Layer 2: Le Fondamenta della Network Security

di Marco Misitano, pubblicato si ICT Security

I grattacieli si costruiscono su fondamenta. Tanto piu robuste quanto piu' il grattacielo dev'essere alto, e credo che sia un concetto condiviso da tutti. Le soluzioni di sicurezza ad oggi integrano filtraggio del traffico, connettivitá sicura, rilevamento e prevenzione delle intrusioni, controllo, blocco e disinfezione dei virus, autenticazione e molto altro. Sono soluzioni complesse ed articolate, ciononostante vi e' una tendenza diffusa a costruirle dimenticandosi delle fondamenta, o non dando a queste l'opportuna importanza. Le reti sono costruite secondo dei moduli indipendenti ma fra di loro interconnessi e che si appoggiano l'uno sull'altro secondo quanto definito nel modello OSI (figura 1). I livelli piu' alti di questo modello fanno affidamento su quelli piu bassi per la comunicazione, cosi' per una connessione ad esempio HTTP ci si appoggera' via via agli strati piu bassi, i quali faranno in modo che le informazioni da noi richieste vengano opportunamente codificate e modulate sul mezzo fisico grazie al quale siamo collegati alla rete. Le considerazioni che seguiranno in questo articolo, salvo esplicite eccezioni si riferiranno a topologia ethernet, la piu usata nelle reti locali. Molte di queste considerazioni non sono state di fatto rilevate *in the wild*, ciononostante nulla ci lasci credere che cio che e' stato verificato su una LAN non possa trovare applicazioni piu ampie.

Il Livello 2 (Data Link Layer) fornisce il servizio di trasferimento affidabile dei dati su di un mezzo fisico. Le specifiche di questo layer includono indirizzamento fisico, notifica degli errori, topologia, modalita' di sequenza dei frame (si definisce *frame* un elemento di layer 2, come si definisce *pacchetto* un elemento di layer 3) e controllo del flusso. L'indirizzamento fisico, analogamente all'indirizzamento di rete proprio del livello 3, definisce le modalità con le quali avviene l'indirizzamento dei dispositivi e si basa sugli indirizzi **MAC** (Media Access Control) che hanno una lunghezza di 48 bit ed il formato 12:34:56:78:9A:BC. La notifica degli errori si fa carico di notificare i livelli superiori eventuali errori di trasmissione. La topologia di rete comprende le specifiche che definiscono come i dispositivi sono fisicamente connessi (topologia bus oppure ring), la sequenza dei frame si occupa di rimettere in sequenza frame che siano stati trasmessi fuori sequenza, mentre il controllo del flusso gestisce la trasmissione dei dati in modo tale che un dispositivo ricevente non sia sommerso da flussi di dati superiori alla soglia che può gestire. Recentemente c'e' stata la diffusione delle virtual LAN (VLAN) che permettono, gia a livello 2, di segmentare contesti virtuali di livello 3 in maniera tale, sullo stesso mezzo fisico, di avere diverse reti, virtualmente senza alcun collegamento l'una con l'altra. Gli Switch stessi, che sono devices che nella loro implementazione classica operano a livello 2, si fanno carico di segmentare il traffico, creando dei collegamenti virtuali, fra due host che si parlano, in modo tale da non 'disturbare' altri host sullo stesso segmento di rete. Questo livello del networking e' cosi' trasparente e poco visibile, che molto spesso si tende a darlo per scontato e funzionante, dimenticandosi che su di esso si appoggiano tutte le funzionalita' dei livelli superiori, ed ovviamente anche la sicurezza di questi. Compromettere o

modificare le modalita' di funzionamento del layer 2 significa compromettere tutto quello che su questo si appoggia, a parte quindi le segnalazioni elettriche del cablaggio, tutto. Compromettere il livello 2 significa avere il potere di innescare un effetto domino che puo invalidare ogni accorgimento di sicurezza dei livelli soprastanti.

Attacchi basati su MAC address

I MAC address sono gli indirizzi fisici, unici e statici dei dispositivi, a differenza ad esempio degli indirizzi di rete IP non sono configurabili a piacimento. Tipicamente e' uno switch a connettere fisicamente i diversi dispositivi, ed il principio di funzionamento di uno switch, che come si e' gia detto si occupa di segmentare il traffico creando dei circuiti virtuali tra due host al momento in cui dialogano e' molto semplice: lo switch impara dinamicamente quale indirizzo MAC e' attaccato a quale delle sue porte. Supponiamo che in una fase iniziale sappia che il MAC dell'host A e' collegato alla porta 1 e null'altro. Al momento in cui (figura 2) l'host A - del quale lo switch conosce gia MAC e porta sul quale è collegato - vorrà dialogare con l'host B - del quale lo switch invece non conosce nulla -, esso inviera' il frame proveniente da A, a tutti gli host, compreso lo host C che non e' il destinatario. Non appena l'host B risponderà ad A, lo switch percepirà il MAC address di B, ed avrà imparato che questo si trova attaccato alla porta 2. Ed in futuro evitera' il broadcast iniziale. In questo modo l'host C non vedra' piu il traffico non specificatamente destinato a se stesso salvo questa fase di *learning* da parte dello switch. Semplificando, le informazioni di quale MAC address sia attaccato a quale porta vengono mantenute dallo switch dinamicamente in una tabella alla quale si da il nome di **CAM** (content addressable memory) **Table**. Essendo dinamica ed avendo una memoria di allocazione finita, da questa tabella sono cancellati i dati piu vecchi per far posto a quelli piu nuovi. Il **CAM Overflow** e' un attacco che mira a dare all'host C la visibilita' sempre e di tutto il traffico, effettivamente bypassando la segmentazione che lo switch e' preposto a fare. La tecnica e' quella di mantenere sempre satura questa tabella sempre piena con nuovi record (falsi), facendo 'sentire' allo switch la presenza di migliaia di indirizzi MAC attaccati ad una porta, grazie ad un generatore di MAC address. Lo switch si trovera' quindi nella situazione iniziale di non sapere quale host e' attaccato a quale porta e fara' il broadcast del frame. Si comporterá di fatto come uno hub e tutti vedranno il traffico diretto a chiunque. La sicurezza quindi creata dalla segmentazione del traffico da parte dello switch e' di fatto persa, e tutti i protocolli di piu alto livello (FTP, Telnet, POP3, HTTP...) essendo visibili da tutti saranno soggetti ad attacchi **Man In the Middle** perdendo quindi la confidenzialita', dato che sara' estremamente semplice con uno sniffer avere accesso ad esempio alle password che su questi protocolli viaggiano. Va da se che diversi switch hanno diverse risposte a questo tipo di attacco, ma in linea di massima tutti possono essere suscettibili a questa tecnica. Esistono soluzioni? Certamente si! Funzionalita' specifiche permettono di limitare o comunque controllare il fenomeno del MAC Learning, vale a dire il processo per il quale uno switch 'impara' quale MAC address e' attaccato a quale porta. Si puo infatti **limitare il numero di MAC address per porta**, scartando quelli in soprannumero ed in caso di superamento di questo limite la porta dello switch puo' essere configurata per bloccare lo specifico MAC address in piu o anche per chiudere totalmente la porta che non dara' piu connettivitá. Un'altra tecnica di

prevenzione e' quella dell'utilizzo di **Port Security**, modalita' nella quale si stabilisce staticamente quali MAC address possono attaccarsi a quali porte e non verra' accettato nessun frame proveniente da MAC address differenti. E' certamente una maniera molto drastica e che presuppone una grande pazienza nel definire l'accesso alle risorse, ma e' il modo in cui si ha la migliore certezza di prevenire il **CAM Overflow**; sicuramente una considerazione fattibile in presenza di poche e molto critiche macchine, ad esempio data center ecc..

Attacchi basati su ARP

ARP (Address Resolution Protocol) e' il protocollo che si occupa della risoluzione degli indirizzi di rete di livello 3 (indirizzi IP, per esempio) in indirizzi di livello 2 (indirizzi MAC) . Il principio di funzionamento e' molto semplice (figura 3): Quando l'host W vuole comunicare con l'host Y ad esempio con protocollo IP, W inviera' un pacchetto IP con il proprio indirizzo IP sorgente e l'indirizzo IP di destinazione che sara' quello di Y, questo secondo lo schema di comunicazione del livello 3. A livello 2, la comunicazione per avvenire dovra' basarsi sugli indirizzi MAC, quindi verra' inviata una *ARP request* in broadcast a tutti i computer della rete locale. Ogni computer esaminera' questa richiesta e se scopre di essere il vero destinatario, rispondera' e comunichera' il suo indirizzo MAC, come fará Y (figura 3), altrimenti ignorerà la richiesta. A questo punto, W manterra' in memoria l'informazione contenente la mappatura fra l'indirizzo IP ed il MAC address. L'insieme di queste informazioni si definisce ARP table, e risiedera' ella memoria di ogni host. Cosa succede al momento in cui uno host riceve una informazione ARP che non ha richiesto ? Si parla in questo caso di **Gratuitous ARP** ed il comportamento della maggior parte dei sistemi operativi al momento in cui ricevono una informazione che non hanno richiesto e che recita all'incirca "*il mio indirizzo IP e' 1.2.3.4 ed il mio MAC address 12:34:56:78:9A:BC* ", **la prenderanno per buona**, aggiornando la loro ARP table con la nuova informazione. Questo comportamento puo certamente essere sfruttato per reinstradare il traffico a piacimento dell'attaccante. Supponiamo (figura 4) che l'host W invii, ad intervalli regolari, ogni qualche secondo l'informazione " *sono 1.2.3.1 ed il mio mac e' …* ", sostenendo dunque di essere il gateway della LAN (il router, nella figura), ma con il suo **effettivo** MAC address. Verosimilmente gli host X e Y prenderanno per buona l'informazione. Tutte le volte che cercheranno di stabilire una connessione con uno host che non risiede sulla stessa LAN, si affideranno al gateway, o meglio, crederanno di farlo, perché in realta' staranno inviando le informazioni all'host W. Questo non solo ha riceve le informazioni destinate al gateway, puo' anche inviarle successivamente al vero gateway, sia integre che modificate a suo piacimento! Anche in questo caso, con una tecnica di **ARP Spoofing**, si e' arrivati ad un attacco **Man In the Middle**, con addirittura la possibilita' di modificare il traffico in passaggio e inviarlo verso la effettiva destinazione. L'host che genera il traffico originale non nota assolutamente nulla di strano. Che fare per minimizzare il problema ? In questo caso la **Port Security** gia discussa, non aiuta molto, se non a garantire che solo determinati PC abbiano accesso alla rete. E' possibile istruire ogni host a mantenere una **ARP Table statica** in modo da legare indirizzi IP e MAC, questo comporta un significativo sforzo da parte dell'amministratore di rete per distribuire a tutti gli host questa tabella, ciononostante questo e' fattibile in ambienti piccoli e ad alta criticita' come ad esempio specifici server di data center. Da non

dimenticarsi inoltre che alcuni sistemi operativi, pur mantenendo un'ARP table statica, ricevendo informazioni dinamiche, la sovrascriveranno, intendendo che le informazioni appena ricevuta siano piu aggiornate. La **ARP Inspection** e' una funzionalita' di alcuni tipi di switch di permettere o meno determinato tipo di traffico ARP in base alla sorgente ed alla destinazione. Uno strumento dunque efficace per limitare l'arrivo a destinazione di informazioni false e mirate allo **ARP Spoofing**. Lo svantaggio di **ARP Inspection** e' quello di essere disponibile solo su alcuni switch e con particolari versioni del software. Anche le **Private VLAN** possono dimostrare efficacia nel contenere Gratuitous ARP e ARP Spoofing. Una **Private VLAN** e' una VLAN nella quale tutti gli host, pur avendo lo stesso spazio di indirizzamento, non possono direttamente parlare fra di loro, non senza passare attraverso un device di livello 3, che puo' quindi filtrare il traffico in maniera molto piu granulare. Non puo quindi esserci traffico di livello 2 fra questi pur appartenenti alla stessa VLAN. All'interno di una Private VLAN un'host, gia a livello 2 puo' "parlare" solamente con il proprio gateway.

Bypass delle VLAN

Si e' parlato della utilità delle VLAN nel separare, sullo stesso mezzo fisico, diverse sottoreti. Le VLAN sono dunque un meccanismo, di livello 2, di separazione di diversi contesti. Il funzionamento delle VLAN si basa prevalentemente sullo standard **802.1q** che prevede l'utilizzo di una etichetta (tag) su ogni frame, in modo da distinguere la VLAN di appartenenza del frame. Alcune porte degli switch danno accesso solo ad alcune VLAN, mentre altre portano tutte le VLAN che uno switch gestisce. Queste si chiamano **trunk port**, ed un **trunk** e' un collegamento che porta svariate VLAN, ad esempio trasportandole da uno switch all'altro. Per una piu semplice gestione dei trunk e delle porte si utilizza il **Dynamic Trunk Protocol (DTP)** che automatizza la configurazione delle porte con riguardo alle VLAN alle quali devono dare accesso. Porte trunk dello stesso switch possono essere configurate in modalità diverse in base al loro comportamento durante la negoziazione del trunk con una altra porta. Le modalità possono essere :"auto" (la porta si adegua a qualsiasi richiesta) , "on" (la porta vuole essere trunk e non negozia), "off" (la porta non vuole essere trunk e non negozia), "desirable" (la porta gradirebbe comportarsi come trunk se l'altra parte e' d'accordo), "non-negotiate" (la porta vuole essere trunk in una modalita' ben definita e non e' disposta a negoziare). Va da se che la modalitá "auto" e' il default su molti switch, e che, mediante l'invio di opportune segnalazioni **DTP**, un qualsiasi host attaccato ad una qualsiasi porta in modalità "auto" puo' far si che questa diventi una **trunk port** e invii all'host stesso traffico originariamente destinato ad altre VLAN. In questo modo il PC sará membro virtualmente di tutte le VLAN ed avra'accesso al traffico anche non a lui destinato! Su questa considerazione si basa un famoso studio della sicurezza delle VLAN pubblicato dal SANS institute nel 2000 (vedi referenze), che presuppone comunque una porta configurata in modalita' favorevole alla negoziazione dello stato di **trunk**. La soluzione? Semplicissima, evitare di configurare in modalita' favorevole le porte che si sa che non dovranno mai funzionare in trunk mode.

Piu interessanti sono le considerazioni in risposta alla domanda **e' possibile "saltare" da una VLAN ad un'altra senza farne parte?** Certamente. Si e' detto che cio che differenzia un frame nell'appartenenza ad una o ad un'altra VLAN e' l'etichetta **802.1q**. Lo switch tipicamente processa in hardware queste etichette, le

rimuove al momento di instradare su di una VLAN e quindi invia il pacchetto sulla VLAN corretta. Consideriamo (figura 5) due switch A e B sui quali si attestano una VLAN "gialla" ed una VLAN "rossa" e collegati fra di loro con un **trunk** che le porta entrambe. Gli host W e Z non avranno accesso agli host X ed Y secondo le definizioni di funzionamento date. Supponiamo pero' che l'host W invii una frame con una doppia etichetta 802.1q, una rossa ed una gialla,come illustrato nella freccia (1). Lo switch A al ricevere questo frame, toglierá la prima etichetta 802.1q e lo invierá sul trunk (2). Lo switch B al ricevere questo frame con l'etichetta gialla dal trunk, instraderá il frame sulla VLAN gialla, (3) dopo avergli tolto la seconda etichetta. Il pacchetto contenuto nel frame originale e' quindi arrivato a destinazione su di una VLAN diversa. Di tutte le tecniche questa e' probabilmente la piu accademica e la meno utile. Il pacchetto infatti puo' arrivare a destinazione, ma non tornare indietro, non essendo l'host Y preparato ad inviare frame con doppia etichetta. Soluzioni comuni al VLAN bypass sono di **disabilitare il DTP** laddove non e' strettamente necessario, **scegliere con criterio le modalita' di autonegoziazione delle porte**, evitando modalita' automatiche e semiautomatiche quanto possibile, scegliere di **usare la tag 802.1q anche sulla VLAN nativa** (il default e' di non usare etichetta se si e' sulla stessa VLAN di appartenenza).

Spanning Tree Protocol

Il protocollo **Spanning Tree (STP)** si occupa di mantenere una topologia senza circoli chiusi, aprendo e chiudendo determinate porte degli switch all'occorrenza, evitando cosi' che il traffico di rete resti pericolosamente in un circolo chiuso. Allo stesso modo, al momento in cui ce ne fosse bisogno, lo STP puo' ricalcolare la topologia della rete, modificandola in modo tale da sopperire a guasti hardware. Lo STP durante il suo funzionamento elegge a "root" uno switch che orchestrerà il il modo di operare del protocollo stesso. Se ci domandiamo se STP possa avere implicazioni di sicurezza, la risposta è ancora una volta si. Un attaccante potrebbe deliberatamente mandare segnalazioni STP agli switch, in modo tale da far ricalcolare la topologia di rete e reinstradare parte o tutto il traffico attraverso se stesso, guadagnando ancora una volta lo status di **Man In the Middle**. Per il contenimento di problemi basati su sovversioni dello STP, Cisco Systems ha dotato i propri switch di due funzionalita' particolarmente efficaci nell'indirizzare questa esigenza. Le segnalazioni sulle quali si basa lo STP sono le cosiddette Bridge Protocol Data Unit (BPDU) ed e' implementabile una funzionalita' denominata **BPDUGuard** che permette ai progettisti di reti di stabilire dei perimetri predefiniti di topologia, minimizzando le variazioni di questa ed evitando che il ricalcalo della topologia possa assumere forme impreviste o indesiderate. Allo stesso modo la funzionalità **RootGuard** fa si che l'elezione del **root bridge** sia limitata ad uno scenario prevedibile, impedendo anche in questo caso che la rete assuma topologie impreviste.

Mentre gli scenari esaminati sono i piu pericolosi, questi non sono da considerarsi la totalita' dei problemi che potrebbero manifestarsi al layer 2. Questi, assieme ad altri processi di questo livello come **Cisco Discovery Protocol (CDP)**, **Dynamic Host Configuration Protocol (DHCP)**, ed altri ancora devono farci considerare la solidita' delle fondamenta sulle quali costruiamo la sicurezza di livello applicativo, e di rete, che possono essere invalidate da una totale disattenzione verso i livelli piu bassi.

Interessanti studi sono stati fatti, in particolare sull'ARP in una sua implementazione sicura, il Secure ARP (S-ARP) assodato che il suo livello di sicurezza attuale e' tutta'altro che sufficiente. Anche il framework di autenticazione 802.1x che permette la autenticazione degli utenti prima di dare loro accesso alla rete ha un ruolo di importanza crescente, vista la diffusione degli accessi di rete ovunque e per chiunque nelle grandi aziende. E, come sempre, valgono le regole d'oro della sicurezza: **Conoscere perfettamente il funzionamento delle tecnologie che si implementano** e **negare tutto cio che non e' esplicitamente necessario e permesso.** Anche in questo caso, i default possono non essere la migliore scelta da un punto di vista della sicurezza. Di recente anche i tradizionali Intrusion Detection Systems (IDS) rilevano attacchi come quelli citati in questo articolo, e se correttamente implementate le funzionalità, il layer 2 puo' fornirci il massimo livello di confidenzialita', integrita', disponibilità e separazione dei dati, sul quale costruire la politica di sicurezza aziendale, grazie a sempre piu raffinate funzionalita' di controllo di comportamenti anomali a questo livello.

Referenze:

Douglas E. Comer : Internetworking with TCP/IP,
Vol. I, Cap. 11 "Protocol Layering"

Cisco Systems: Introduction to the internet
http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm

@stake: Secure Use of VLANs: An @stake Security Assessment
http://cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf

A. Ornaghi : Studio e analisi degli attacchi "ARP poisoning" e delle possibili contromisure
http://alor.antifork.org/projects/s-arp/thesis.pdf

D. Bruschi, A. Ornaghi, E. Rosti : S-ARP: a Secure Adderess Resolution Protocol
http://www.acsac.org/2003/papers/111.pdf

Cisco systems: Application note, SAFE Enterprise Layer 2 Addendum
http://cisco.com/warp/public/cc/so/cuso/epso/sqfr/sfblu_wp.pdf

SANS Institute: Are there Vulnerabilites in VLAN Implementations?
http://www.sans.org/resources/idfaq/vlan.php

FIGURE

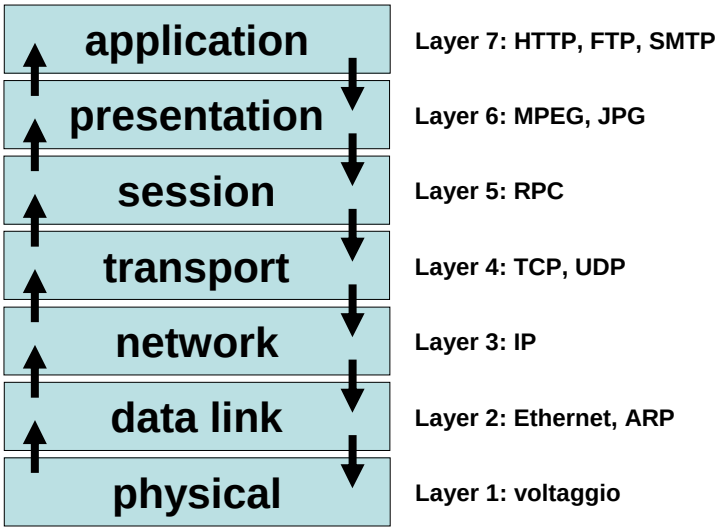

figura 1:
il modello OSI

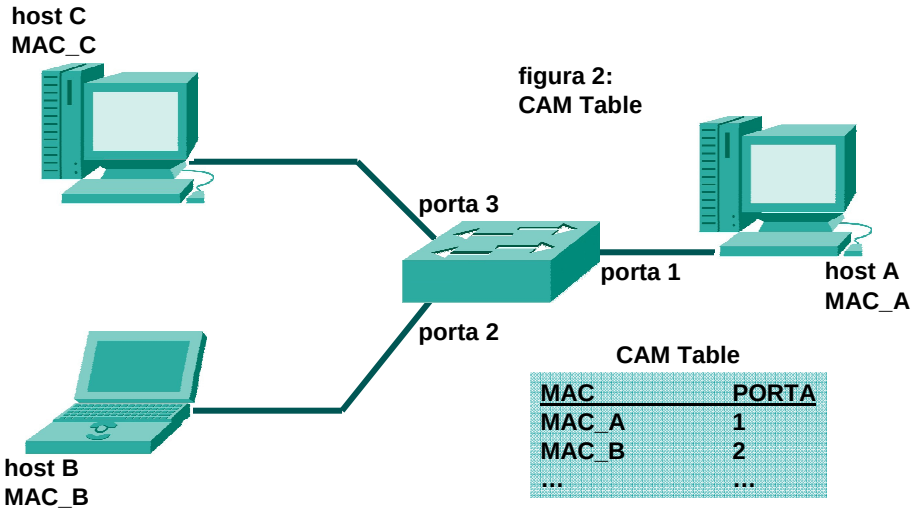

figura 2:
CAM Table

CAM Table

MAC	PORTA
MAC_A	1
MAC_B	2
...	...

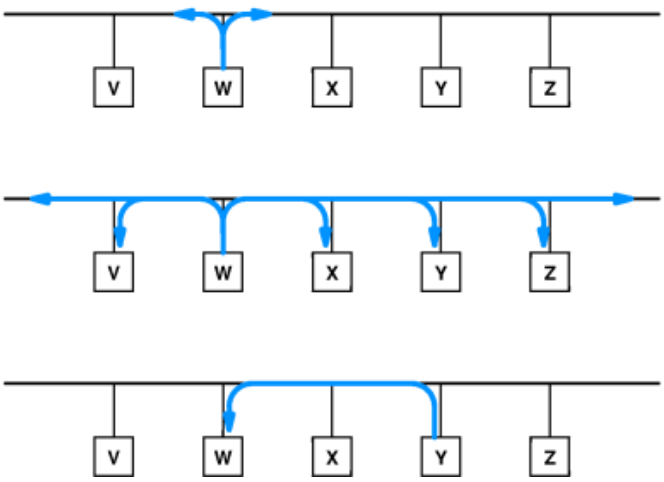

figura 3:
ARP Request

figura 4:
Gratuitous ARP

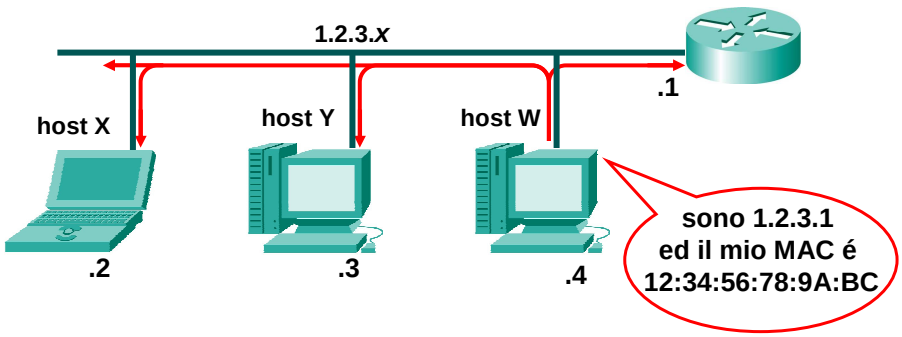

figura 5:
VLAN “hopping”