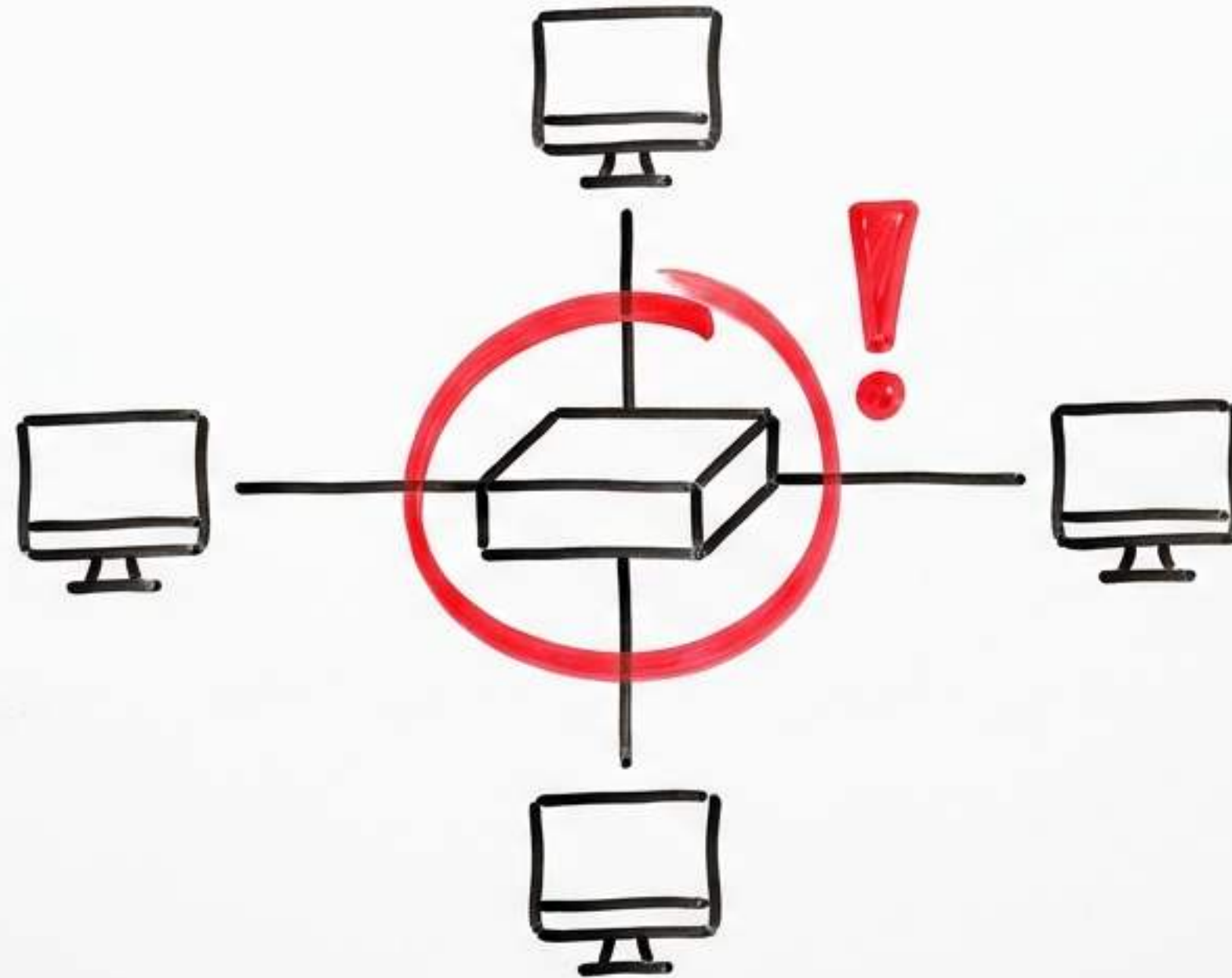
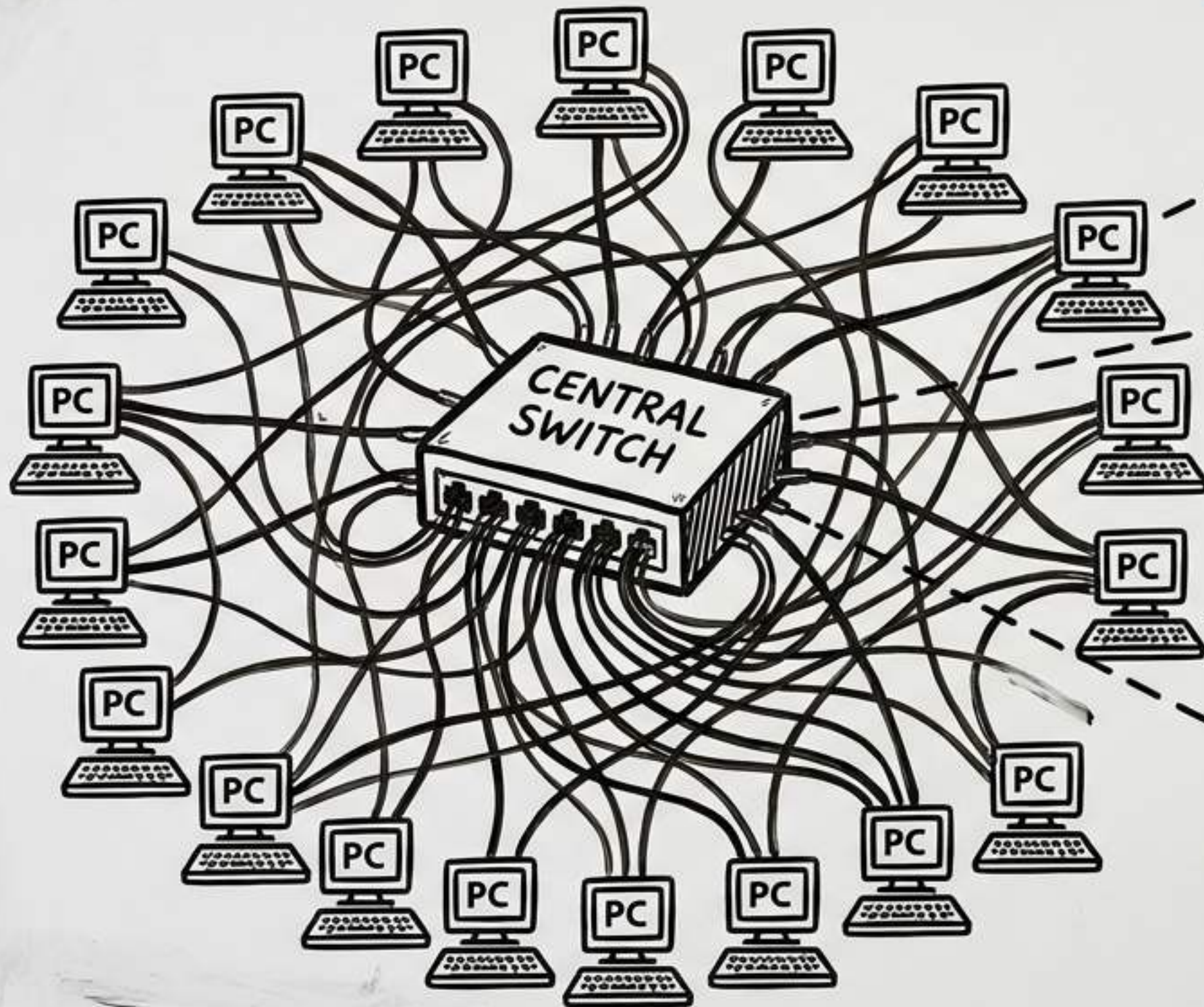


Domini di Broadcast e Colli di Bottiglia

Anatomia del fallimento delle LAN tradizionali piatte



L'illusione della LAN piatta



Progettazione di base:
Centinaia di host collegati
su un unico switch (o in
cascata).

Separazione limitata:
Lo switch separa i Domini
di Collisione, ma crea un
enorme collo di bottiglia.

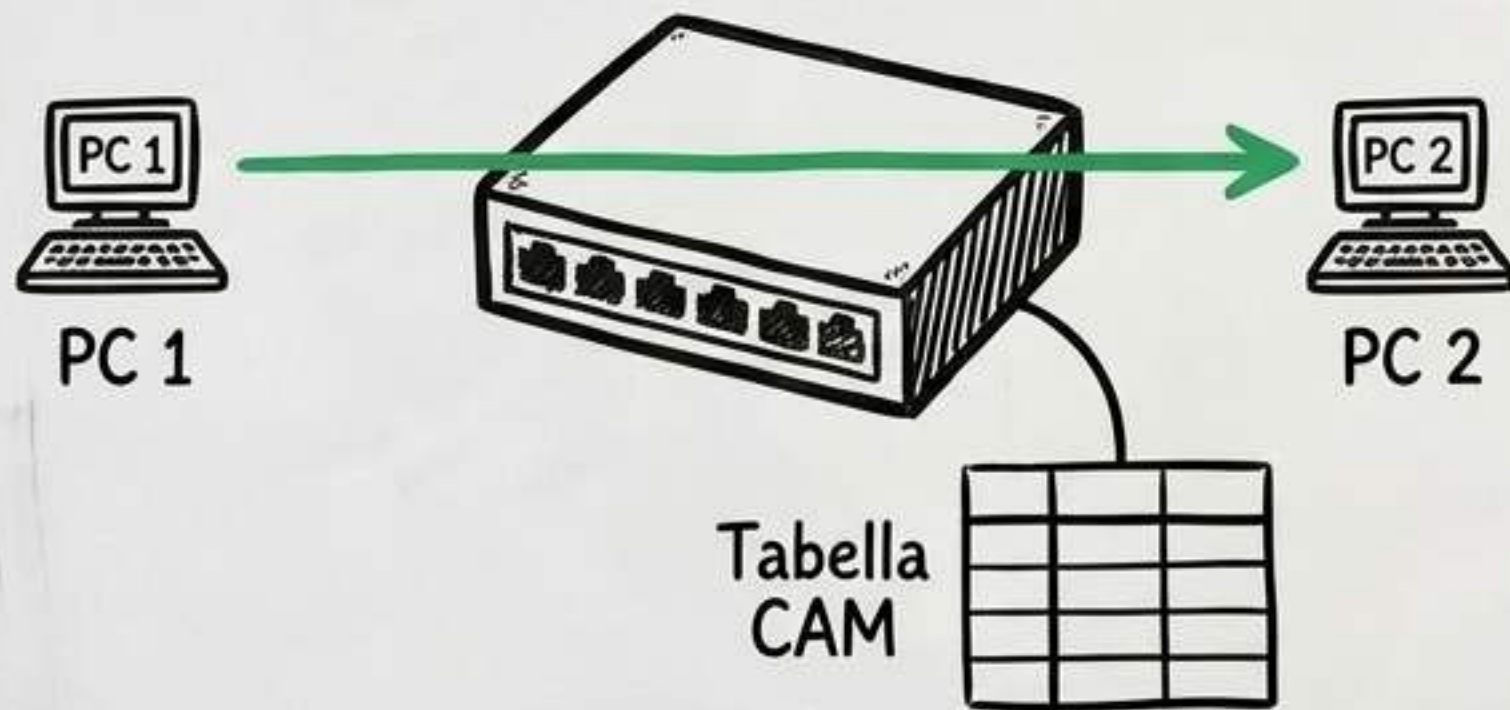
**Livello 2 (Data Link)
- Sottorete Unica**

L'apparenza: Logica,
semplice ed economica.

La realtà: Vulnerabile non
appena la rete scala.

L'intelligenza parziale dello Switch

Traffico Unicast



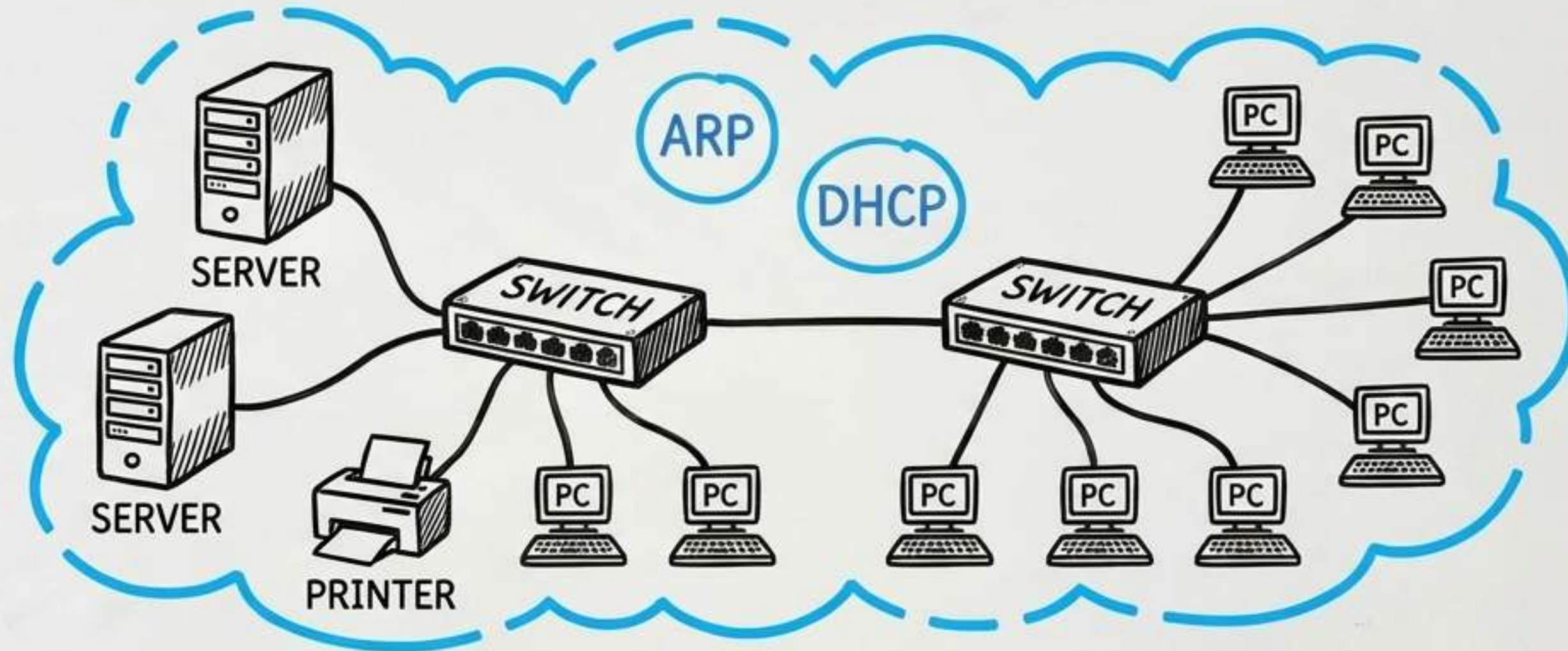
Inoltro selettivo tramite Tabella CAM.
La banda resta intatta.

Traffico Broadcast



Lo switch non filtra il broadcast.
L'hardware replica il frame su tutte
le porte attive (FF:FF:FF:FF:FF:FF).

I confini del Dominio di Broadcast



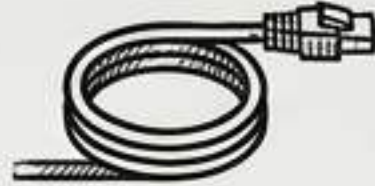
Definizione:

L'insieme di tutti i dispositivi e cavi raggiungibili da un singolo frame di broadcast. (In IPv4 non segmentato = l'intera sottorete IP).

Dipendenza Sistemica:

- ARP: Risoluzione da IP a MAC address.
- DHCP: Richiesta di indirizzi dinamici.
- Senza broadcast, la rete locale IPv4 smette di funzionare.

Vulnerabilità 1: Il costo occulto sulla CPU



1. Ricezione: La NIC rileva il MAC FF:FF:FF... ed accetta il frame.



2. Memoria: Il frame viene trasferito nella RAM.



3. Blocco Hardware: La NIC lancia un **Hardware Interrupt (IRQ)** alla CPU.



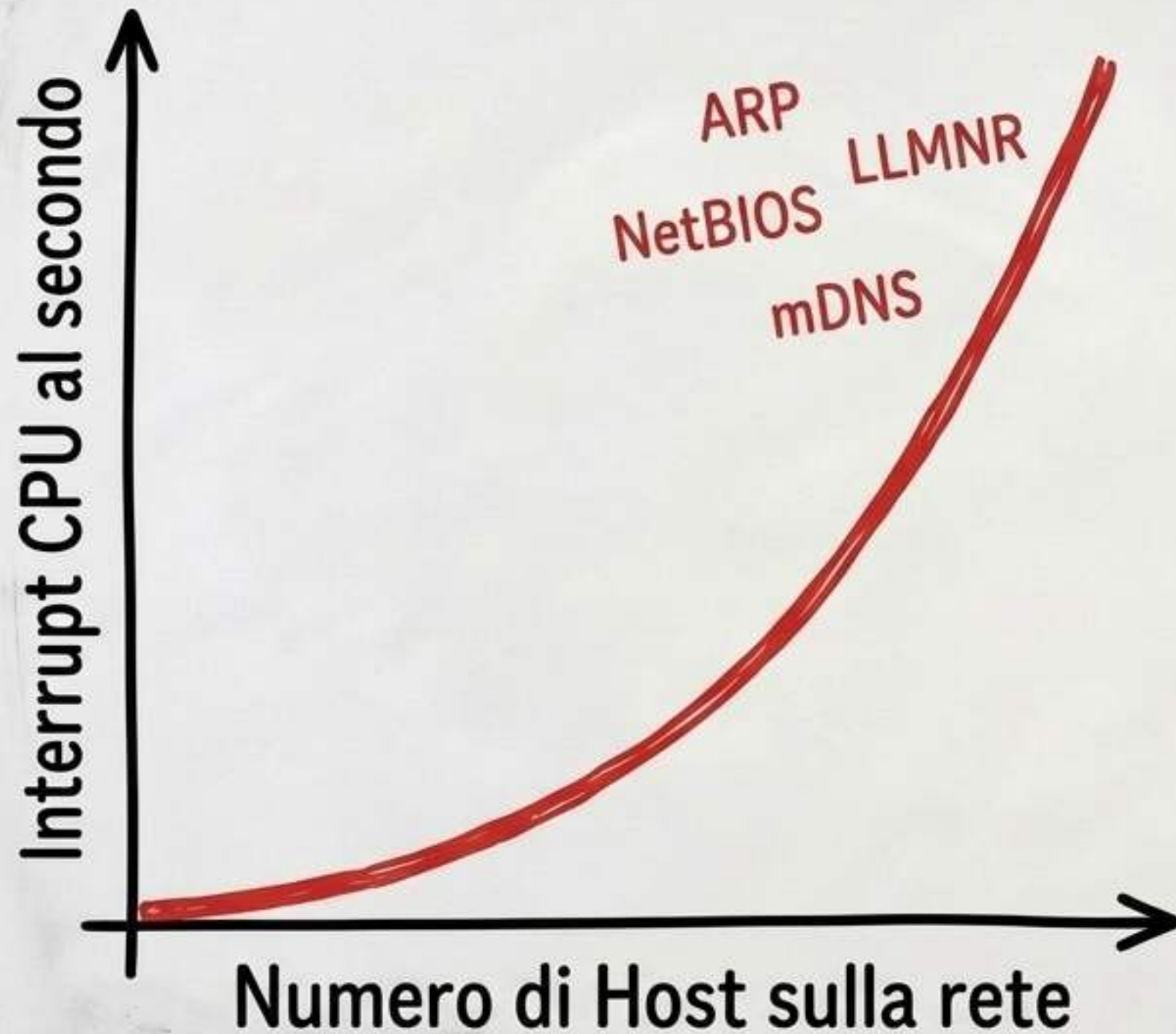
4. Analisi Kernel: Il sistema operativo si ferma per analizzare il payload IP.



5. Scarto: Nel 99% dei casi, il pacchetto non è per questo PC e viene cestinato.



Morte per mille tagli

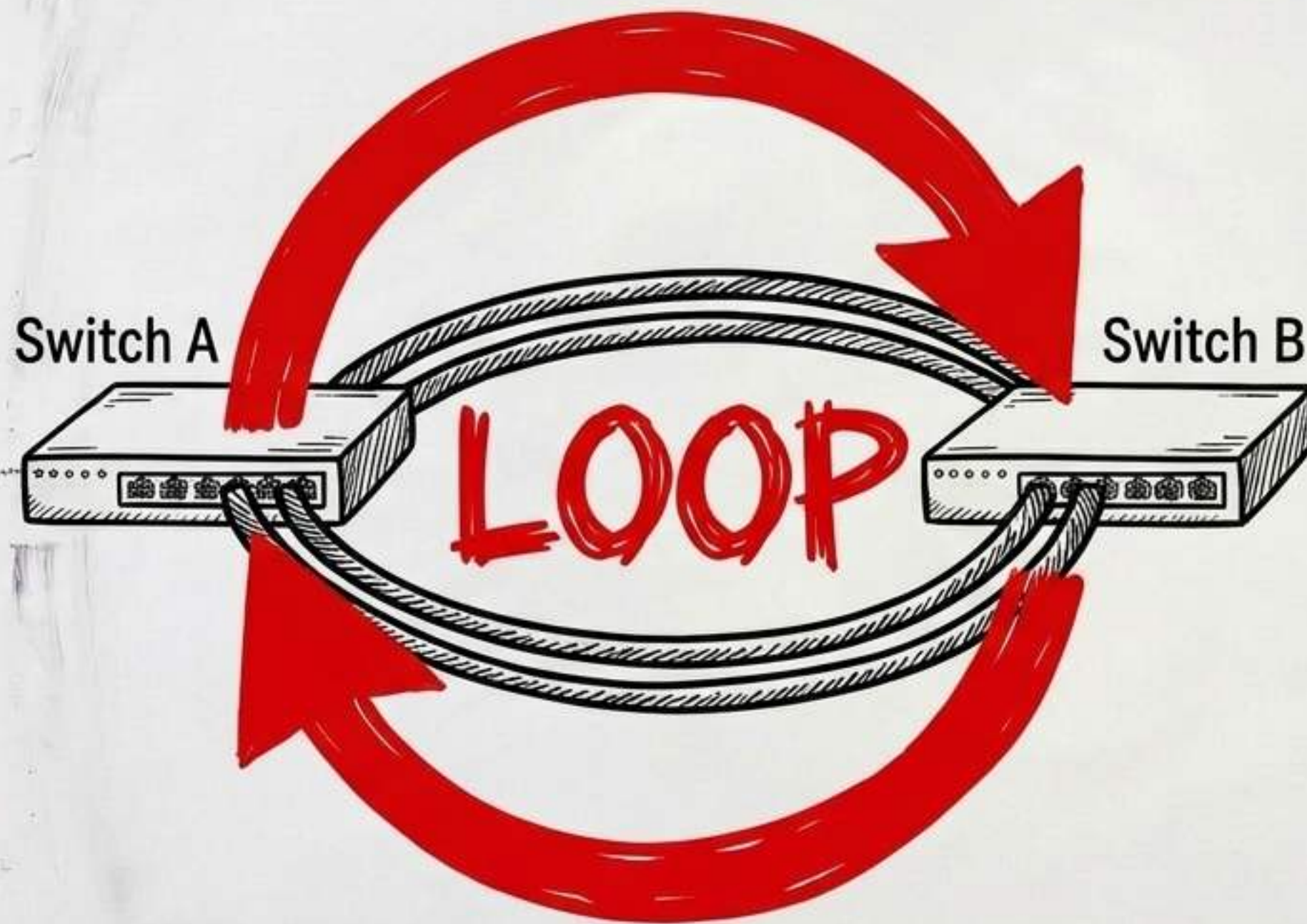


Rumore di Fondo: 500 macchine in un unico dominio generano traffico costante.

L'Impatto:

- Migliaia di interrupt al secondo.
- Bombardamento indiscriminato di server e telefoni VoIP.
- Esito: Micro-rallentamenti, Jitter (latenza variabile) e degrado generale.

Vulnerabilità 2: Tempeste di Broadcast



L'innesco: L'errore umano

Un cavo collegato per sbaglio chiude un anello fisico. Il protocollo di salvaguardia STP (Spanning Tree) fallisce o è disabilitato.

L'effetto a catena:

- Lo Switch A inonda il broadcast verso lo Switch B.
- Lo Switch B lo inonda indietro allo Switch A.
- Il ciclo si ripete all'infinito su ogni porta saturando la rete.

Il tallone d'Achille del Livello 2

Pacchetto IP
(Livello 3)

TTL (Time to Live)
= 255... 254... 0



Frame Ethernet
(Livello 2)



Nessun
meccanismo
di scadenza

La differenza strutturale:
I pacchetti IP hanno una **data di scadenza (TTL)**.
I frame Ethernet possono esistere per sempre.

Il Collasso: Milioni di copie dello stesso frame **saturano il backplane** interno degli apparati in **pochi millisecondi**. I **LED lampeggiano** fissi all'unisono. **La rete muore.**

Vulnerabilità 3: Sicurezza e Fiducia Cieca



L'Attacco (ARP Spoofing):

L'attaccante invia un Gratuitous ARP: "Il MAC del Default Gateway è diventato il mio". I PC aggiornano la propria cache ARP in buona fede e il traffico segreto fluisce verso l'attaccante.

Isolamento impossibile:

Essendo il broadcast udibile da chiunque, bloccare questo attacco in un dominio piatto richiede configurazioni manuali e complesse porta-per-porta.

Saturazione CAM (MAC Flooding)

Tabella Memoria CAM

A1:B2:C3:D4:E5:F6	A1:B2:C3:D4:E5:F6	CA:FE:BA:BE:00:03
DE:AD:BE:EF:00:01	DE:AD:BE:EF:00:01	CA:FE:BA:BE:00:04
FE:ED:FA:CE:00:02	A1:B2:C3:D4:E5:F3	CA:FE:BA:BE:00:05
CA:FE:BA:BE:00:03	A1:B2:C3:D4:E5:F4	CA:FE:BA:BE:00:08
A1:B2:C3:DF:00:04	DE:AD:BE:EF:00:05	FE:ED:C3:D4:00:06
FE:AA:BA:EF:00:05	CC:D0:DA:FA:00:06	CA:FE:BA:BE:00:07
CA:FE:BA:BE:00:07	ED:ED:BA:BE:00:07	CA:FE:BA:BE:00:03



~~SWITCH~~



L'Attacco: Inondazione di centinaia di migliaia di frame con MAC sorgenti casuali e falsificati.

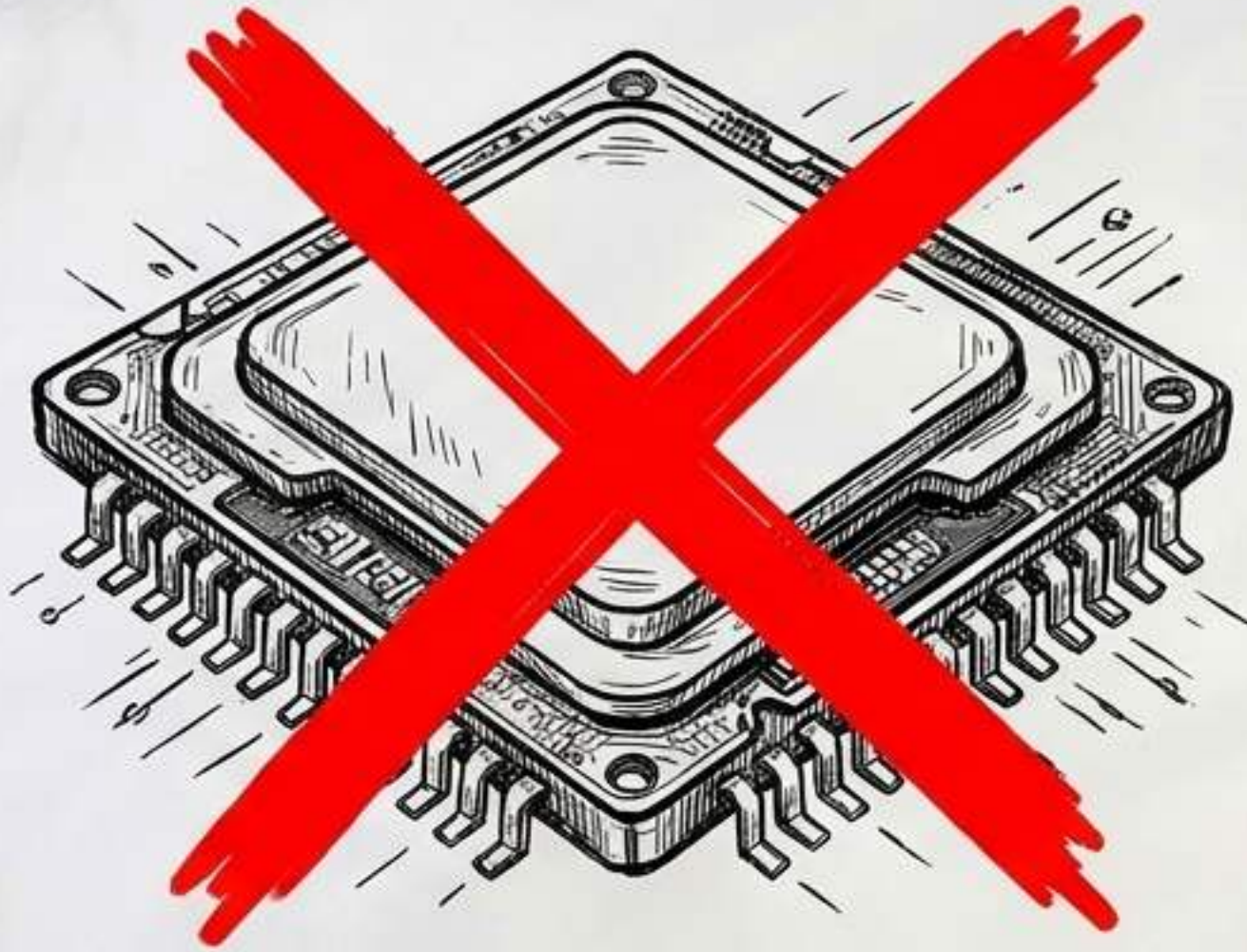
Reazione Hardware (Fail-Open): La memoria CAM si riempie. Lo switch regredisce, iniziando a comportarsi come un vecchio Hub, inondando in broadcast il traffico Unicast.

Risultato: L'attaccante cattura l'intero traffico di rete in chiaro (es. tramite Wireshark).

Matrice Diagnostica: I 3 vettori di fallimento

	Vettore	Causa Hardware/Logica	Impatto Finale
	Performance	Interrupt CPU da broadcast normali (ARP/DHCP)	Jitter e degrado continuo dispositivi
	Stabilità	Loop fisici + Assenza di TTL in Ethernet	Broadcast Storm e paralisi totale
	Sicurezza	Fiducia del broadcast + Memoria CAM limitata	ARP Spoofing (MitM) e intercettazione Hub fail-open

L'hardware potente non è la soluzione



Switch più potenti:

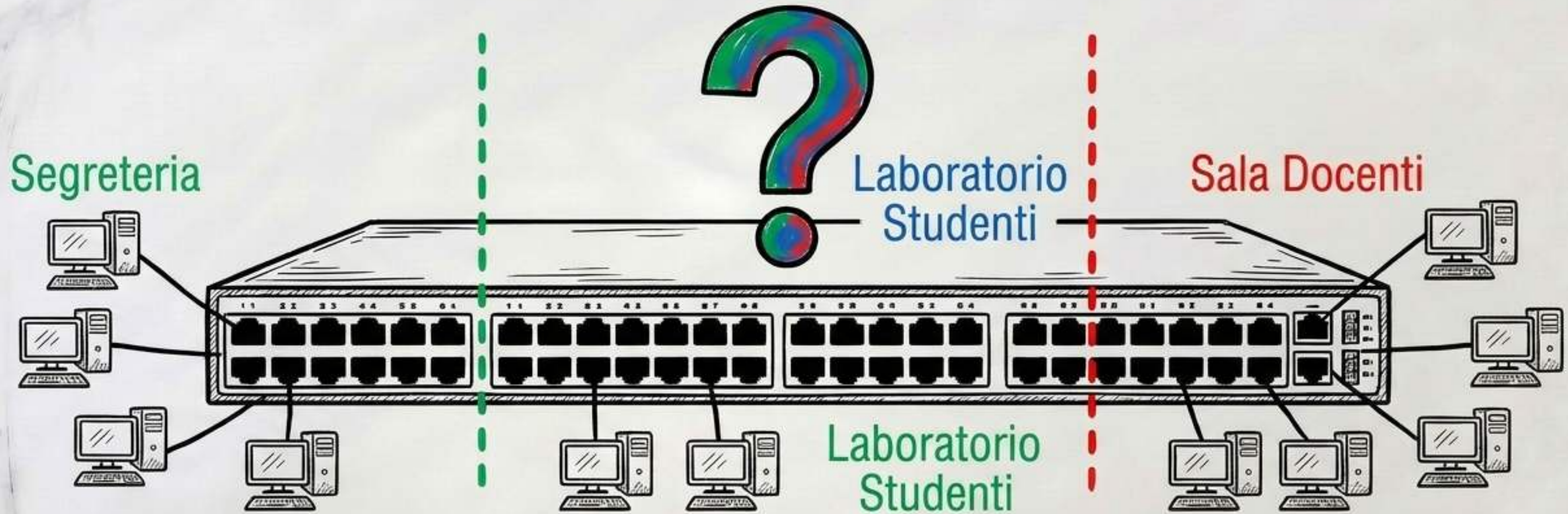
Acquistare CPU più grandi o cavi più veloci non ferma la logica infinita dei loop, né previene gli attacchi di spoofing. Il problema è architetturale, non di potenza.



Router Fisici:

Un router blocca i broadcast nativamente agendo a Livello 3. Ma acquistare decine di router dedicati per separare fisicamente ogni singolo ufficio è economicamente folle e totalmente inflessibile.

L'esigenza vitale di Segmentazione Logica



La Sfida Architetture:

Come possiamo far credere ai computer della Segreteria, dei Docenti e degli Studenti di essere collegati a tre switch fisicamente separati (rompendo i domini di broadcast)...

Il Vincolo:

...pur mantenendo tutti i cavi fisicamente attaccati a quell'unico switch da 48 porte?

Soluzione -> Virtual LAN (VLAN)