ Fornisce un meccanismo di accesso al canale se il mezzo di comunicazione è condiviso con altri dispositivi
 - ❖ Utilizza indirizzi di livello 2 (detti indirizzi "MAC") negli header dei frame per identificare mittente e destinatario
 - Diverso dall'indirizzo IP!
- Consegna affidabile tra nodi adiacenti
 - ❖ Sappiamo come ottenere questo servizio
 - ❖ Poco usato su link a basso tasso di errore (es., fibre ottiche)
 - ❖ Link wireless: alti tassi di errore
 - **D**: perché inserire controllo di errore sia a livello 2 sia a livello 4?

Servizi di livello data link

□ Controllo di flusso:

- ❖ Adatta la velocità di trasmissione alle possibilità di trasmettitore e ricevitore

□ Rilevamento di errore:

- ❖ Errori causati da attenuazione eccessiva del segnale, rumore, ...
- ❖ Il ricevitore può rilevare la presenza di errori
 - E di conseguenza avvertire il mittente e/o scartare il pacchetto

□ Correzione d'errore:

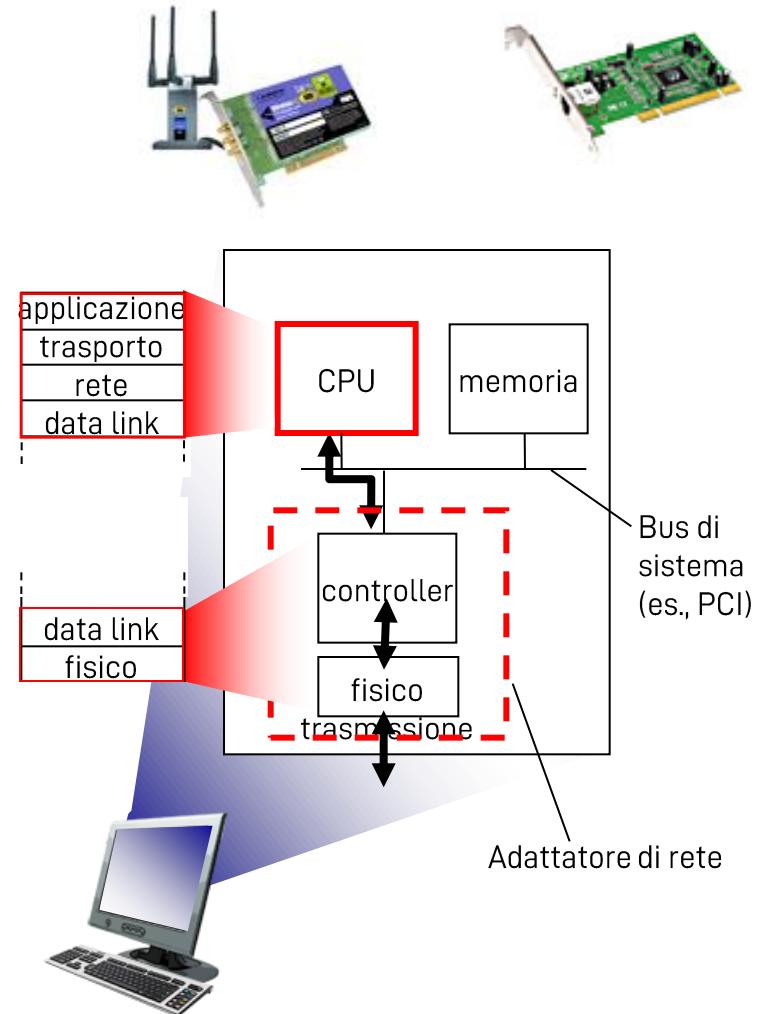
- ❖ Il ricevitore identifica e corregge gli errori sui bit senza richiedere ritrasmissioni

□ Half-duplex e full-duplex

- ❖ In un collegamento full-duplex, i nodi possono trasmettere e ricevere contemporaneamente (in uno half-duplex, no)

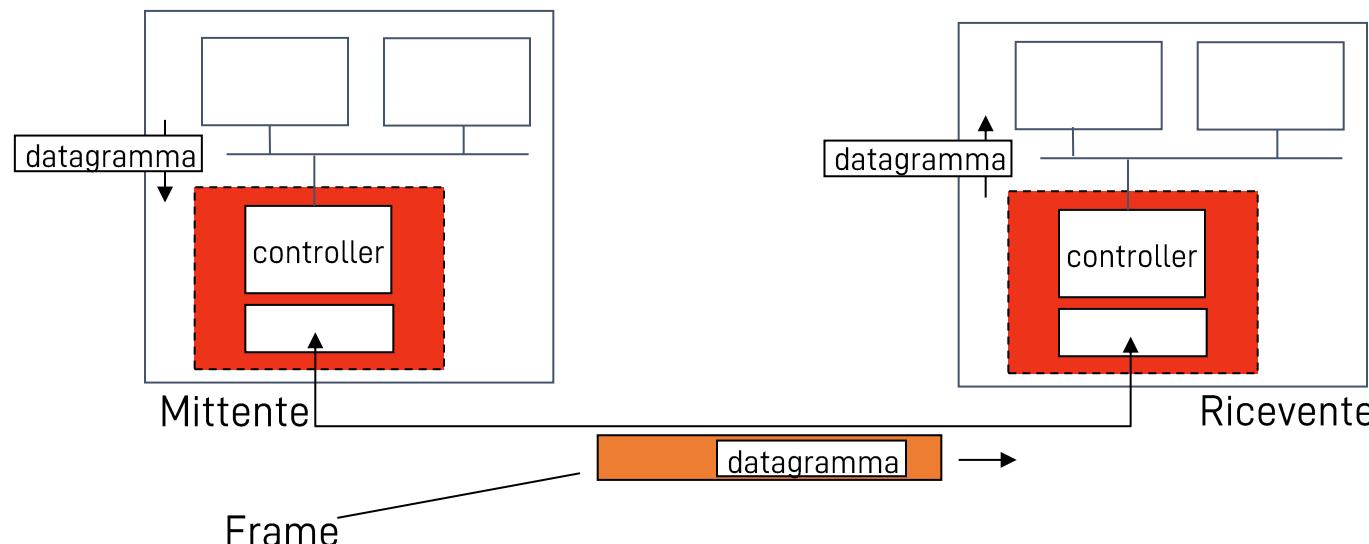
Chi implementa il livello data link?

- Implementato in **tutti** gli host
- Di solito, come firmware di un "adattatore di rete" (detto anche "network interface card", NIC) o su un chip
 - ❖ Scheda Ethernet, scheda 802.11; chipset Ethernet
 - ❖ Nota: implementa sia il livello data link sia il livello fisico
- Collegata direttamente al bus di sistema dell'host
- Combinazione di hardware, software, firmware



Comunicazione tra adattatori di rete

- Mittente:
 - ❖ Incapsula un datagramma in un frame
 - ❖ Aggiunge bit ulteriori per controllo di errore, controllo di flusso, ecc.
- Ricevente
 - ❖ Cerca eventuali errori, collabora al controllo di flusso, ecc.
 - ❖ Estraе il datagramma e lo passa ai livelli superiori

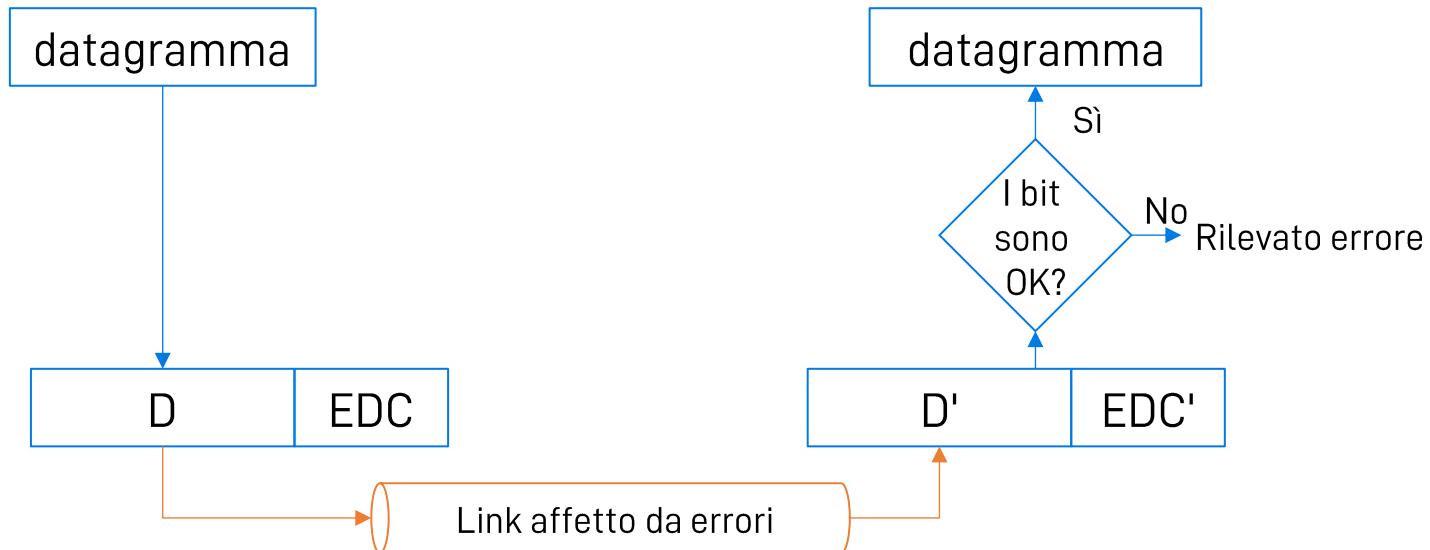


Sommario

- Livello data link
- Rilevamento e correzione di errori, CRC
- Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ IEEE 802 ed Ethernet
- Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Rilevamento di errori

- EDC = Bit ridondanti inseriti per Error Detection and Correction
- D = Dati protetti dall'EDC (o anche campi dell'header)
- Il rilevamento di errore non è mai affidabile al 100%!
 - ❖ Il protocollo potrebbe non accorgersi di qualche errore
 - ❖ Maggiore è la ridondanza, maggiore è la protezione (in generale)



Controllo di parità

- Singolo bit di parità:
 - ❖ Rileva errori singoli
- Esempio: "even parity"
 - ❖ Il numero totale di 1 deve essere pari
- Parità su due dimensioni
 - ❖ Rileva e corregge singoli errori sui bit
- Esempio: even parity su due dimensioni
 - ❖ Sinistra: nessun errore
 - ❖ Destra: singolo errore rilevato e correggibile

data bits	parity bit
0111000110101011	1

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

Correzione di errori tramite ridondanza

- CCFooommree vvveeeddheeetxtee,
lllaab rrrijddqowonnnndajannmzzyaaa
pppeegrrlmpmgeehteee dddiii rrriiklbleewvvvaaruruee eee
ccoooorrreegggtteearreee aaalllcxcuzunnmiii eeerrjooprqqwii
- Un'operazione detta "interleaving" (che consiste nel riordino dei bit) fornisce anche una protezione contro errori a "raffica" (burst)
 - ❖ Messaggio: HELLO
 - ❖ Ridondanza: HHH EEE LLL LLL 000
 - ❖ Interleaving: HEL LOH ELL OHE LLO
 - ❖ Raffica di errori: HEL LOH E~~XX~~ ~~XXX~~ LLO
 - ❖ De-interleaving: HH~~X~~ E~~E~~ X LXL LX~~L~~ OXO
 - ❖ Scelta a maggioranza: HELLO

Cyclic redundancy check (CRC)

- Algoritmo più efficiente per il rilevamento di errore
- Considera i bit di dati come un numero binario D
- Sceglie una sequenza di $r+1$ bit (detta "generatore"), e un numero G (noto sia al mittente sia al ricevente)
- Obiettivo: comporre il CRC (R) scegliendo r bit in modo che:
 - ❖ I dati D siano esattamente divisibili per G (modulo 2) con resto R
 - O in altre parole, che la concatenazione $\langle D, R \rangle$ sia divisibile per G
 - ❖ Il ricevente conosce G: se divide $\langle D, R \rangle$ per G e resto $\neq 0 \rightarrow$ errore!
 - ❖ Può rilevare anche errori a raffica, se meno di r bit errati consecutivi
- Nota: per concatenare D ed R basta calcolare:
 - ❖ $\langle D, R \rangle = (D \times 2^r) \text{ XOR } R$

D: bit dati da proteggere

R: r bit del CRC

Aritmetica intera modulo 2

- ❑ Solo una breve ricapitolazione
- ❑ La somma si calcola bit a bit, ma senza riporti
- ❑ La sottrazione si effettua sempre bit a bit, ma senza prestiti
- ❑ Alla fine, l'operazione è la stessa: lo XOR

	1	0	0	1	1	0	1	1
+	1	1	0	0	1	0	1	0
	0	1	0	1	0	0	0	1

	1	1	1	1	0	0	0	0
-	1	0	1	0	0	1	1	0
	0	1	0	1	0	1	1	0

Calcolo di un CRC

D: bit dati da proteggere

R: r bit del CRC

- Se vogliamo che $D \times 2^r \text{ XOR } R$ sia un multiplo di G, serve che:
 - ❖ $D \times 2^r \text{ XOR } R = nG$
- Aggiungiamo R (cioè effettuiamo XOR R) ad entrambi i membri:
 - ❖ $D \times 2^r = nG \text{ XOR } R$
- L'equazione mostra che se dividiamo $D \times 2^r$ per G, il resto è R
 - ❖ Come dire che se $a = qb + r$
 - $\text{quoziente}(a/b) = q$
 - $\text{resto}(a/b) = r$
- Quindi quello che calcoliamo è
 - ❖ $\text{CRC} \rightarrow R = \text{resto}(D \times 2^r / G)$

Divisione standard modulo 2

□ Dividendo = 85731, divisore = 79, quoziente = 1085, resto = 16

			8	5	7	3	1
1		-	7	9			
			6	7			
0		-	0	0			
			6	7	3		
8		-	6	3	2		
			4	1	1		
5		-	3	9	5		
			1	6			

Esempio di CRC e divisione modulo 2

- La divisione intera modulo 2 si fa come al solito, ma con la sottrazione modulo 2 senza prestito
 - ❖ Esempio: $G = 1001$, $D = 101110$, $D * 2^r = 101110000$, $R = 011$

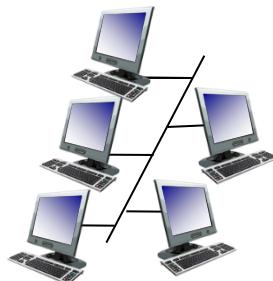
		1	0	1	1	1	0	0	0	0
1	-	1	0	0	1					
					1	0	1			
0	-	0	0	0						
					1	0	1	0		
1	-	1	0	0	1					
						1	1	0		
0	-	0	0	0						
					1	1	0	0		
1	-	1	0	0	1					
						1	0	1	0	
1	-	1	0	0	1					
						0	1	1		

Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocoli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ IEEE 802 ed Ethernet
- ❑ Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Tipi di collegamento

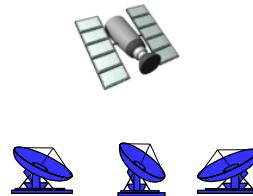
- Punto-punto
 - ❖ PPP per accesso dial-up
 - ❖ Collegamento punto-punto tra uno switch Ethernet e un host
- Broadcast (mezzo di trasmissione condiviso)
 - ❖ Vecchie versioni di Ethernet
 - ❖ Hybrid fiber-coaxial (HFC) per TV e Internet
 - ❖ 802.11 wireless LAN



Cavo condiviso (es.,
Vecchie versioni Ethernet)



Canale radio RF
(es., 802.11 WiFi)



Canale radio RF
(satellite)



Persone ad un party
(mezzo aereo condiviso,
segnali acustici)

Protocolli per il controllo dell'accesso multiplo

- ❑ Canale broadcast condiviso
- ❑ Due o più trasmissioni simultanee partono da nodi diversi: si crea interferenza
 - ❖ Se un nodo riceve due o più segnali nello stesso momento si verifica una collisione
- ❑ Protocollo di accesso multiplo
 - ❖ Algoritmo distribuito che determina come i nodi condividano il canale, quando un nodo può trasmettere e quando no
 - ❖ In un canale broadcast condiviso gli “accordi” di trasmissione vengono preso comunicando sullo stesso canale usato per i dati!
 - Nella maggioranza dei casi non c’è un canale esterno dedicato al coordinamento (“out-of-band” channel)

Un protocollo MAC ideale

□ **MAC: multiple access control**

□ Dato:

- ❖ Un canale broadcast capace di supportare comunicazioni a R bit/s

□ Vorremmo che:

1. Quando un nodo trasmette, possa farlo a velocità R
2. Quando M nodi vogliono trasmettere, possano farlo ad un tasso medio pari a R/M
3. Il sistema fosse completamente decentralizzato:
 - Nessun "centro stella" che coordina le trasmissioni degli altri
 - Nessuna sincronizzazione di clock
4. ...e se possibile che fosse semplice

Protocolli MAC: tassonomia

□ Tre classi:

❖ A ripartizione delle risorse di canale

- Dividono il canale in "sotto-canali" più piccolo (es. Slot temporali, sotto-frequenze, codici di spreading)
- Allocano ciascun sotto-canale a un nodo in modo esclusivo

❖ Ad accesso casuale

- Il canale non viene suddiviso, si accetta che si verifichino collisioni
- Si cerca comunque di minimizzarle

❖ A "turni" intelligenti

- I nodi accedono al canale a turno, ma i nodi con molti dati da trasmettere possono ottenere turni più lunghi

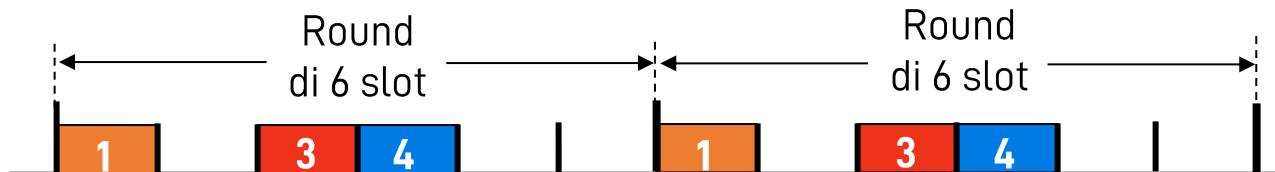
Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ Protocolli "a turni"
 - ❖ IEEE 802 ed Ethernet
- ❑ Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Ripartizione delle risorse: TDMA

TDMA: time division multiple access

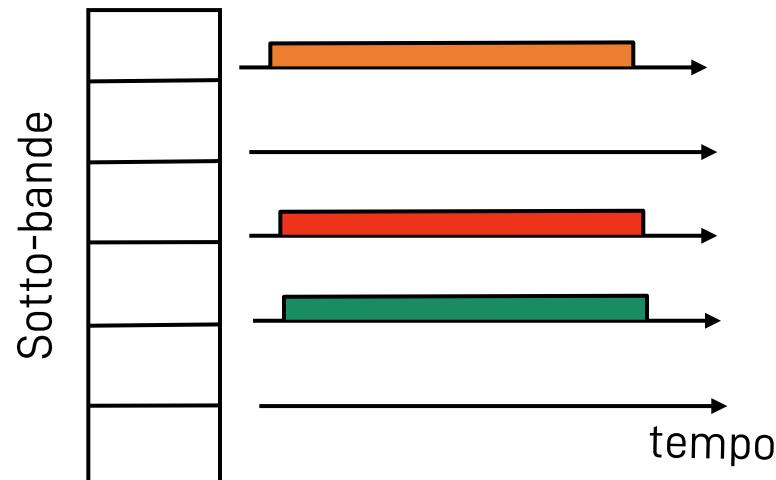
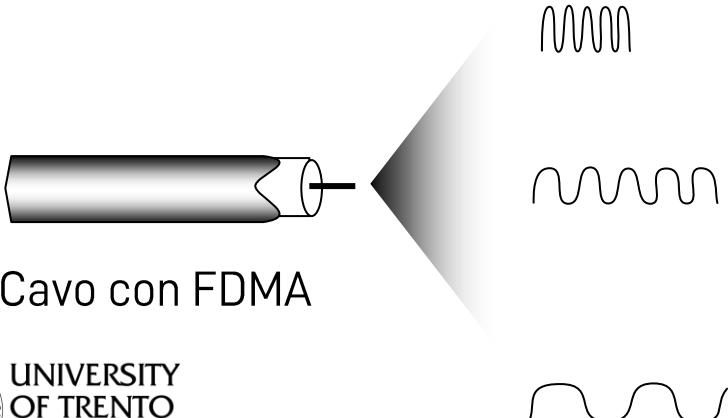
- Accesso al canale in "round"
- Ogni nodo ottiene uno slot di durata fissa in ogni round
 - ❖ Lunghezza = tempo di trasmissione di un pacchetto
- Gli slot inutilizzati rimangono liberi in ogni caso
- Esempio: LAN con 6 nodi, di cui il nodo 1, il nodo 3 e il nodo 4 hanno pacchetti da trasmettere, mentre gli slot 2, 5 e 6 rimangono vuoti
- I round si chiamano più tipicamente "frame" (sorry)



Ripartizione delle risorse: FDMA

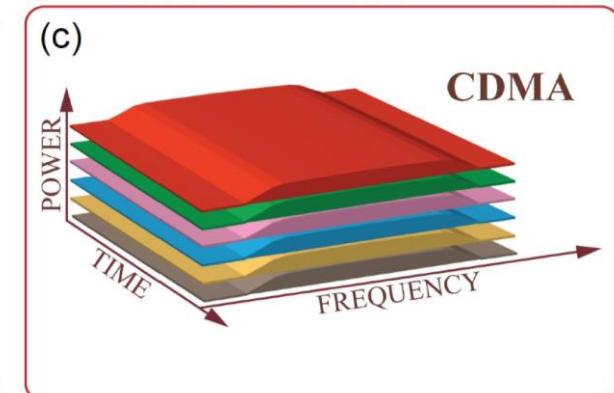
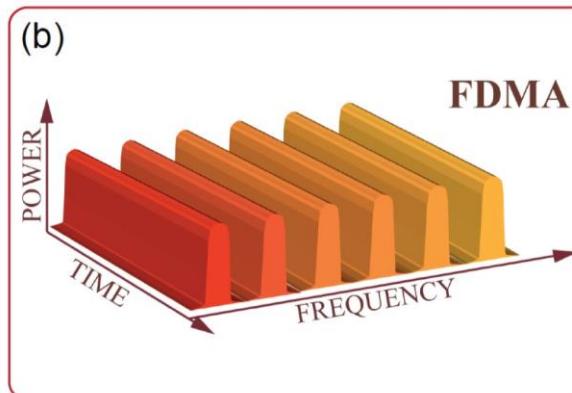
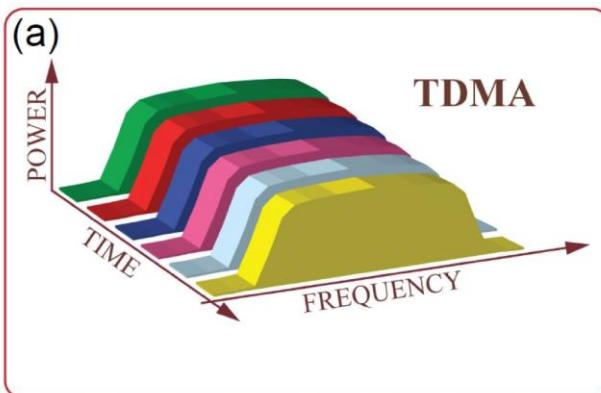
FDMA: frequency division multiple access

- Spettro del canale suddiviso in "sotto-bande"
- Ad ogni stazione si assegna una sotto-banda
- Quando una sotto-banda non viene usata per trasmettere, la risorsa rimane inutilizzata
- Esempio: LAN con 6 nodi, di cui il nodo 1, il nodo 3 e il nodo 4 hanno pacchetti da trasmettere, mentre le sotto-bande 2, 5 e 6 rimangono vuote



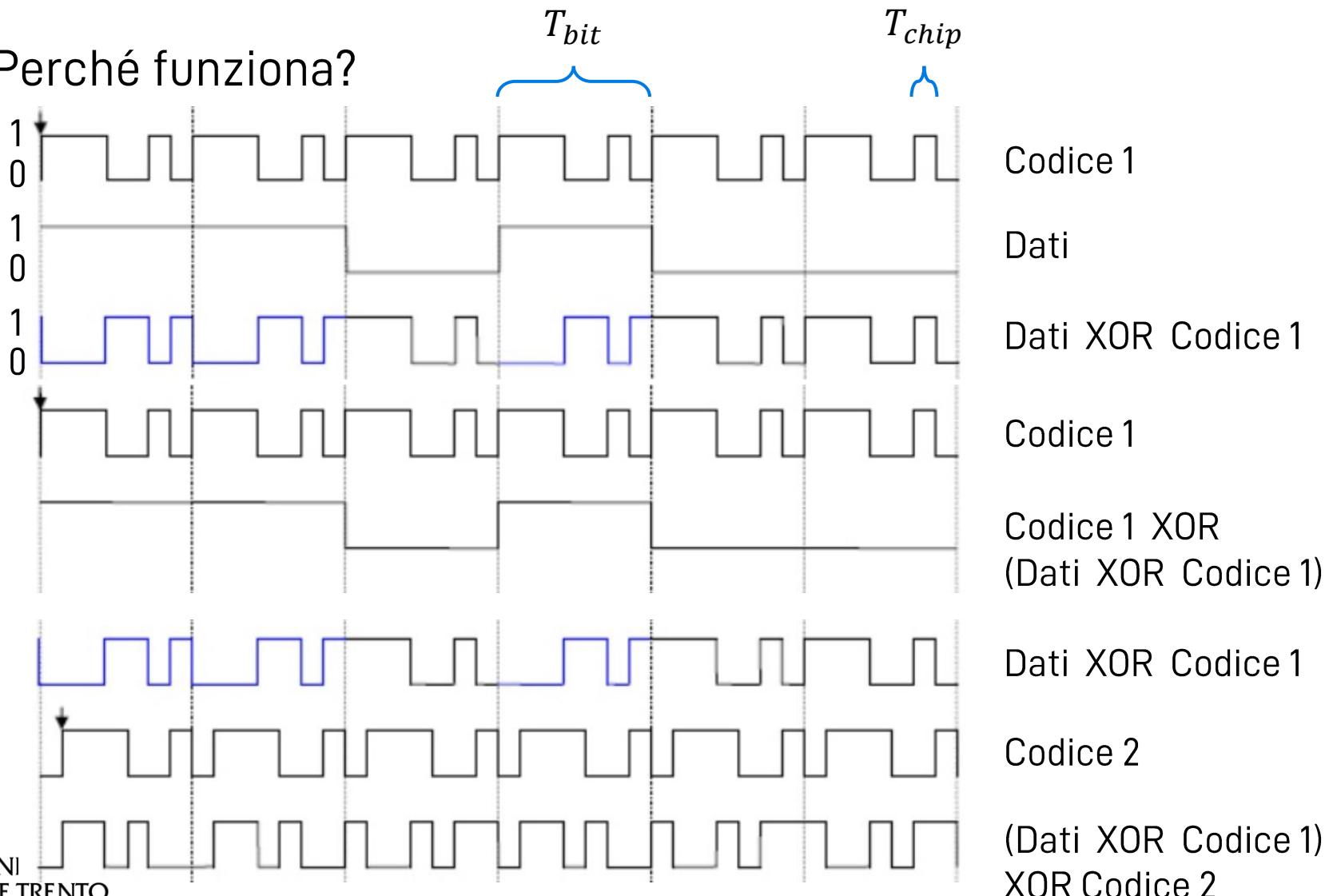
Ripartizione delle risorse: CDMA

- **CDMA: code-division multiple access**
- La ripartizione delle risorse avviene assegnando un “codice” diverso ad ogni nodo
 - ❖ “Codice” = sequenza di “chip” che commuta più rapidamente di quanto commutino i bit
- Confronto con TDMA e FDMA



Ripartizione delle risorse: CDMA

□ Perché funziona?



Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ Protocolli "a turni"
 - ❖ IEEE 802 ed Ethernet
- ❑ Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Protocolli ad accesso casuale

- Quando un nodo ha un pacchetto da trasmettere
 - ❖ Può trasmettere al data rate massimo, R
 - ❖ Non c'è coordinamento con gli altri nodi prima della trasmissione
- Se due o più nodi trasmettono contemporaneamente → collisione
- Un protocollo ad accesso casuale specifica:
 - ❖ Come (e se) rilevare le collisioni
 - ❖ Come (e se) recuperare uno stato di collisione (ad esempio, imponendo a ciascun nodo di riprovare dopo un ritardo casuale)
- Esempi di protocolli ad accesso casuale:
 - ❖ Slotted ALOHA
 - ❖ ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA

Slotted ALOHA

Assunzioni

- ❑ Tutti i pacchetti (frame) hanno la stessa lunghezza
- ❑ Il tempo è suddiviso in slot, ciascuno lungo quanto un pacchetto
- ❑ I nodi possono trasmettere solo all'inizio di uno slot
- ❑ I nodi sono sincronizzati
- ❑ Se 2 o più nodi trasmettono, tutti vedono la collisione

Come funziona

- ❑ Quando un nodo ha qualcosa da inviare, lo invia nello slot immediatamente successivo
- ❑ Se non ci sono collisioni: il nodo può trasmettere ancora nello slot seguente
- ❑ Se c'è una collisione: il nodo ritrasmette il pacchetto con probabilità p in ogni slot seguente finché non ha successo

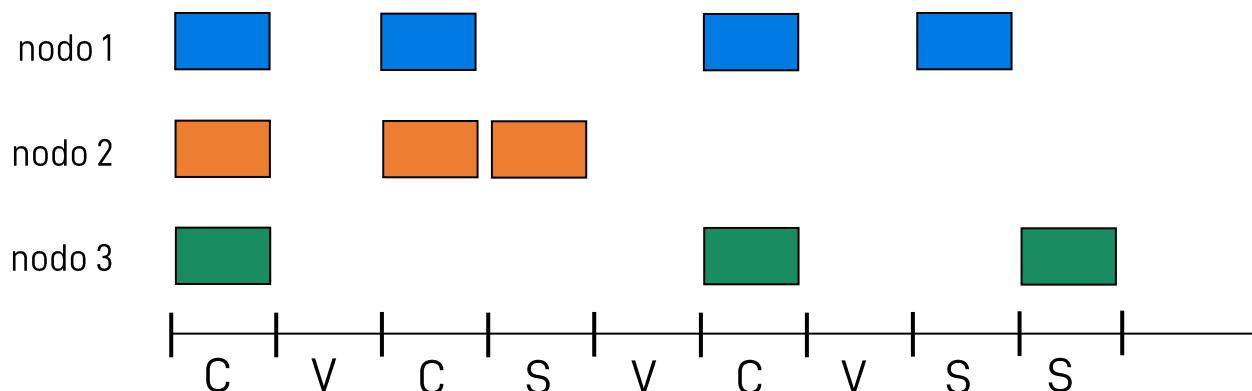
Slotted ALOHA

□ Vantaggi:

- ❖ Se un solo nodo è attivo, può usare il canale continuamente
- ❖ Decentralizzato: serve solo sincronizzarsi sullo slot
- ❖ Molto semplice

□ Svantaggi:

- ❖ Le collisioni sono probabili e sprecano risorse
- ❖ Gli slot potrebbero rimanere vuoti
- ❖ Si potrebbe rilevare la collisione senza aspettare la fine di una trasmissione
- ❖ Sincronizzarsi richiede coordinamento



Slotted ALOHA: calcolo efficienza

□ Assunzioni

- ❖ Tutti i pacchetti hanno la stessa dimensione
- ❖ Chiamiamo $G \geq 0$ il traffico offerto (numero medio di pacchetti inviati sul canale da tutte le stazioni in uno slot, includendo trasmissioni e ritrasmissioni)
- ❖ La probabilità che ci siano k pacchetti da trasmettere in uno slot ha una distribuzione statistica di Poisson

- $P[k] = \frac{G^k e^{-G}}{k!}$

□ Throughput ideale = 1 (**D**: perche?)

□ Throughput effettivamente ottenuto: $P[k = 1] = Ge^{-G}$

□ Quale valore di G massimizza il throughput?

- ❖ Risolviamo $\frac{d(Ge^{-G})}{dG} = 0$ ottenendo $G^* = 1$

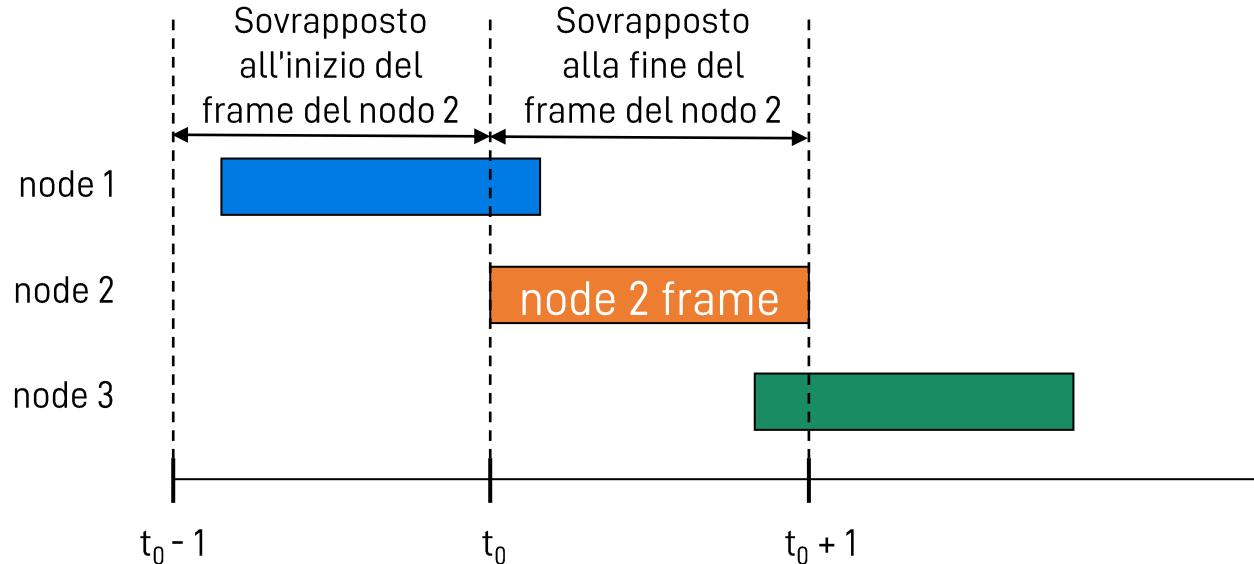
- ❖ Sostituiamo e otteniamo un throughput massimo pari a $\frac{1}{e} \approx 0.368$

Slotted ALOHA: un altro metodo

- Supponiamo di avere N nodi, e che ciascuno trasmetta in un certo slot con probabilità p
- Probabilità che un nodo trasmetta con successo: $p(1 - p)^{N-1}$
- Probabilità che un nodo qualunque abbia successo:
 - ❖ $\binom{N}{1}p(1 - p)^{N-1} = Np(1 - p)^{N-1}$
- Troviamo il valore di p che massimizza $Np(1 - p)^{N-1}$
 - ❖ $\frac{d Np(1-p)^{N-1}}{d p} = 0 \rightarrow p^* = \frac{1}{N}$
 - ❖ Quindi $Np^*(1 - p^*)^{N-1} = \left(1 - \frac{1}{N}\right)^{N-1}$
- Se la rete è fatta di un numero abbastanza grande di nodi
 - ❖ $\lim_{N \rightarrow \infty} \left(1 - \frac{1}{N}\right)^{N-1} = e^{-1} \approx 0.368$

ALOHA puro (non slotted)

- Aloha: ancora più semplice, nessuna sincronizzazione
- Quando un frame arriva, viene trasmesso subito
- La probabilità di collisione aumenta:
 - ❖ Un frame inviato a t_0 collide con altri frame inviati in $[t_0-1, t_0+1]$



ALOHA puro: efficienza

□ Assunzioni

- ❖ Tutti i pacchetti hanno la stessa dimensione, infiniti host
- ❖ Chiamiamo $G \geq 0$ il traffico offerto (numero medio di pacchetti inviati sul canale da tutte le stazioni in uno slot, includendo trasmissioni e ritrasmissioni)
- ❖ La probabilità che ci siano k pacchetti da trasmettere in uno slot ha una distribuzione statistica di Poisson

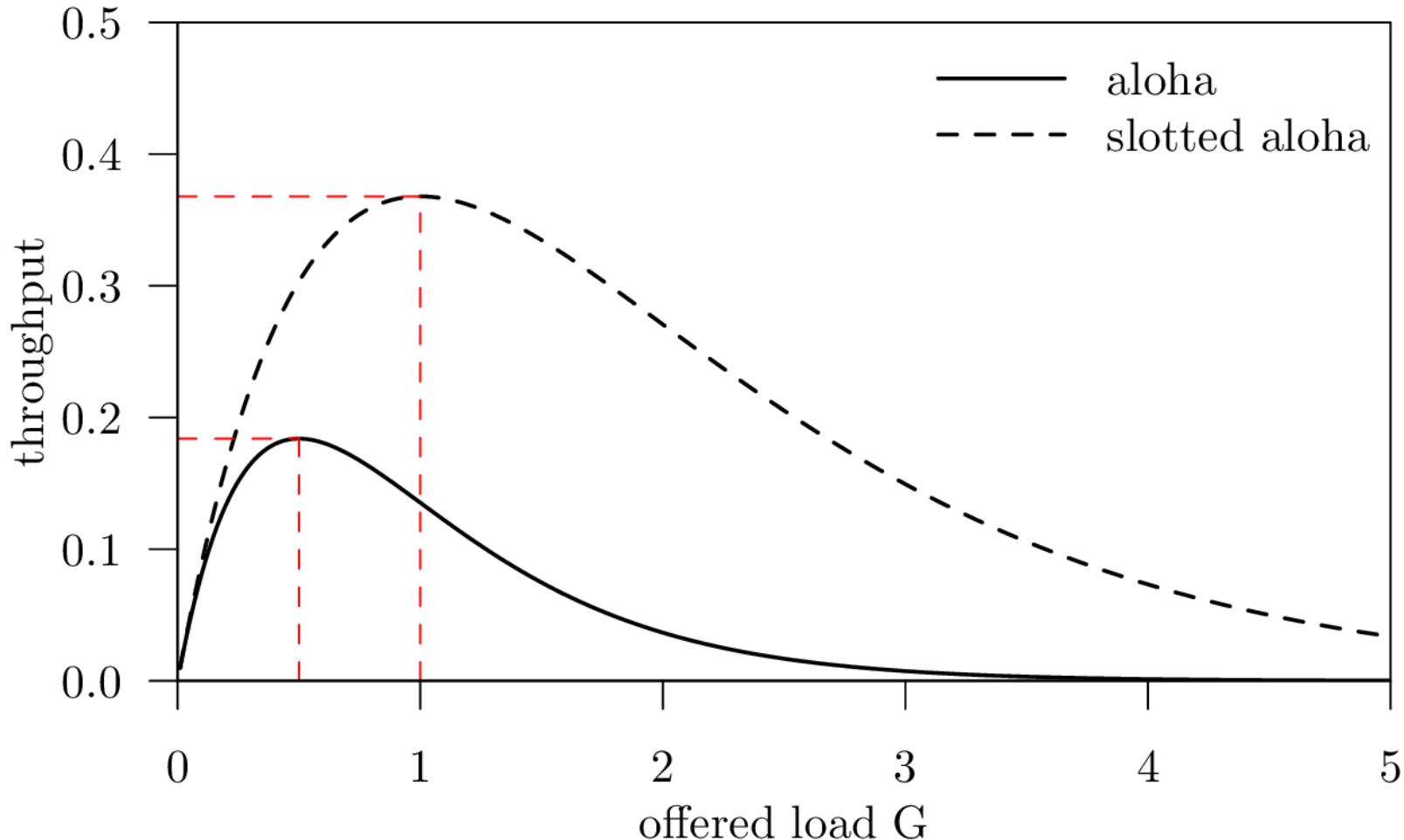
- $P[k] = \frac{G^k e^{-G}}{k!}$:

□ Throughput: probabilità che un solo frame venga trasmesso durante il periodo di vulnerabilità $[t_0-1, t_0+1]$

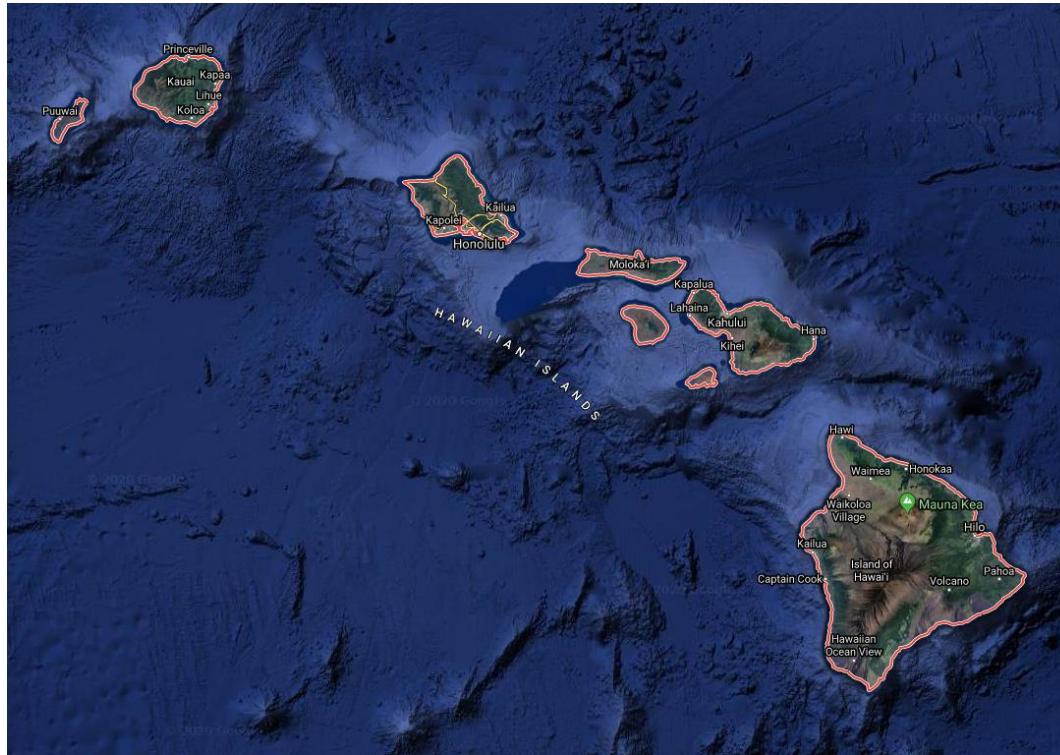
ALOHA puro: efficienza

- Probabilità che un solo frame venga trasmesso al tempo t:
 - ❖ $P[k = 1] = Ge^{-G}$
- Probabilità che non ci siano frame la cui trasmissione inizia nell'intervallo $[t_0 - 1, t_0]$
 - ❖ $P[k = 0] = e^{-G}$
- Throughput: probabilità che una trasmissione abbia successo:
 - ❖ $P[k = 1] \times P[k = 0] = Ge^{-2G}$
- Throughput massimo:
 - ❖ Risolviamo $\frac{dGe^{-2G}}{dG} = 0$ ottenendo $G = \frac{1}{2}$
 - ❖ Sostituendo, otteniamo un throughput massimo pari a $\frac{1}{2e} \approx 0.184$
 - ❖ Metà di quello dello slotted ALOHA → D: perché?

Throughput: confronto



Un po' di storia



- Verso la fine del 1960: ALOHA network (Norman Abramson)
 - ❖ Primo sistema radio a commutazione di pacchetto (Hawaii)
 - ❖ Primo sistema di accesso distribuito al mezzo radio

Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ Protocolli "a turni"
 - ❖ IEEE 802 ed Ethernet
- ❑ Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Carrier sense multiple access (CSMA)

- CSMA: carrier sense multiple access
 - ❖ "Carrier" (cioè "portante") è un termine che si riferisce al segnale che trasporta l'informazione
- In termini umani: ascolta prima di parlare
 - ❖ Se il canale viene valutato vuoto: si trasmette un intero frame
 - ❖ Se il canale viene valutato occupato: si ritarda la trasmissione

Versioni di CSMA: persistenza

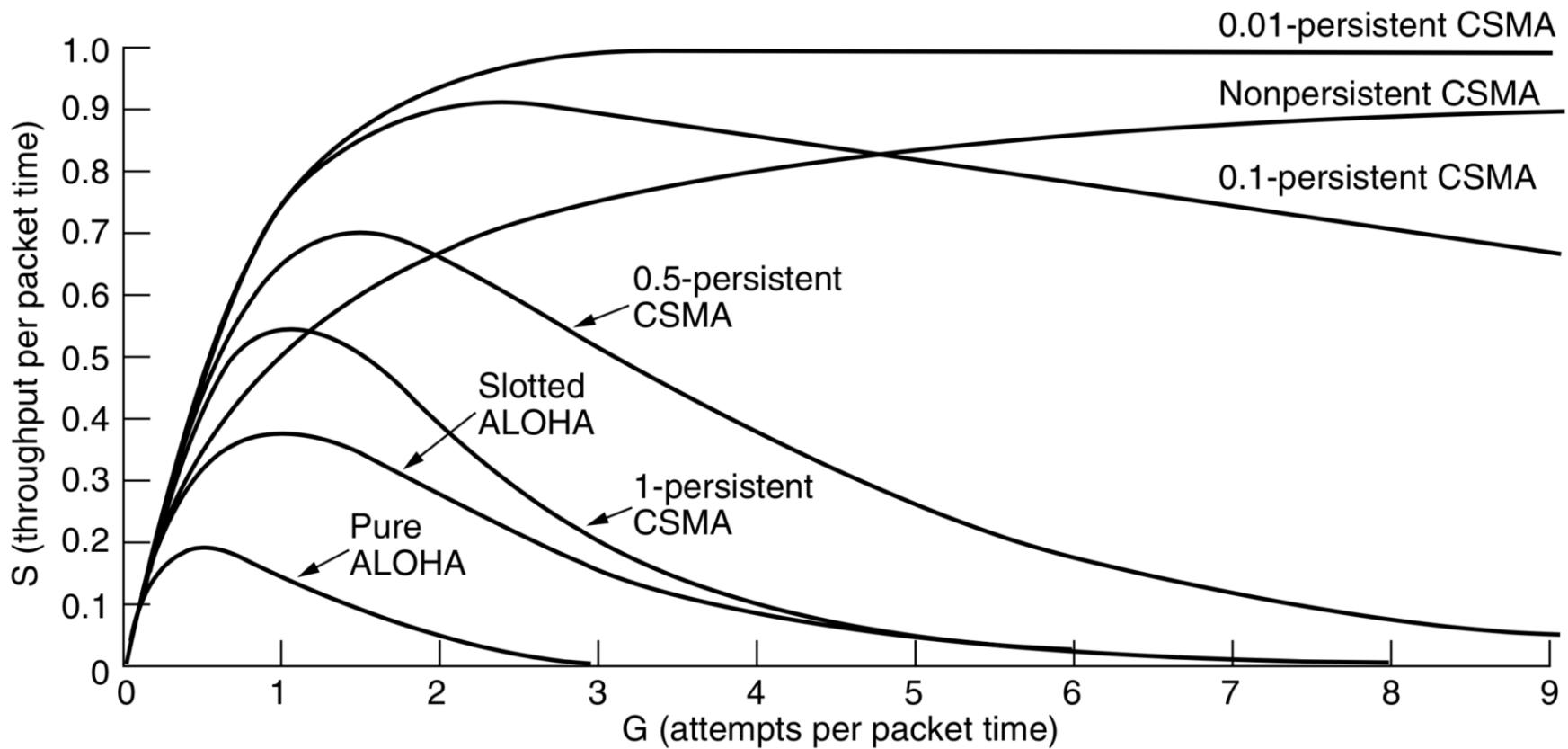
- Non-persistente (0-persistente):
 - ❖ Quando un nodo è pronto a mandare un frame
 - Se il canale è vuoto: → trasmette
 - Se il canale è occupato → attende un tempo casuale e molto più lungo del tempo di trasmissione, esaurito il quale ritenta
- 1-persistente
 - ❖ Quando un nodo è pronto a mandare un frame
 - Se il canale è vuoto: → trasmette
 - Se il canale è occupato:
 - Attende finché non si libera
 - Dopodiché trasmette subito
- Se si verifica una collisione, il nodo attende un tempo casuale, poi ritenta seguendo la stessa procedura

CSMA p-persistente

- Quando un nodo è pronto a mandare un frame
 - ❖ Se il canale è vuoto: → trasmette
 - ❖ Se il canale è occupato:
 - Attende finché non si libera
 - Dopodiché
 - Con probabilità p → trasmette il frame
 - Con probabilità $1 - p$ → attende un tempo casuale e molto più lungo del tempo di trasmissione, poi ritenta
- Se si verifica una collisione, il nodo attende un tempo casuale, poi ritenta seguendo la stessa procedura
- Nota: se avete il libro di Tanenbaum, troverete le regole un po' diverse
 - ❖ Tanenbaum segue l'articolo originale di Tobagi e Kleinrock [1], che è un po' ambiguo sulle regole

[1] L. Kleinrock and F. A. Tobagi, "Packet Switching in Radio Channels: Part I-Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics", in IEEE Transactions on Communications, vol. COM-23, no. 12, December 1975

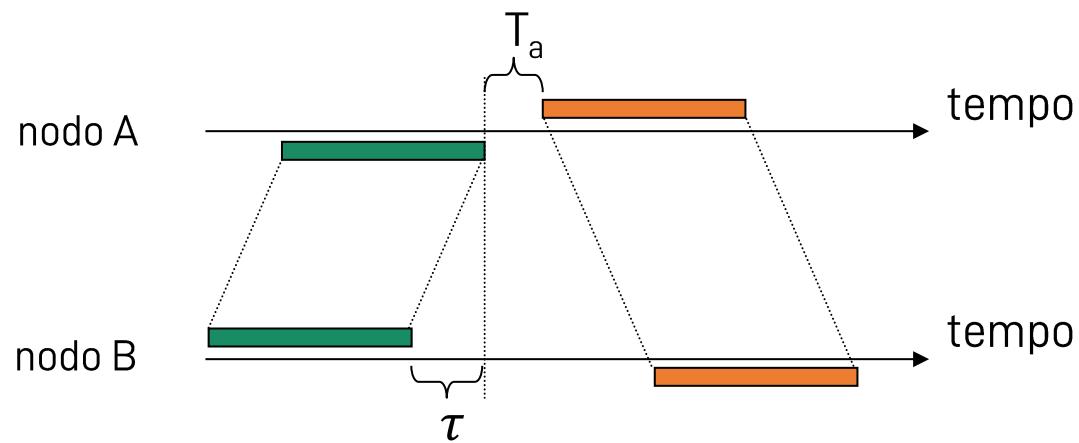
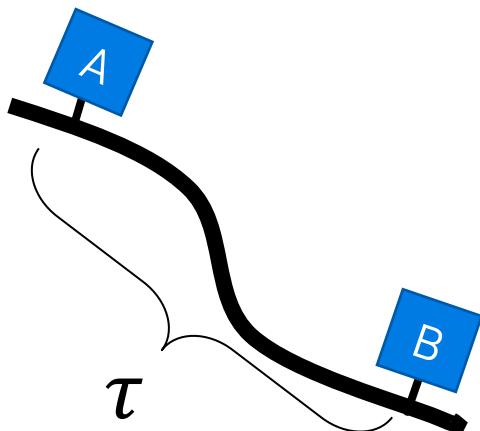
Throughput di CSMA: confronto



Source: "Computer Networks" book by Tanenbaum

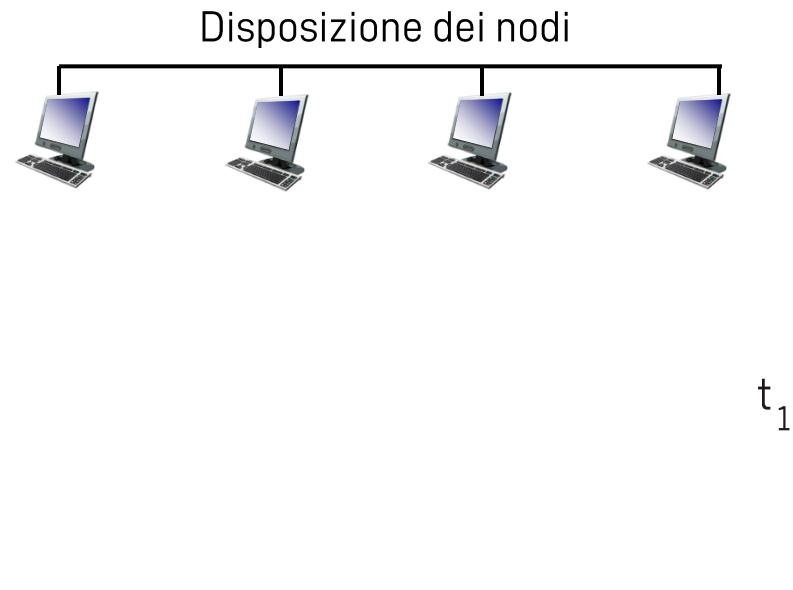
CSMA: periodo di vulnerabilità

- Il periodo di vulnerabilità dipende dal tempo di propagazione τ e dal tempo richiesto per rilevare se il canale è occupato, T_a
 - ❖ Se un nodo trasmette ma il segnale non ha raggiunto tutti gli altri nodi, un altro nodo potrebbe iniziare a trasmettere
 - ❖ Periodo di vulnerabilità: $T_v = \tau + T_a$
- In generale, CSMA si usa quando $\tau \ll T$ (tempo di trasmissione)



CSMA: collisioni

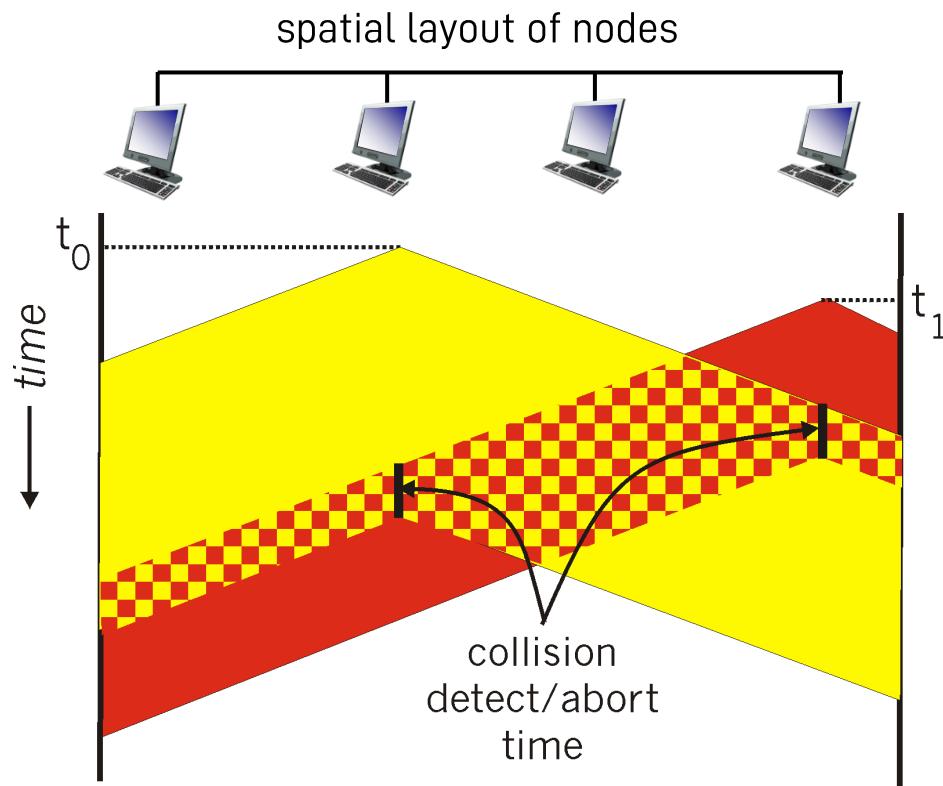
- ❑ Anche con il CSMA ci possono essere collisioni: esiste un ritardo di propagazione, quindi due nodi potrebbero non rilevare in tempo i rispettivi segnali
- ❑ Collisione: spreca l'intero tempo di trasmissione
 - ❖ La distanza (e quindi il tempo di propagazione) giocano il ruolo più importante nel determinare la probabilità di collisione



CSMA/CD (collision detection)

- CSMA/CD: usa comunque il carrier sensing, e se il canale è occupato posticipa le trasmissioni come nel normale CSMA
- In aggiunta
 - ❖ Permette di rilevare le collisioni entro breve
 - ❖ Permette di interrompere le trasmissioni e ridurre lo spreco di risorse di comunicazione (uso canale, energia)
- Collision detection:
 - ❖ Facile nelle LAN cablate:
 - Full-duplex
 - La potenza del segnale ricevuto è confrontabile con quella del segnale trasmesso da un nodo
 - ❖ Piuttosto difficile nelle reti wireless
 - Potenza segnale ricevuto << Potenza segnale trasmesso
- Analogia umana: il chiacchierone educato

CSMA/CD (collision detection)



CSMA/CA (collision avoidance)

- Si usa quando non si possono rilevare le collisioni e inoltre:
 - ❖ $T \gg \tau + T_a$
 - ❖ Tipico per tutte le LAN wireless
- CSMA 1-persistente non funziona bene in questo caso
 - ❖ Le collisioni sono più probabili
 - ❖ ... e non si possono rilevare
- CSMA p-persistente è altrettanto subottimo
 - ❖ Il parametro p è fisso, mentre dovrebbe essere adattato alle condizioni di rete (traffico, numero di nodi, ...)

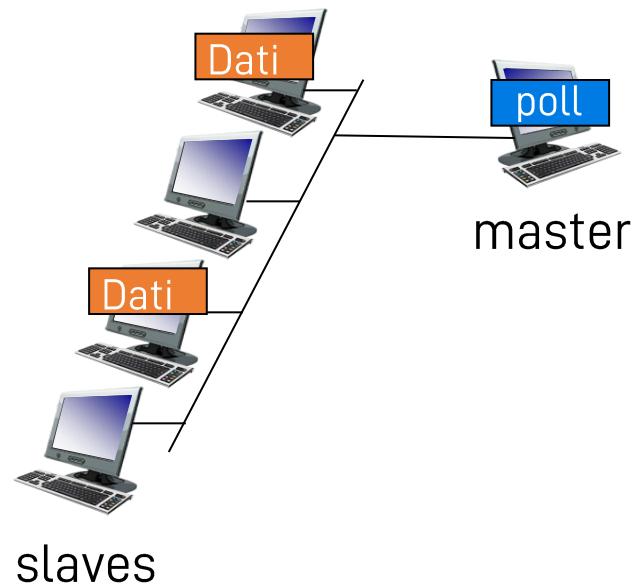
Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ **Protocolli "a turni"**
 - ❖ IEEE 802 ed Ethernet
- ❑ Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Protocolli MAC “a turni”

Polling:

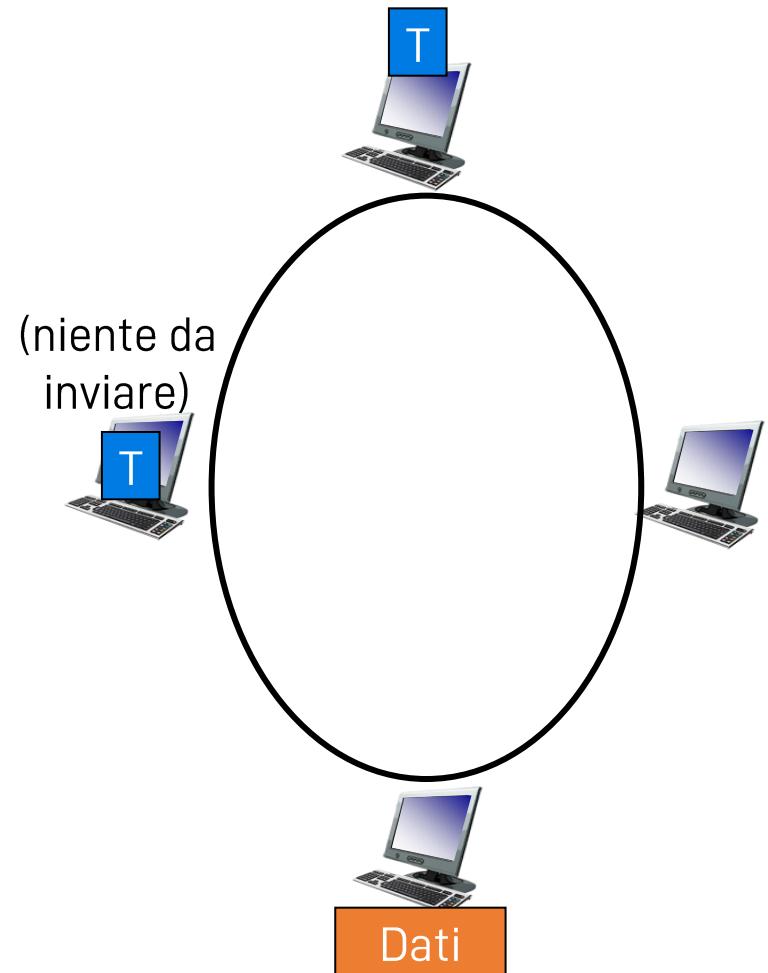
- Un nodo master “invita” gli altri nodi (“slave”) a trasmettere a turno
- Usato di solito se i dispositivi slave hanno poche risorse o poca “intelligenza”
- Problemi:
 - ❖ I messaggi di polling occupano il canale (overhead)
 - ❖ Latenza elevata
 - ❖ Single point of failure (master)



Protocolli MAC “a turni”

Token passing:

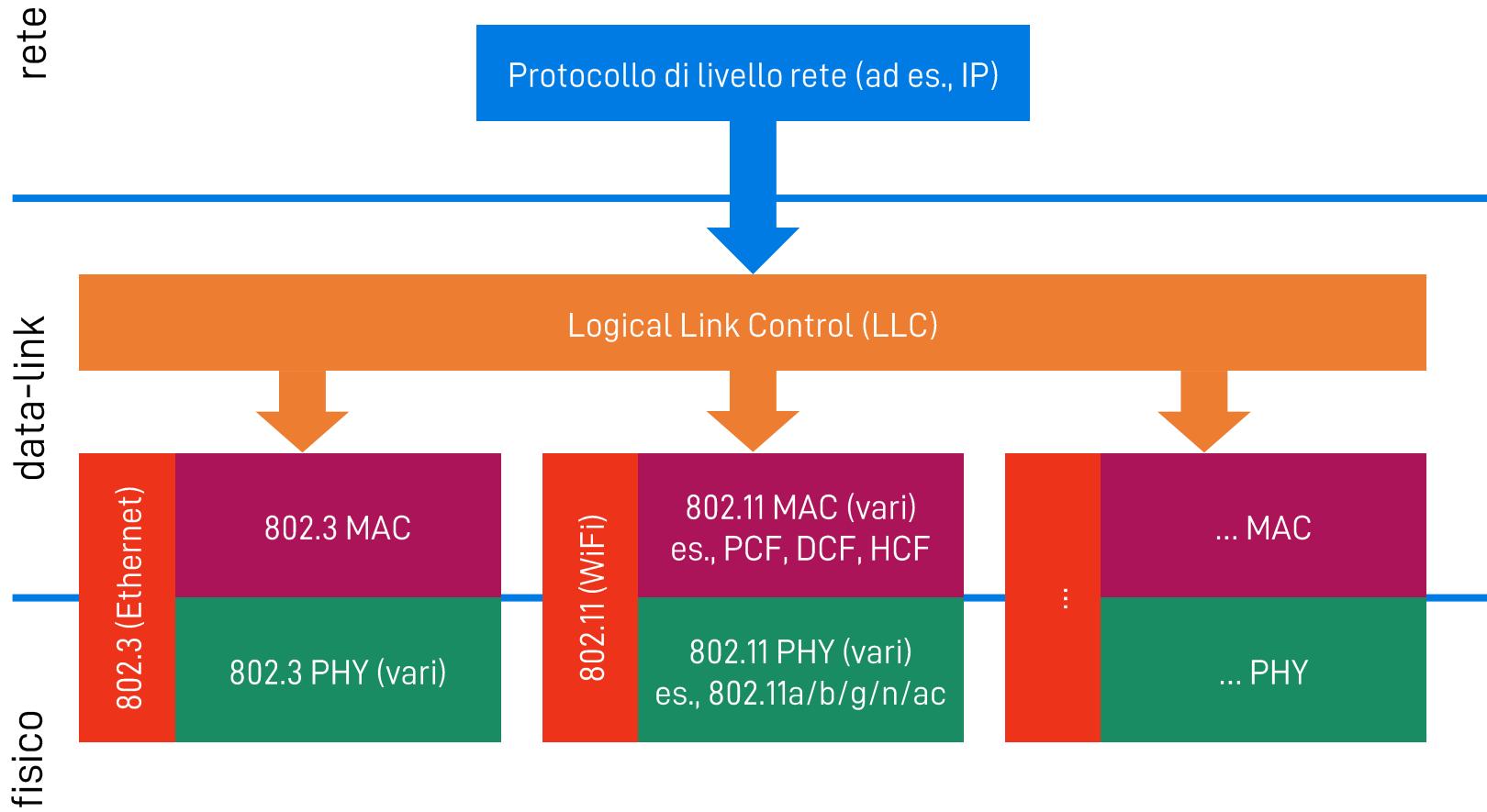
- ❑ Il diritto di trasmettere è rappresentato dal possesso di un token (“gettone”)
- ❑ Il token si passa sequenzialmente da un nodo all’altro
- ❑ Il token è un pacchetto
- ❑ Problemi:
 - ❖ Overhead dovuto al token
 - ❖ Latenza
 - ❖ Single point of failure (token)



Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ Protocolli "a turni"
 - ❖ IEEE 802 ed Ethernet
- ❑ Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Gruppo di standard IEEE 802



Gruppo di standard IEEE 802

- Le prime standardizzazioni iniziarono negli anni '80
 - ❖ 802.1: LAN Internetworking
 - ❖ 802.2: LLC Sublayer
 - ❖ 802.3: Ethernet
 - ❖ 802.4: Token Bus
 - ❖ 802.5: Token Ring
 - ❖ 802.6: DQDB (for MANs)
 - ❖ 802.7: Broadband Technical Advisory Group
 - ❖ 802.8: Fiber-Optic Technical Advisory Group
 - ❖ 802.9: Integrated Data and Voice Networks
 - ❖ 802.10: Network Security
 - ❖ 802.11: Wireless LAN (/a/b/g/h/f/s/n/p/ac/...)
 - ❖ 802.12: 100base VG
 - ❖ 802.13: 100base X
 - ❖ 802.15: Personal Area Networks
 - .1 → Bluetooth
 - .4 → ZigBee
 - ❖ 802.16: Wireless MAN
 - WiMax & Co.
 - ❖ ...

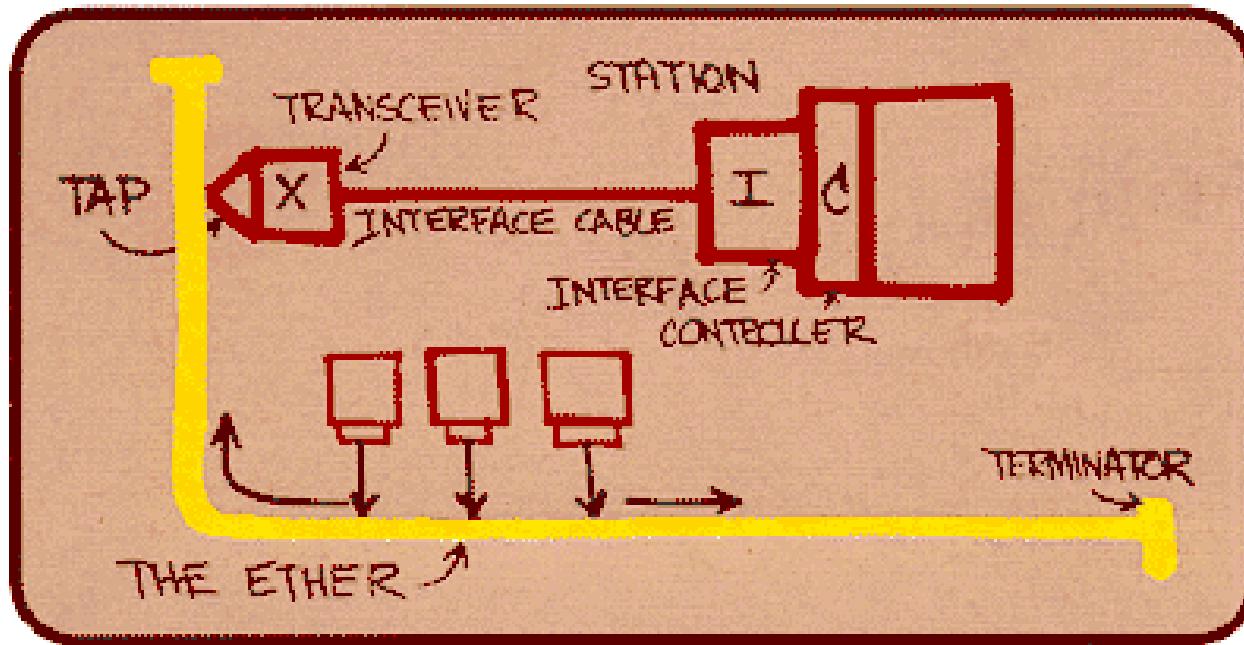
Ethernet

De facto, lo standard dominante nelle reti cablate:

- ❑ E' stata la prima tecnologia LAN di uso massivo
- ❑ Un singolo chip supporta varie velocità (es., Broadcom BCM5761)
- ❑ Semplice ed economico
- ❑ Continua a migliorare 10 Mbit/s → 10+ Gbit/s

Name	Standard	Status	Mbit/s	Pairs	Distance	Cable
10BASE-T	802.3i-1990	Legacy	10	2	100 m	Cat. 3
100BASE-TX	802.3u-1995	Current	100	2	100 m	Cat 5e
1000BASE-T	802.3ab-1999	Current	1000	3	100 m	Cat 5e
5GBASE-T	802.3bz-2016	Current	5000	4	100 m	Cat 6
10GBASE-T	802.3an-2016	Current	10000	4	100 m	Cat 6A
25GBASE-T	802.3bq-2016	Future	25000	4	30 m	Cat 8
40GBASE-T	802.3bq-2016	Future	40000	4	30 m	Cat 8

Nascita di Ethernet



- Robert Metcalfe, 1973, Xerox Palo Alto Research Center
- Carrier Sense Multiple Access / Collision Detection and exponential backoff → 3 Mbit/s
- US Patent 4.063.220, 1977

Nascita di Ethernet

□ Da Spurgeon, «**Ethernet – The definitive guide**»

In late 1972, Metcalfe and his Xerox PARC colleagues developed the first experimental Ethernet system to interconnect the Xerox Alto, a personal workstation with a graphical user interface. The experimental Ethernet was used to link Altos to one another, and to servers and laser printers.

The signal clock for the experimental Ethernet interface was derived from the Alto's system clock, which resulted in a data transmission rate on the experimental Ethernet of 2.94 Mbps. Metcalfe's first experimental network was called the Alto Aloha Network.

In 1973 Metcalfe changed the name to "Ethernet," to make it clear that the system could support any computer--not just Altos--and to point out that his new network mechanisms had evolved well beyond the Aloha system.

He chose to base the name on the word "ether" as a way of describing an essential feature of the system: the physical medium (i.e., a cable) carries bits to all stations, much the same way that the old "luminiferous ether" was once thought to propagate electromagnetic waves through space. Thus, Ethernet was born.

Standardizzazione di Ethernet: da DIX a 802.3

- 1980: DIX Ethernet standard
 - ❖ DIX = Digital-Intel-Xerox vendor consortium
 - ❖ Interoperabilità tra i prodotti delle tre aziende
- 1982: Xerox rinuncia al marchio "Ethernet"
- 1985: IEEE 802.3
 - ❖ Ethernet diventa uno standard IEEE 802
 - Solo cambiamenti minori rispetto a DIX
 - Inizio dell'interoperabilità globale
 - ❖ Velocità: 10 Mbit/s
 - ❖ Mezzo di comunicazione:
 - Cavo coassiale spesso, max 500 m (10BASE5)
 - Cavo coassiale sottile, max 185 m (10BASE2)
 - Estensione di gittata fino a un limite massimo tramite ripetitori (<4)



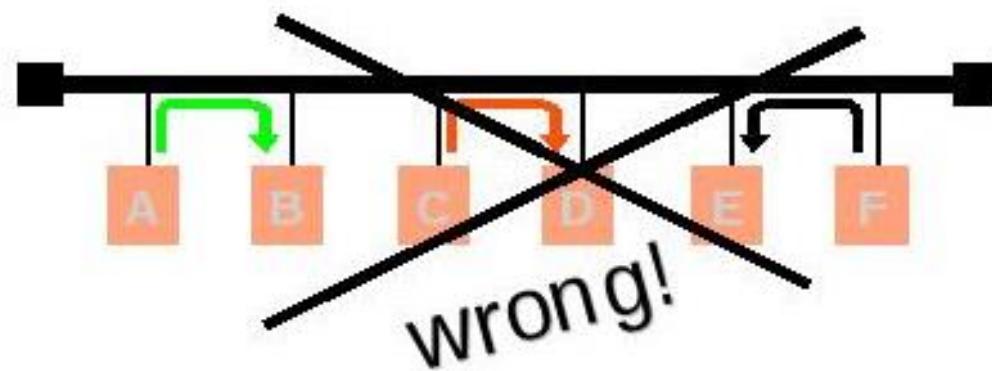
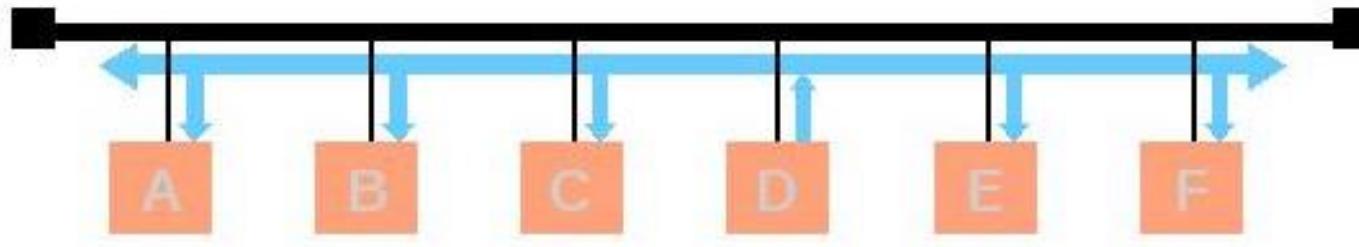
Thick-RG213



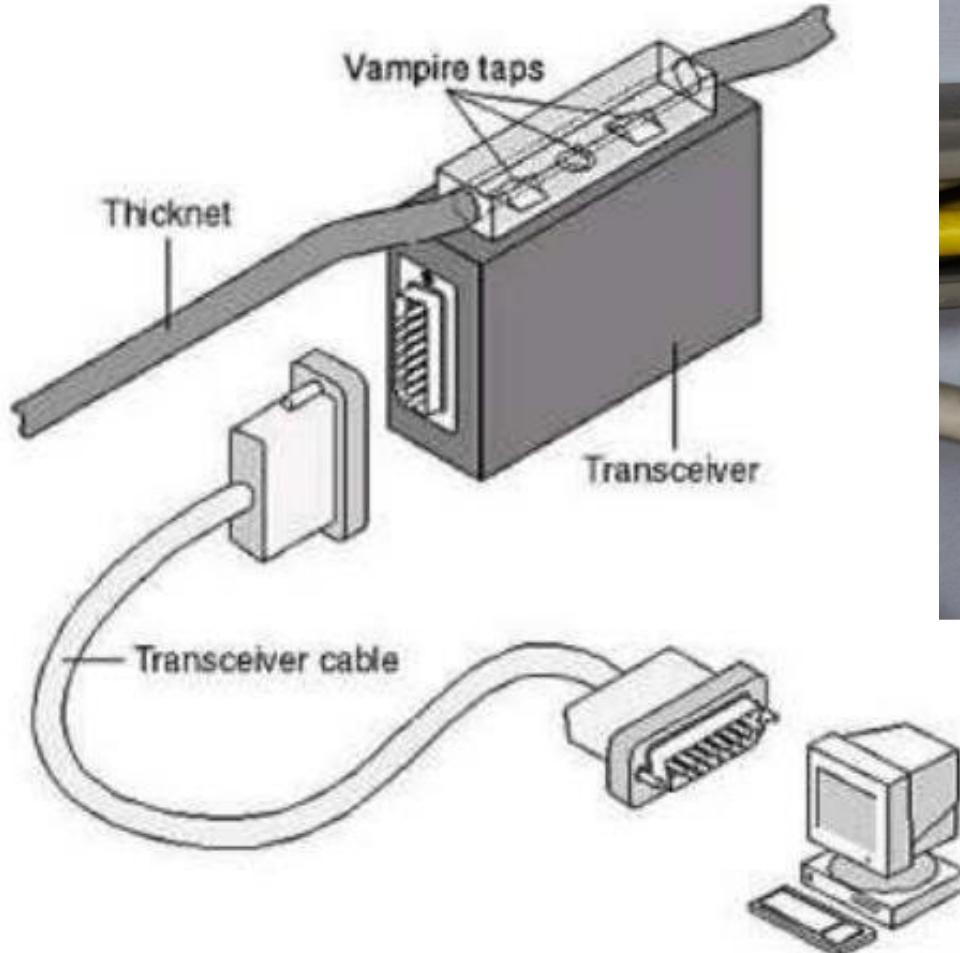
Thin-RG58

Prima topologia Ethernet: il bus

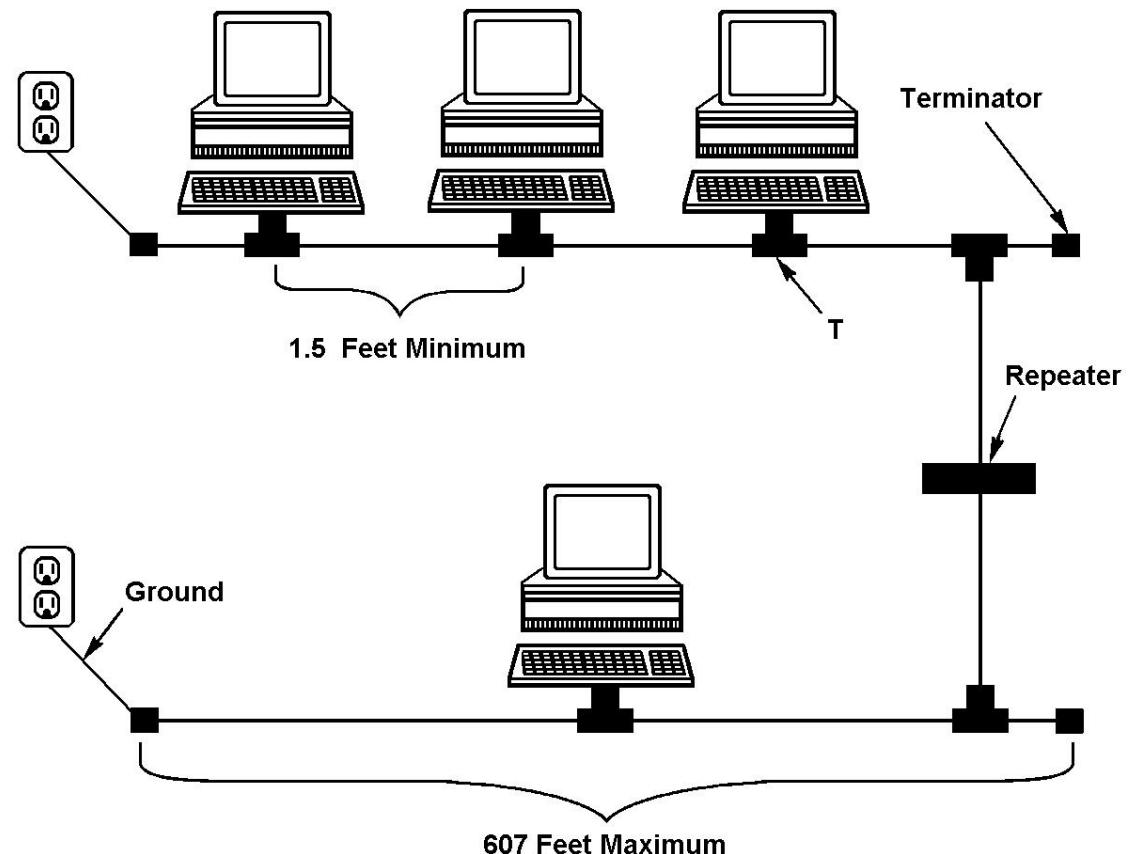
- Mezzo di trasmissione condiviso (ad accesso multiplo)
 - ❖ Thick / thin coaxial cable



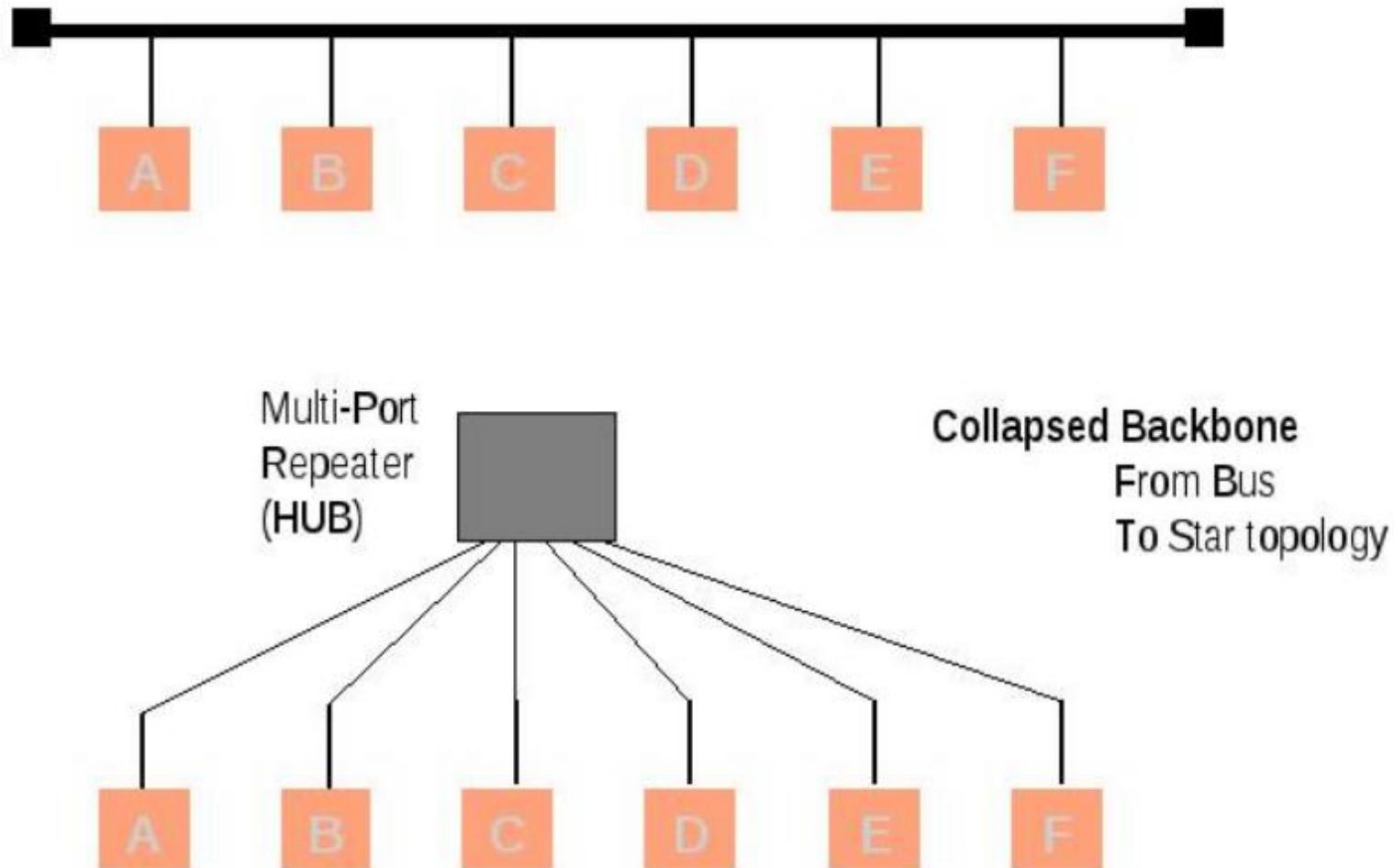
Transceiver Ethernet (10Base5)



Transceiver Ethernet (10Base-2)

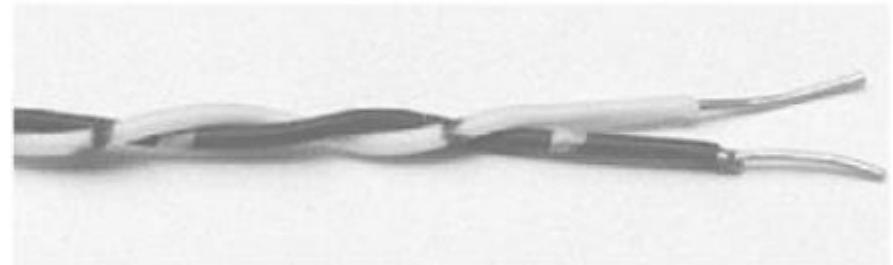


Idea spartiacque (1990): gli hub ...

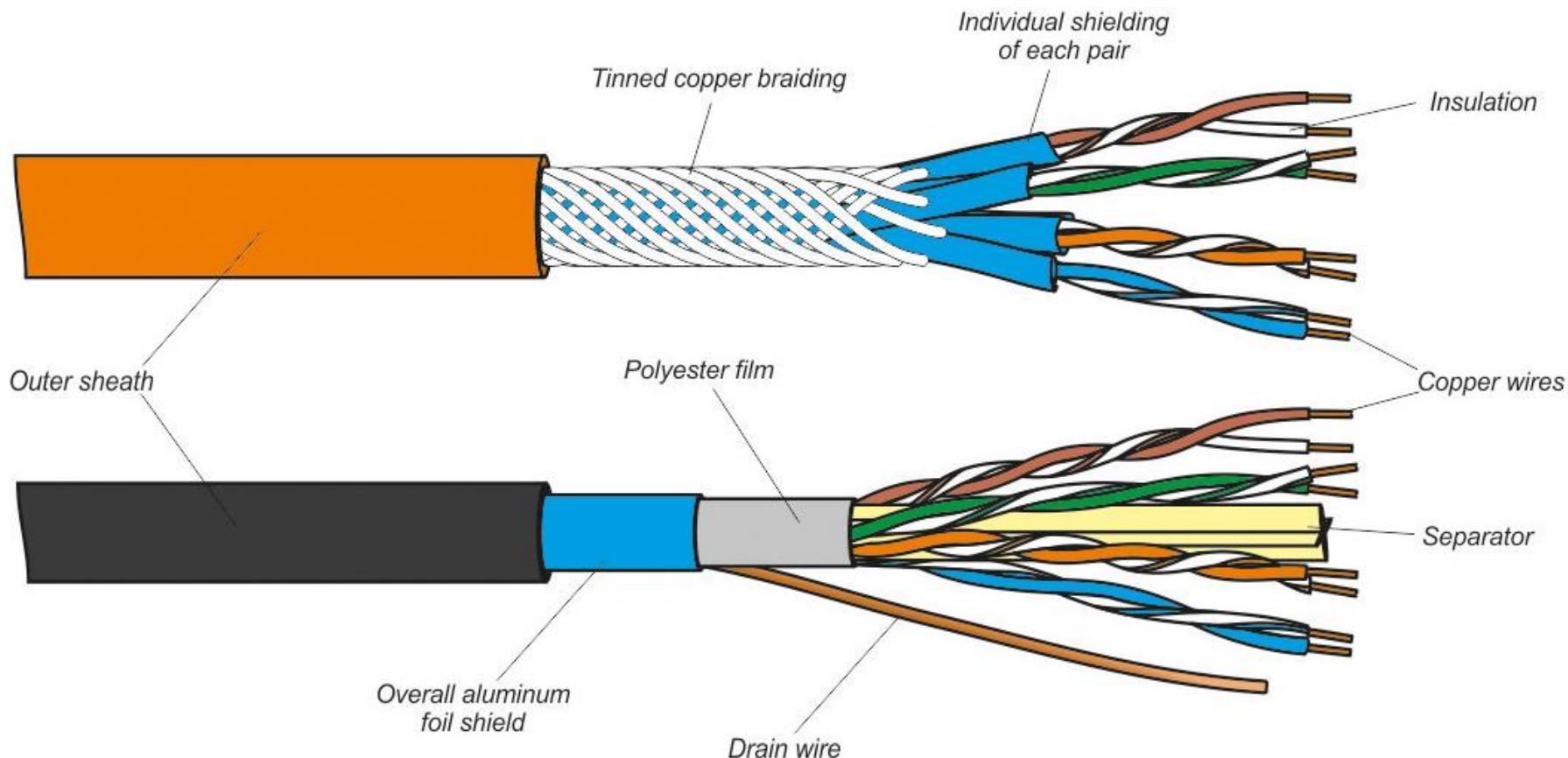


... i doppini incrociati ...

- Inventati da SynOptics comms
- Unshielded, shielded, foiled, ...
- Risolvono molti problemi di gestione e installazione
- Permettono di eliminare il «tubo giallo»
 - ❖ Da qui in poi, il mercato di Ethernet decolla veramente



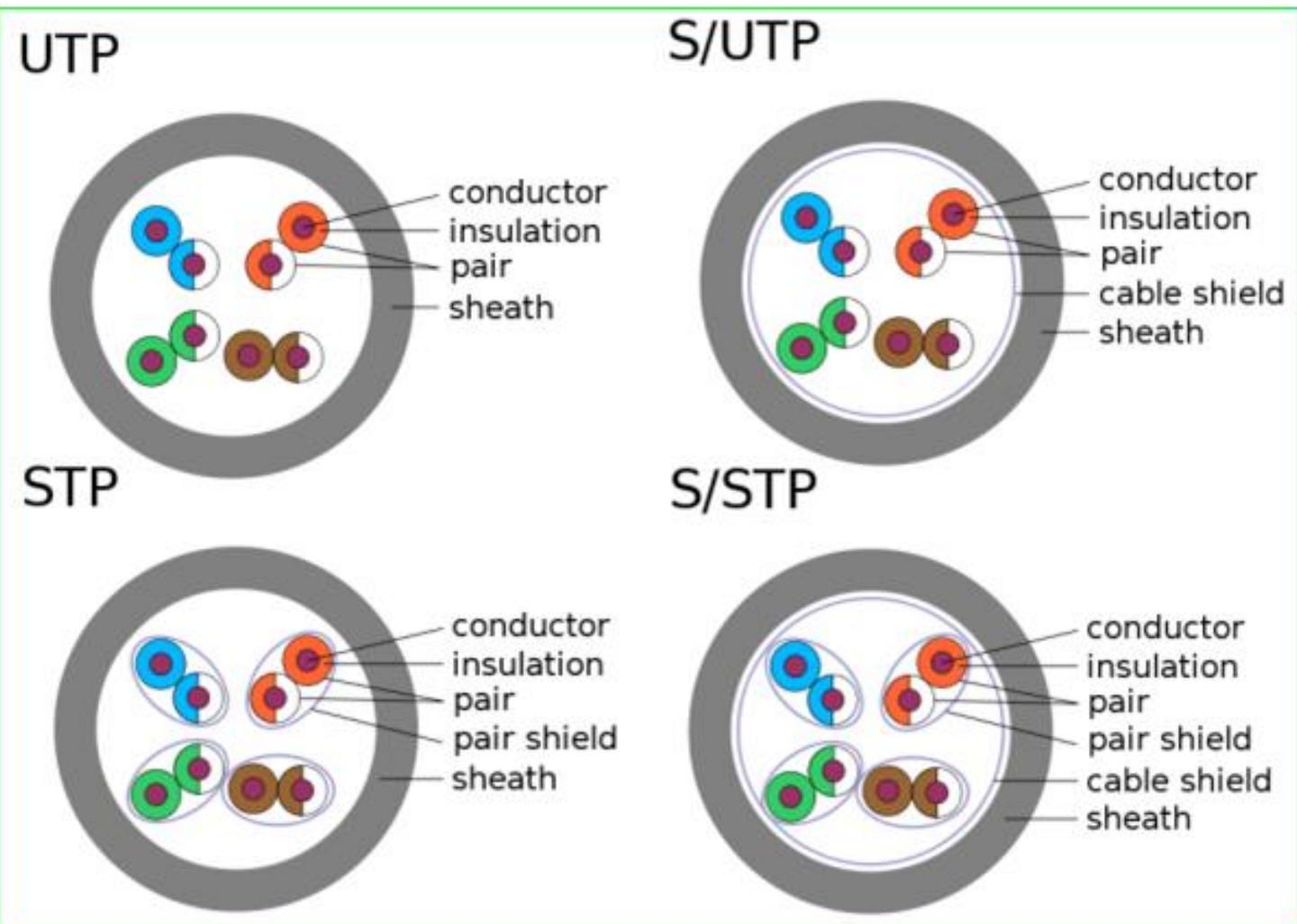
Cavi a doppino intrecciato (twisted pair)



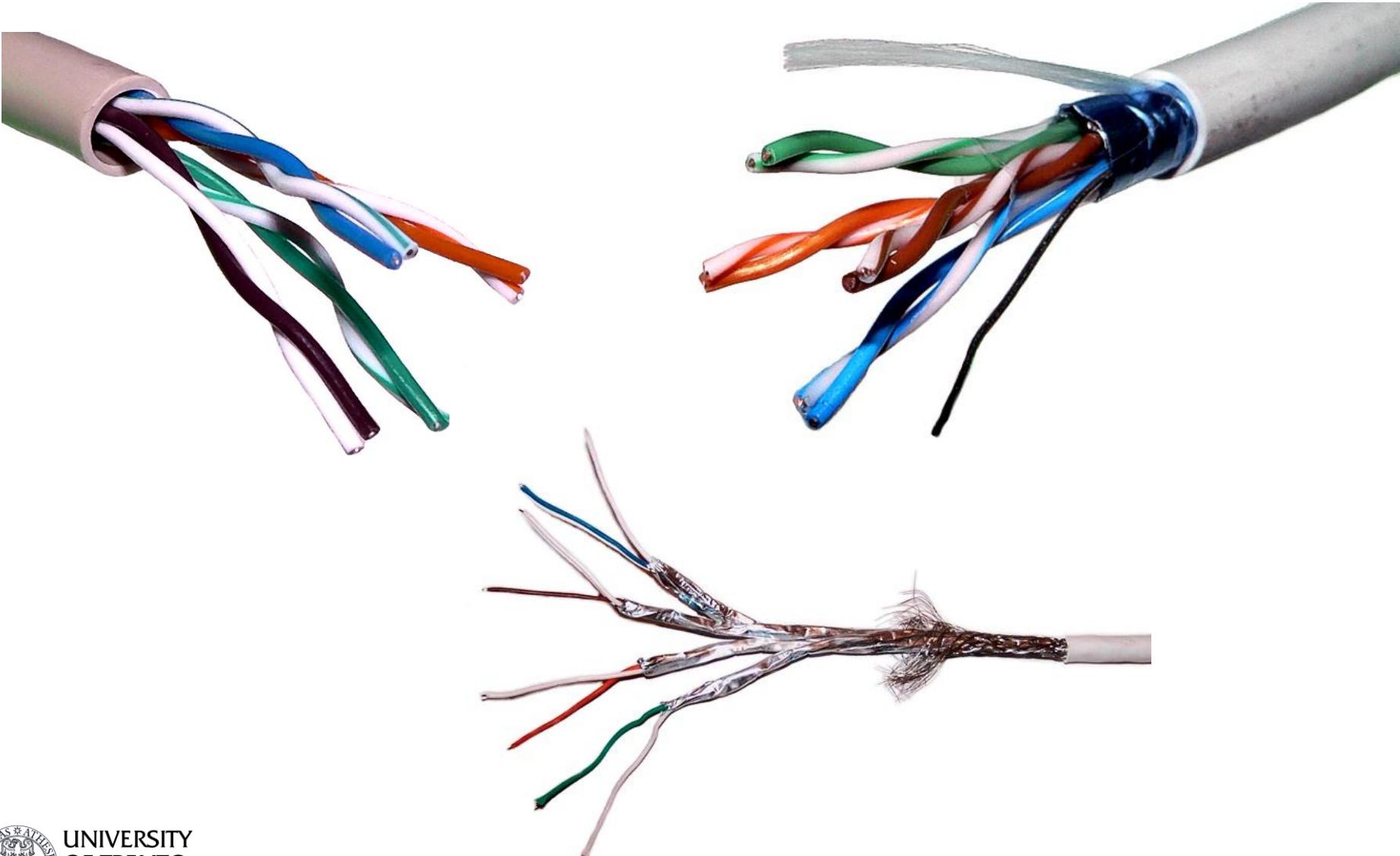
Denominazione sintetica dei cavi

- ❑ X / Y TP
- ❑ X è la schermatura dell'intero cavo
 - ❖ U : unshielded
 - ❖ F : foiled (di solito, una lamina di alluminio)
 - ❖ S : maglia metallica intrecciata (di solito, rame placcato alluminio)
 - ❖ SF : entrambe
- ❑ Y è la schermatura di ogni doppino
 - ❖ U : unshielded
 - ❖ F : shielded
- ❑ Esempi: U/UTP? F/UTP? S/FTP?

Sezione di cavi con/senza schermature



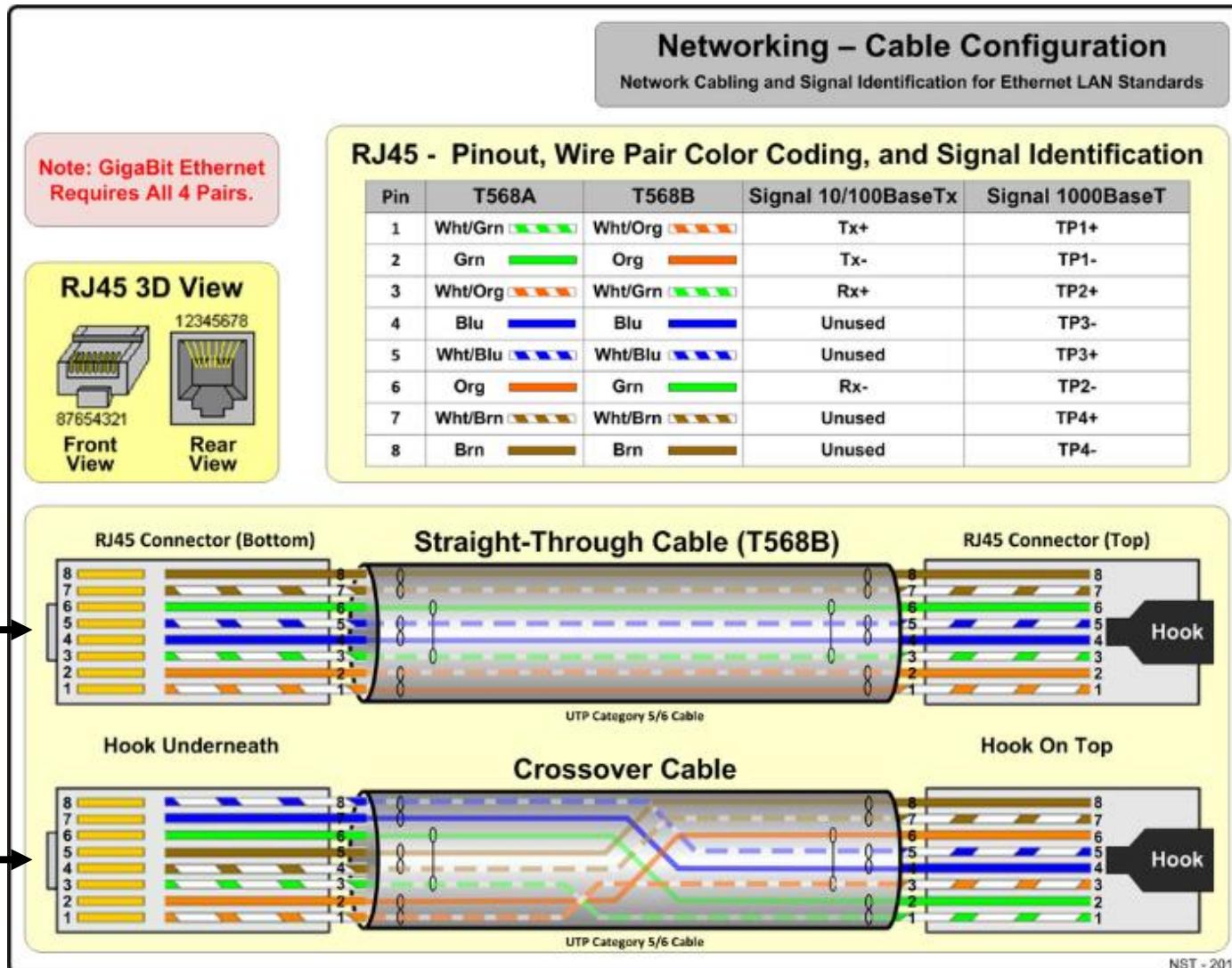
Cavi reali



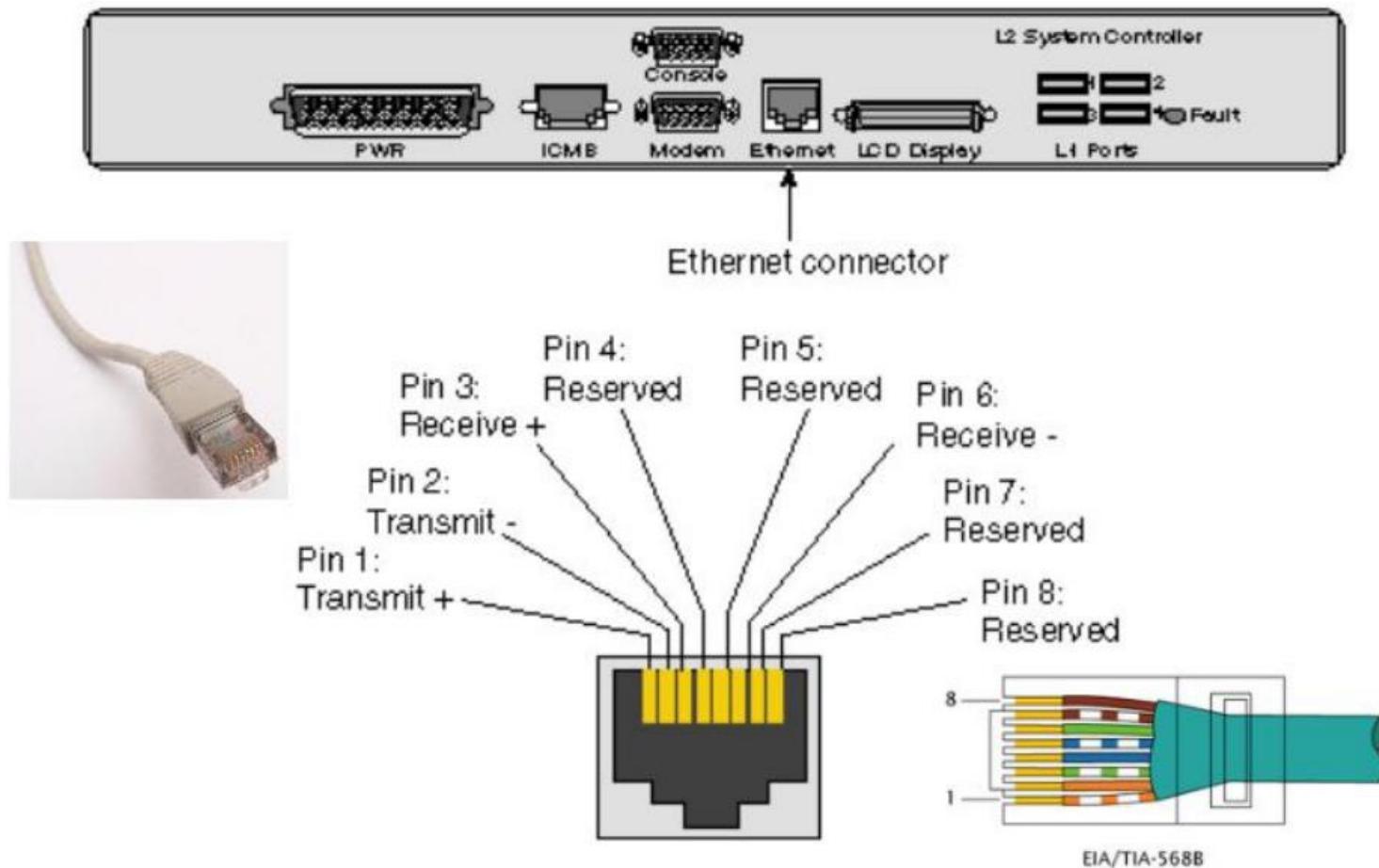
Cavi usati nello standard Ethernet

Name	Standard	Status	Mbit/s	Pairs	Distance	Cable
10BASE-T	802.3i-1990	Legacy	10	2	100 m	Cat. 3
100BASE-T1	802.3bw-2015	Legacy	100	1	15 m	Cat. 5e
100BASE-TX	802.3u-1995	Current	100	2	100 m	Cat 5e
1000BASE-T	802.3ab-1999	Current	1000	3	100 m	Cat 5e
1000BASE-T1	802.3bp-2016	Current	1000	1	40 m	Cat 6A
2.5GBASE-T	802.3bz-2016	Current	2500	4	100 m	Cat 5e
5GBASE-T	802.3bz-2016	Current	5000	4	100 m	Cat 6
10GBASE-T	802.3an-2016	Current	10000	4	100 m	Cat 6A
25GBASE-T	802.3bq-2016	Future	25000	4	30 m	Cat 8
40GBASE-T	802.3bq-2016	Future	40000	4	30 m	Cat 8

Connessione di cavi e connettori



...e infine il connettore RJ45



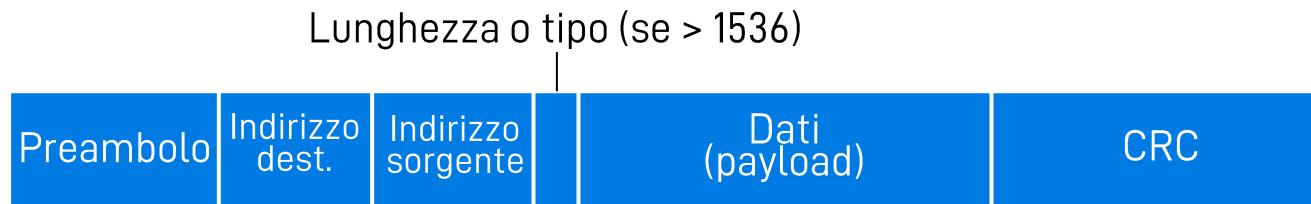
D: per quale tipo di cavo si usa questo connettore?

Struttura del frame Ethernet

La scheda di rete del mittente incapsula un datagramma di IP (o di un altro protocollo di rete) in un frame Ethernet come segue

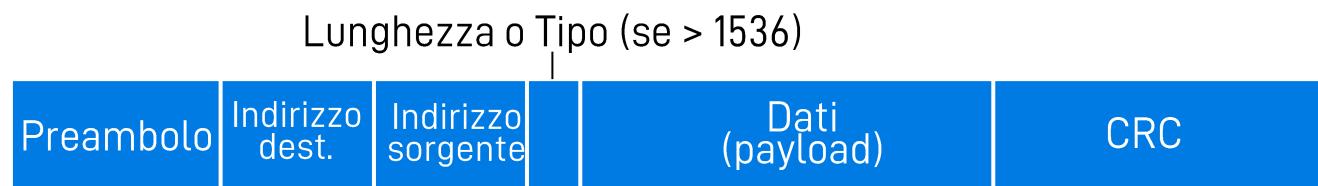
□ Preambolo:

- ❖ 7 bytes **10101010** seguiti da un byte **10101011**
- ❖ Si usa per sincronizzare il clock del ricevitore e del trasmettitore



Struttura del frame Ethernet

- Indirizzi: 6 byte per gli indirizzi MAC (livello 2) di sorgente e dest.
 - ❖ Se la scheda di rete riceve un frame diretto a sè, o diretto a un indirizzo broadcast (es. i pacchetti ARP), passa il payload del frame ai protocolli di livello rete
 - ❖ Altrimenti, scarta il frame
 - ❖ **D:** perché l'indirizzo di destinazione viene prima di quello sorgente?
- Tipo: indica il protocollo di livello superiore (tipicamente IP, ma ce ne possono essere altri, es., Novell IPX, AppleTalk)
- CRC: cyclic redundancy check
 - ❖ Se si rilevano errori, il frame viene scartato (no ARQ)
 - ❖ **D:** perché il CRC viene per ultimo?



Ethernet: connessione? ACK/NACK?

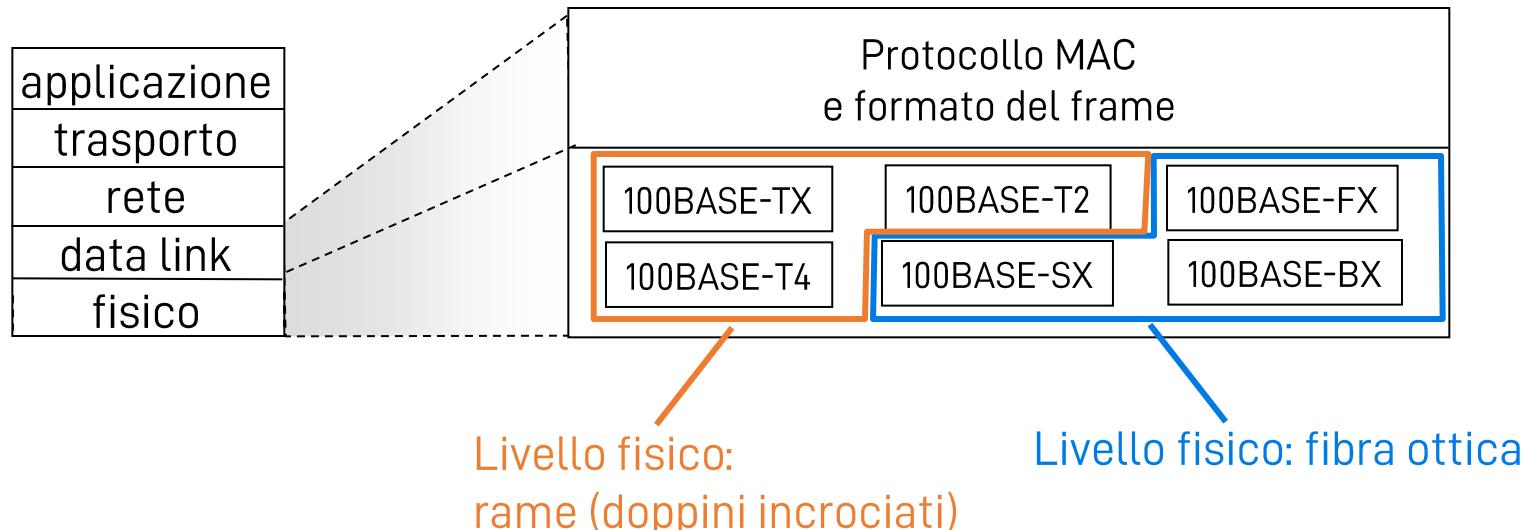
- **Connectionless:** nessuno scambio di messaggi di controllo tra le interfacce di rete di mittente e destinatario
- **Non affidabile:**
 - ❖ Non si usano ACK/NACK per recuperare frame persi tramite ritrasmissioni
 - ❖ Non si usano codici a correzione di errore, solo CRC
 - ❖ Quindi, i dati nel payload del frame si recuperano solo se un protocollo di livello più alto (es. TCP) implementa controllo di errore

Algoritmo CSMA/CD in Ethernet

1. La scheda di rete riceve un datagramma dal livello di rete e lo incapsula in un frame
2. Se una scheda di rete vede il canale libero, comincia a trasmettere; se lo vede occupato, attende finché non è libero e poi trasmette
3. Se la trasmissione termina senza rilevare altre trasmissioni, la scheda ritiene di aver trasmesso con successo il frame
4. Altrimenti, se la scheda rileva una collisione, trasmette un segnale di "abort"
5. Con ogni collisione, la scheda sceglie a caso il backoff tra il valore 0 e il valore $(2^k - 1)T$, $k \leq 7$, dove T è il tempo necessario a trasmettere 512 bit

Standard Ethernet 802.3: livello fisico e data link

- Molti standard Ethernet differenti
 - ❖ Il protocollo MAC e formato sono comuni
 - ❖ Diverse velocità di trasmissione
 - 2 Mbit/s, 10 Mbit/s, 100 Mbit/s, 1 Gbit/s, 10 Gbit/s, 40 Gbit/s
 - ❖ Diversi mezzi fisici: cavi a doppini incrociati, fibra ottica, ...



Evoluzione di Ethernet

- Fast Ethernet
 - ❖ 100 Mbit/s
 - ❖ Funziona sia con gli switch sia con un canale condiviso e CSMA/CD
- Gigabit Ethernet
 - ❖ 1 and 10 Gbit/s
 - ❖ Solo reti con switch
- 40/100 Gigabit Ethernet
 - ❖ 40 and 100 Gbit/s
 - ❖ Solo reti con switch
 - ❖ Principalmente su fibra ottica
 - Fino a 40 km di distanza

Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ Protocolli "a turni"
 - ❖ IEEE 802 ed Ethernet
- ❑ **Ethernet switching**
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Switch Ethernet

- Hub: ripetitore di livello 1
- Switch: dispositivo di livello 2 (data link): ruolo più *attivo*
 - ❖ Memorizza e inoltra i frame Ethernet
 - ❖ Esamina il MAC address dei frame che arrivano
 - Li inoltre selettivamente su uno o più link collegati
 - Solo se necessario, ricorre a CSMA/CD per accedere al canale
- Trasparente
 - ❖ Gli host non sanno (né hanno bisogno di sapere) se sono collegati a uno switch
- Plug-and-play, autoapprendimento
 - ❖ Non c'è bisogno di configurare esplicitamente gli switch per nessuna operazione di base

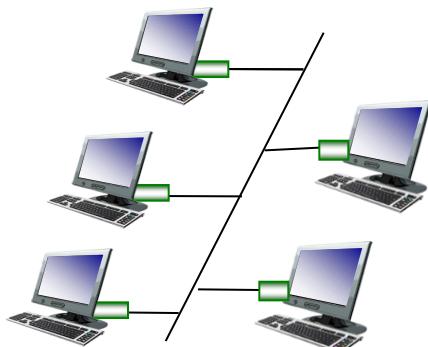
Ethernet e domini di collisione

□ Topologia a bus

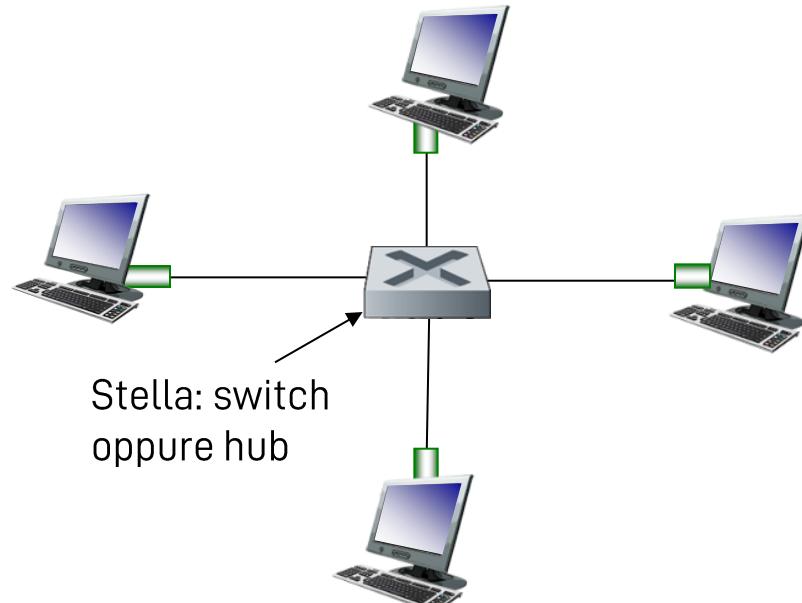
- ❖ Tutti i nodi sono nello stesso dominio di collisione, ovvero chiunque può potenzialmente collidere con chiunque altro

□ Topologia a stella: la prevalente al giorno d'oggi

- ❖ Se il centro stella è un hub (ripetitore layer-1): stesso dominio di collisione
- ❖ Se il centro stella è uno switch (layer-2): diverso dominio di collisione per ogni host

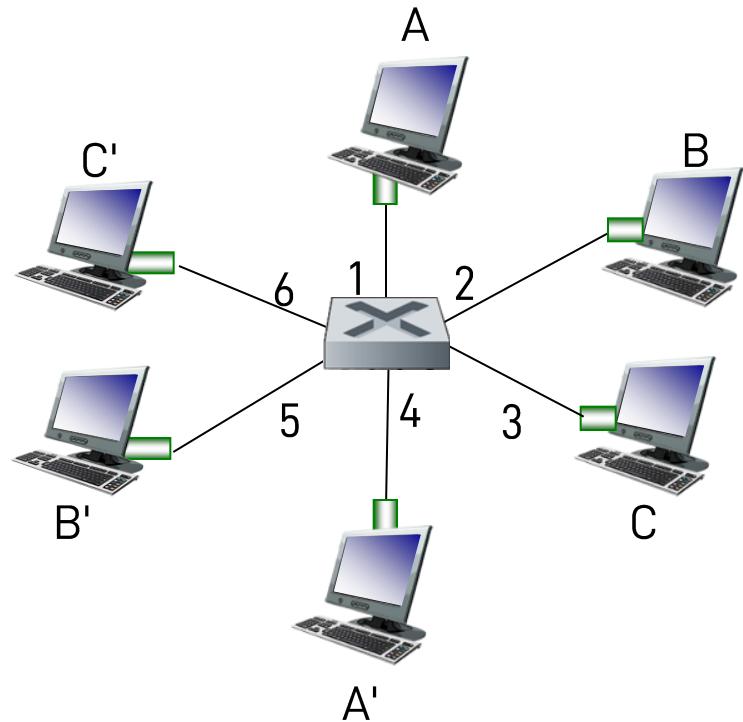


Bus (cavo coassiale)



Switch: trasmissioni simultanee

- In una rete "switched", ogni host ha un canale dedicato per comunicare con lo switch
- Si usa il protocollo Ethernet su ciascun link, ma gli unici nodi a usarlo sono l'host e lo switch
 - ❖ No collisioni, full duplex
 - ❖ Ogni link è un dominio di collisione a parte
- Quindi: A e A' possono comunicare insieme a B e B', senza collidere



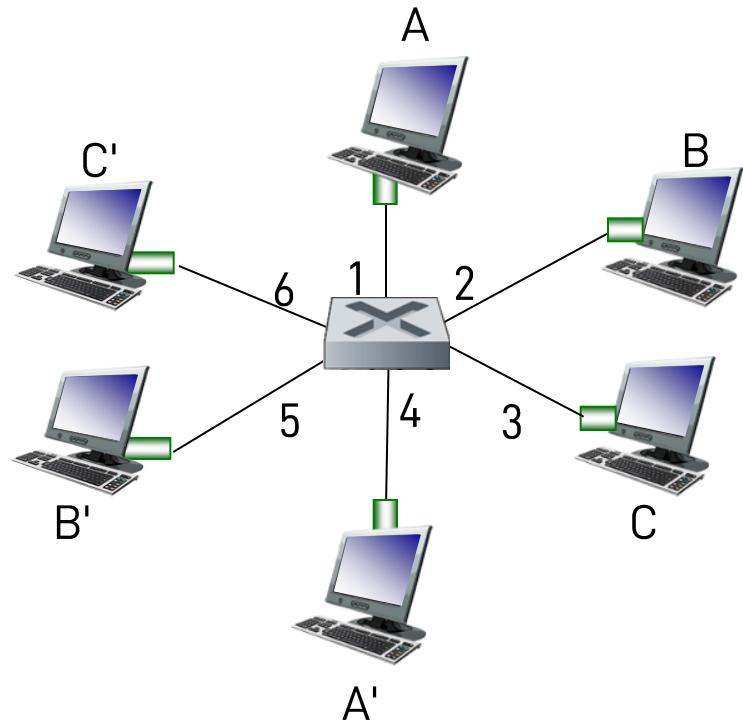
Switch con 6 interfacce
(1,2,3,4,5,6)

Tabella di inoltro degli switch

- Come fa lo switch a sapere che A' è raggiungibile tramite l'interfaccia 4 e B' tramite 5?
- Mantiene una tabella del tipo:

MAC address dell'host	Interfaccia per raggiungere l'host	Time to live
...

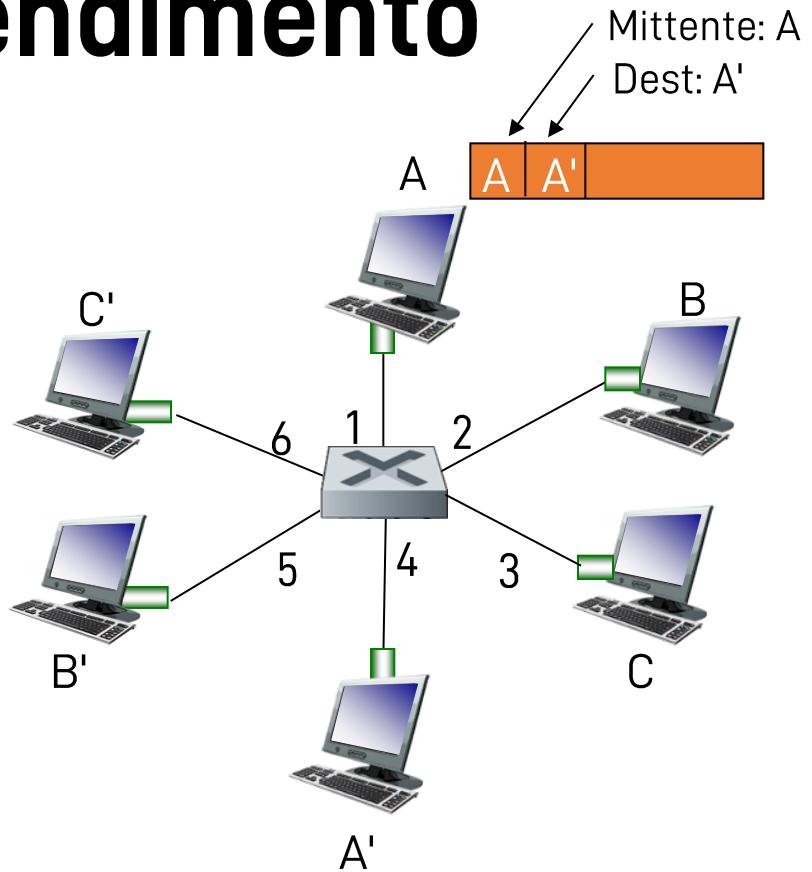
- Come viene mantenuta la tabella?
 - ❖ Autoapprendimento
 - ❖ Aggiornando le corrispondenze quando si ricevono nuovi frame
 - ❖ Cancellando le righe vecchie



Switch con 6 interfacce
(1,2,3,4,5,6)

Switch: autoapprendimento

- ❑ "Backward learning"
- ❑ Lo switch impara quali host possono essere raggiunti attraverso ogni interfaccia
 - ❖ Alla ricezione di un frame, si annota la porta da cui proviene e l'indirizzo MAC dell'host



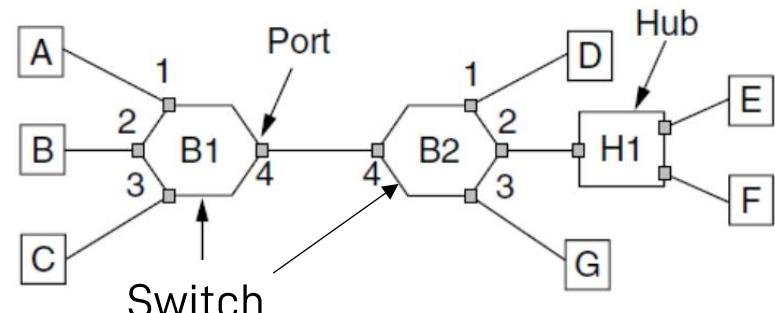
MAC address	Interfaccia	TTL
A	1	60

Tabella dello switch
(inizialmente vuota)

Switch: filtraggio e inoltro dei frame

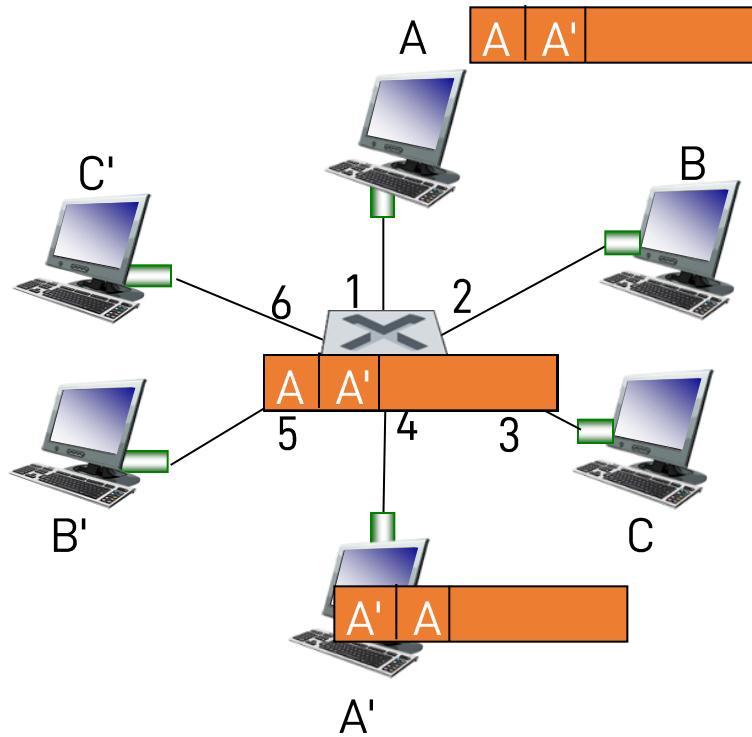
Quando si riceve un frame

- ❑ Si aggiorna la tabella
- ❑ Si inoltra il frame
- ❑ Se si trova una riga nella tabella che indica come raggiungere la destinazione del frame
 - ❖ Se la destinazione si trova su una porta diversa da quella del mittente
 - Inoltra il frame
 - ❖ Altrimenti \leftarrow D: Come può essere?
 - Scarta il frame
- ❑ Se non c'è una riga nella tabella
 - ❖ Flooding del frame su tutte le interfacce (eccetto quella di arrivo)



Altro esempio

- Destinazione A': porta di uscita sconosciuta
 - ❖ Flooding
- Destinazione A nota:
 - ❖ Si invia il frame selettivamente su quel link

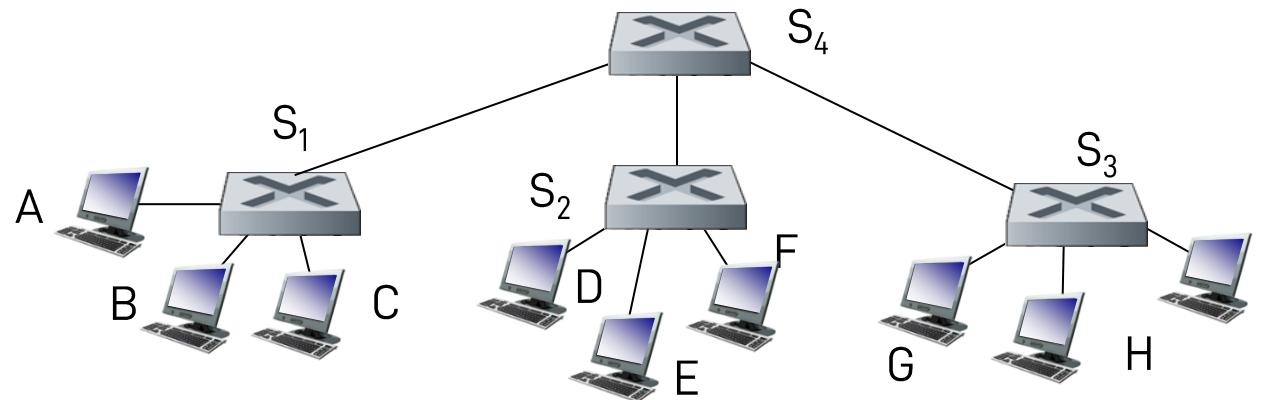


MAC addr	interface	TTL
A	1	60
A'	4	60

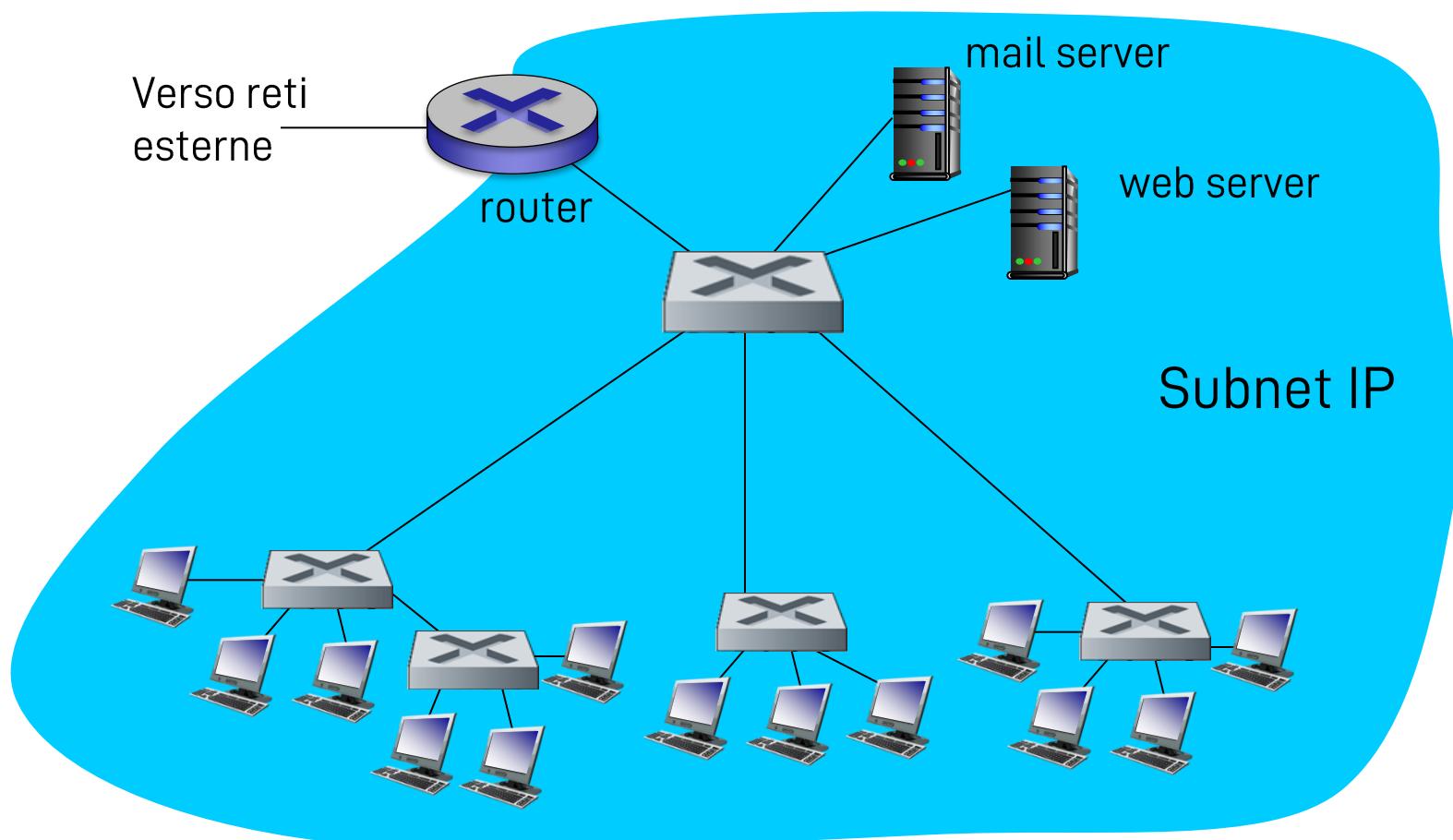
switch table
(initially empty)

Caso con switch multipli

- Gli switch apprendono automaticamente anche quando sono connessi in topologie più complesse
- Es.: A vuole trasmettere a G → Come fanno gli switch a capire su quali porte inviare i frame?
 - ❖ Autoapprendimento, esattamente come nel caso di un solo switch



Rete istituzionale (molto semplice)



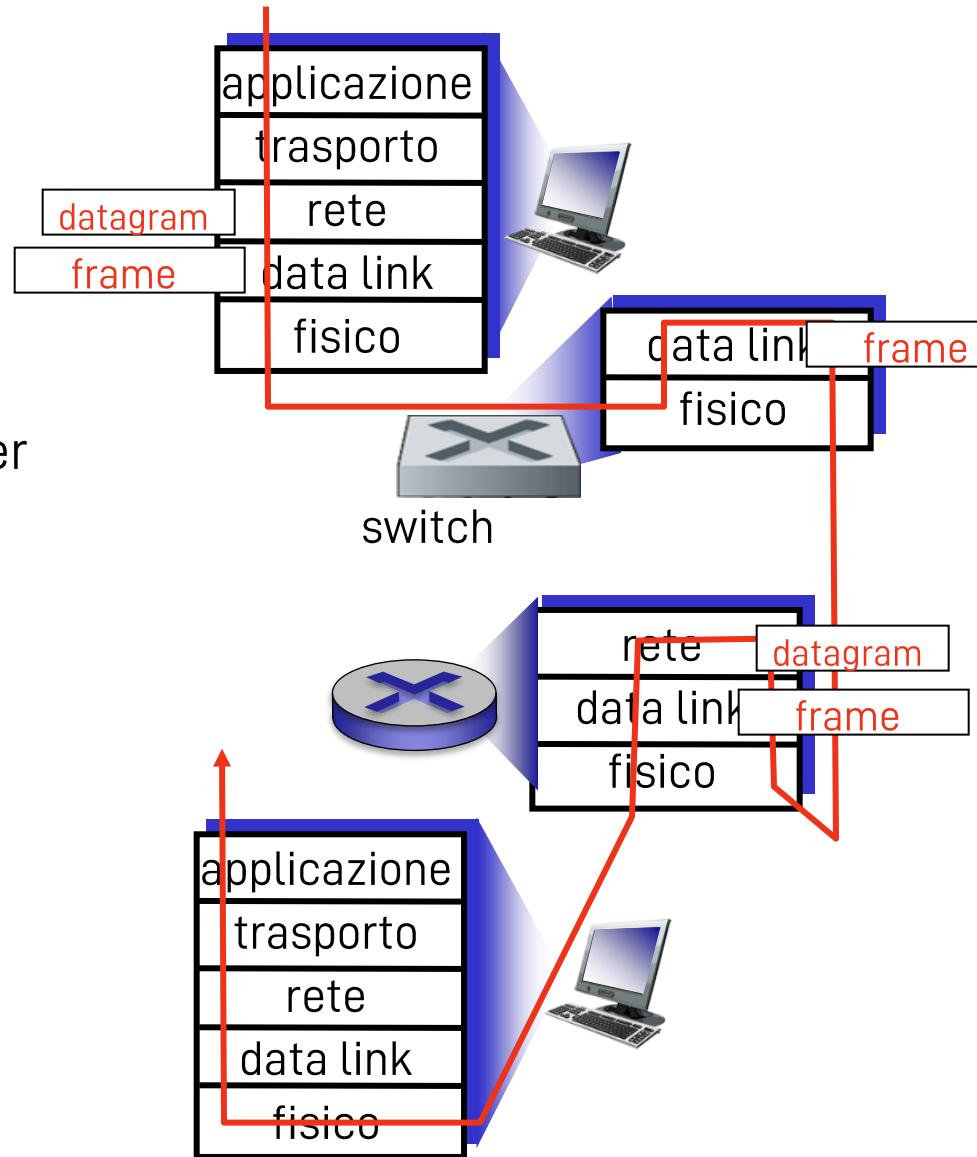
Switch, router e hub

□ Store-and-forward:

- ❖ Router: dispositivi di livello di rete (esaminano gli header dei datagrammi)
- ❖ Switch: dispositivi di livello data link (esaminano gli header dei frame)
- ❖ Hub : puri ripetitori di segnale

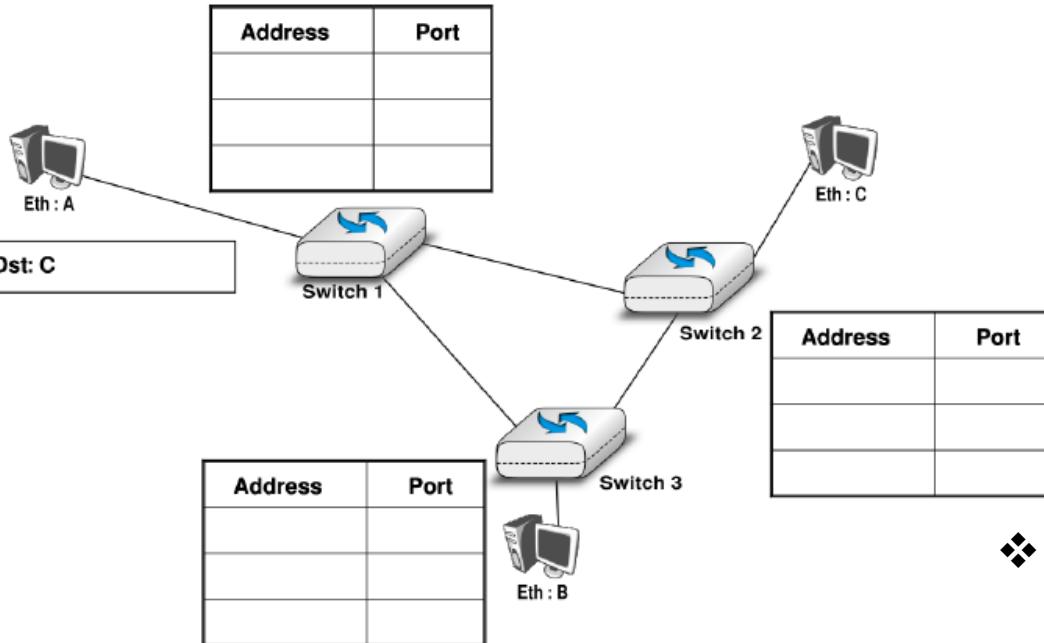
□ Tabelle di inoltro:

- ❖ Router: riempiono le tabelle usando algoritmi di routing, indirizzi di rete (es. IP)
- ❖ Switch: apprendono le tabelle di inoltro usando il flooding e i MAC address (livello 2)
- ❖ Hub: nulla



Switch collegati ad anello (loop)

- Cosa succede al boot di questa rete?
 - ❖ Tutte le tabelle degli switch sono vuote
 - A invia a C: Switch 1 non sa dove sia C → flooding
 - Nemmeno Switch 2 sa dove sia C → flooding
 - Switch 3 riceve frame sia da 1 sia da 2, ma non sa dove sia C → flooding
 - ❖ Refresh dei TTL delle tabelle
 - Le righe non si cancellano
 - I frame potrebbero circolare continuamente nell'anello



Switch collegati ad anello (loop)

- Questi loop tra switch saturano in fretta la capacità dei link e sovraccaricano gli apparati
- Facili da creare: collegate due porte di uno switch alla stessa LAN
- Soluzioni
 - ❖ Evitare del tutto i loop
 - Perché mai? I loop forniscono ridondanza, quindi robustezza contro la rottura di qualche link
 - ❖ Rompere fisicamente il loop (es., disconnettere qualche cavo)
 - ❖ Usare una topologia logica più efficiente di quella fisica
 - **D:** Quale topologia, per definizione, non ha loop?

Spanning tree per switch

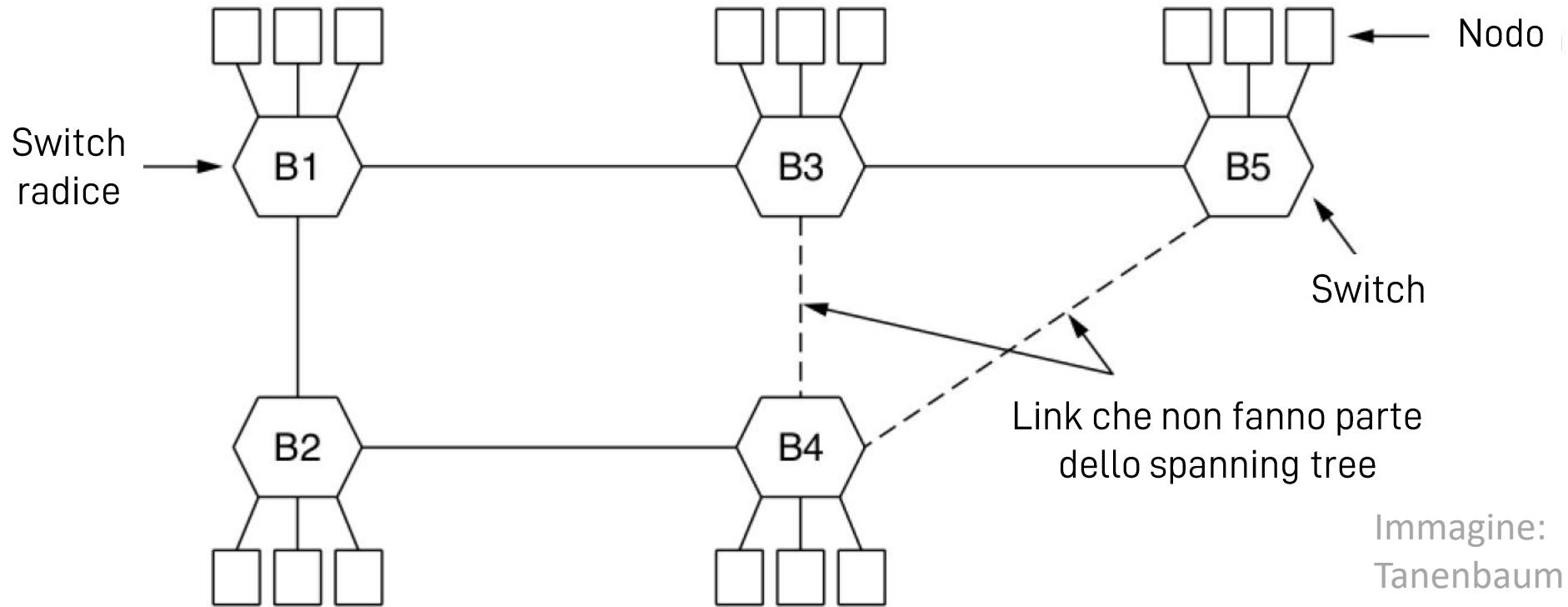
□ Prerequisiti

- ❖ Formazione dell'albero automatica e adattamento dinamico

□ Spanning Tree Protocol (STP)

- ❖ Tutti gli switch hanno un unico identificatore da 64 bit così formato:
 - I primi 16 bit impostati dall'amministratore di rete
 - Gli ultimi 48 bit: il MAC address dello switch (impostato di fabbrica)
- ❖ STP costruisce un albero con radice nello switch che ha l'ID più basso
- ❖ Feature utile: i bit più significativi sono configurabili, quindi l'amministratore può scegliere dove piazzare la radice
 - Vicino al router di bordo della LAN
 - Noto il traffico, nella posizione che non eccede la capacità dei link
 - ...

Spanning tree per switch



- Loop evitati disattivando i link B3-B4 e B4-B5
- Non si ha necessariamente il percorso più corto per ogni pacchetto

Spanning Tree Protocol (STP)

- ❑ Gli switch si scambiano pacchetti di controllo chiamati Bridge Protocol Data Unit (BPDU)
 - ❖ Contengono l'**ID** del mittente e il **costo** del link
- ❑ Quando lo switch A riceve un BPDU da B, controlla gli ID, e se quello di A è più piccolo, la porta di B verso A diventa radice dell'albero per B
- ❑ Altrimenti, tra tutte le porte da cui si riceve una BPDU
 - ❖ La porta da cui A riceve la BPDU con il costo più basso diventa la radice dell'albero per A (diciamo che questa BPDU veniva da B)
 - ❖ B diventa progenitore di A nell'albero
 - ❖ A aggiorna il proprio costo a $c = COST_A + COST_B$
 - ❖ Le porte da cui A riceve una BPDU con costo $> c$ diventano «designated ports» (figli di A nell'albero)
 - ❖ Le porte da cui A riceve una BPDU con costo $= c$ diventano «blocked ports»
 - Sono altri potenziali progenitori di B, che creerebbero loop a livelli più alti dell'albero, se usate

Spanning Tree Protocol (STP)

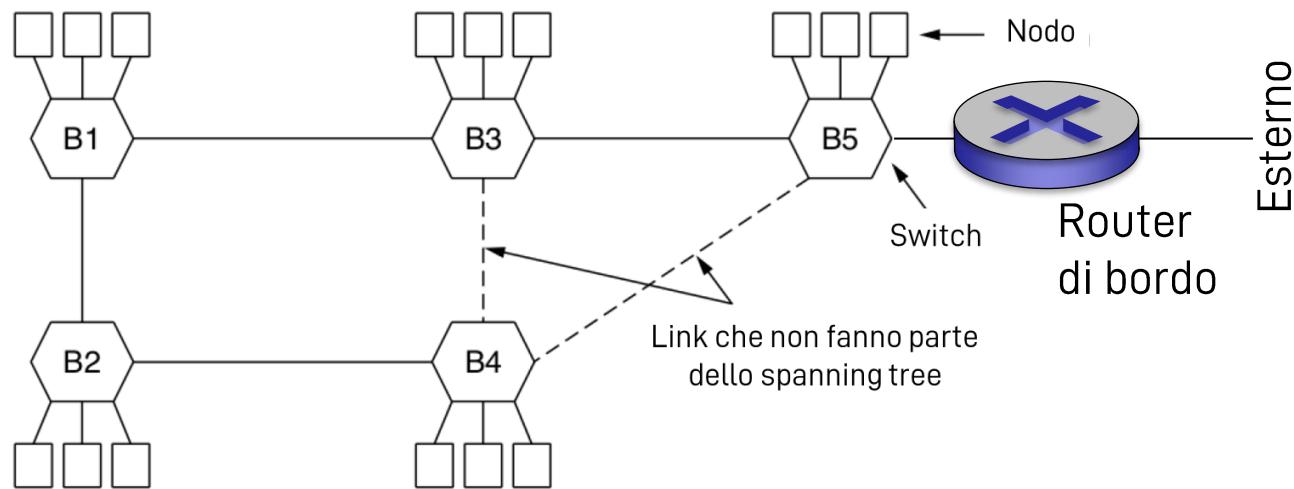
Port state	Receives BPDUs	Sends BPDU	Handles data frames
Blocked	yes	no	no
Root	yes	no	yes
Designated	yes	yes	yes

- Le BPDU vengono inviate periodicamente per rilevare cambiamenti
 - ❖ Ogni nodo le invia solo alle «designated ports»
 - ❖ Le porte «Blocked» non sono mai coinvolte nella trasmissione di BPDU

Variazioni di STP

- Le BPDU vengono re-inviate periodicamente
 - ❖ La radice invia la BPDU a tutte le sue porte «designated»
 - ❖ Gli altri switch ricevono la BPDU e la inoltrano alle proprie porte «designated»
- L'ultima BPDU ricevuta «invecchia» ogni secondo
- Quando l'età supera un valore massimo, serve un cambio di topologia dell'albero
 - ❖ Il processo di formazione riparte da zero
 - ❖ Finché l'albero non converge, gli switch non inoltrano traffico

Performance di STP



- Alcuni collegamenti sono più lunghi del percorso minimo
- La radice dell'albero che può essere collocata su uno switch conveniente
 - ❖ D: se le connessioni sono di tipo 1000 Base-T, e ogni nodo della topologia qui sopra genera 100 Mbit/s di traffico verso l'esterno, è meglio posizionare la radice dell'albero su B5 o su B1?

Chi ha inventato STP?

□ Radia Perlman

- ❖ La incaricarono di risolvere il problema dei loop nelle reti di switch
- ❖ Le diedero una settimana, ci mise due giorni



Chi ha inventato STP?

- Col tempo rimasto, ci scrisse su una poesia ☺

*I think that I shall never see
a graph more lovely than a tree
A tree whose crucial property
is loop-free connectivity
A tree which must be sure to span
so packets can reach every LAN*

*First the Root must be selected
by ID it is elected
Least cost paths from Root are traced
in the tree these paths are placed
A mesh is made by folks like me
then bridges find a spanning tree*



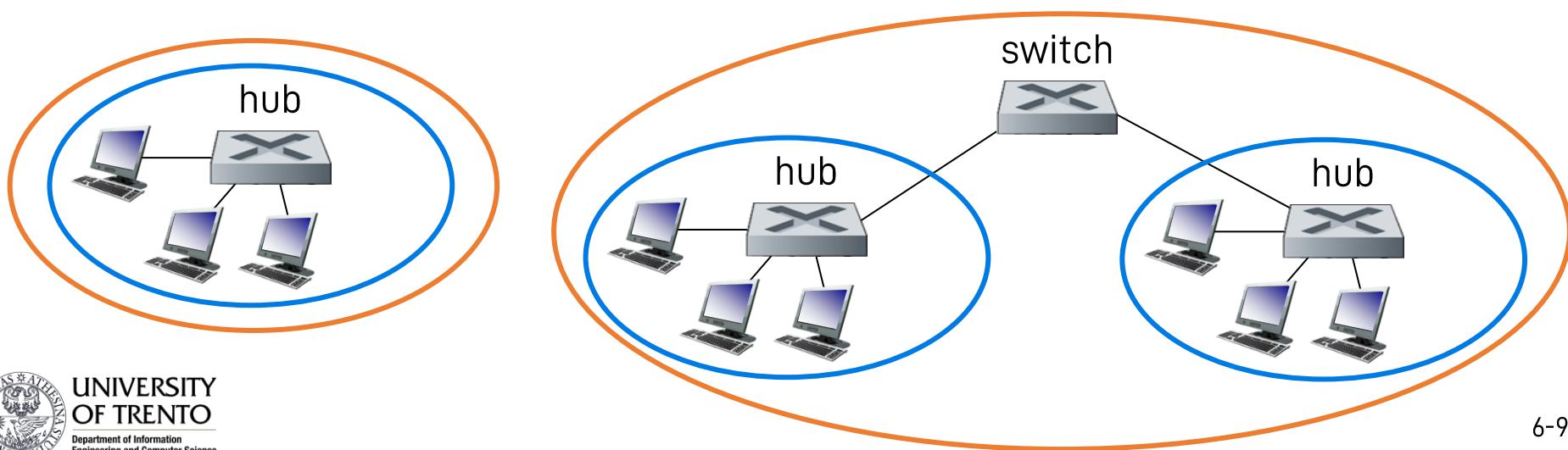
Domini di broadcast e di collisione

□ Dominio di collisione

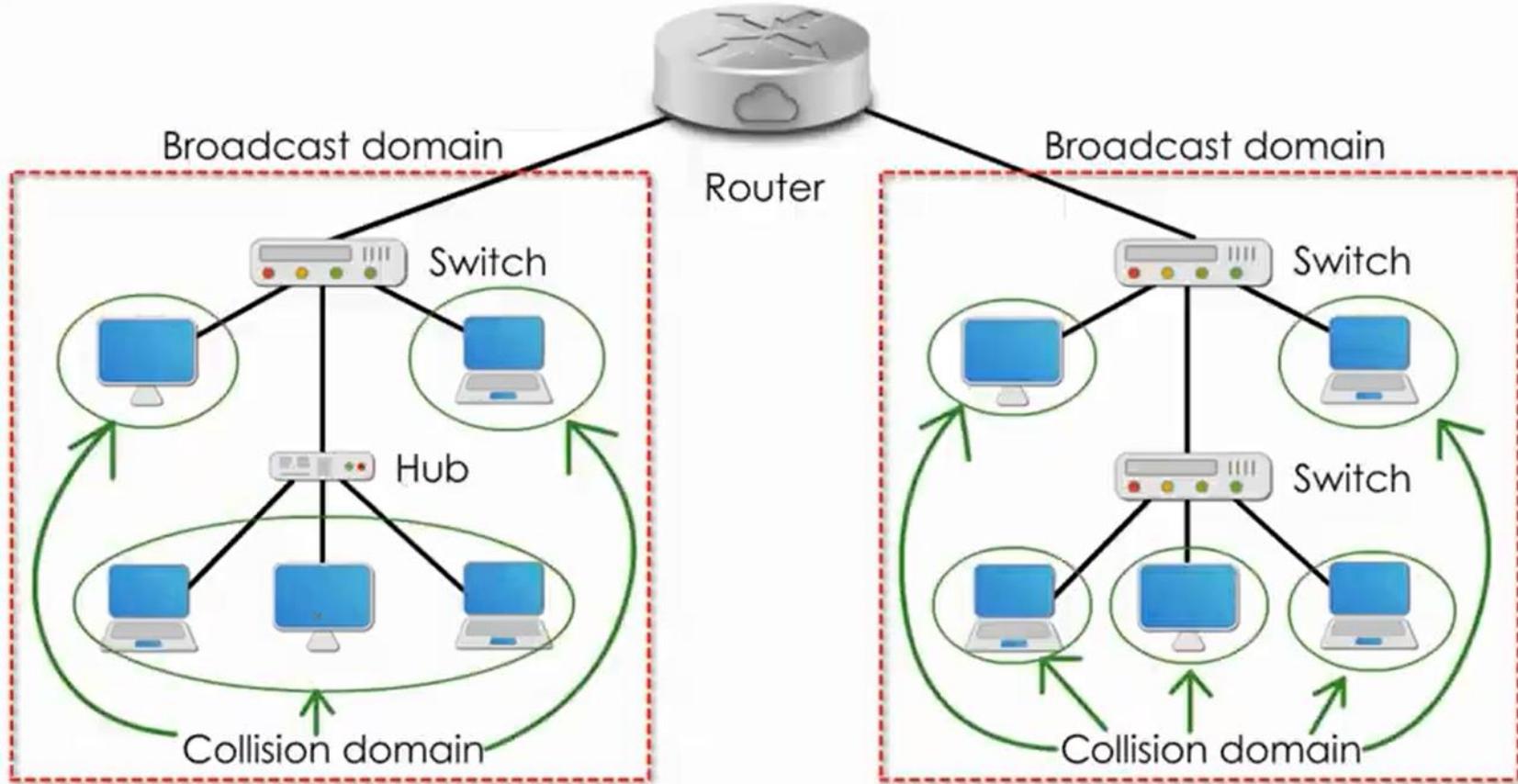
- ❖ Parte della rete in cui, se due nodi trasmettono contemporaneamente, si verifica una collisione

□ Dominio di broadcast

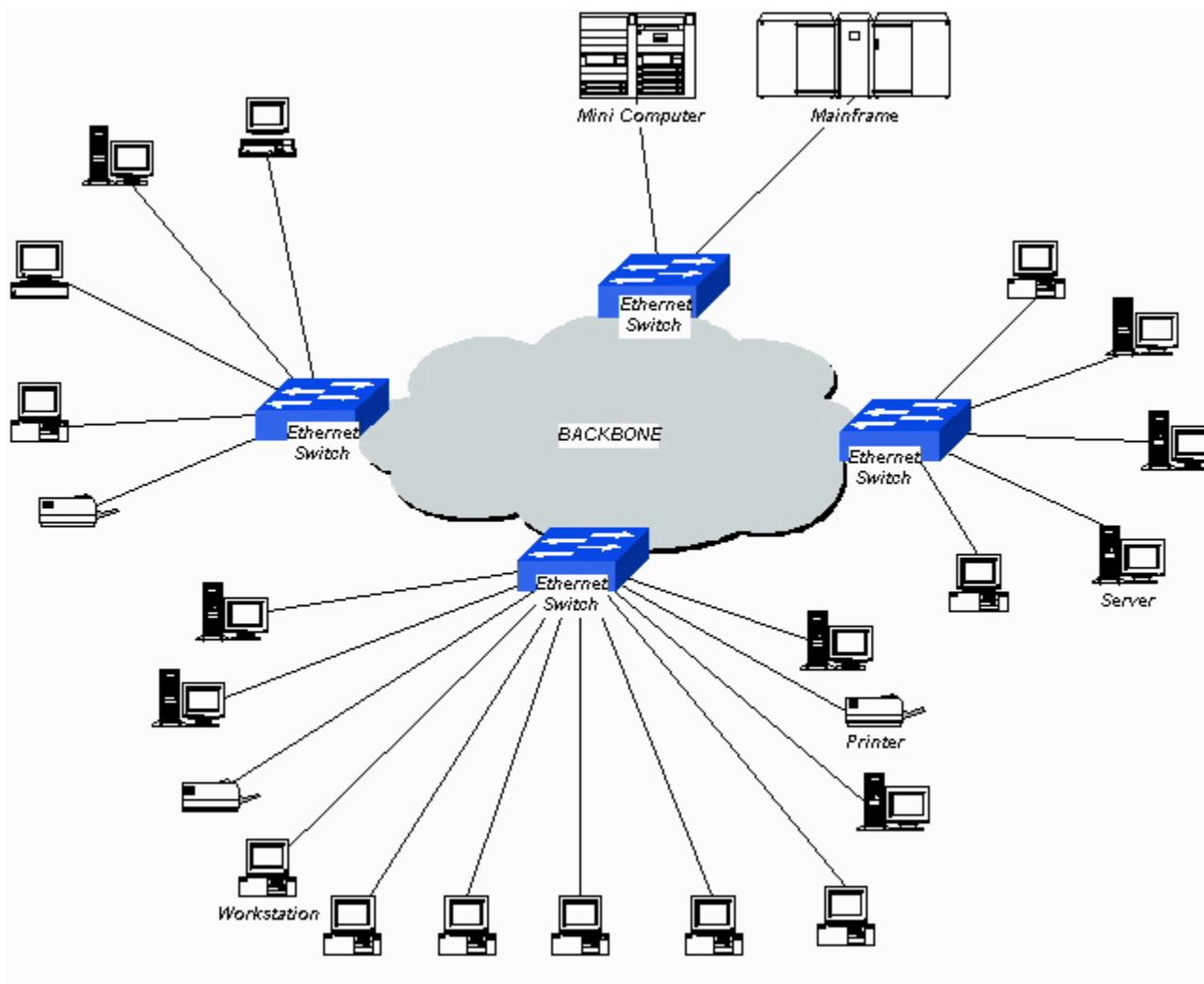
- ❖ Parte della rete che può essere raggiunta attraverso un messaggio di broadcast di livello 2
- ❖ I nodi collegati alla stessa infrastruttura di livello 2 sono parte dello stesso dominio di broadcast



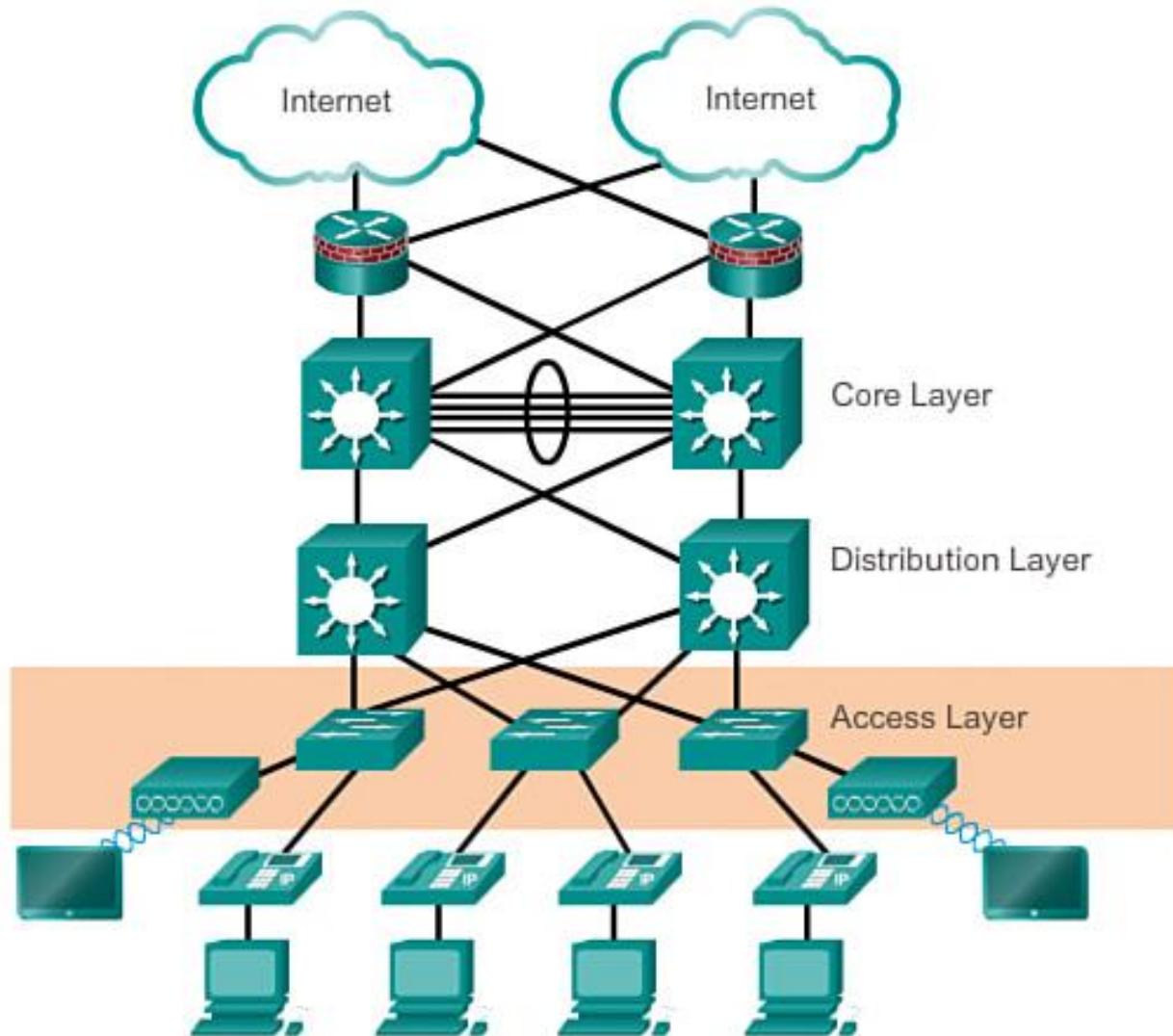
Altro esempio



Tipica configurazione «moderna»



Tipica configurazione moderna



Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ Protocolli "a turni"
 - ❖ IEEE 802 ed Ethernet
- ❑ Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ **VLAN**
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Organizzazione logica delle LAN

- Ci sono molti buoni motivi per ripartire gruppi di host su LAN diverse, anche quando questi sono connessi alla stessa infrastruttura di rete
 - ❖ Separazione di intenti
 - Una LAN potrebbe contenere tutti i server esposti verso l'esterno (web, mail, database, etc.)
 - Una LAN diversa potrebbe essere riservata alle informazioni sensibili (es. database delle Risorse Umane con profili dei dipendenti) ed essere inaccessibile da fuori
 - ❖ Carico
 - Esperimenti sulla rete potrebbero generare traffico incontrollato e saturare la LAN
 - ❖ Separare i domini di broadcast
 - LAN più grandi diffondono i messaggi di broadcast su molti più link (inefficiente, meglio mantenere la località)

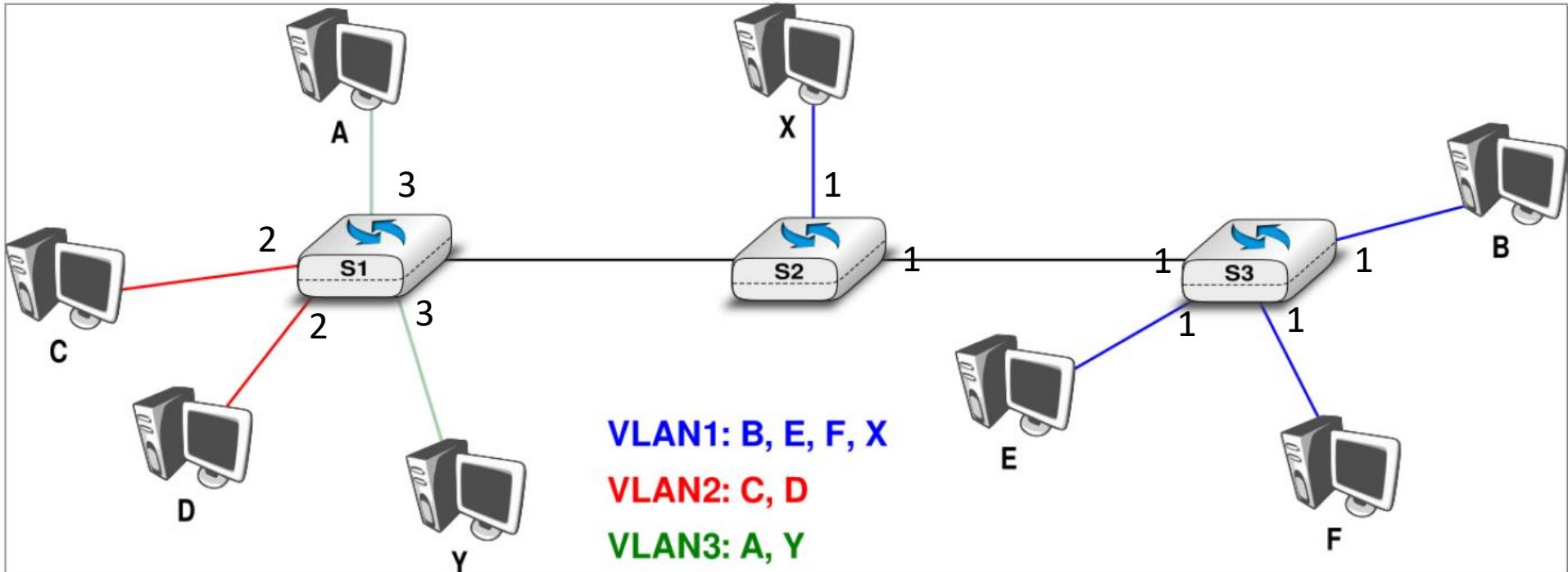
Organizzazione logica delle LAN

- ❑ In passato: connessione e disconnessione di cavi dagli switch
- ❑ Problema ovvio: ci sono cambiamenti continui in una rete
 - ❖ IT dovrebbe passare molto tempo a cambiare i cablaggi, spostare host da un'area all'altra, sostituire gli switch che hanno finito le porte con switch più grandi (e più costosi) ...
 - ❖ In alcuni casi, gli apparati di rete sono lontani o irraggiungibili
- ❑ Molto meglio gestire queste situazioni via software invece che «fisicamente»
- ❑ Soluzione: Virtual LANs (VLANs)

Virtual LAN (VLAN)

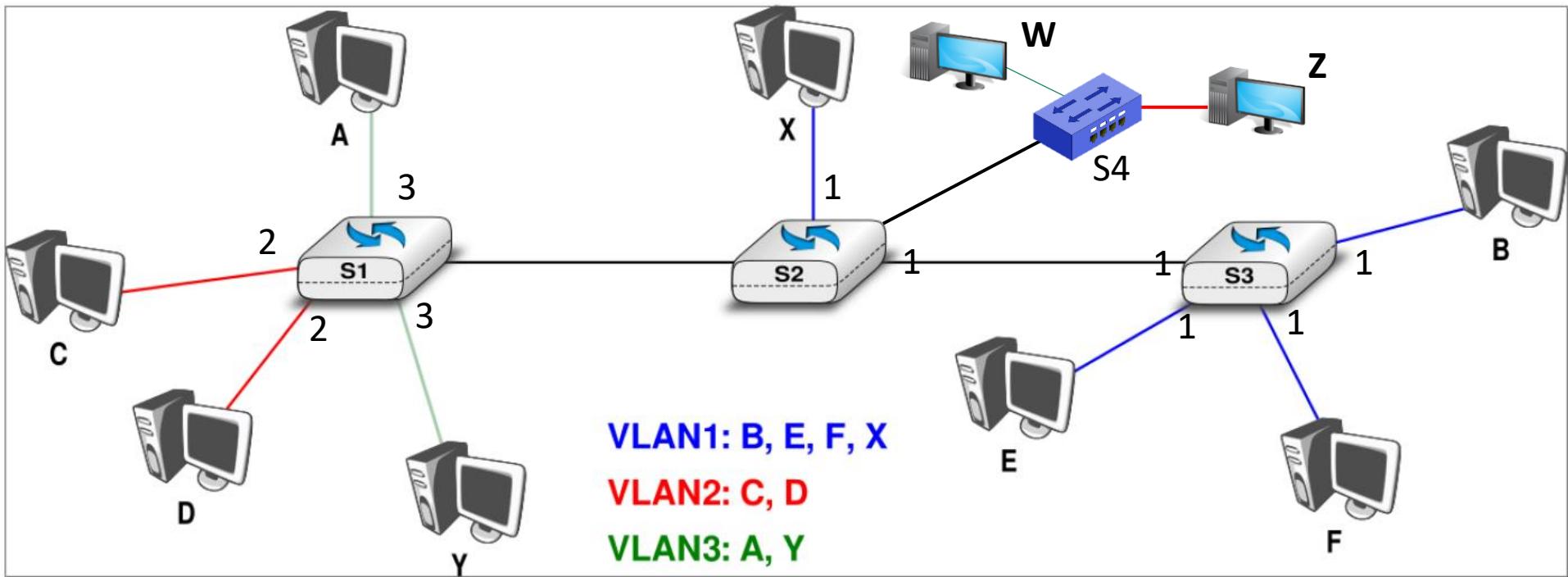
- Le VLAN non sono altro che un insieme di porte di uno o più switch di rete
- Uno switch può supportare VLAN multiple
 - ❖ (Non è detto che tutti gli switch supportano le VLAN!!)
- Gli switch eseguono un processo di backward learning indipendente per ogni VLAN
- Broadcast
 - ❖ I frame in broadcast, o i frame per cui non esiste una riga nella tabella di inoltro, vengono inviati in broadcast
solo alle porte che fanno parte della stessa VLAN del mittente

Esempio di VLAN



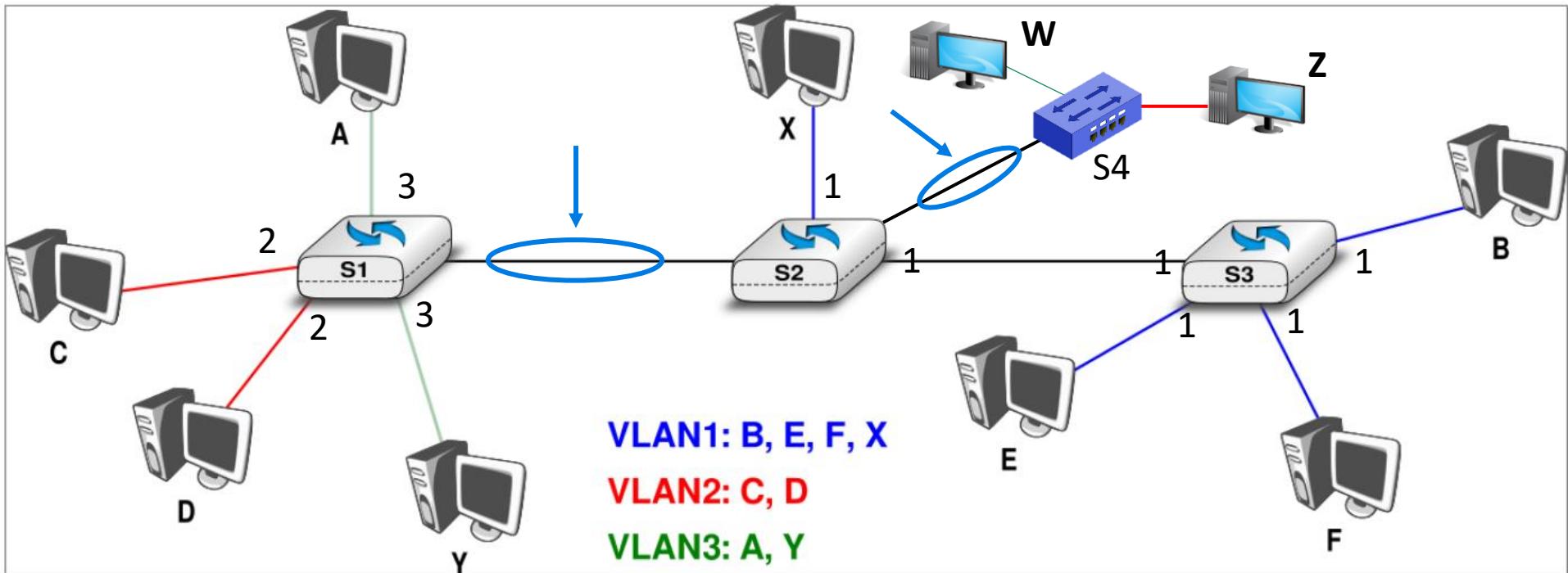
- Tre VLAN, con nodi connessi a switch diversi
- L'etichetta k su una porta indica che lo switch inoltra su quella porta il traffico della VLAN k

Esempio di VLAN



- **D:** come cambiano le etichette se il nuovo terminale Z deve essere allacciato alla **VLAN2**?
- **D:** e se W deve essere allacciato alla **VLAN3**?

Esempio di VLAN

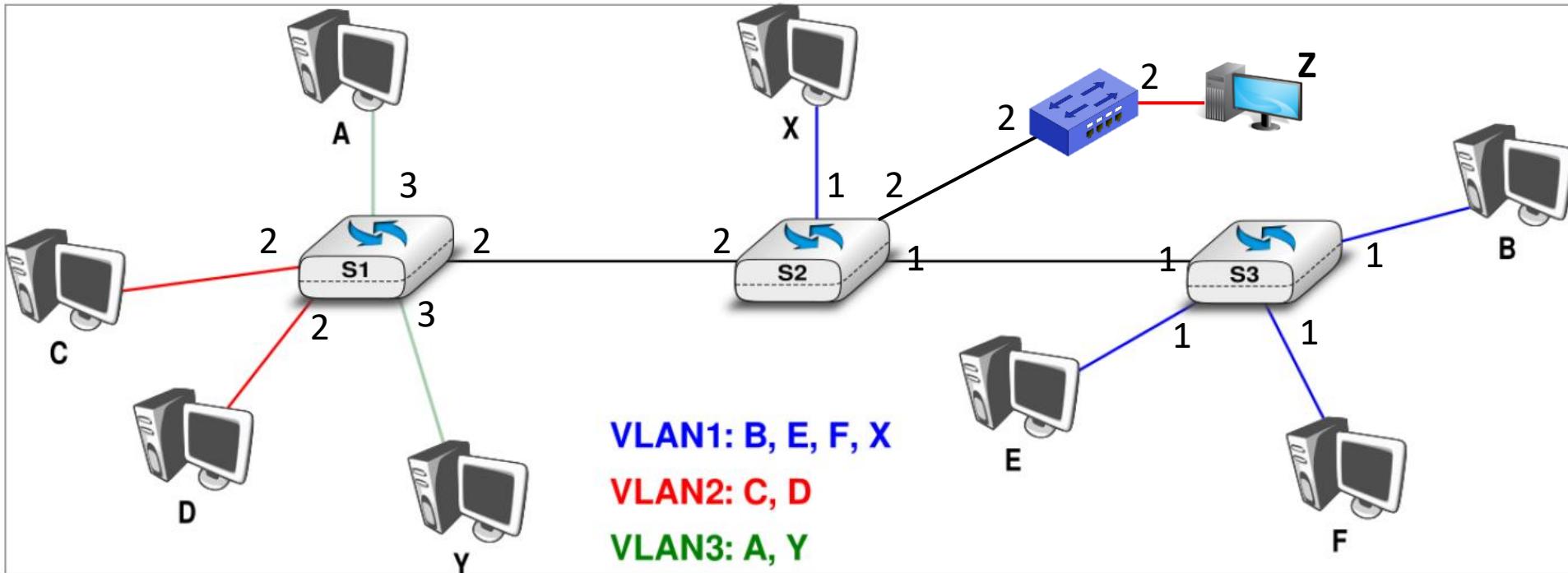


- Questi due link devono trasportare il traffico di diverse VLAN
- Configurazione in «trunk» delle porte corrispondenti
 - ❖ Trunk = Porte abilitate a inoltrare tutto il traffico VLAN, a meno che una configurazione più avanzata non preveda diversamente

VLAN con switch multipli

- Problema: lo standard Ethernet 802.3 non prevedeva VLAN
 - ❖ Finché le VLAN coinvolgono un solo switch, non è necessario cambiare lo standard
 - ❖ Se le VLAN si estendono su switch multipli, gli switch devono conoscere la VLAN per tutti i frame che gestiscono
- Serve l'etichetta che specifica il VLAN ID
- Problema: non c'erano bit disponibili a questo scopo nel formato dei frame Ethernet!
 - ❖ Gettiamo via e rifacciamo tutte le schede di rete Ethernet?
 - ❖ Usiamo dei bit del campo dati?
E se il campo dati è già alla massima lunghezza possibile?

VLAN con switch multipli: 802.1Q

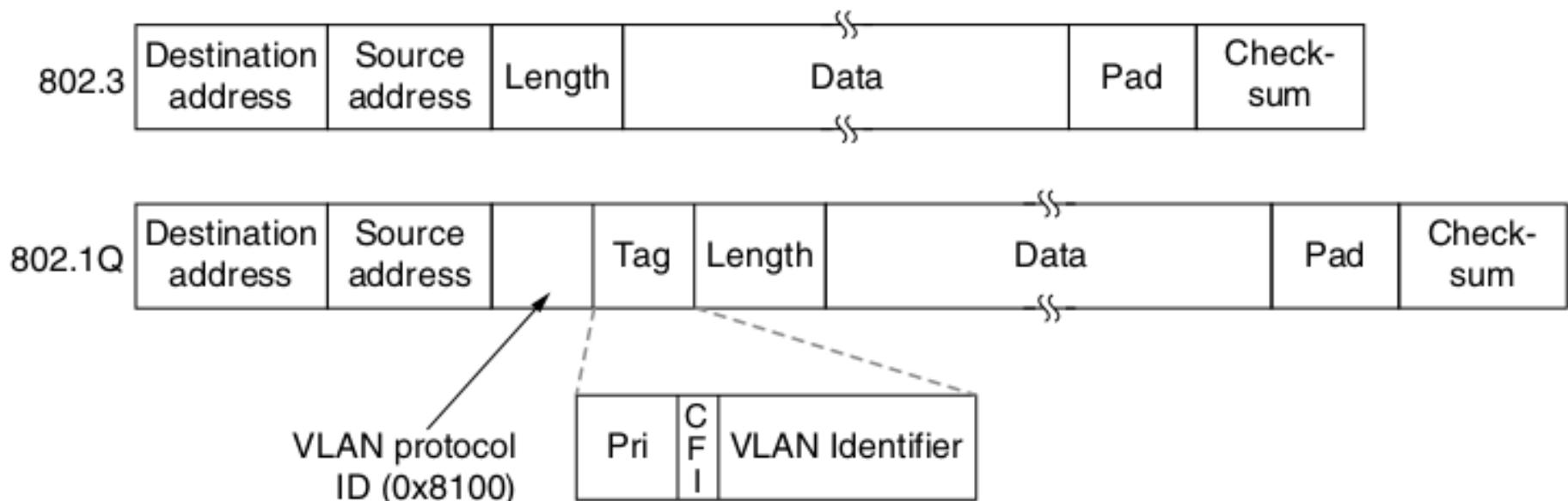


□ Osservazioni chiave:

- ❖ Solo gli switch devono conoscere le VLAN associate alle porte, gli host non hanno bisogno di essere «VLAN-aware»
- ❖ Quindi non c'è bisogno di cestinare tutte le schede di rete degli host

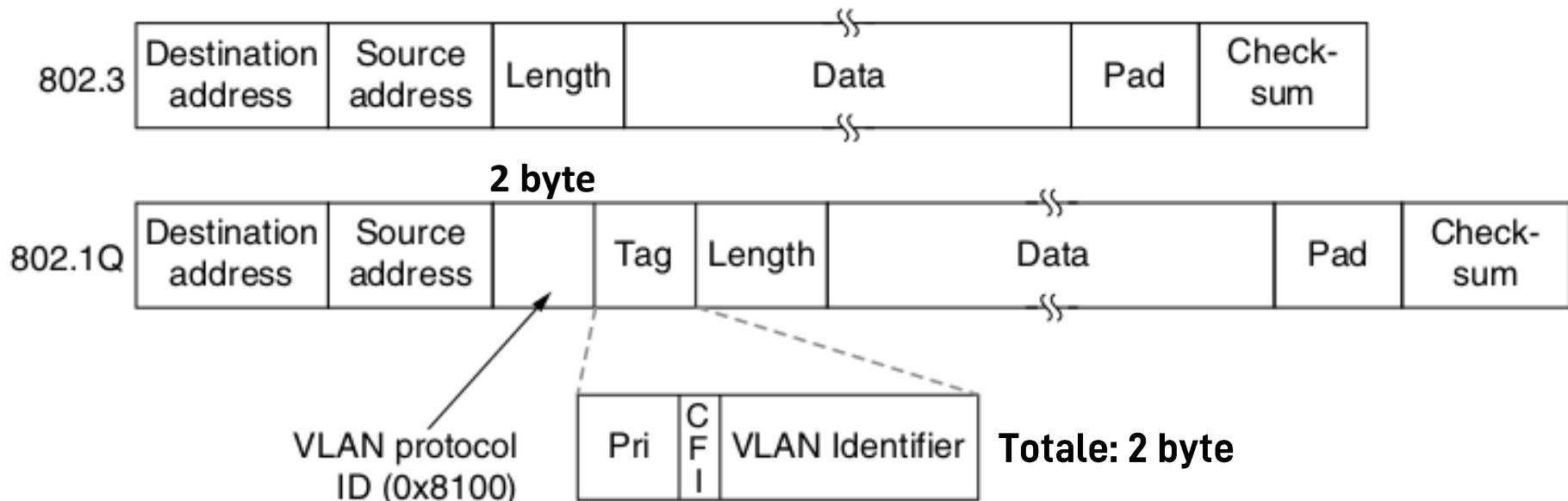
VLAN con switch multipli: 802.1Q

- A valle di questa discussione, nel 1998 il comitato IEEE 802.1Q fece l'impensabile, e cambiò lo standard Ethernet



VLAN con switch multipli: 802.1Q

- VLAN protocol ID: fissato a 0x8100
- VLAN ID: etichetta di 12 bit, 0: no VLAN, 0xFFFF: riservato
- 802.1Q inserì anche altri campi che non hanno a che fare con le VLAN:
 - ❖ Pri: priorità del frame, aiuta a implementare politiche di qualità del servizio
 - ❖ CFI (Canonical Format Indicator): inizialmente specificava se l'ordine dei byte era big endian o little endian, poi fu usato in 802.5 (token ring)



Retrocompatibilità delle VLAN

- Non c'è bisogno che gli host supportino le VLAN:
se necessario, gli switch possono manipolare i frame
per aggiungere o togliere i campi relativi alle VLAN
- Una porta può accettare frame con e senza tag,
e anche frame con tag diversi
- Un host che usa VLAN può inviare frame con ID diversi, ad es.
 - ❖ Un ID per il traffico dati
 - ❖ Un ID (eventualmente con priorità più alta) per traffico VoIP
 - ❖ ...

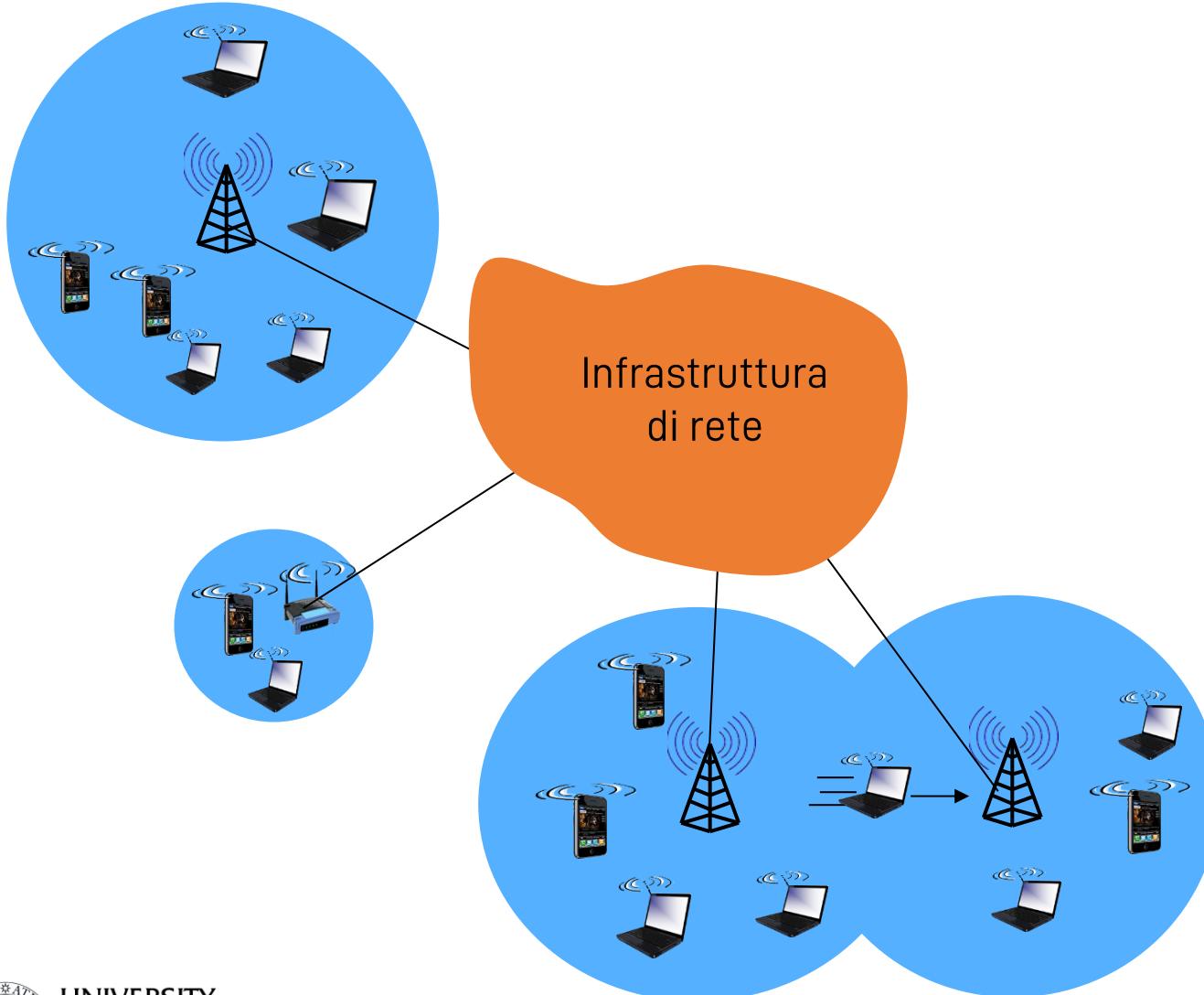
Retrocompatibilità delle VLAN

- Se un frame 802.1Q (con campi VLAN) arriva ad uno switch che non supporta le VLAN
 - ❖ Nel caso peggiore, lo switch non riconosce il frame e lo scarta
 - ❖ Caso migliore: lo switch non supporta le VLAN ma conosce lo standard (tipico per switch recenti)
 - Lo switch inoltra comunque il frame secondo la propria tabella di inoltro, ignorando i campi VLAN

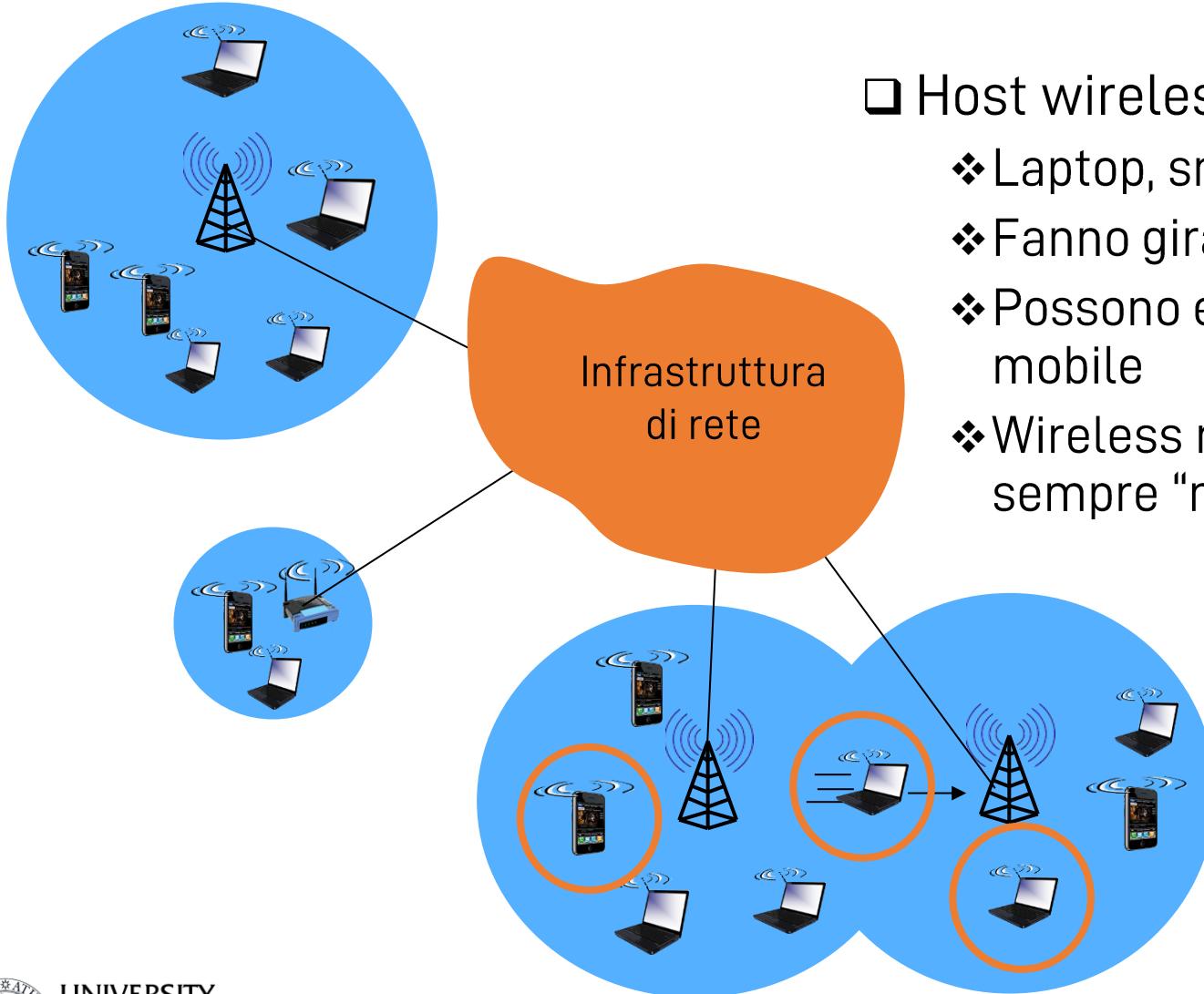
Sommario

- ❑ Livello data link
- ❑ Rilevamento e correzione di errori, CRC
- ❑ Protocolli e tecnologie per l'accesso multiplo al canale
 - ❖ TDMA, FDMA, CDMA
 - ❖ Slotted ALOHA, ALOHA
 - ❖ CSMA, CSMA/CD, CSMA/CA
 - ❖ Protocolli "a turni"
 - ❖ IEEE 802 ed Ethernet
- ❑ Ethernet switching
 - ❖ Backward learning
 - ❖ Spanning tree per switch
 - ❖ VLAN
- ❑ IEEE 802.11 WiFi
 - ❖ Terminologia e architettura
 - ❖ Protocollo MAC
 - ❖ Frame e indirizzi 802.11

Elementi di una rete wireless



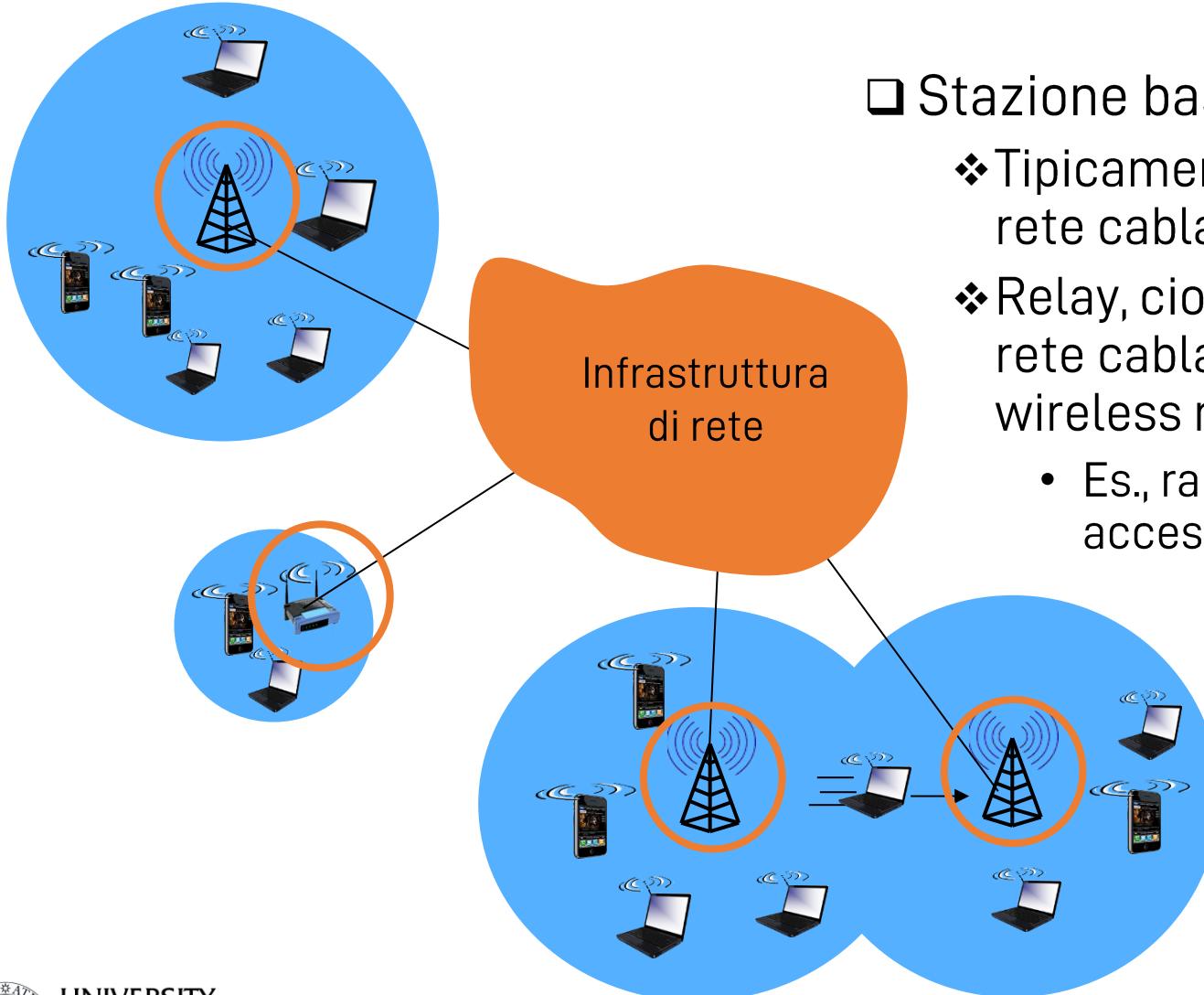
Elementi di una rete wireless



□ Host wireless

- ❖ Laptop, smartphone
- ❖ Fanno girare applicazioni
- ❖ Possono essere statici o mobile
- ❖ Wireless non significa sempre "mobile"

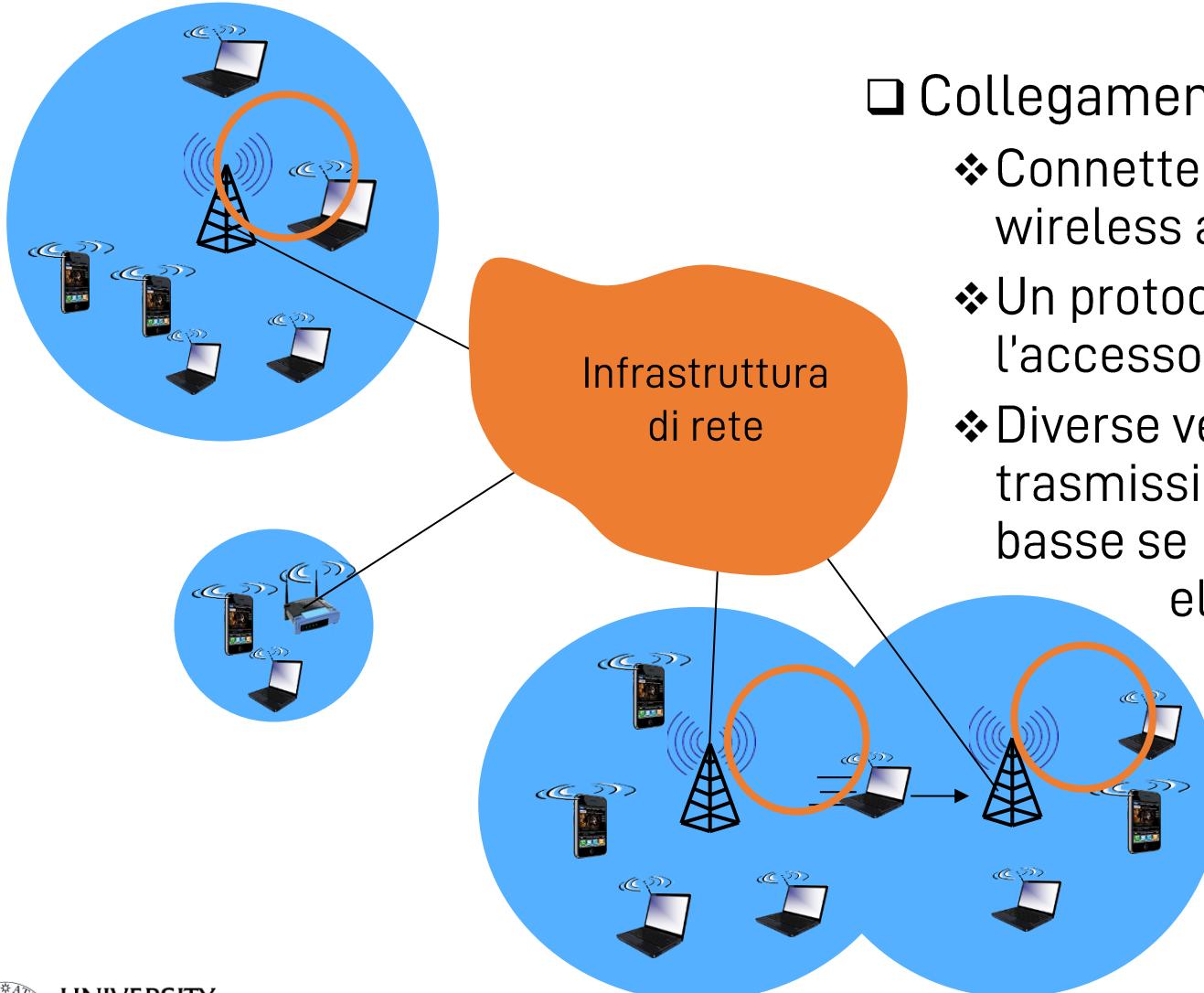
Elementi di una rete wireless



□ Stazione base

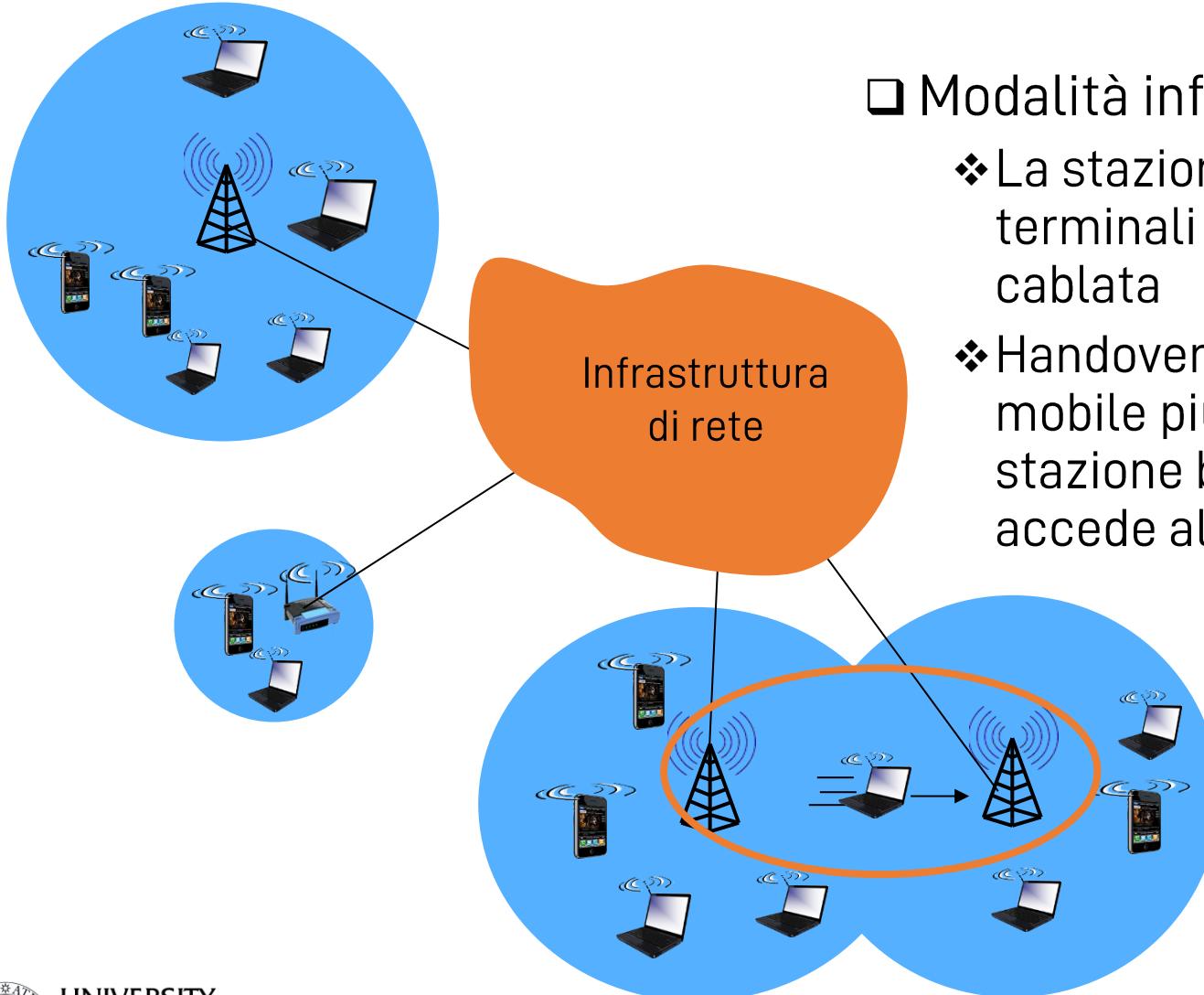
- ❖ Tipicamente connessa a una rete cablata
- ❖ Relay, cioè fa da ponte tra la rete cablata e gli host wireless nei pressi
 - Es., radiobase cellulari, access point 802.11

Elementi di una rete wireless



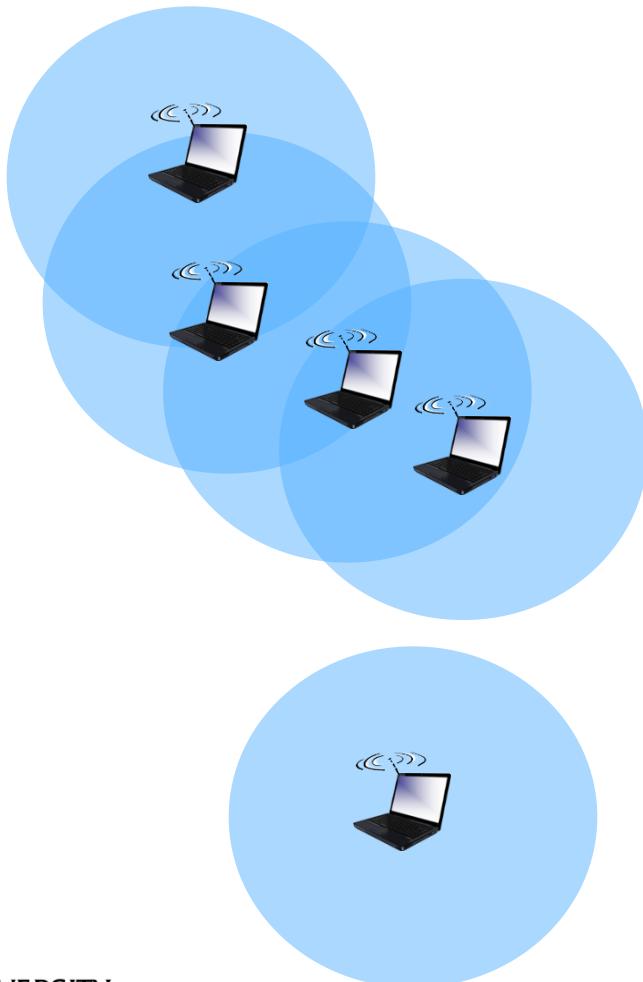
- Collegamento wireless
 - ❖ Connnette i terminali wireless alle stazioni base
 - ❖ Un protocollo MAC coordina l'accesso al link
 - ❖ Diverse velocità di trasmissione, spesso più basse se le distanze sono elevate

Elementi di una rete wireless



- Modalità infrastrutturata
 - ❖ La stazione base connette i terminali wireless alla rete cablata
 - ❖ Handover: un terminale mobile può cambiare la stazione base tramite cui accede alla rete cablata

Elementi di una rete wireless



□ Modalità ad hoc

- ❖ Non ci sono stazioni base
- ❖ I nodi possono trasmettere solo agli altri nodi entro il loro raggio di copertura
- ❖ I nodi si organizzano tra loro in una rete
 - Scoperta automatica dei vicini
 - Determinazione dei percorsi multi-salto

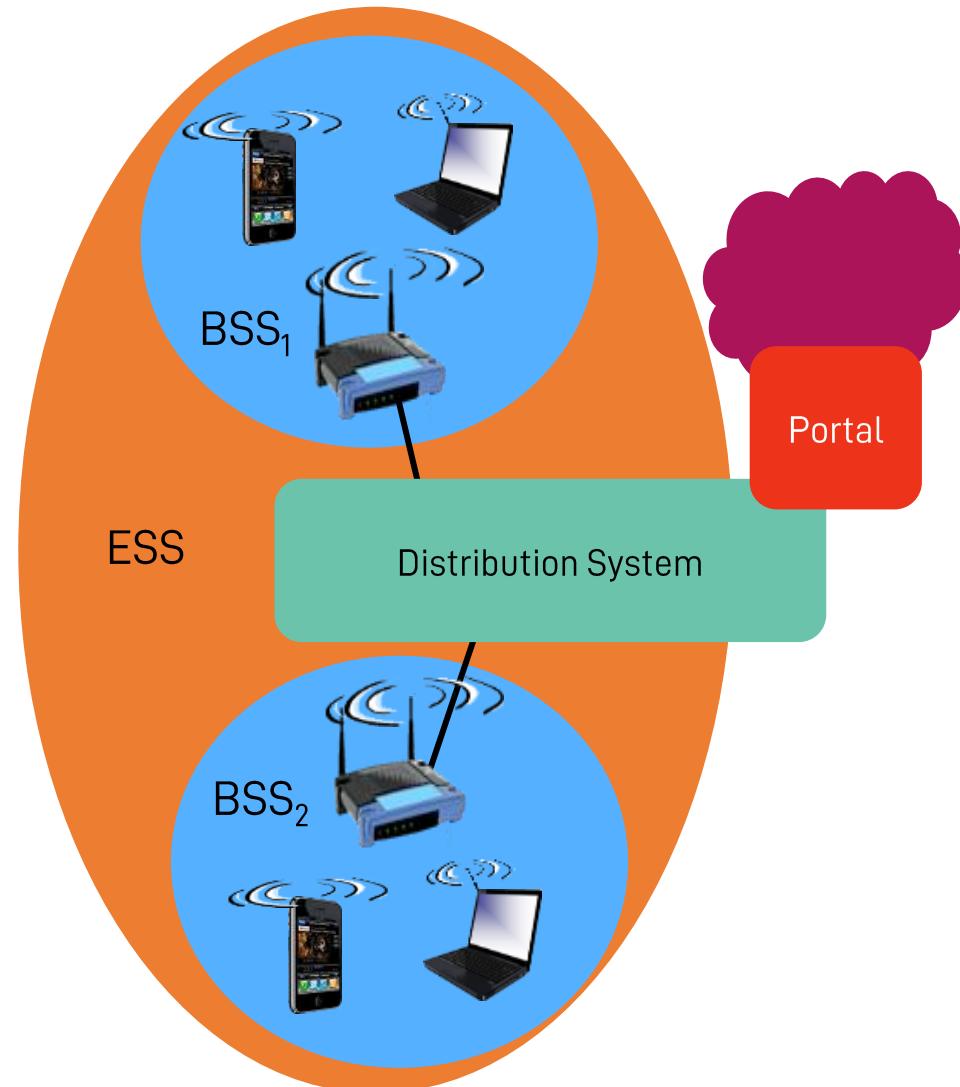
Tassonomia di una rete wireless

	Non multi-salto	Multi-salto
Presenza di infrastruttura	L'host si connette alla stazione base (WiFi, WiMAX, cellulare) che lo connette a Internet	L'host potrebbe dover inviare i propri messaggi attraverso altri nodi wireless prima di giungere a un nodo connesso a Internet: “mesh network”
Senza infrastruttura	Nessuna stazione base, nessuna connessione a Internet (es., Bluetooth)	Nessuna stazione base, nessuna connessione a Internet, può essere necessario rimbalzare il segnale a diversi nodi prima di raggiungere la destinazione

Wireless LAN IEEE 802.11

- 802.11b
 - ❖ 2.4-5.8 GHz (spettro libero da licenze, ISM)
 - ❖ Fino ad 11 Mbit/s
 - ❖ Le trasmissioni avvengono come in un CDMA, ma tutti i nodi usano lo stesso codice (dà comunque un po' di robustezza contro l'interferenza)
- 802.11a
 - ❖ 5-6 GHz range
 - ❖ Fino a 54 Mb/s
- 802.11g
 - ❖ 2.4-5.8 GHz
 - ❖ Fino a 54 Mb/s
- 802.11n: antenne multiple
 - ❖ 2.4-5.8 GHz range
 - ❖ Fino a 600 Mbit/s per 3 flussi radio contemporanei (150 Mbit/s per stazione)
- 802.11ac: canali con più banda e più flussi radio
 - ❖ Fino a 6.9 Gbit/s per 4 flussi radio (fino a 1.1 Gbit/s per tutte le stazioni servite da un AP)
- 802.11ax (WiFi 6)
 - ❖ Fino a 11 Gbit/s per 8 flussi radio (1375 Mbit/s per stazione)

Architettura di riferimento per una WLAN

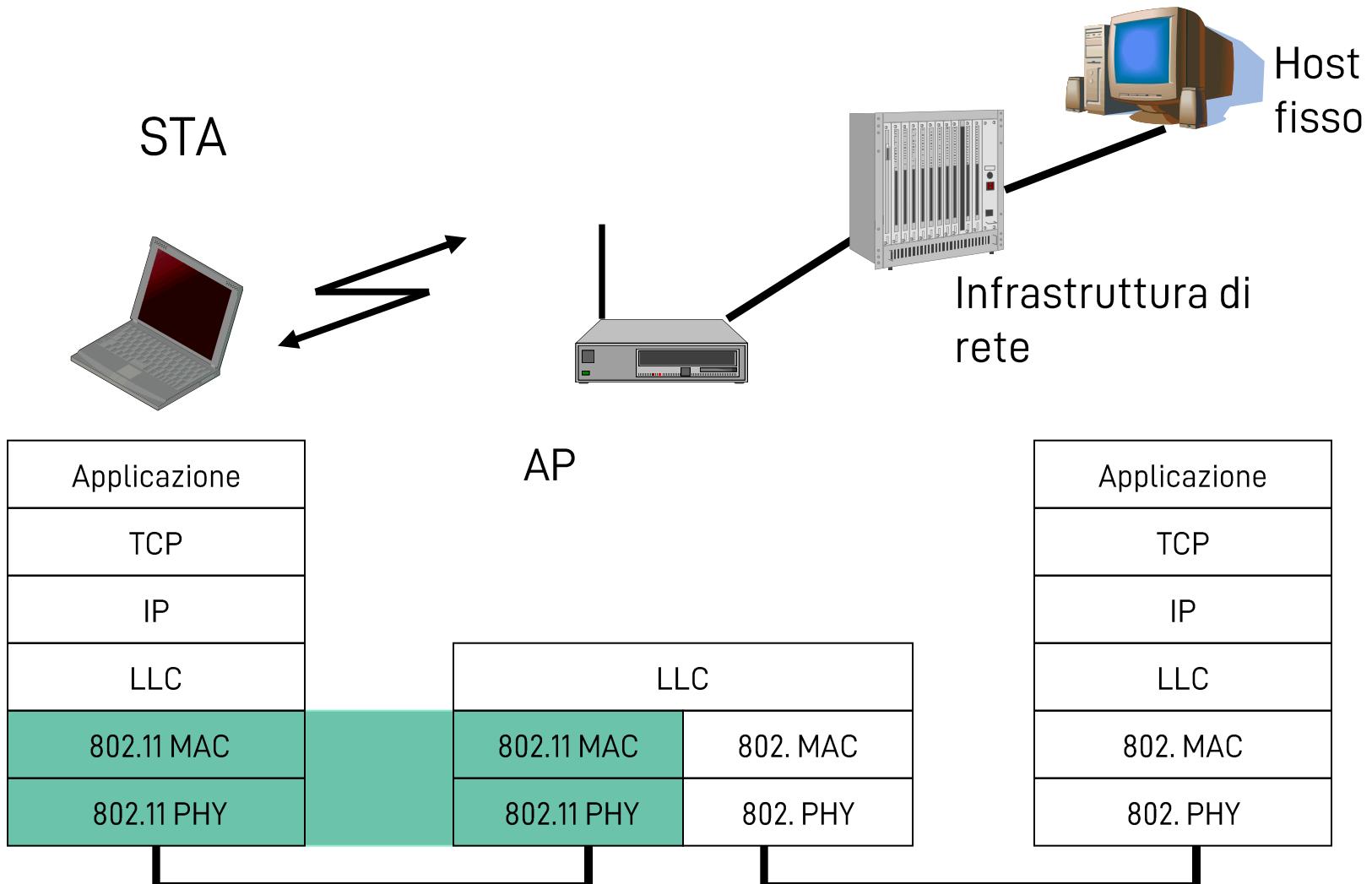


- Stazione wireless (STA)
 - ❖ O terminale / host / nodo di rete
- Basic Service Set (BSS)
 - ❖ Gruppo di STA che usano lo stesso canale radio
- Access Point (AP)
 - ❖ Stazione integrata nella LAN e connessa al sistema di distribuzione (di connettività)
- Sistema di distribuzione
 - ❖ Fornitore di connettività (verso altri BSS, verso Internet ...)
- Extended Service Set (ESS): unisce più BSS in un'unica rete logica
- Portale
 - ❖ Ponte verso altre reti

Architettura di riferimento

- Basic Service Set (BSS)
 - ❖ Insieme di STA che usano lo stesso protocollo MAC e competono per l'accesso allo stesso canale radio condiviso
 - ❖ Si può immaginare come una cella in una rete cellulare
- Un BSS può essere isolato o connesso a un sistema di distribuzione attraverso un AP
- Gli AP funzionano, di fatto, come switch
- I protocolli MAC possono essere completamente distribuiti o controllati centralmente dall'AP
- Un ESS (più BSSs interconnessi da un sistema di distribuzione) ESS appare come una sola LAN logica alle STA

Architettura dei protocoli



802.11: canali e associazione

- 802.11b: spettro di frequenze da 2,4 GHz a 2,485 GHz suddiviso in 11 canali (fino a 14 in certi stati)
- L'amministratore dell'AP sceglie la frequenza usata dall'AP
 - ❖ Ci può essere interferenza se più AP vicini scelgono lo stesso canale (anche se impostate la "selezione automatica")
- Host: si deve "associare" con un AP
 - ❖ Ascolta su tutti i canali disponibili alla ricerca di frame speciali chiamati "beacon", che contengono il nome di rete (service set ID, SSID) e l'indirizzo MAC dell'AP
 - ❖ Scelgono a quale AP associarsi
 - ❖ Potrebbero doversi autenticare
 - ❖ Di solito usano DHCP per ottenere un indirizzo IP della stessa sottorete di cui fa parte l'AP

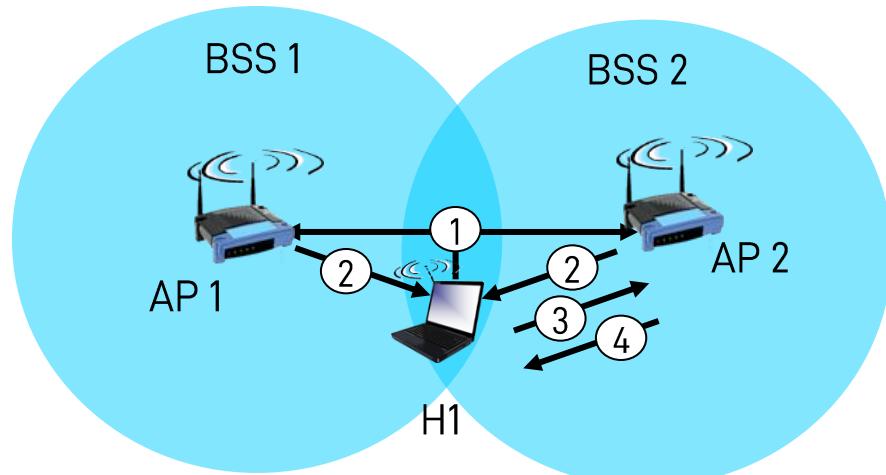
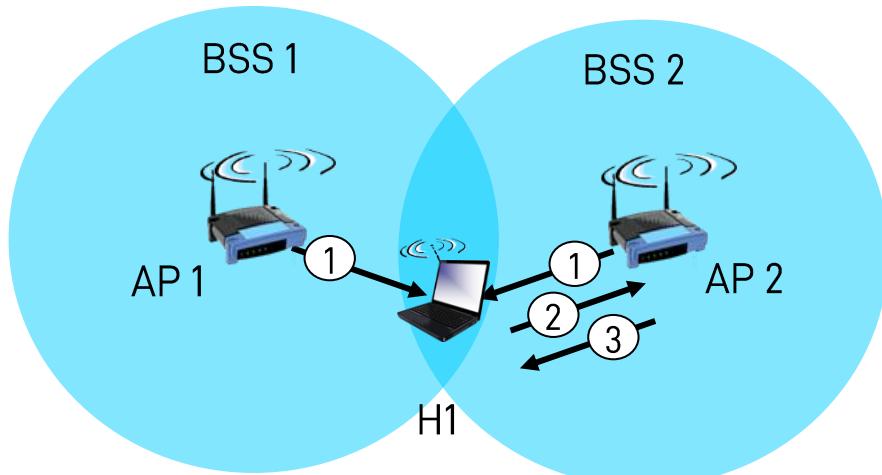
802.11: scansione passiva e attiva

□ Scansione passiva:

- ❖ L'AP invia i beacon
- ❖ H1 invia una richiesta di associazione all'AP scelto
- ❖ L'AP risponde con una conferma alla richiesta di H1

□ Scansione attiva:

- ❖ H1 invia a tutti i vicini un frame di "probe request"
- ❖ Gli AP rispondono con un "probe response"
- ❖ Seguono richiesta e conferma di associazione



Caratteristiche dei collegamenti wireless

- Molte differenze chiave rispetto ai collegamenti cablati
 - ❖ Meno potenza del segnale ricevuto: i segnali radio si attenuano fortemente mentre si propagano
 - ❖ Interferenza da altre fonti radio: le frequenze degli standard WiFi (esempio: 2,4 GHz) sono usate anche da altri dispositivi (telefoni, forni a microonde), anche altri oggetti (es., i motori) creano disturbi
 - ❖ Propagazione "multipath": il segnale radio si riflette su oggetti e superfici, creando copie che raggiungono al destinatario con ritardi leggermente diversi
- Rende la comunicazione wireless più difficile dal punto di vista fisico, anche su un semplice collegamento punto-punto

Collision Detection: impossibile

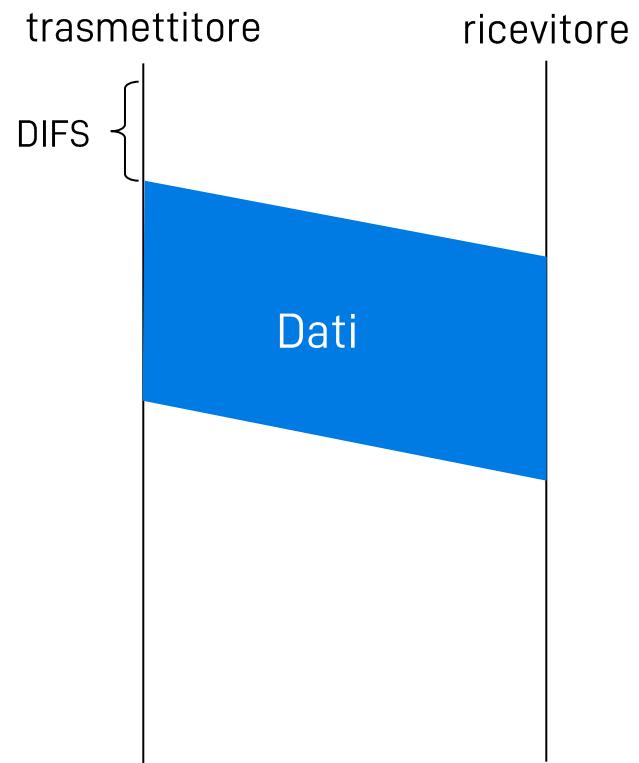
- Per capire come si propaga un'onda radio, immaginate che l'antenna sia un punto, e che da lì si estenda una sfera di raggio crescente
 - ❖ La potenza del segnale, inizialmente concentrata sull'antenna, si deve distribuire su sfere sempre più grandi (la cui superficie cresce come r^2)
- L'attenuazione segue quindi una legge quadratica:
 - ❖ $P_{rx} = k P_{tx} / d^2$
 - ❖ d è la distanza (il raggio della sfera)
 - ❖ k è una costante che conteggia altri fattori di attenuazione, di solito è < 1
- Un'antenna non può trasmettere e ricevere contemporaneamente
- Autointerferenza: pensiamo ad un AP con 2 antenne
 - ❖ Un'antenna riceve contemporaneamente dall'altra antenna (a 10 cm) e da una STA disposta a 10 m dall'AP
 - ❖ Rapporto tra le potenze ricevute: $P_{rx}(10\text{ cm}) / P_{rx}(10\text{ m}) = 10\ 000$

MAC 802.11

- Basato su CSMA con Collision Avoidance “CA”
 - ❖ Le STA che hanno dati da trasmettere si contendono l'accesso al canale radio
 - ❖ Una STA ripete la contesa ogni volta che deve trasmettere dati
 - ❖ Eccezioni: in alcune versioni più avanzate di 802.11 (es., 802.11n/ac) si può concedere il canale ad una STA per un periodo di tempo più lungo di un frame
 - Questo periodo si chiama TXOP
 - Permette al trasmettitore di inviare più frame senza contendere ogni volta

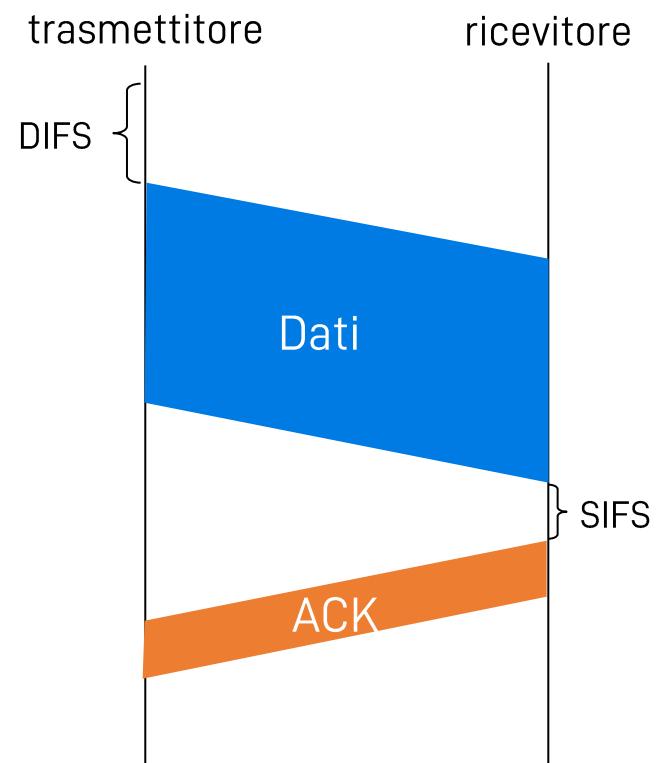
MAC 802.11: Trasmettitore CSMA

1. Se il canale rimane libero per un tempo chiamato Distributed Inter-Frame Space (DIFS)
 - ❖ Si trasmette l'intero frame
 - ❖ Altrimenti si entra in backoff (passo 2)
 2. Se il canale è occupato
 - ❖ Si sceglie un tempo di backoff casuale
 - ❖ Se il countdown arriva a 0 mentre il canale è libero
 - Si trasmette alla fine del timer
- Se non si riceve nessun ACK
 - ❖ Si aumenta il valore massimo del tempo di backoff
 - ❖ Si sceglie un nuovo tempo di backoff
 - ❖ Si ripete il passo 2



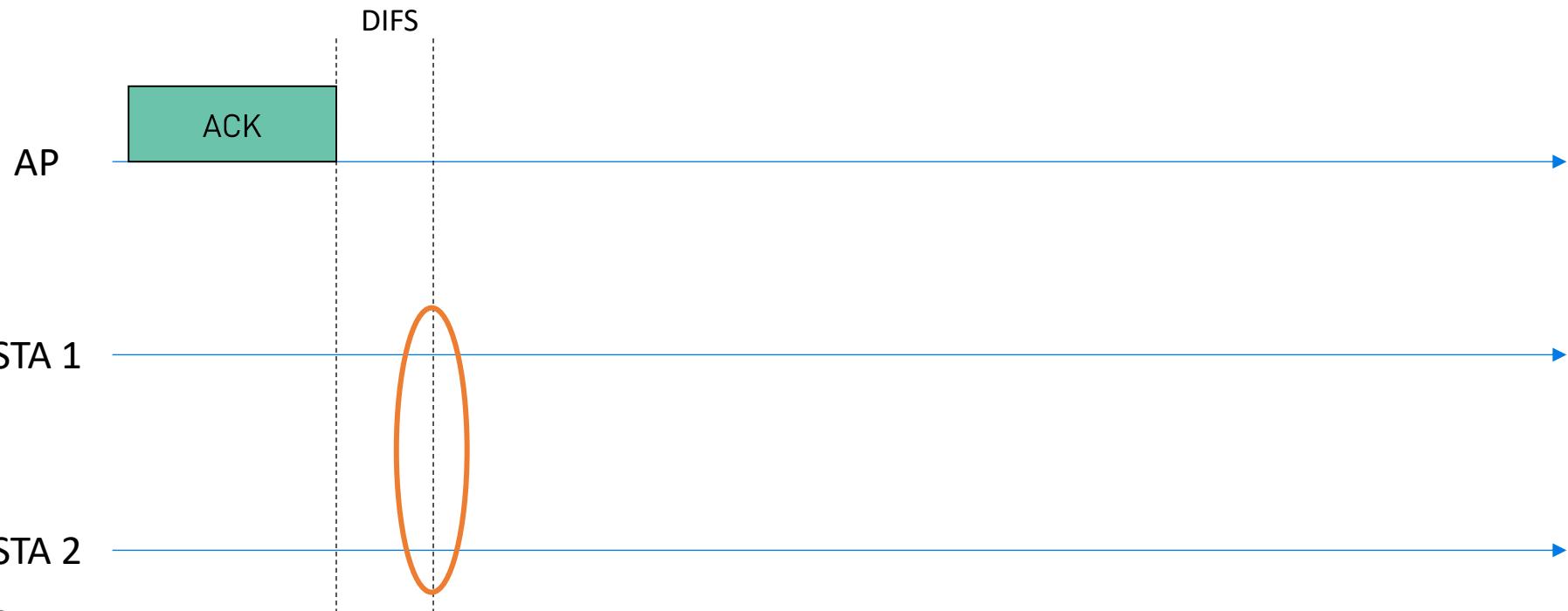
MAC 802.11: Ricevitore CSMA

- Se il frame viene ricevuto correttamente
 - ❖ Si invia un ACK dopo un intervallo di tempo chiamato Short Inter-Frame Space (SIFS)
 - ❖ SIFS < DIFS (**D**: perché?)
- Gli ACK sono necessari
 - ❖ Collisioni dopo il backoff
 - ❖ Errori di trasmissione
 - ❖ Problema del terminale nascosto



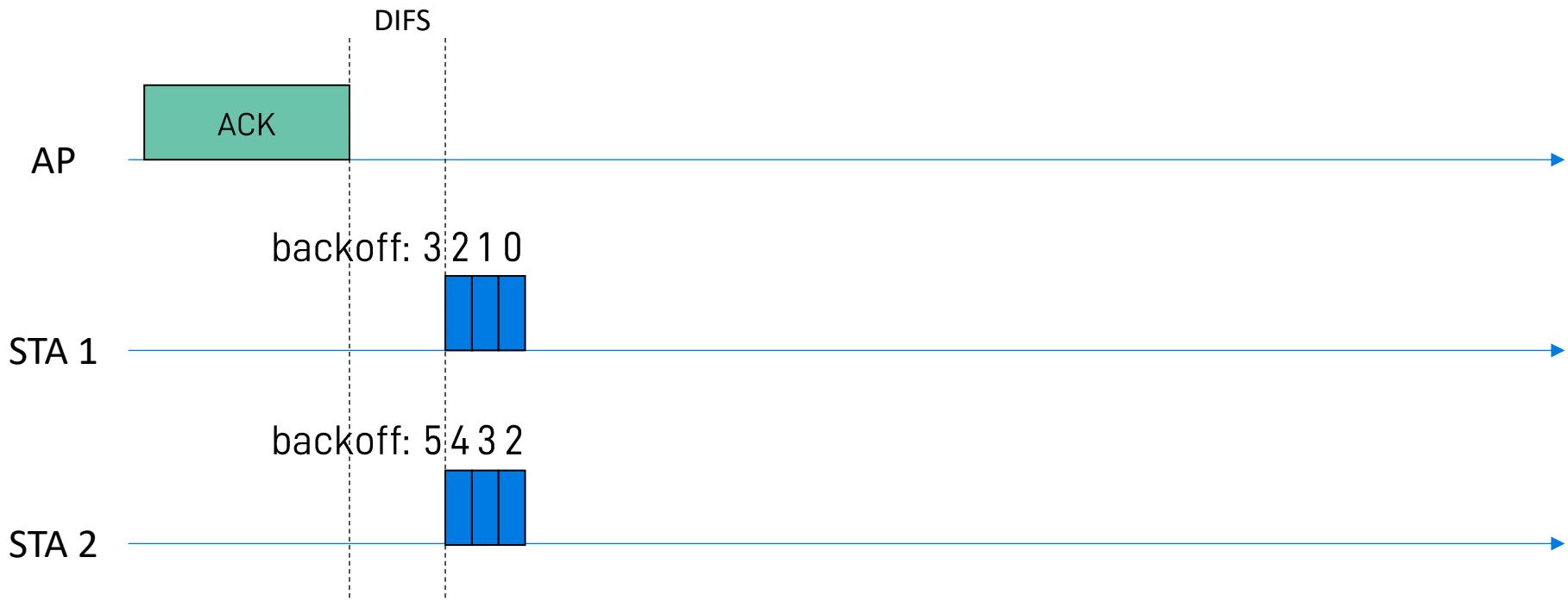
MAC 802.11: CSMA/CA completo

- STA 1 e STA 2 devono trasmettere un frame all'AP
- Dopo che il canale è percepito libero per un DIFS, estraggono a caso un intero (backoff) tra 0 e CW – 1 (CW = Contention Window)
 - ❖ Es.: STA 1 estrae 3, mentre STA 2 estrae 5



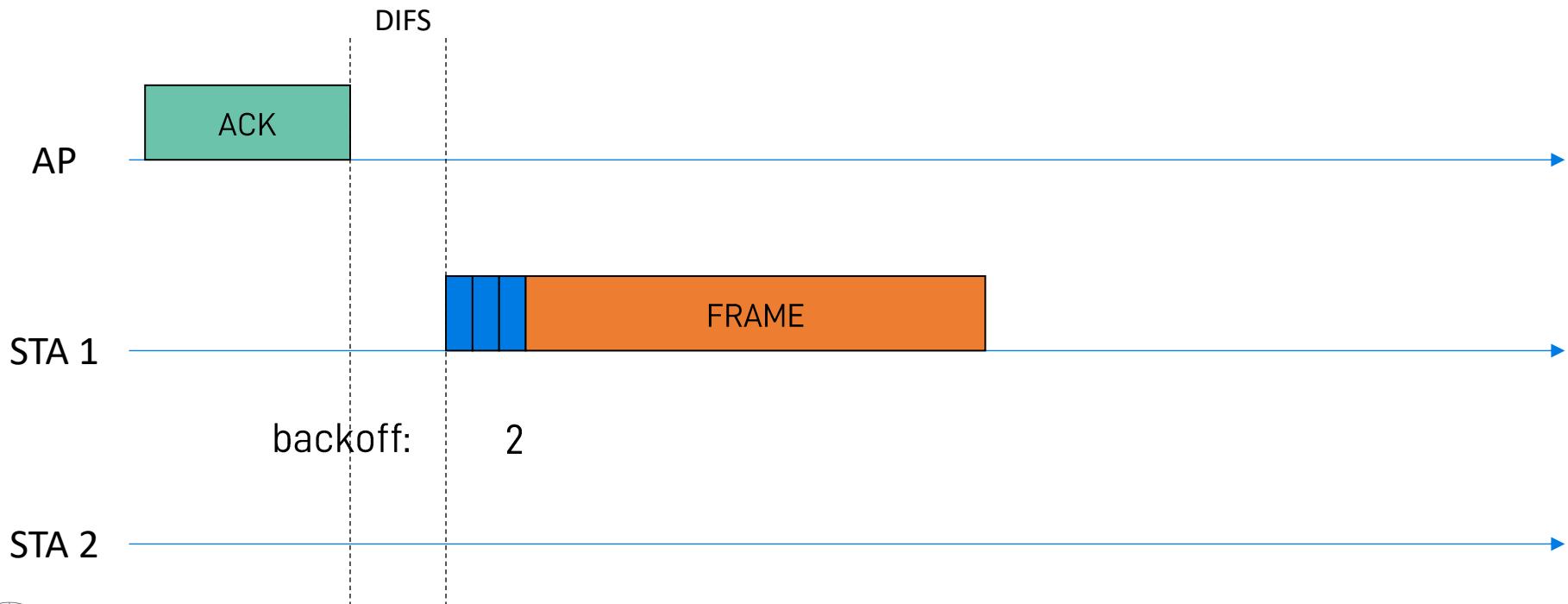
MAC 802.11: CSMA/CA completo

- Le STA iniziano il conto alla rovescia
- STA 1 arriva a 0 per prima → inizia a trasmettere



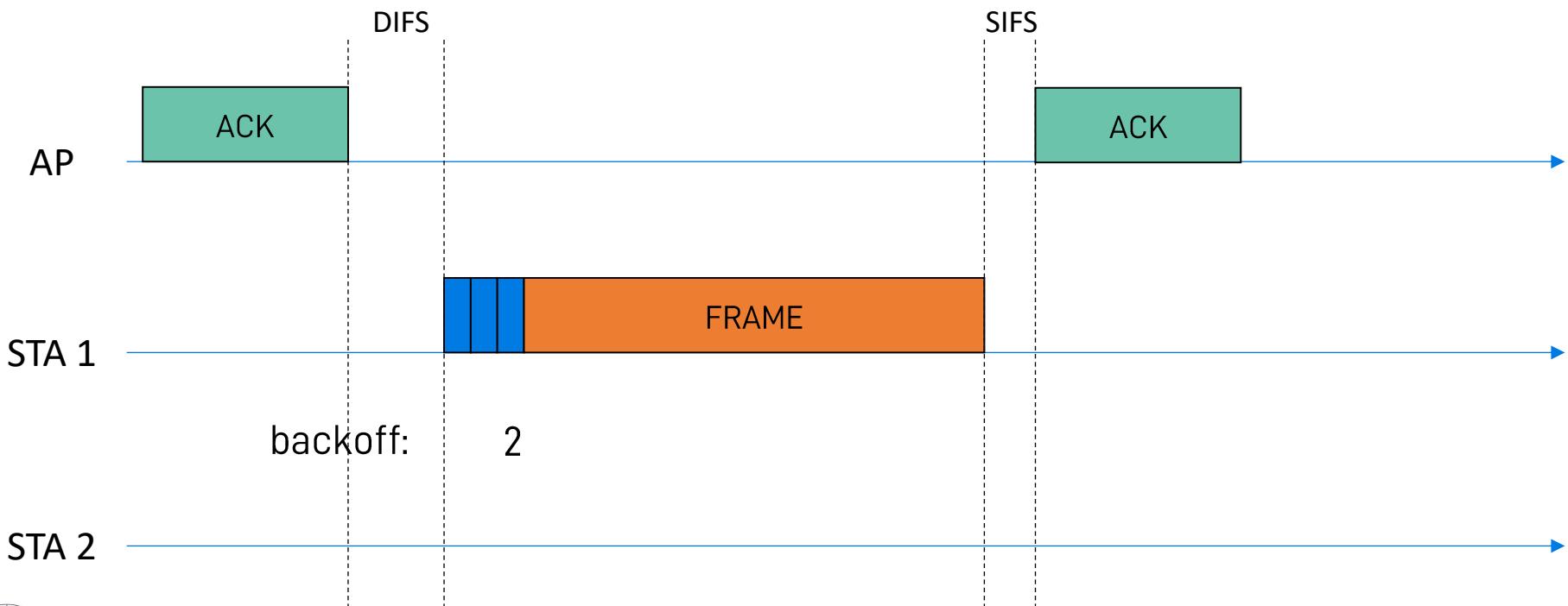
MAC 802.11: CSMA/CA completo

- Quando STA 1 trasmette, STA 2 è ancora in backoff
- Percepisce che il canale è ora occupato
 - ❖ Congela il conto alla rovescia e aspetta
 - ❖ Quanto aspetta? Un campo dell'header del frame chiamato NAV specifica il tempo per cui il canale rimarrà occupato



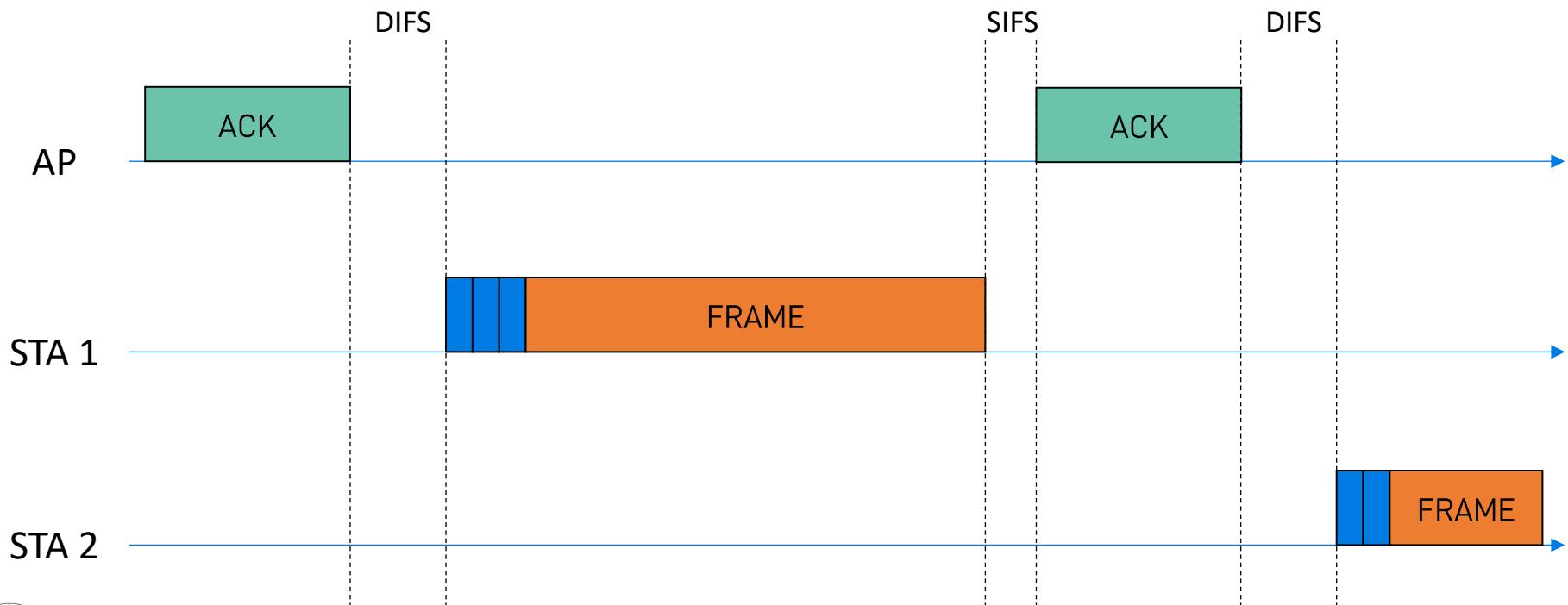
MAC 802.11: CSMA/CA completo

- Quando l'AP riceve correttamente il frame, invia un ACK dopo un SIFS



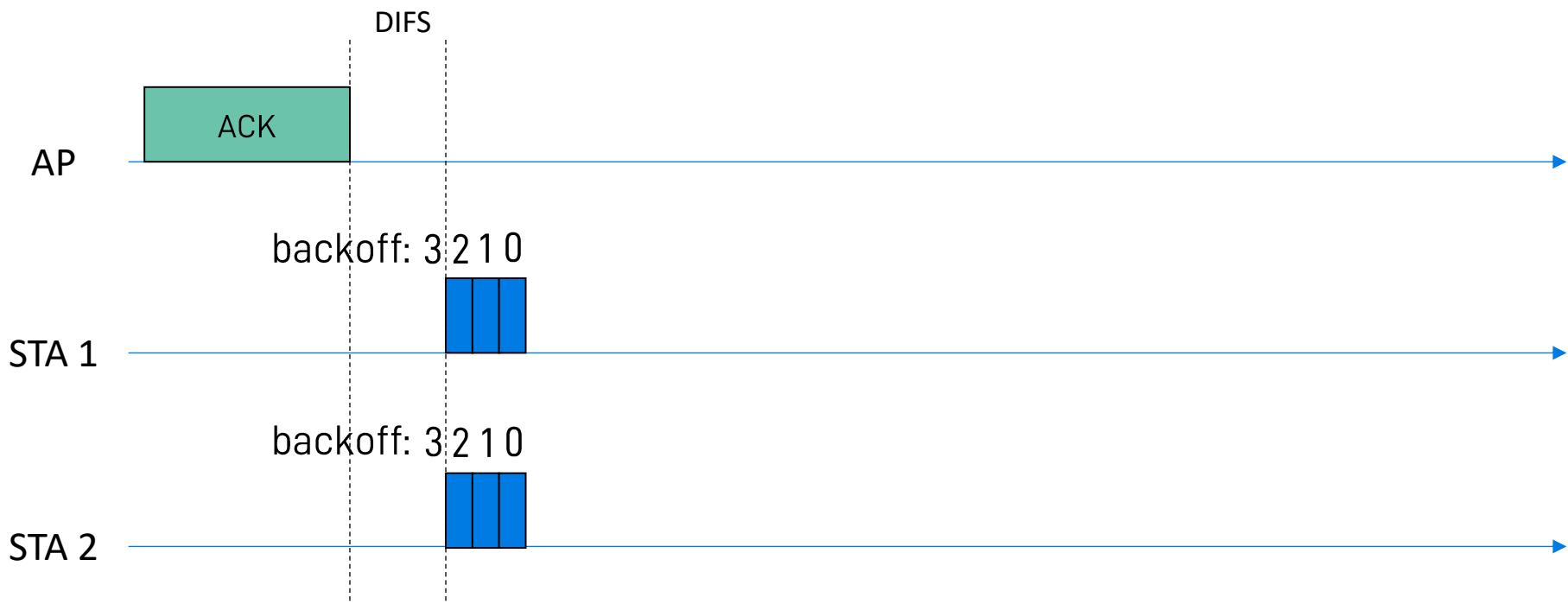
MAC 802.11: CSMA/CA completo

- Un DIFS dopo l'ACK, STA 2 riprende il conto alla rovescia da dove l'aveva lasciato e poi trasmette



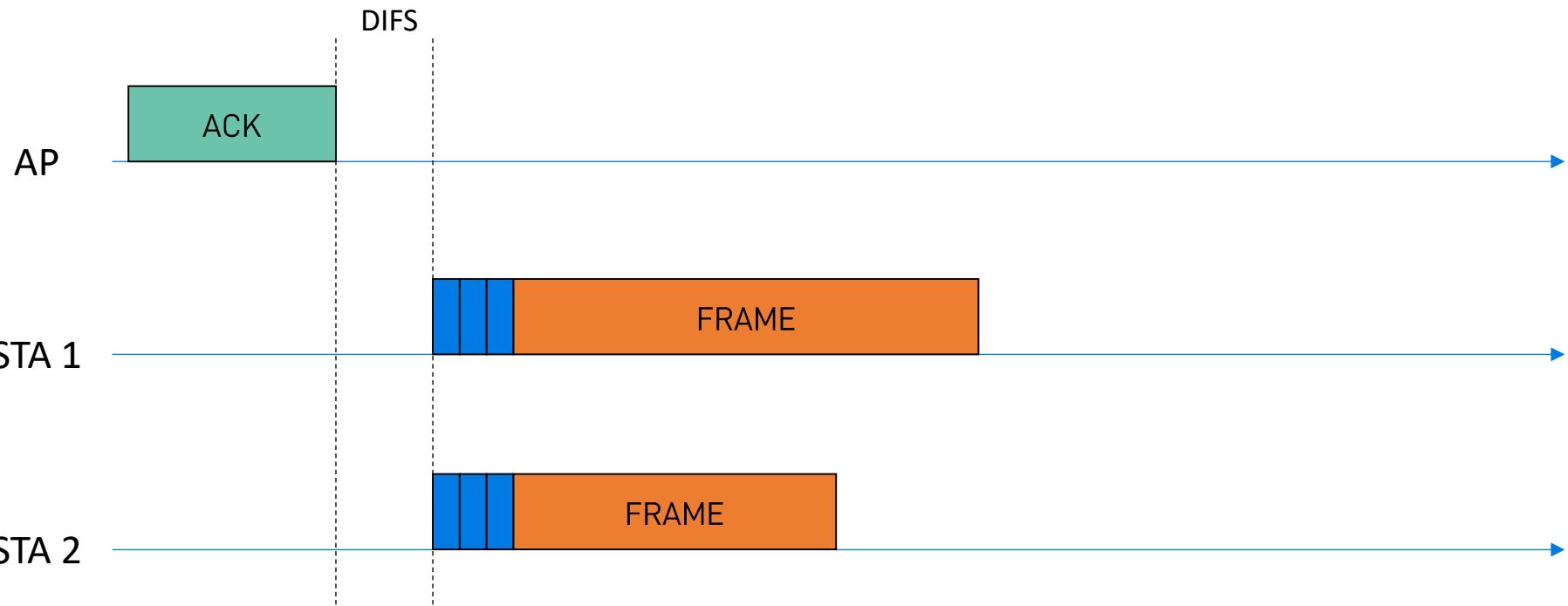
MAC 802.11: CSMA/CA completo

- Assumiamo che STA 1 e STA 2 scelgano lo stesso backoff
- STA 1 and STA 2 arrivano a 0 insieme → entrambi trasmettono



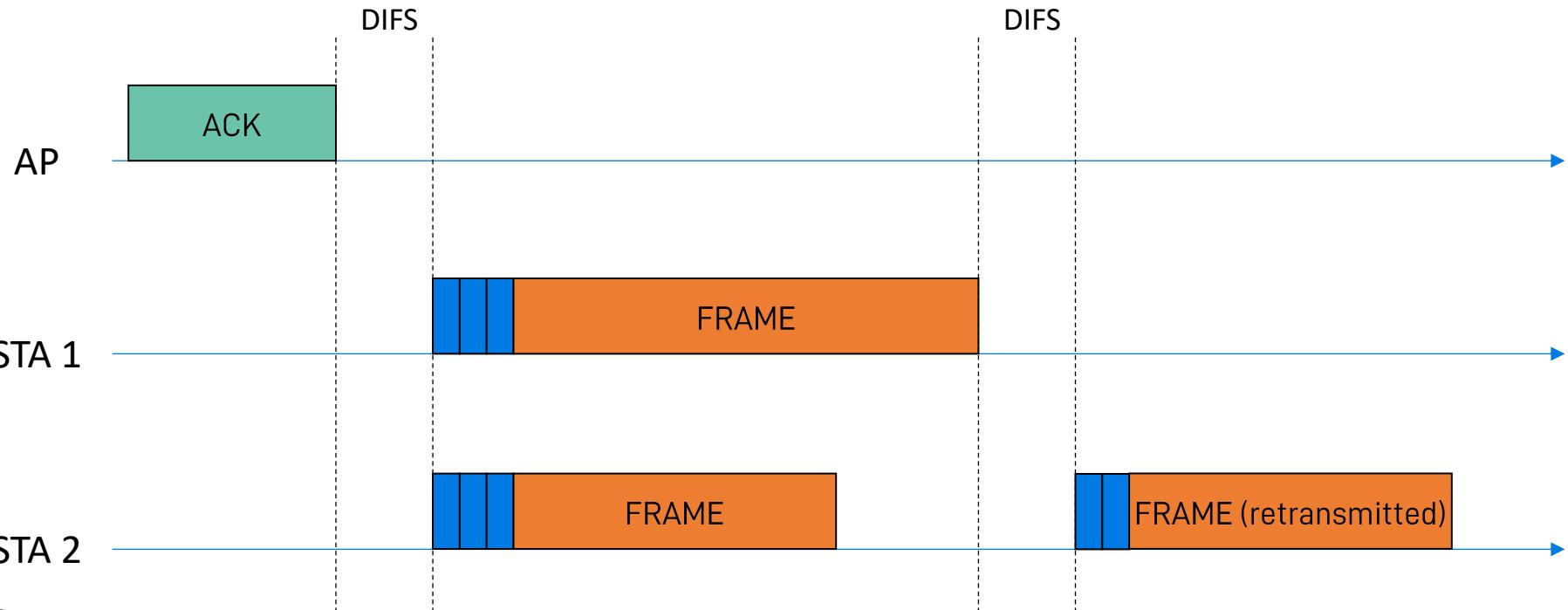
MAC 802.11: CSMA/CA completo

- ❑ No collision detection: si inviano interamente entrambi i frame
- ❑ L'AP non riesce a ricevere nessuno dei due frame
 - ❖ Quindi non invia ACK



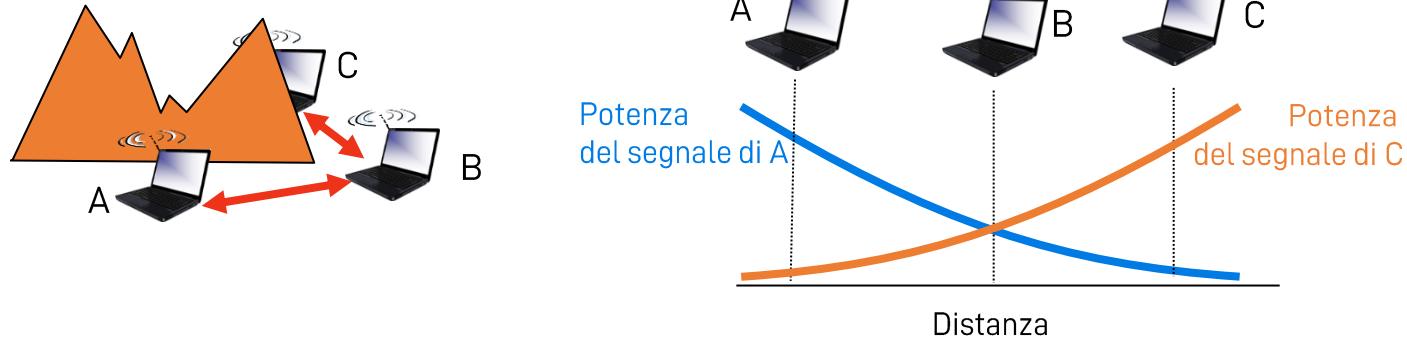
MAC 802.11: CSMA/CA completo

- A questo punto, dopo un DIFS, STA 1 e STA 2
 - ❖ Raddoppiano il valore della CW ($CW = CW * 2$)
 - ❖ Estraggono un backoff casuale tra 0 e $CW - 1$
 - ❖ Ripetono la procedura di accesso (qui, ora vince STA 2)



Problema del terminale nascosto

- Terminale nascosto: A e C sentono B, ma non si sentono a vicenda a causa di ostacoli interposti, o pesante attenuazione
 - ❖ Può causare collisioni sistematiche

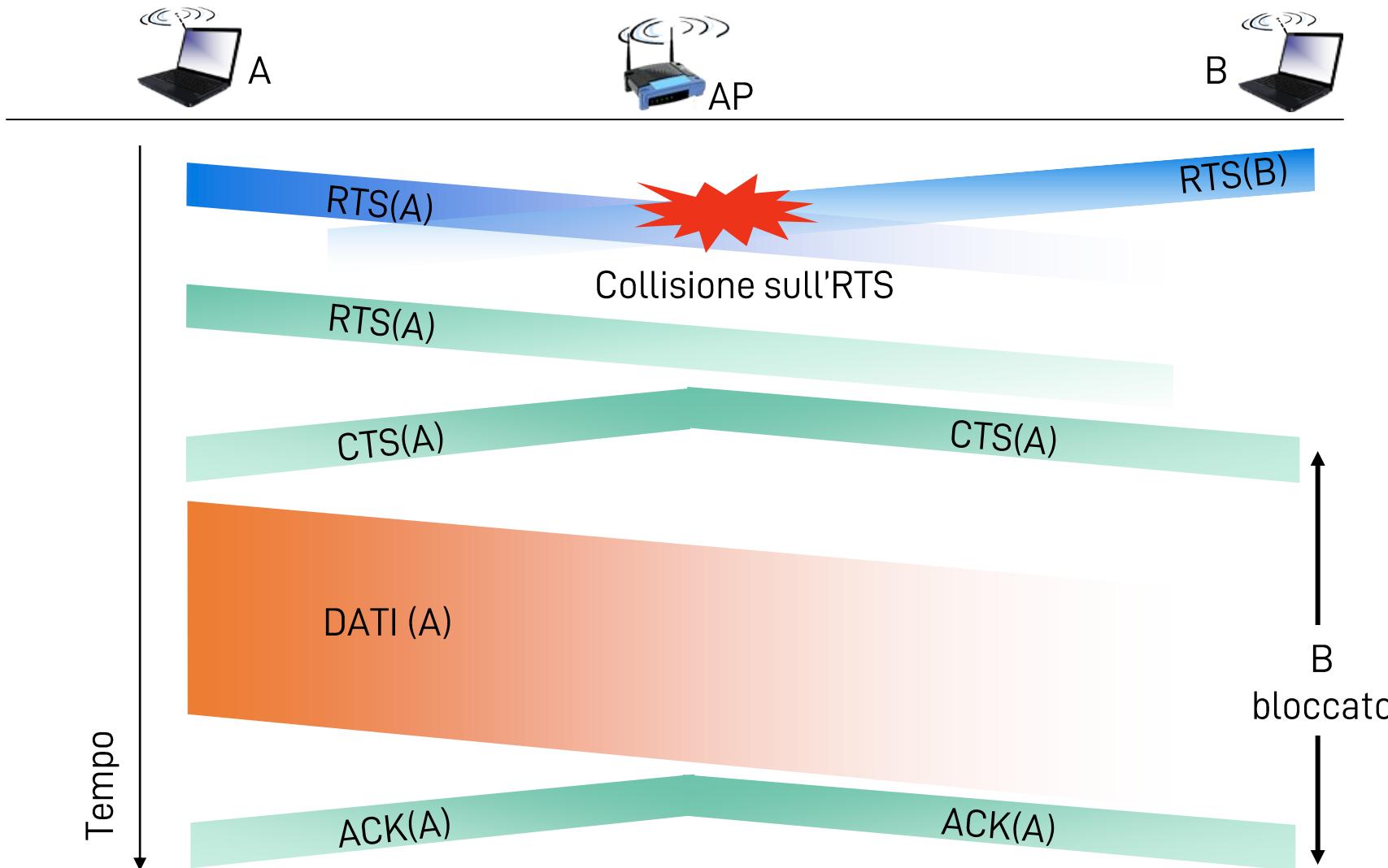


- Obiettivo: evitare le collisioni su B
 - ❖ Soluzione: CSMA/CA con handshaking

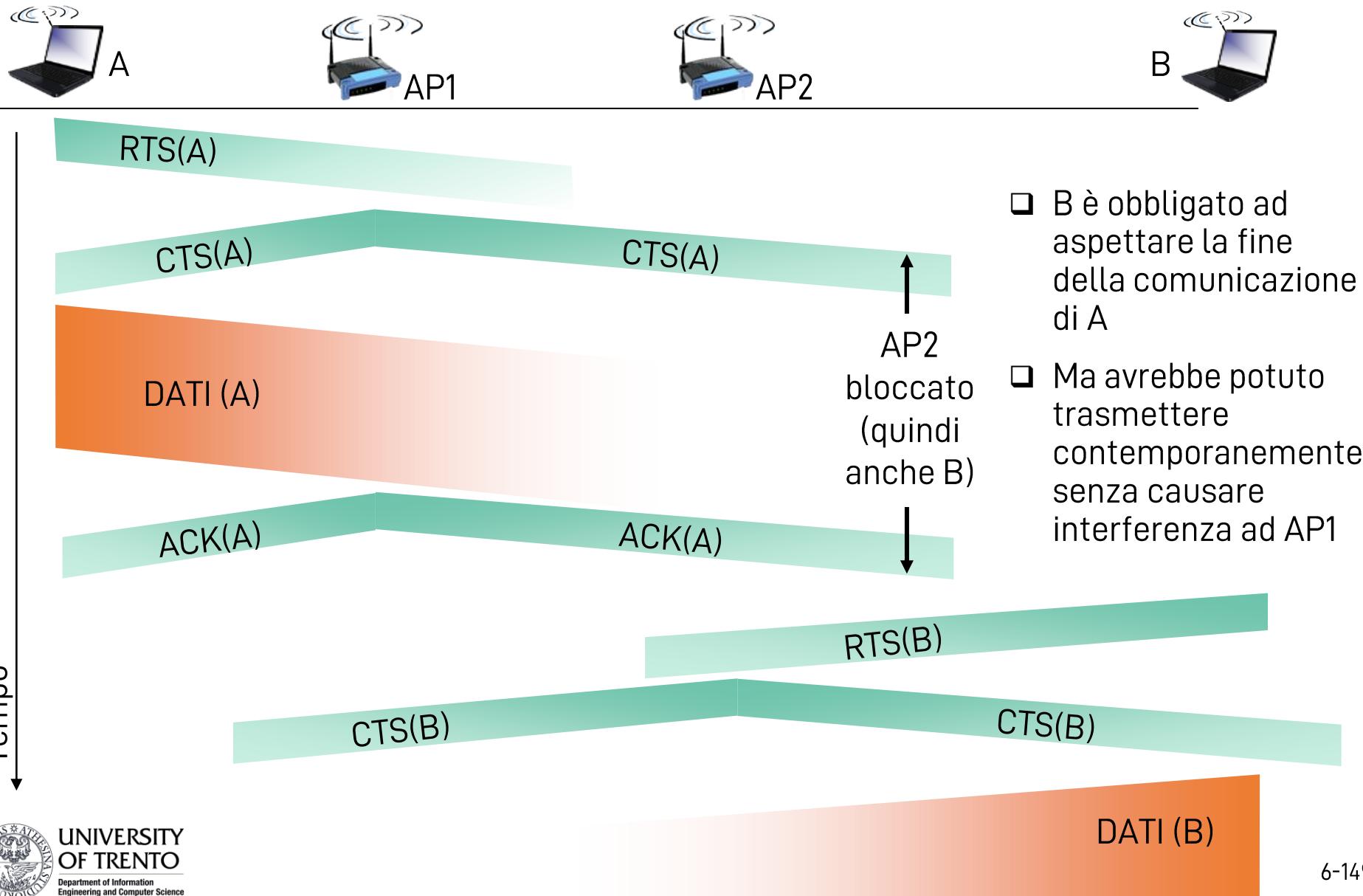
Coordinamento a livello MAC: messaggi RTS e CTS

- L'handshake serve a prenotare esplicitamente il canale
 - ❖ Tramettitore: invia Request To Send (RTS)
 - ❖ Ricevitore: risponde con un Clear To Send (CTS)
- Il CTS prenota il canale per il trasmettitore, e notifica la trasmissione imminente ad altre STA (anche se nascoste)
 - ❖ Mitiga il problema del terminale nascosto
 - ❖ ...al prezzo di un overhead maggiore
- Gli RTS e i CTS sono messaggi brevi
 - ❖ Se collidessero, la collisione durerebbe meno
 - ❖ Si sprecano meno risorse radio
 - ❖ **D:** quale problema si introduce?

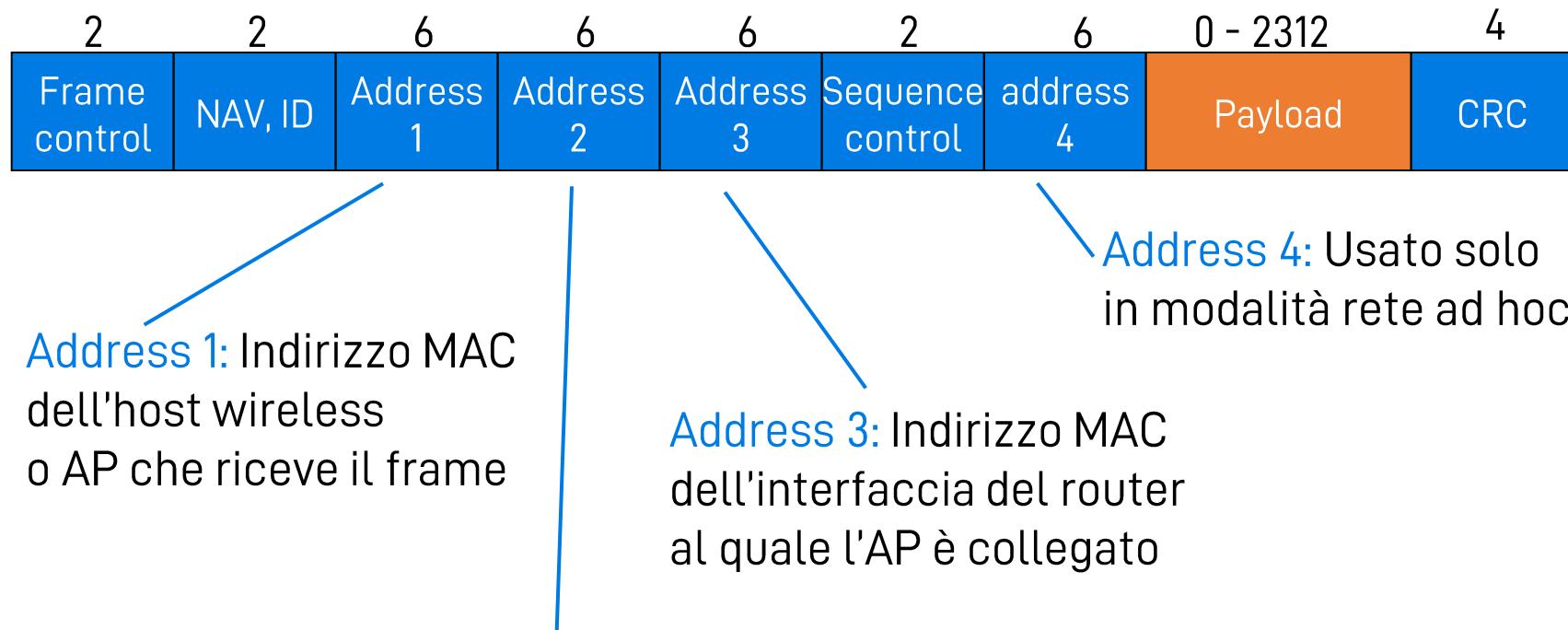
Scambio RTS-CTS



Problema del terminale esposto



Indirizzamento e frame 802.11



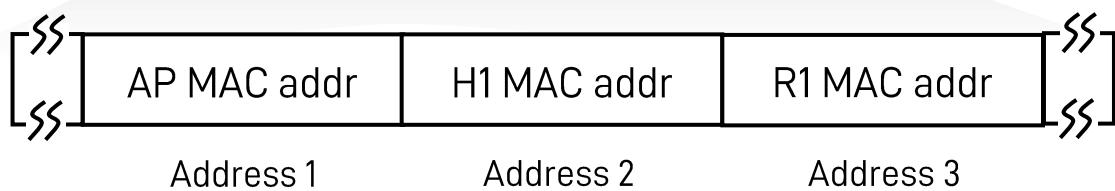
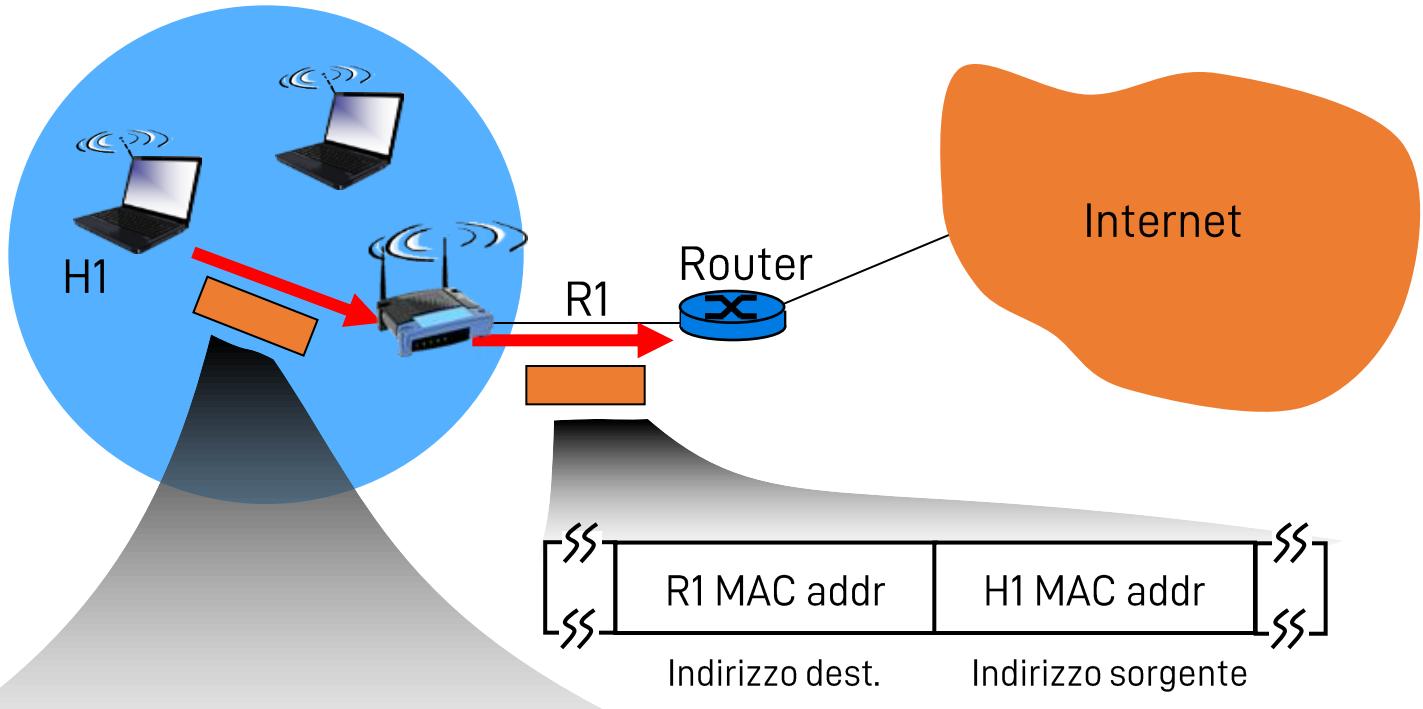
Address 1: Indirizzo MAC
dell'host wireless
o AP che riceve il frame

Address 3: Indirizzo MAC
dell'interfaccia del router
al quale l'AP è collegato

Address 2: Indirizzo MAC dell'host wireless
o AP che trasmette il frame

Address 4: Usato solo
in modalità rete ad hoc

Indirizzamento e frame 802.11



Frame 802.11