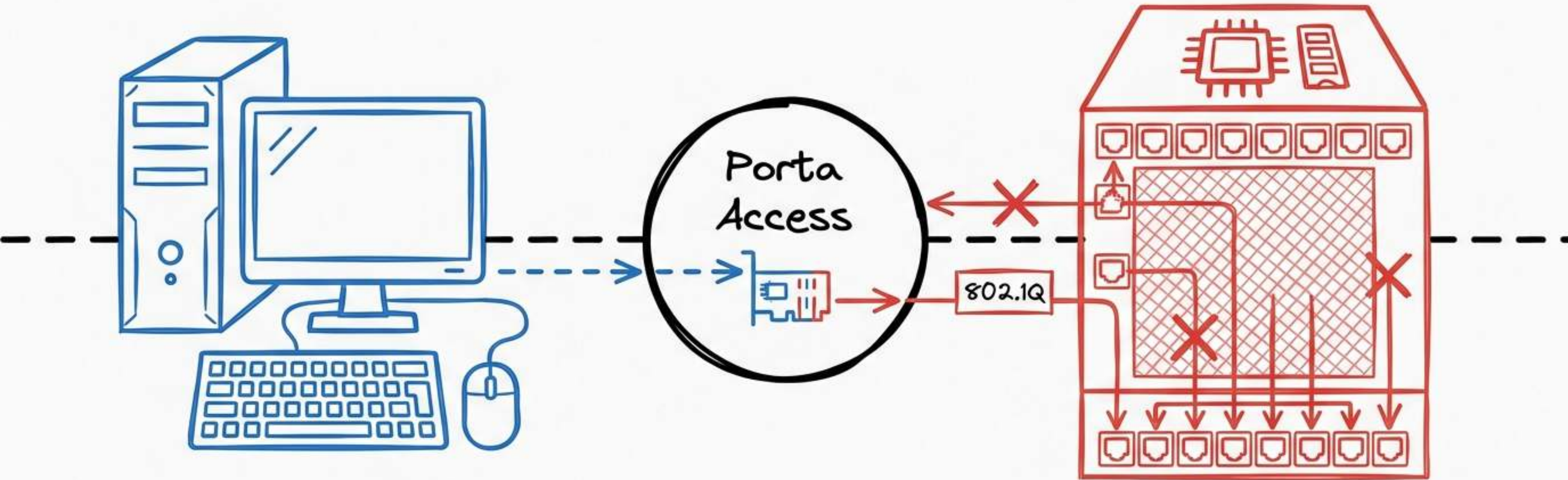
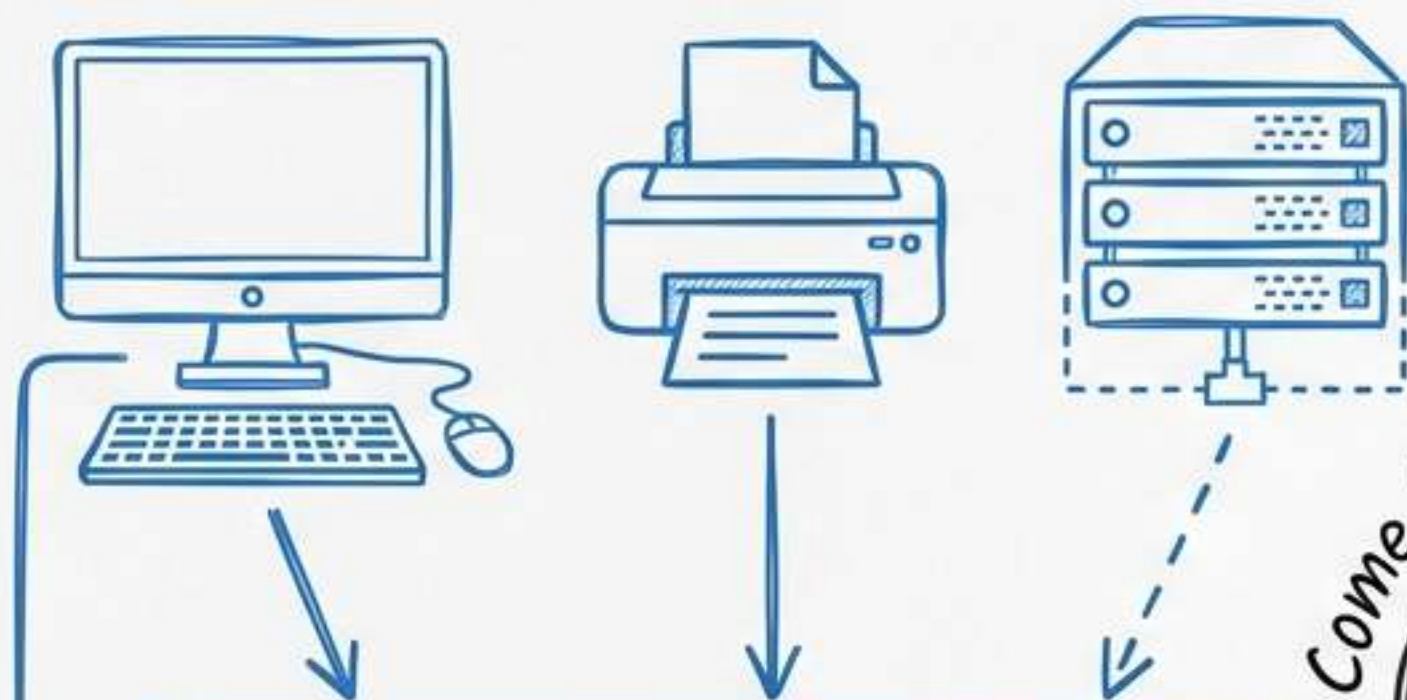


Architettura VLAN: *Le Porte Access*



Il ruolo cruciale delle porte di accesso:
segmentazione, sicurezza e traduzione del traffico di rete.

Dispositivi Finali



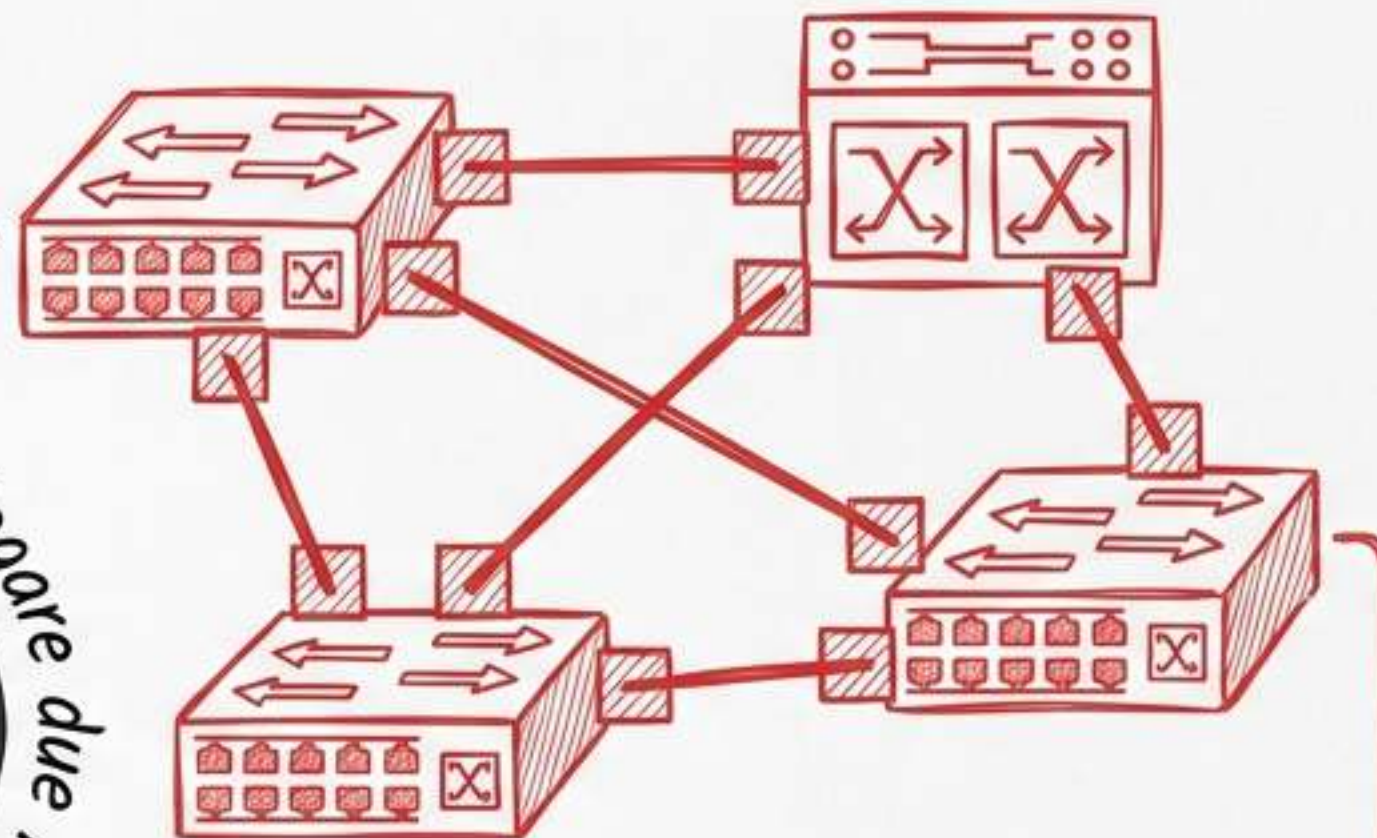
Linguaggio: Ethernet Standard (IEEE 802.3)

Stato: VLAN-unaware (Ignorano l'esistenza delle reti virtuali).

Aspettativa: Ricevere e inviare pacchetti dati puliti.

Come facciamo a far dialogare due incompatibili??

Rete Core



Linguaggio: IEEE 802.1Q (Tagging)

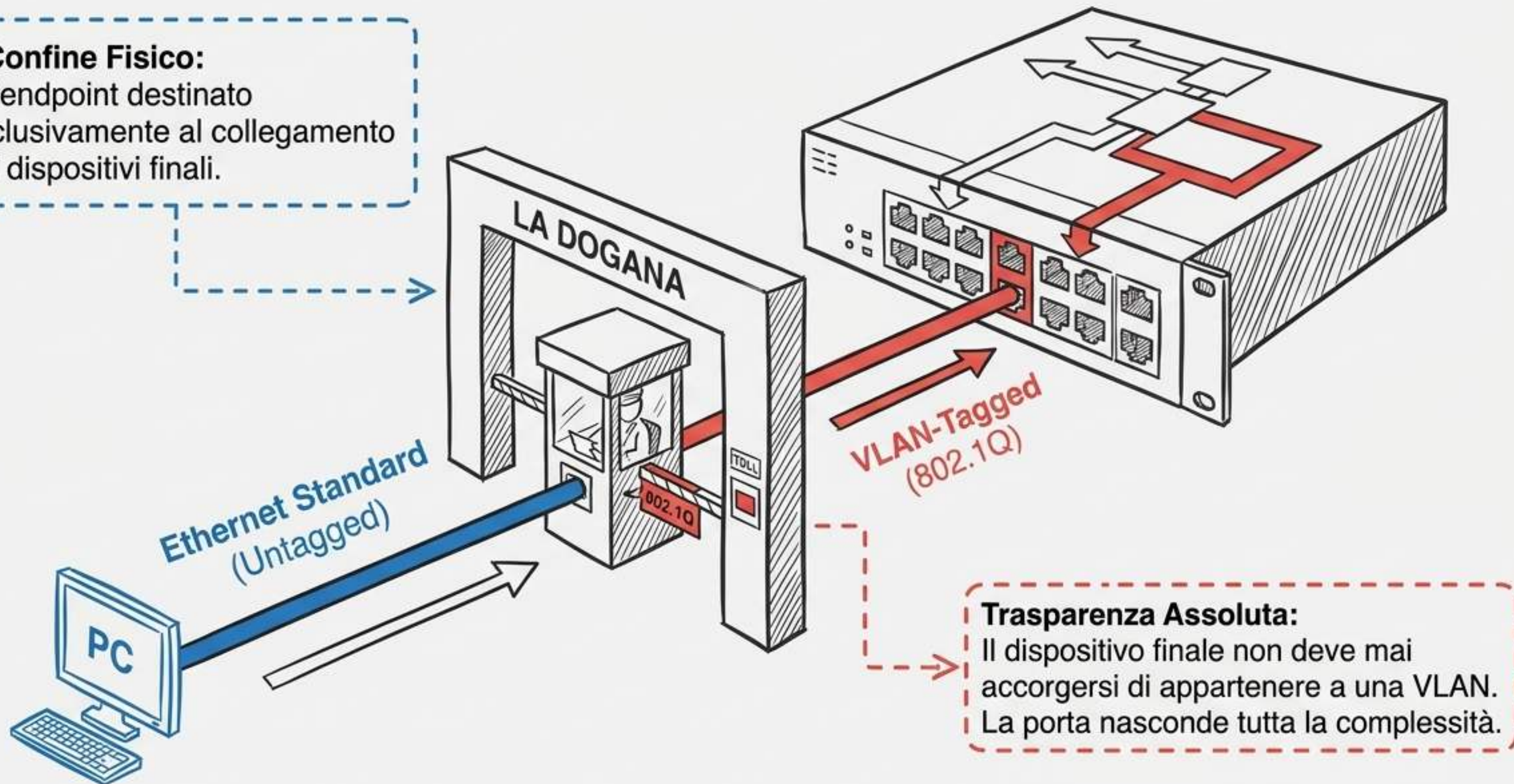
Stato: VLAN-aware.

Aspettativa: Usare etichette (tag) per separare i flussi informativi.

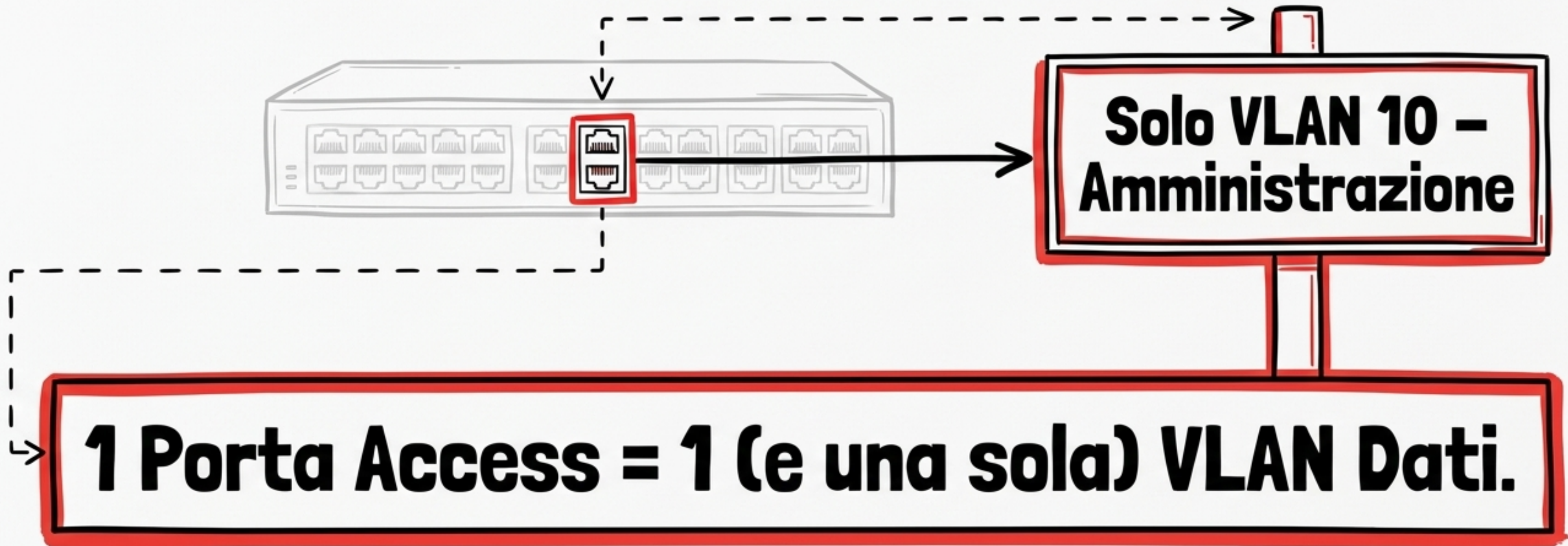
La Porta Access: Il Traduttore di Livello 2 ("La Dogana")

Il Confine Fisico:

È l'endpoint destinato esclusivamente al collegamento dei dispositivi finali.

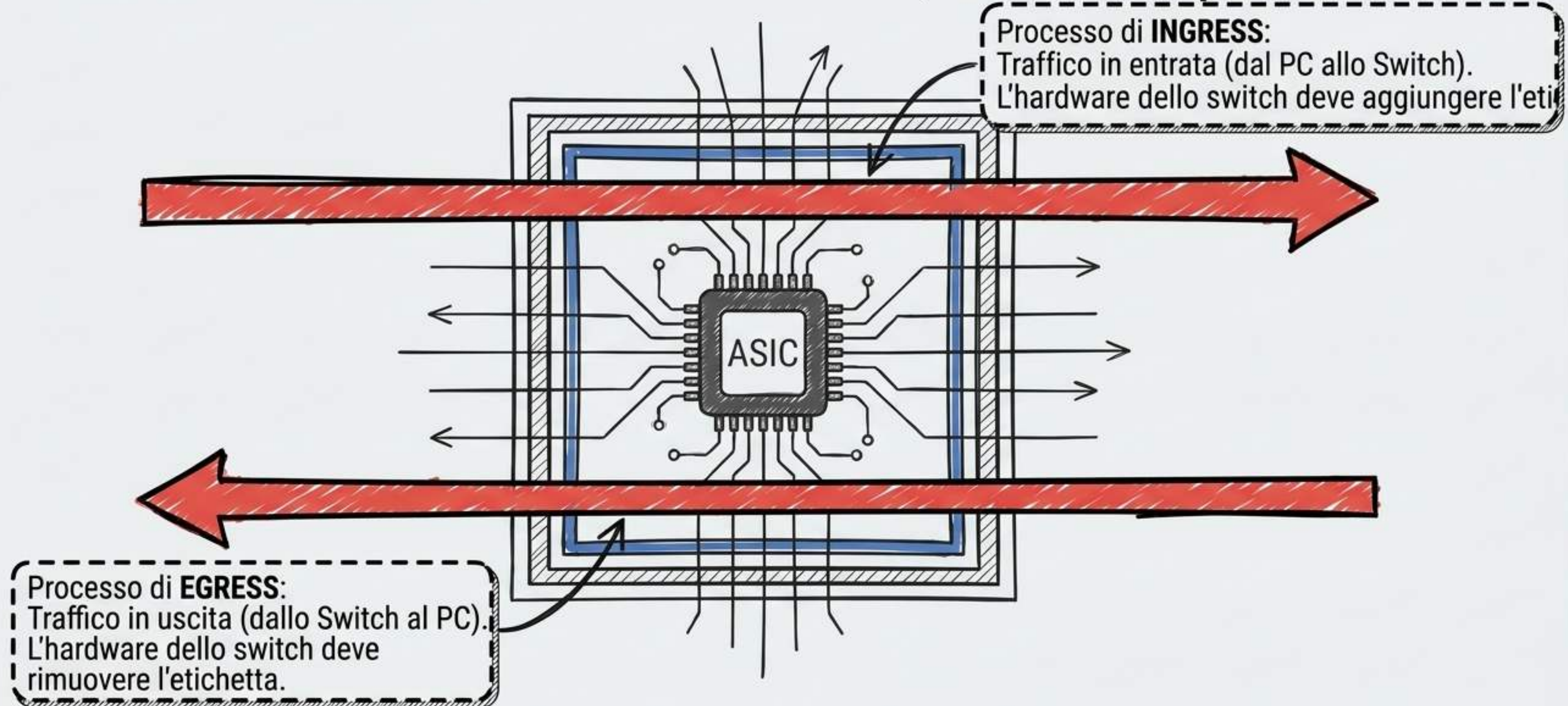


L'Equazione della Porta Access

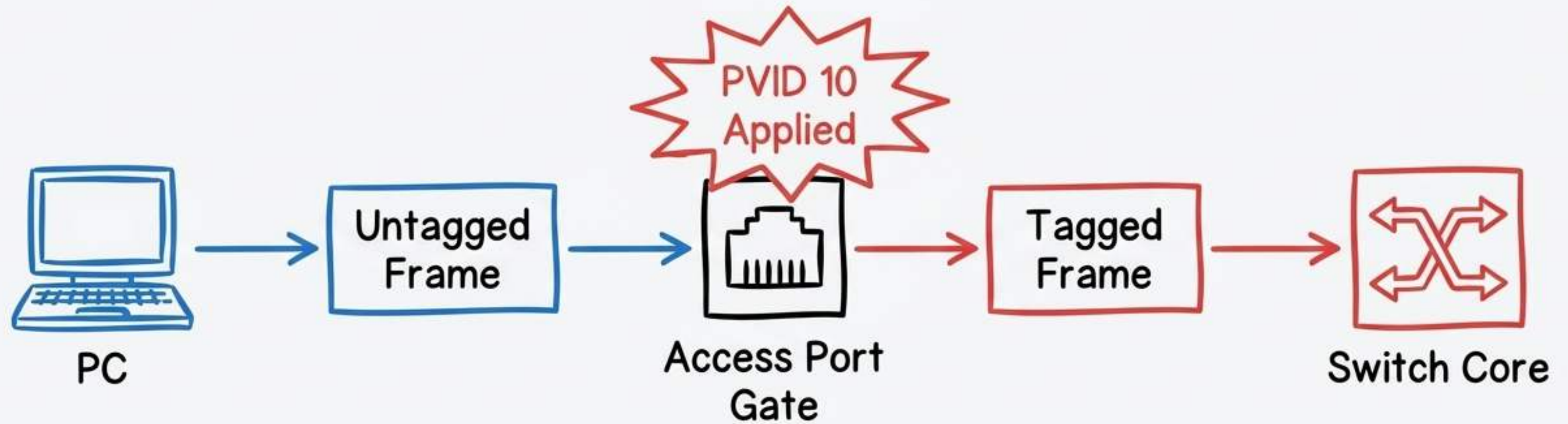


La porta diventa un vicolo cieco logico, dedicato esclusivamente a una specifica sottorete. Il traffico di altre VLAN non vi può transitare.

Il Processore ASIC: Due Direzioni, Due Comportamenti

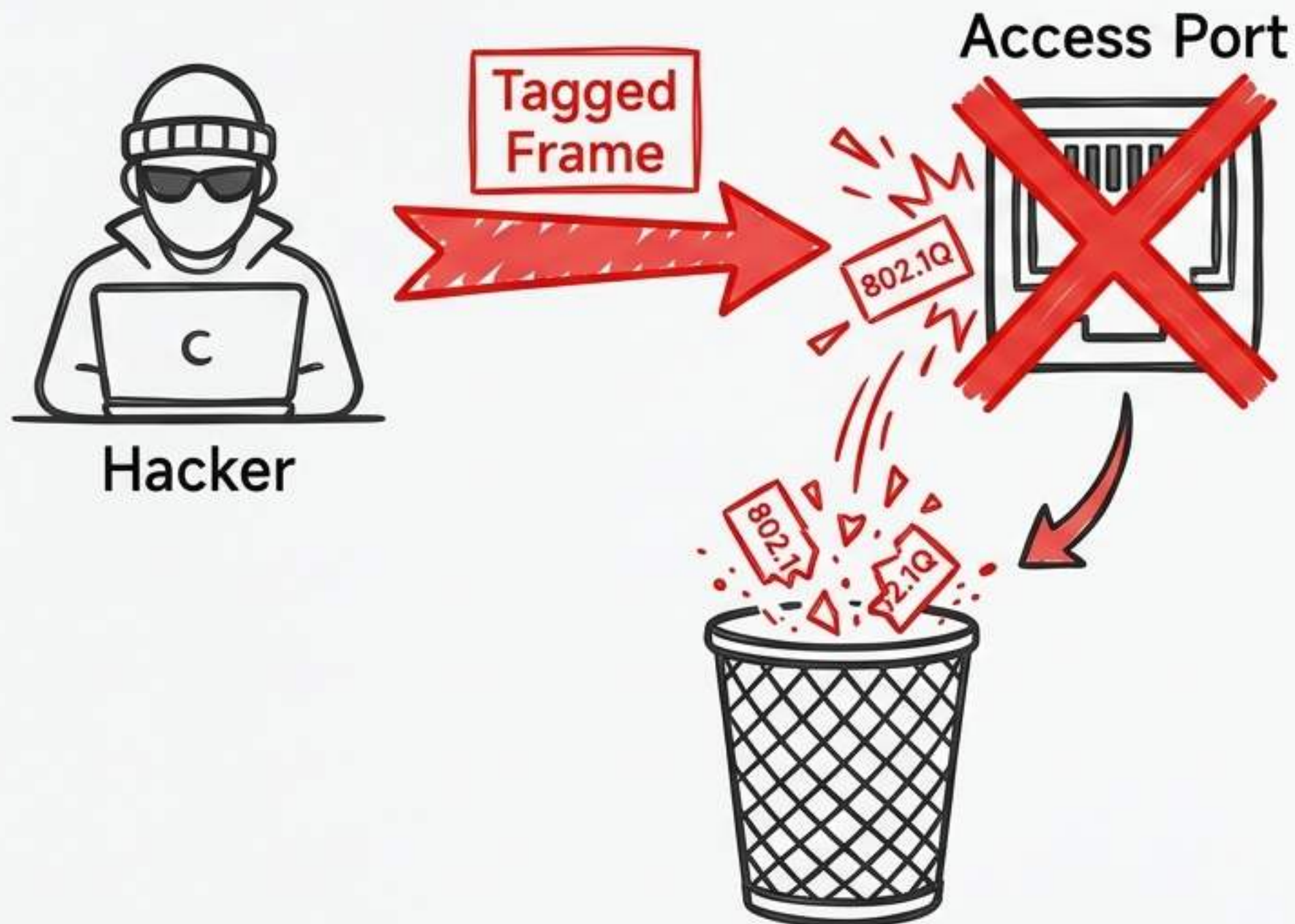


Processo di Ingress: Etichettare l'ignoto



Step 1:	Il PC genera e invia un normale frame Ethernet (Untagged).
Step 2:	Il frame attraversa il cavo ed entra nella porta Access.
Step 3:	L'hardware dello switch ispeziona il frame e applica istantaneamente il PVID (Port VLAN ID) assegnato a quella specifica porta.
Step 4:	Da quel nanosecondo, il frame viaggia nei circuiti dello switch come VLAN 10.

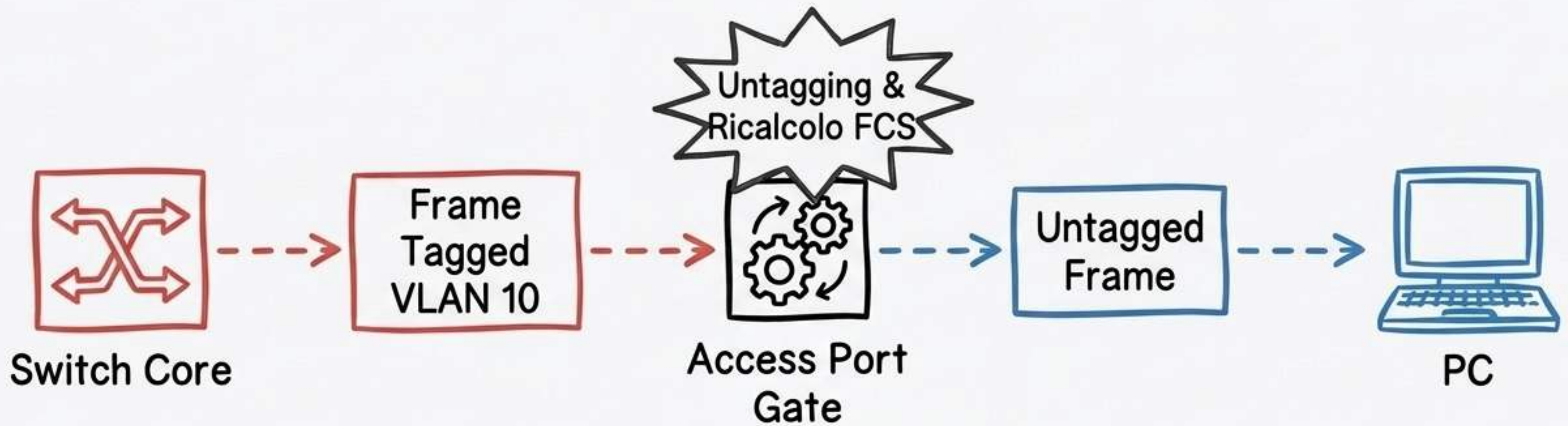
La Difesa Ingress (Strict Access)



Cosa succede se un utente malintenzionato inietta un frame già etichettato (Tagged 802.1Q) per saltare in una VLAN protetta?

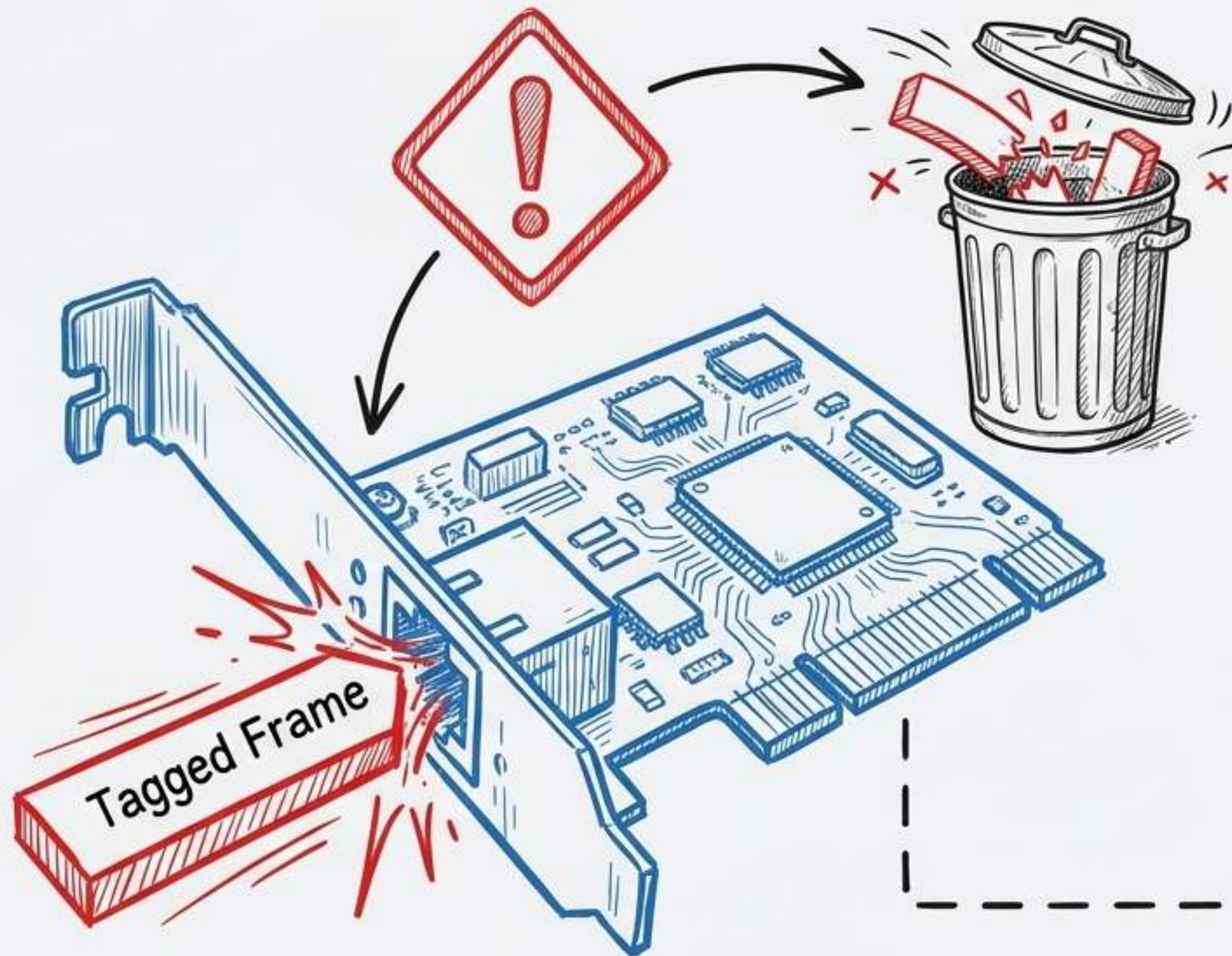
Drop Istantaneo. Una porta in modalità strict Access si aspetta solo traffico Untagged. Se rileva un Tag, lo scarta immediatamente. Nessuna eccezione.

Processo di Egress: Restituire la Purezza



Step 1:	Il pacchetto etichettato VLAN 10 arriva alla porta di destinazione per uscire.
Step 2:	L'hardware dello switch esegue l'Untagging: strappa letteralmente i 4 byte dell'etichetta 802.1Q dal frame.
Step 3:	Lo switch ricalcola il checksum (FCS) alla fine del frame per garantirne l'integrità.
Step 4:	Spara sul cavo un frame Ethernet standard , puro e immacolato verso il PC.

L'Illusione del Livello 2: Perché l'Untagging è vitale?



Il Problema Hardware:

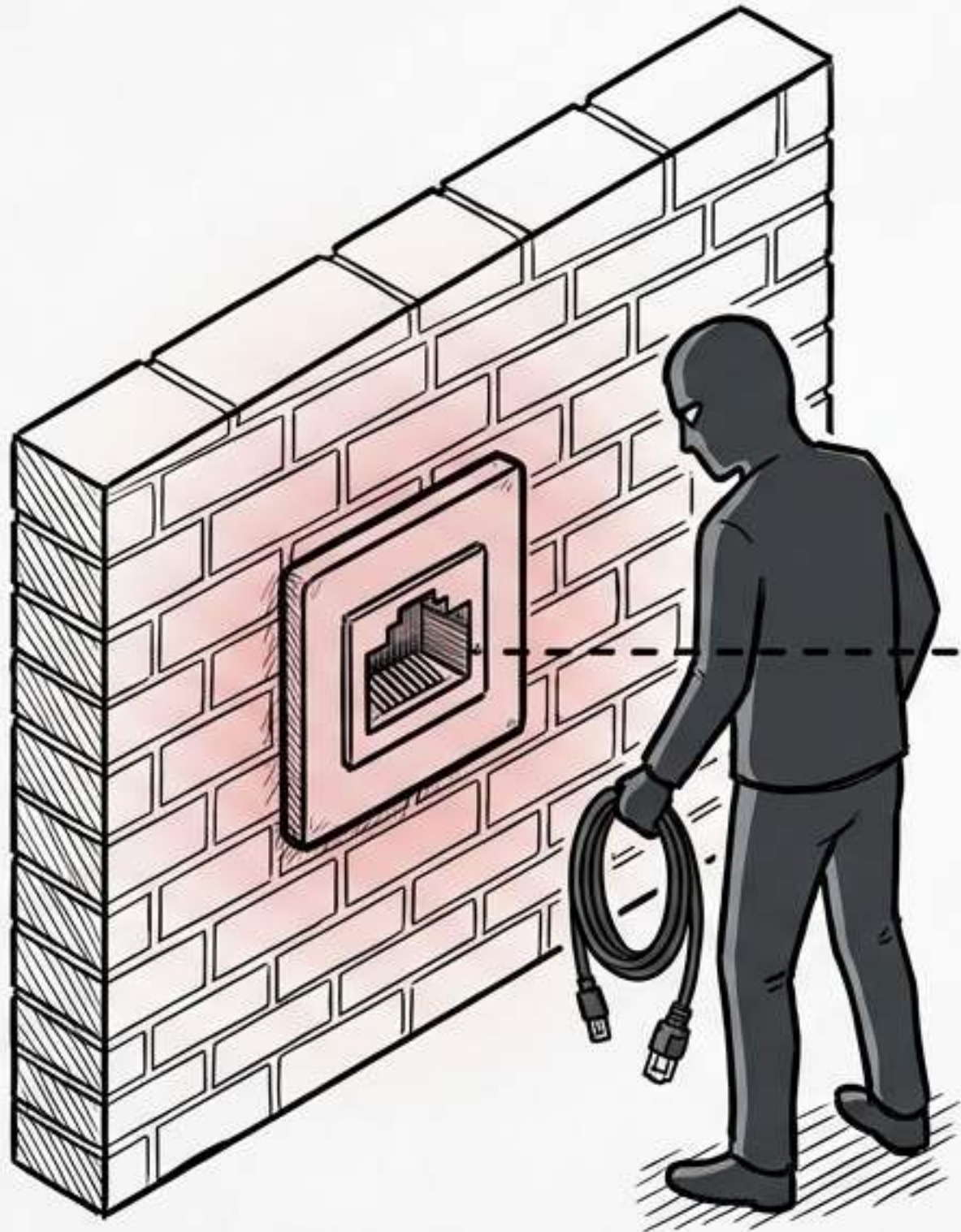
I computer standard non sanno leggere le etichette 802.1Q.

La Reazione del Sistema Operativo:

Se per un errore di configurazione un frame Tagged dovesse raggiungere un PC Windows o Linux, il driver della scheda di rete lo interpreterebbe come un pacchetto anomalo (malformed).

Risultato: Il sistema operativo lo distruggerebbe ancor prima di passarlo all'utente.

Sicurezza Perimetrale: Il Punto Debole Fisico



Il Contesto: Le porte Access sono l'unico componente di rete fisicamente esposto negli uffici, nelle aule e nelle prese a muro.

Il Rischio: Rappresentano il perimetro esterno della rete aziendale, ovvero il punto più vulnerabile per gli attacchi di Livello 2.

L'Imperativo: Richiedono l'attivazione di rigidi protocolli di blocco (Feature di Sicurezza).

La Matrice Diagnostica delle Difese

Feature	Minaccia	Meccanismo	Azione
Port Security	Utenti abusivi / Attacchi di MAC Flooding / Hub non autorizzati.	Memorizza il MAC address autorizzato, limitando il numero di dispositivi fisici.	Blocca istantaneamente il traffico dei MAC sconosciuti.
BPDU Guard	Switch pirata (Sabotaggio della topologia Spanning Tree).	Ispeziona l'arrivo di pacchetti BPDU (che un PC non dovrebbe MAI generare).	Spegne la porta mettendola in stato di Err-Disable.

Il Paradosso Aziendale (Un cavo, due dispositivi)

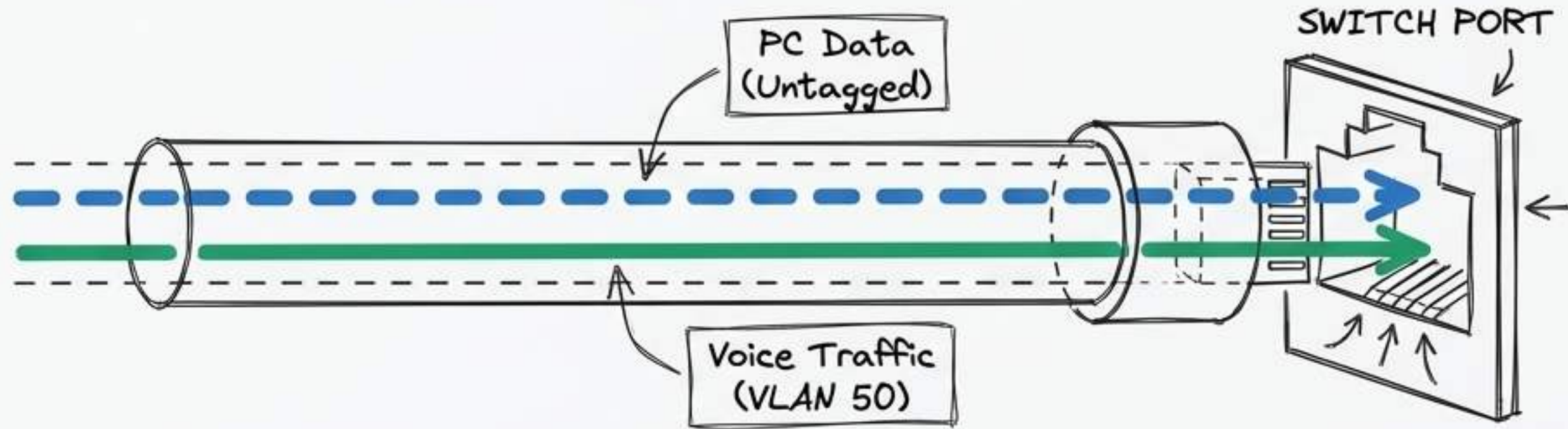


Il Conflitto:
Abbiamo stabilito che:
1 Porta Access = 1 sola
VLAN.

La Realtà:
Per risparmiare cavi a muro, gli uffici collegano il Telefono IP aziendale alla presa, e il PC in PC in cascata al telefono.

Il Problema:
I flussi (Voce e Dati) viaggiano sullo stesso filo di rame, ma devono finire in due VLAN separate. Come è possibile se la porta è di tipo Access?

L'Eccezione Geniale: La Voice VLAN



Flusso Dati: Il PC invia traffico Untagged. Lo switch lo accetta e gli assegna normalmente il PVID della VLAN Dati (es. VLAN 10). ➡ ➡

Flusso Voce: Il Telefono IP (un mini-switch intelligente) invia ➡
traffico già etichettato con 802.1Q (es. VLAN 50). ➡ 

La Magia: Configurando la Voice VLAN, lo switch accetta questa etichetta in via eccezionale, senza scartarla. ➡ 
Diventa un mini-Trunk mascherato da porta Access. 

Mettiti alla Prova: Lo Scenario dell'Amministratore



- Il Setup:** Assegna la Porta 10 alla VLAN 20 (Stampanti) come rigida Porta Access.
- L'Errore:** Accedi al pannello web della stampante e attivi l'opzione 'Usa VLAN 20'.
La stampante inizia a etichettare (taggare) lei stessa i frame 802.1Q prima di inviarli verso lo switch.
- La Domanda:** Secondo le regole ferree del processo di Ingress, cosa farà l'ASIC dello switch ai documenti che gli utenti vogliono stampare?

Soluzione: Il Teorema Finale



Risposta: Lo switch scarnerà (Drop) tutti i pacchetti. Non verrà stampato nulla.

Il Perché: Non importa se l'etichetta della stampante (VLAN 20) coincide con quella della porta (VLAN 20). Una porta in modalità strict Access si aspetta solo traffico Untagged. La presenza di un tag 802.1Q provoca la distruzione immediata del frame per sicurezza.



Le porte Access sono traduttori trasparenti: la complessità delle VLAN deve rimanere nel cuore della rete, mai nei dispositivi finali.