Fondamenti dell'Architettura Internet e Vulnerabilità Intrinseche dei Protocolli IP/TCP

(Appunti elaborati a partire dalle slide del corso
Network and System Defense, A.A. 2025/2026)

Leonardo Polidori, Edoardo Marchionni, Chat GPT

29 ottobre 2025

Indice

3 NET_03 — Virtual LANs (VLAN)

3.0.1 Definizione e motivazione

Gli **switch Ethernet** tradizionali segmentano i domini di collisione ma non i domini di broadcast. Ciò significa che tutti gli host connessi a uno switch appartengono allo stesso dominio di broadcast e ricevono tutti i frame inviati in broadcast (come richieste ARP o DHCP).

Questa architettura è semplice ma poco scalabile: in reti di grandi dimensioni, il traffico broadcast può saturare la banda disponibile e ogni problema (come un loop o un attacco) può propagarsi a tutti gli host della rete.

Per risolvere questo limite si introduce il concetto di **Virtual LAN (VLAN)**, cioè la creazione di *più domini di broadcast logici* all'interno della stessa infrastruttura fisica. Ogni VLAN rappresenta una "rete virtuale" indipendente, isolata logicamente dalle altre pur condividendo gli stessi apparati.

3.0.2 Limiti delle reti fisicamente separate

Storicamente, la separazione dei domini di broadcast veniva realizzata con **sottoreti IP fisiche**, ciascuna connessa a un proprio switch e router. Tuttavia questo approccio presenta diversi limiti:

- necessità di cablaggi distinti e di apparati separati per ogni subnet anche se gli switch sono sullo stesso piano (fisico) come mostrato in Figura 10;
- difficoltà di riconfigurazione in caso di spostamento di host tra subnet diverse;
- costi di gestione e manutenzione elevati.

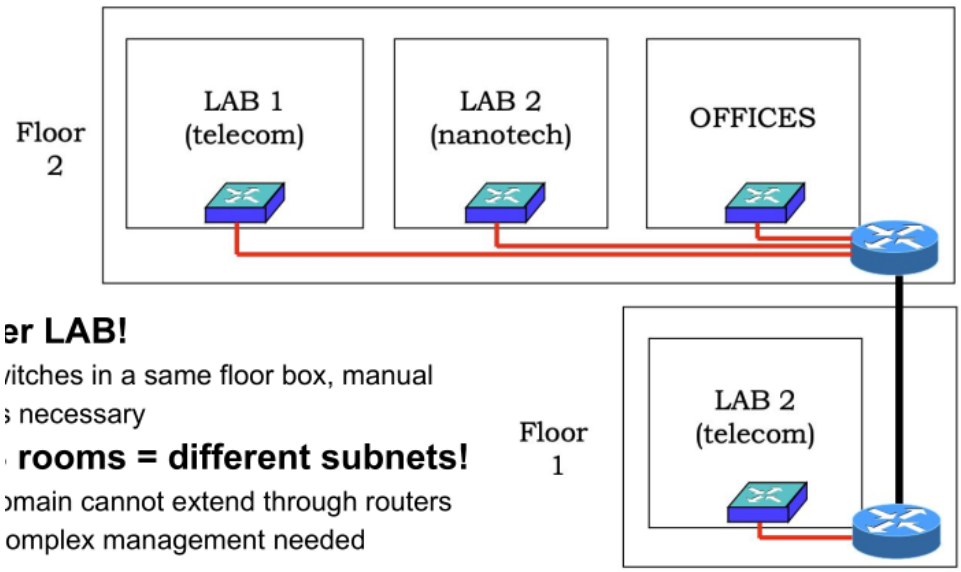

Figura 10: Physical ip subnet

Con l'introduzione degli **switch di Layer 3**, la velocità di routing non è più un problema, ma resta la necessità di una gestione logica più flessibile. Le VLAN forniscono questa flessibilità permettendo di isolare logicamente i gruppi di dispositivi in base a criteri funzionali, e non fisici.

3.0.2.1 Benefici principali delle VLAN

- **Confinamento del broadcast:** il traffico broadcast resta confinato all'interno della VLAN di appartenenza.
- **Scalabilità e ordine:** la rete può essere gestita come un insieme di domini separati, semplificando la diagnostica.
- **Sicurezza:** la separazione logica riduce la superficie d'attacco e impedisce la propagazione di minacce L2 tra gruppi diversi.

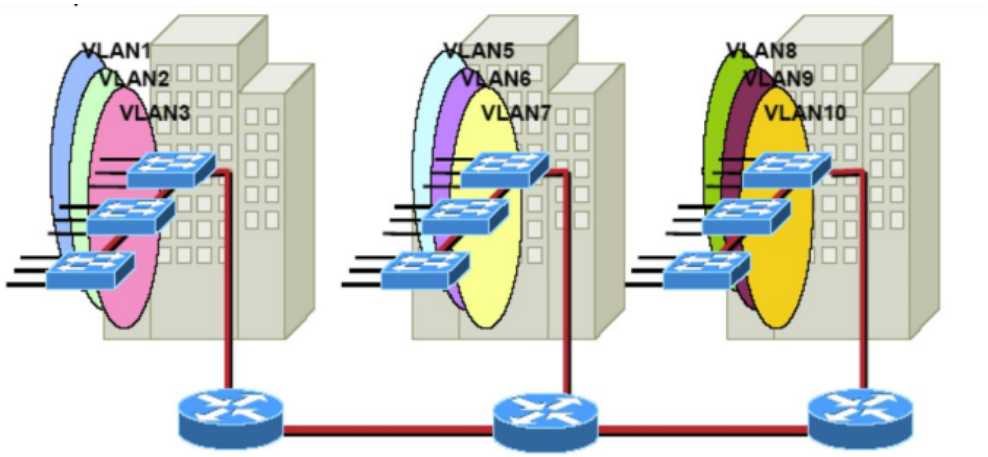

Figura 11: VLAN=area che limita il broadcast domain

3.1 Assegnazione e membership delle VLAN

3.1.1 Criteri di assegnazione

Un dispositivo può essere assegnato a una VLAN in base a diversi criteri:

- **Per porta (Port-based VLAN):** lo switch associa staticamente una VLAN a ogni porta. È il metodo più comune e lo standard definito da IEEE 802.1Q.
- **Per MAC address (User-based VLAN):** la VLAN è determinata dal MAC del dispositivo o dall'identità dell'utente autenticato (es. via 802.1X).
- **Per protocollo (Protocol-based VLAN):** introdotto da IEEE 802.1v, assegna la VLAN in base al protocollo di livello 3 (IP, IPX, ecc.).
- **Combinato (Cross-layer):** alcune implementazioni permettono regole gerarchiche, ad esempio prima per protocollo, poi per MAC, e infine per porta.

3.1.2 Vista logica

Ogni VLAN rappresenta un dominio di broadcast indipendente e, di conseguenza, è normalmente associata a una **sottorete IP dedicata**. La comunicazione tra VLAN diverse richiede un dispositivo L3 (router o Layer 3 switch (figura 12)) che svolga la funzione di *inter-VLAN routing*.

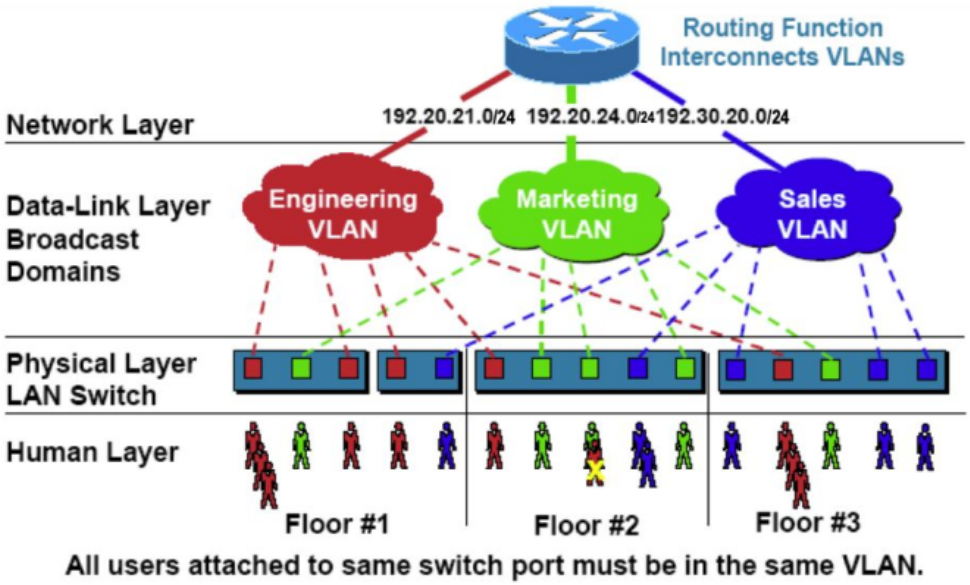

Figura 12: Physical vs logical view

3.1.2.1 Router "one-armed" In una configurazione one-armed router, una **singola interfaccia fisica** del router viene utilizzata per gestire **più VLAN** contemporaneamente. Ciò avviene tramite la creazione di **sub-interfacce virtuali**, ognuna associata a una VLAN specifica.

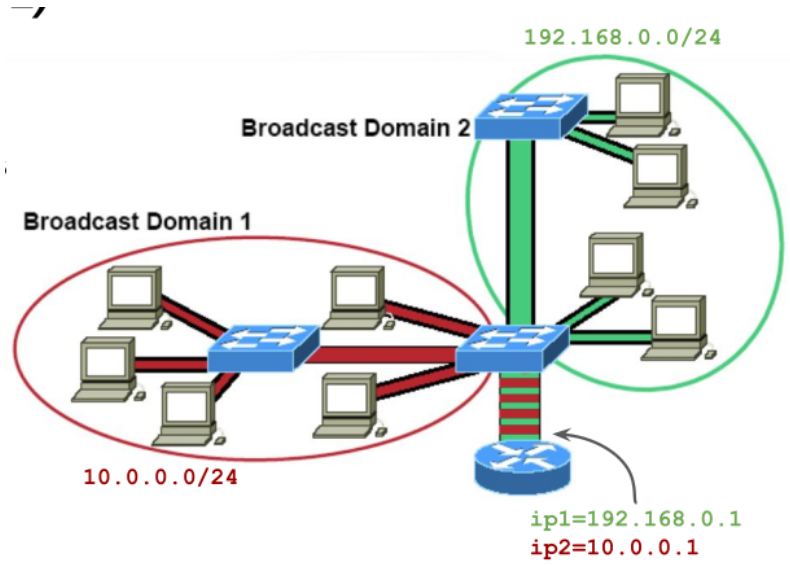

Figura 13: VLAN e sottoreti IP collegate tramite sub-interfacce

Listing 3: Esempio di configurazione router one-armed

```
ip link add link eth0 name eth0.10 type vlan id 10
ip link add link eth0 name eth0.20 type vlan id 20
ip addr add 10.0.10.1/24 dev eth0.10
ip addr add 10.0.20.1/24 dev eth0.20
```

In questo esempio, l'interfaccia fisica `eth0` viene suddivisa in due sub-interfacce virtuali, `eth0.10` e `eth0.20`, rispettivamente associate alle VLAN 10 e 20. A ciascuna sub-interfaccia viene assegnato un indirizzo IP appartenente alla sottorete della relativa VLAN.

In questo modo, il router può fornire servizi di **routing inter-VLAN**, agendo come **gateway predefinito** per ciascuna rete logica, pur utilizzando una sola porta fisica. Tale approccio è comune nei laboratori e negli ambienti di test, dove si vuole semplificare la topologia riducendo il numero di interfacce fisiche necessarie.

3.2 Trasporto dei frame: Tagging IEEE 802.1Q

Lo standard **IEEE 802.1Q** permette di far convivere più VLAN sullo stesso collegamento fisico. Per farlo, inserisce all'interno dei frame Ethernet un piccolo campo aggiuntivo, chiamato *tag VLAN*, che identifica la VLAN di appartenenza del frame. A seconda del tipo di collegamento, gli switch 802.1Q gestiscono questi tag in modo diverso, distinguendo tre tipologie di porte.

3.2.1 Porte di tipo Access, Trunk e Hybrid

- **Access Port:** collega un host finale (ad esempio un PC o una stampante). I frame che transitano su una porta di questo tipo sono sempre *senza tag* (*untagged*). Lo switch associa internamente la porta a una specifica VLAN, aggiungendo o rimuovendo automaticamente il tag durante il transito interno.
- **Trunk Port:** collega due apparati di rete (ad esempio switch–switch o switch–router). Trasporta frame appartenenti a più VLAN contemporaneamente, inviandoli e ricevendoli *con tag* 802.1Q. In questo modo, ciascun frame mantiene l'informazione sulla VLAN di origine anche attraverso un link condiviso.
- **Hybrid Port:** gestisce sia frame *taggati* che *non taggati*. I frame non taggati vengono automaticamente associati alla **Native VLAN**, mentre quelli taggati mantengono il proprio VLAN ID. Questo tipo di porta è utile quando si collegano dispositivi che supportano il tagging VLAN insieme ad altri che non lo supportano.

3.2.2 Access links

Un **Access link** è un collegamento che parte da una **porta di tipo Access**, ossia una porta configurata per appartenere a una singola VLAN. Questo tipo di collegamento è utilizzato per connettere dispositivi finali (come PC, stampanti o server) oppure piccoli hub o switch non gestiti.

I frame che transitano su una porta di tipo Access sono sempre *non taggati* (*untagged*): gli host collegati inviano e ricevono normali frame Ethernet, senza alcuna informazione sulla VLAN. È lo switch che, internamente, associa la porta a una VLAN e gestisce l'inserimento o la rimozione del *tag 802.1Q* quando il frame entra o esce dalla rete VLAN-aware.

In questo modo, i dispositivi connessi non devono essere consapevoli dell'esistenza delle VLAN: dal loro punto di vista fanno parte semplicemente di una rete Ethernet dedicata, tipicamente corrispondente a una specifica sottorete IP.

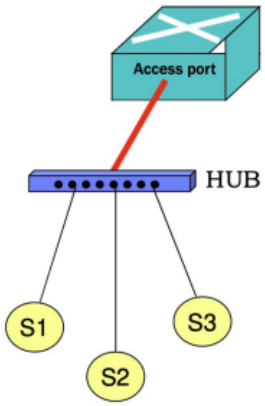

Figura 14: Esempio di collegamento Access link tra host e switch VLAN-aware

3.2.3 Access links nelle regioni legacy

In alcuni contesti, detti **legacy regions**, un access link può estendersi attraverso piccole LAN composte da più switch che non supportano le VLAN (*VLAN-unaware switches*). In questi casi, l'intera rete tradizionale viene vista dallo switch VLAN-aware come un unico segmento Ethernet appartenente a una sola VLAN.

Tutti i dispositivi collegati all'interno di tale regione condividono la stessa VLAN, anche se gli switch intermedi non gestiscono i tag 802.1Q. Questo approccio consente di integrare reti esistenti non VLAN-aware in un'infrastruttura moderna basata su VLAN.

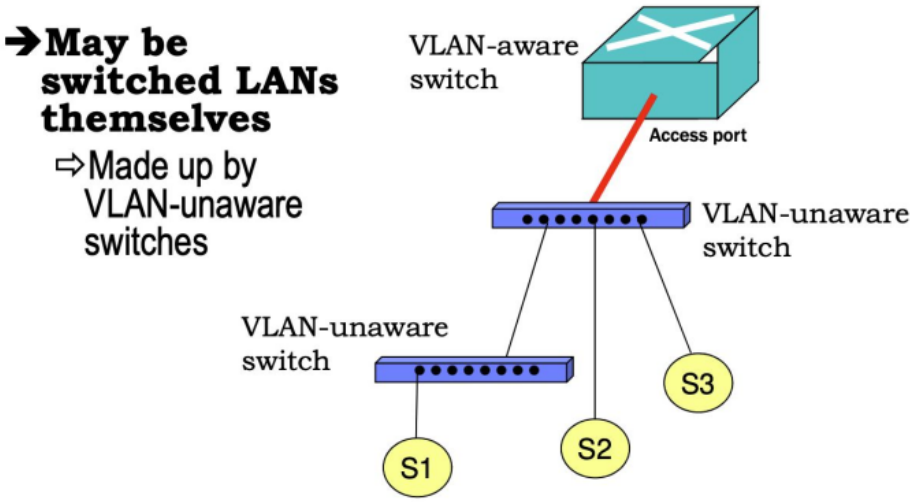

Figura 15: Access link esteso in una regione legacy con switch non VLAN-aware

3.2.4 Trunk links

Un **Trunk link** è un collegamento che parte da una **porta di tipo Trunk**, utilizzato per trasportare frame appartenenti a più VLAN contemporaneamente. È tipicamente impiegato nei collegamenti *switch–switch* o *switch–router*, dove è necessario far transitare traffico di più reti logiche sullo stesso mezzo fisico.

A differenza delle porte Access, le porte Trunk trasmettono e ricevono **frame taggati** con l'identificatore VLAN secondo lo standard **IEEE 802.1Q**. Il tag 802.1Q consente di distinguere

a quale VLAN appartiene ciascun frame, evitando la confusione tra traffici di reti diverse che condividono il link.

Un trunk link **non appartiene direttamente a una VLAN**, ma può trasportare:

- frame provenienti da *tutte* le VLAN configurate sullo switch;
- oppure frame appartenenti solo a un sottoinsieme di VLAN selezionate.

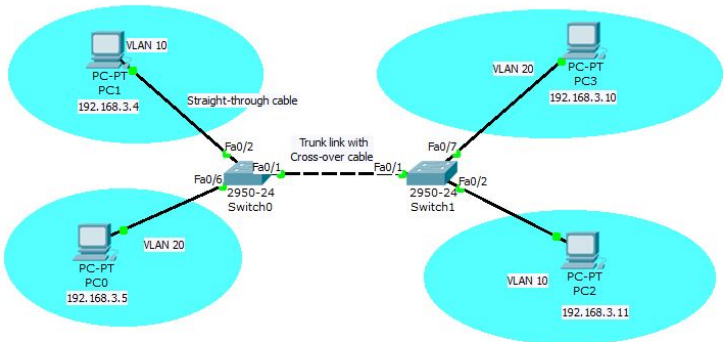

Figura 16: Esempio di collegamento Trunk tra apparati VLAN-aware

3.2.5 Hybrid links

Le **Hybrid links** rappresentano un'evoluzione dei trunk link e supportano sia **frame taggati** sia **frame non taggati**. I frame taggati mantengono il proprio VLAN ID, mentre i frame non taggati vengono associati a una VLAN predefinita (la **Native VLAN**).

Questo tipo di collegamento è utile quando sullo stesso link devono transitare:

- traffici di apparati VLAN-aware (che utilizzano frame taggati);
- e traffici di dispositivi legacy o VLAN-unaware (che inviano frame non taggati).

In sostanza, un hybrid link permette di far convivere traffico VLAN multiplo e traffico Ethernet standard sullo stesso collegamento, garantendo compatibilità tra apparati di diversa generazione. Nelle implementazioni moderne, molti switch trattano di fatto tutti i link come *ibridi*, in grado di gestire dinamicamente entrambe le tipologie di frame.

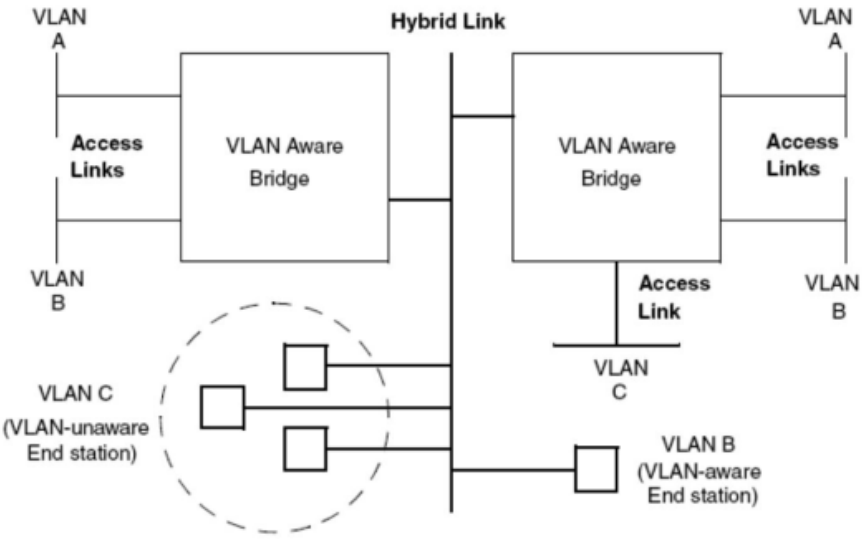

Figura 17: Esempio di Hybrid link che trasporta frame taggati e non taggati

In figura si nota come il collegamento ibrido consenta il transito simultaneo di traffico proveniente da VLAN diverse, includendo anche host non VLAN-aware (VLAN C), senza compromettere la separazione logica delle altre VLAN taggate.

3.2.6 Una stazione può appartenere a più VLAN?

In generale, un host connesso tramite una **Access port** appartiene a una sola VLAN, poiché i frame che transitano su quella porta sono sempre *non taggati* e associati a una singola rete logica.

Tuttavia, è possibile che una stessa stazione appartenga a **più VLAN** contemporaneamente. Questo avviene quando la stazione dispone di una **interfaccia trunk**, in grado di inviare e ricevere *frame taggati 802.1Q* appartenenti a VLAN diverse.

Un caso tipico è quello dei **server multi-VLAN**, che devono comunicare con più reti logiche (o sottoreti IP) attraverso un'unica interfaccia fisica. In tali scenari, il sistema operativo del server crea **sub-interfacce virtuali** (es. `eth0.10`, `eth0.20`), ciascuna configurata con un VLAN ID differente, consentendo la separazione logica del traffico pur utilizzando la stessa scheda di rete.

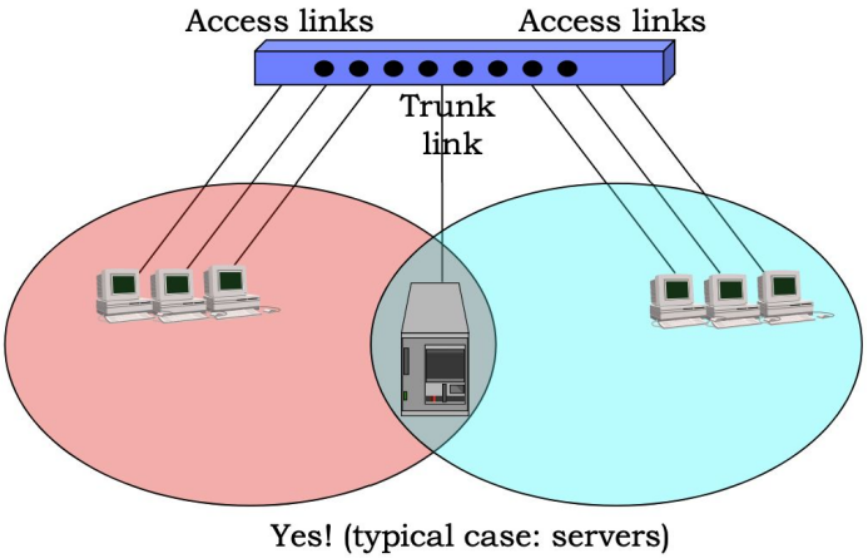

Figura 18: Esempio di stazione connessa a più VLAN tramite interfaccia trunk

In sintesi, solo le stazioni dotate di interfacce *VLAN-aware* possono appartenere a più VLAN: sono esse a gestire il tagging e l'instradamento del traffico tra le diverse reti logiche.

Laboratorio

3.3 Laboratorio 3: Configurazione VLAN e router one-armed

In questo laboratorio si analizza il funzionamento delle VLAN e del **routing inter-VLAN** attraverso un router connesso tramite una singola interfaccia fisica (*one-armed router*). L'obiettivo è comprendere come i frame vengano trasportati attraverso collegamenti di tipo *Access*, *Trunk* e *Hybrid* secondo lo standard IEEE 802.1Q.

Topologia di rete

La rete è composta da:

- uno **switch VLAN-aware** con tre porte configurate come Access (VLAN 10 e 20) e una porta configurata come Trunk verso il router;
- due host collegati alle porte Access, ciascuno appartenente a una VLAN distinta;
- un router configurato con sub-interfacce virtuali (`eth0.10`, `eth0.20`) per fornire connettività inter-VLAN.

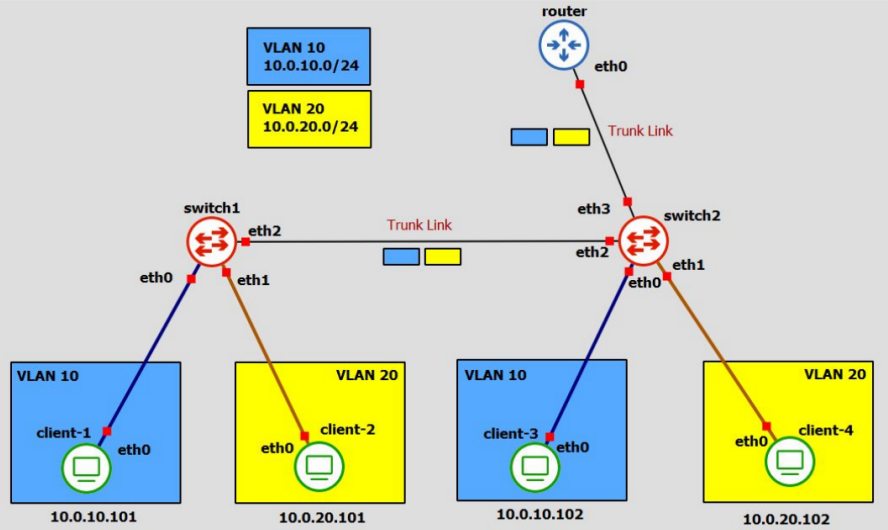

Figura 19: Topologia del Laboratorio 3: VLAN e router one-armed

Configurazione di esempio

Listing 4: Configurazione delle VLAN sul router one-armed

```
# Creazione delle sub-interfacce VLAN
ip link add link eth0 name eth0.10 type vlan id 10
ip link add link eth0 name eth0.20 type vlan id 20

# Assegnazione degli indirizzi IP (gateway delle rispettive VLAN)
ip addr add 10.0.10.1/24 dev eth0.10
ip addr add 10.0.20.1/24 dev eth0.20

# Attivazione delle interfacce
ip link set eth0.10 up
ip link set eth0.20 up
```

Sul lato switch:

Listing 5: Configurazione delle VLAN sullo switch

```
# Creazione VLAN
vlan 10
vlan 20

# Assegnazione delle porte
interface eth1
 switchport mode access
 switchport access vlan 10

interface eth2
 switchport mode access
 switchport access vlan 20

# Porta trunk verso il router
interface eth0
 switchport mode trunk
 switchport trunk allowed vlan 10,20
```

Funzionamento del laboratorio

Il laboratorio ha lo scopo di mostrare in modo pratico il funzionamento delle **VLAN** e del **router one-armed**, ovvero una configurazione in cui un unico collegamento fisico tra router e switch trasporta il traffico di più VLAN tramite **frame taggati IEEE 802.1Q**.

3.3.0.1 Isolamento del traffico Gli host collegati alle **porte Access** appartengono ciascuno a una VLAN distinta. I frame che transitano su queste porte sono *non taggati* e vengono separati dallo switch in base alla VLAN di appartenenza. In questo modo, gli host di VLAN diverse non possono comunicare direttamente: lo switch isola i domini di broadcast e impedisce la comunicazione a livello 2.

3.3.0.2 Routing inter-VLAN Per permettere la comunicazione tra VLAN diverse, il traffico deve passare attraverso il router. La connessione tra router e switch avviene tramite una **porta di tipo Trunk**, che trasporta i frame di più VLAN aggiungendo un tag 802.1Q a ciascun frame. Sul router, l'interfaccia fisica (ad esempio `eth0`) è suddivisa in più **sub-interfacce virtuali** (`eth0.10`, `eth0.20`, ecc.), ognuna configurata con:

- un **VLAN ID** specifico;
- un indirizzo IP che funge da **gateway** per la relativa VLAN.

Quando un host della VLAN 10 invia un pacchetto verso un host della VLAN 20:

1. il frame raggiunge lo switch sulla porta Access e viene inoltrato sul trunk verso il router con tag VLAN 10;
2. il router riceve il frame su `eth0.10`, lo elabora a livello 3 e decide di inoltrarlo sulla sub-interfaccia `eth0.20`;
3. il router rimanda il frame allo switch, questa volta con tag VLAN 20;
4. lo switch rimuove il tag e lo invia alla porta Access corrispondente alla VLAN 20.

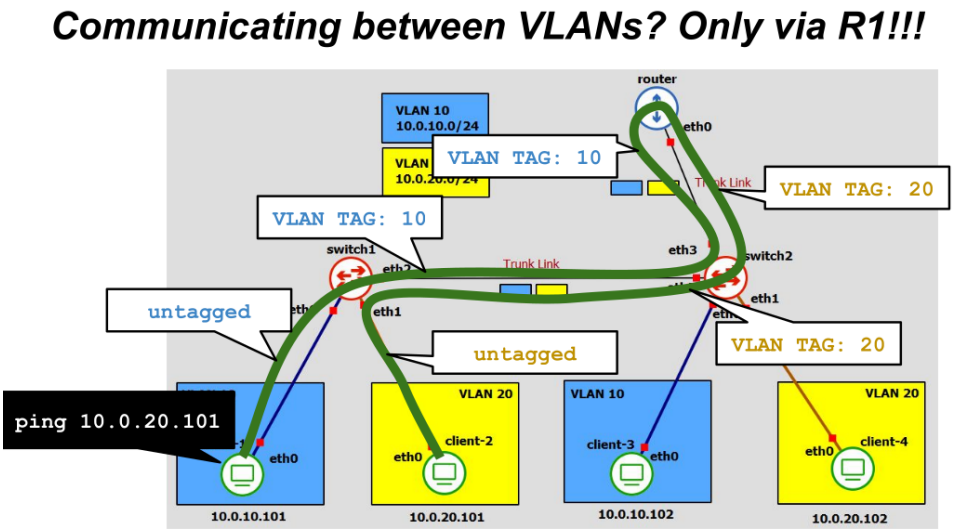

Figura 20: Comunicazione tra diverse vlan

3.3.0.3 Verifica del comportamento Nel laboratorio si può verificare che:

- gli host della stessa VLAN comunicano direttamente a livello 2, senza passare dal router;
- la comunicazione tra VLAN diverse avviene tramite il router (routing inter-VLAN);
- tutto il traffico tra router e switch è trasportato sul link trunk mediante frame taggati 802.1Q.

3.3.0.4 Osservazione pratica Catturando il traffico con `tcpdump` o `Wireshark` sull'interfaccia trunk, è possibile osservare i **tag VLAN** all'interno dei frame Ethernet. Ciò consente di verificare visivamente il meccanismo di separazione e instradamento del traffico tra le diverse VLAN.

3.4 Sicurezza delle VLAN e vulnerabilità di livello 2

Le VLAN migliorano l'isolamento logico del traffico, ma non eliminano le minacce presenti a livello di collegamento. Un attaccante connesso alla rete locale può sfruttare debolezze dei protocolli di livello 2 (Ethernet e ARP) o configurazioni errate degli switch per intercettare, modificare o dirottare il traffico di rete.

3.4.1 Minacce principali

3.4.1.1 1) MAC Flooding (CAM Overflow) Gli switch mantengono in memoria una **Content Addressable Memory (CAM)**, che associa indirizzi MAC a porte fisiche. Un attaccante può inviare migliaia di frame con indirizzi MAC falsi, riempiendo la tabella CAM e provocando un *overflow*. Quando la tabella è satura, lo switch non riesce più a determinare su quale porta si trova un determinato MAC e inizia a inoltrare i frame in **broadcast**, esponendo il traffico all'attaccante.

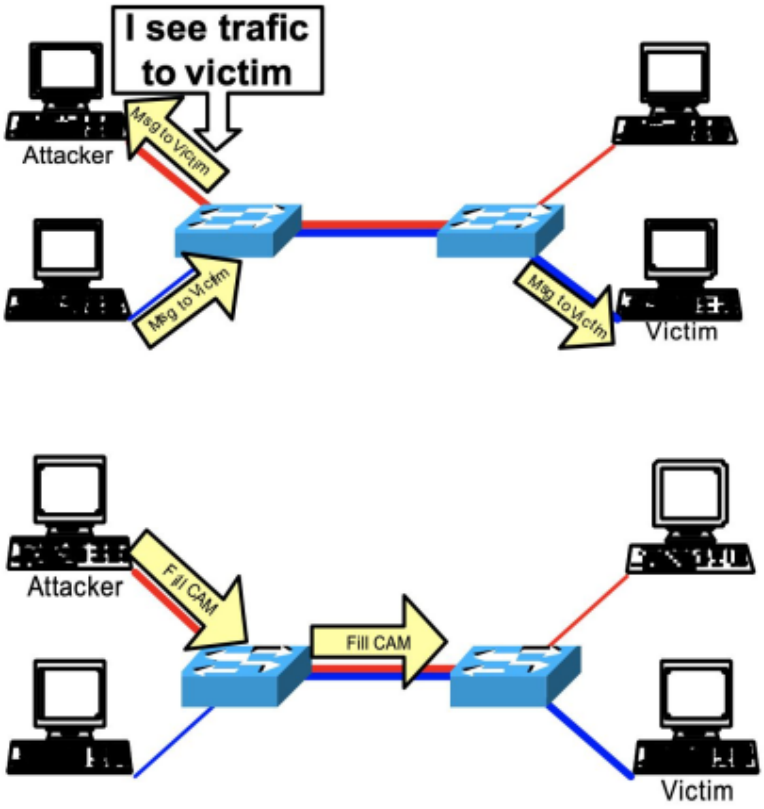

Figura 21: Esempio di MAC flooding

Mitigazione: abilitare la **port security**, limitando il numero di MAC address appresi per ciascuna porta, e disattivare l'apprendimento dinamico dove non necessario.

3.4.1.2 2) ARP Spoofing / Poisoning Il protocollo ARP non prevede autenticazione, quindi un attaccante può inviare **risposte ARP falsificate** per associare il proprio MAC all'indirizzo IP del gateway o di altri host nella stessa VLAN. In questo modo, intercetta o altera il traffico tra due dispositivi (*Man-in-the-Middle*).

Mitigazione: configurare **ARP statici** per i dispositivi critici, utilizzare strumenti di monitoraggio come `arpwatch` o implementare sistemi di protezione come `Dynamic ARP Inspection (DAI)` sugli switch gestiti.

3.4.1.3 3) VLAN Hopping Questa categoria di attacchi consente a un host di inviare o ricevere traffico appartenente a una VLAN diversa da quella assegnata, violando l'isolamento logico. Le due tecniche principali sono:

- **Basic VLAN hopping:** l'attaccante sfrutta il protocollo DTP (*Dynamic Trunking Protocol*) per negoziare automaticamente una connessione di tipo trunk con lo switch, ottenendo accesso a più VLAN.

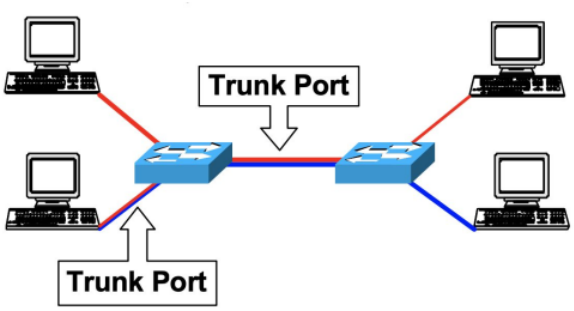

Figura 22: Collegamento tra due switch tramite porte trunk che trasportano il traffico di più VLAN sullo stesso link fisico.

- **Double Tagging:** il frame viene costruito con due tag 802.1Q annidati. Il primo tag (relativo alla VLAN nativa) viene rimosso dallo switch di ingresso, lasciando il secondo, che identifica la VLAN bersaglio.

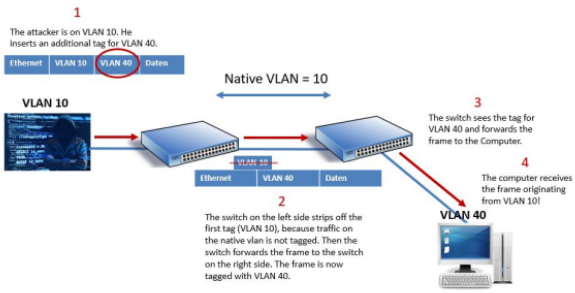

Figura 23: Esempio di attacco **VLAN Double Tagging**: un host malevolo appartenente alla VLAN 10 inserisce due tag 802.1Q (VLAN 10 e VLAN 40). Il primo switch rimuove il tag della VLAN nativa (10) e inoltra il frame, che conserva il secondo tag (40). Il frame attraversa quindi il trunk ed entra nella VLAN 40, violando l'isolamento tra VLAN.

Mitigazione: disabilitare DTP e configurare manualmente le porte come **Access** dove necessario; evitare l'uso della **VLAN 1** come VLAN nativa e assegnare VLAN native dedicate non utilizzate per il traffico utente.

3.4.1.4 4) Attacchi ai protocolli di controllo Oltre agli attacchi diretti alle VLAN, anche i protocolli di **controllo e gestione** utilizzati dagli switch di livello 2 possono essere sfruttati

da un attaccante per alterare la topologia della rete o raccogliere informazioni sensibili. Tra i principali:

3.4.1.4.1 Spanning Tree Attack (BPDU spoofing)

- **Cosa fa lo STP:** gli switch si scambiano BPDU (bridge protocol data units) per eleggere il *root bridge* e stabilire quali porte siano forwarding o blocking, evitando loop.
- **Come attacca l'avversario:** l'attaccante invia BPDU falsi con una priorità molto bassa (o con un bridge ID fittizio), facendo credere agli switch che il suo dispositivo sia il nuovo root.
- **Effetto pratico:** la topologia si ricalcola; alcuni link possono essere forzati in forwarding creando percorsi non previsti, perdita di connettività o instradamento del traffico attraverso il nodo dell'attaccante.
- **Mitigazione:** *BPDU Guard* spegne la porta se riceve BPDU su una porta che dovrebbe essere una porta access (cioè verso host), mentre *Root Guard* impedisce a un certo segmento di diventare root forzando il comportamento previsto.

3.4.1.4.2 VTP Attack (VLAN Trunking Protocol)

- **Cosa fa VTP:** permette di distribuire automaticamente la lista delle VLAN a tutti gli switch del dominio VTP.
- **Come attacca l'avversario:** un dispositivo malevolo si presenta come `server VTP` con una *revision number* superiore; gli altri switch accettano la nuova configurazione e sovrascrivono le VLAN locali.
- **Effetto pratico:** le VLAN possono essere cancellate o modificate su larga scala, causando indisponibilità o perdita dell'isolamento tra reti.
- **Mitigazione:** impostando VTP in *transparent* o disabilitandolo si evita che uno switch accetti e propaghi automaticamente configurazioni provenienti da fonti non affidabili.

3.4.1.4.3 Cisco Discovery Protocol Attack (information leakage)

- **Cosa fa CDP:** i dispositivi Cisco pubblicano informazioni (IP, modelli, versioni) su CDP verso i vicini.
- **Come attacca l'avversario:** un host malintenzionato cattura i pacchetti CDP o ascolta il traffico e ottiene dettagli utili per attacchi mirati (es. versioni vulnerabili).
- **Effetto pratico:** ricognizione facilitata: l'attaccante conosce quali dispositivi e software colpire.
- **Mitigazione:** disabilitando CDP sulle porte utenti si riduce la quantità di informazioni esposte ai terminali non fidati.

Laboratorio

3.5 Laboratorio 4: VLAN Hopping e Double Tagging

3.5.1 Scenario

L'obiettivo del laboratorio è simulare un attacco di **Double Tagging**, in cui un host appartenente alla VLAN nativa tenta di raggiungere host di un'altra VLAN senza passare per il router.

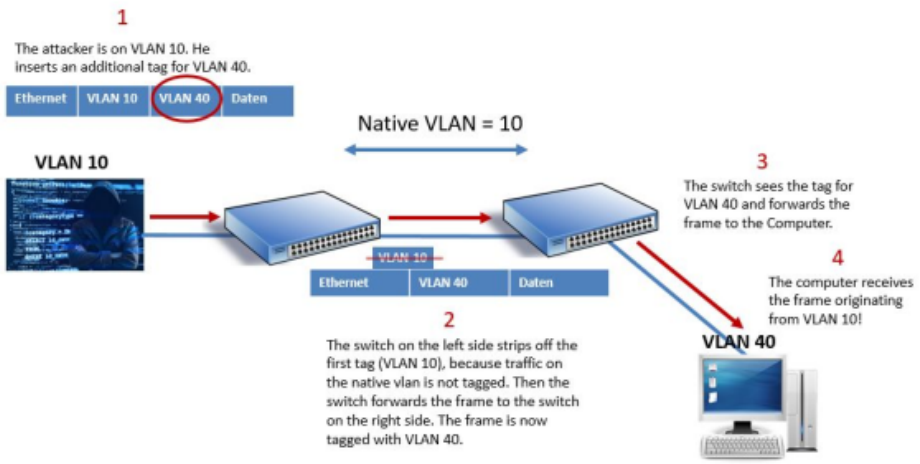

Figura 24: Attacco Double Tagging su trunk VLAN nativa

3.5.2 Configurazione di attacco

Listing 6: Esempio pratico di doppio tagging

```
ip link add link eth0 name eth0.1 type vlan id 1
ip link set eth0.1 up
ip link add link eth0.1 name eth0.1.20 type vlan id 20
ip link set eth0.1.20 up
ip addr add 10.0.20.250/24 dev eth0.1.20
arp -s 10.0.20.102 <MAC-vittima> -i eth0.1.20
ping 10.0.20.102
```

Questo attacco è tipicamente **unidirezionale**: l'attaccante può inviare pacchetti verso la VLAN vittima, ma non ricevere risposte.

3.5.2.1 Mitigazioni

- disabilitare l'auto-trunking (DTP) sulle porte utente;
- non usare VLAN 1 come nativa;
- assegnare VLAN nativa diversa e dedicata solo ai trunk;
- monitorare traffico anomalo su frame doppiamente taggati.

3.6 Autenticazione e controllo d'accesso: IEEE 802.1X

3.6.1 Architettura e funzionamento

IEEE 802.1X definisce un meccanismo di autenticazione basato su porta. Il modello coinvolge tre componenti:

- **Supplicant:** l'host che richiede accesso alla rete;
- **Authenticator:** lo switch o access point che funge da intermediario;
- **Authentication Server:** tipicamente un server RADIUS che verifica le credenziali.

Il protocollo utilizza EAPOL (EAP over LAN) per trasportare le credenziali di autenticazione a livello 2, prima dell'assegnazione IP. Una volta autenticato, l'utente può essere automaticamente assegnato a una VLAN o a specifiche ACL in base all'identità verificata.

3.6.1.1 Vantaggi

- garantisce accesso controllato alle VLAN;
- permette la **VLAN dinamica per utente**;
- si integra con firewall e sistemi NAC per gestione centralizzata.

3.7 Firewall e sicurezza perimetrale

3.7.1 Ruolo del firewall

I firewall rappresentano il principale punto di controllo tra VLAN e verso Internet. Esistono due principali categorie:

- **Packet filtering:** filtra i pacchetti in base a indirizzi, porte e protocolli.
- **Stateful inspection:** tiene traccia dello stato delle connessioni (es. TCP SYN/ACK) consentendo solo traffico di risposta legittimo.

3.7.1.1 Implementazione in Linux Il framework **Netfilter** del kernel Linux implementa le funzioni di firewalling. Il comando `iptables` consente di creare regole di filtraggio e NAT per gestire le comunicazioni tra VLAN e verso l'esterno.

Listing 7: Esempio di filtraggio stateful tra VLAN

```
# Permetti traffico dalla VLAN 10 alla VLAN 20
iptables -A FORWARD -i eth0.10 -o eth0.20 -m state --state ESTABLISHED,RELATED -j
    ACCEPT
iptables -A FORWARD -i eth0.20 -o eth0.10 -j ACCEPT
```

Conclusioni

Le VLAN rappresentano un meccanismo fondamentale di segmentazione logica, riducendo il dominio di broadcast e migliorando ordine e sicurezza. Tuttavia, se configurate in modo errato, possono introdurre vulnerabilità specifiche (es. trunk non protetti o VLAN nativa mal gestita). Una corretta progettazione prevede:

- configurazione manuale e controllata delle porte trunk;
- uso di VLAN dedicate per la gestione e di VLAN nativa distinta da quelle operative;
- integrazione con 802.1X, ACL e firewall per garantire isolamento e autenticazione a ogni livello.