Axhenti
alessandro

SISTEMI E RETI

Stp, vlan, firewall e acl

STP: IL PROTOCOLLO DI COMUNICAZIONE TRA GLI SWITCH

1. Reti locali "segmentate"

Le moderne reti locali sono segmentate tramite switch, suddividendo la rete in segmenti più piccoli per:

- Isolare il traffico tra i segmenti
- Aumentare la larghezza di banda per ogni dispositivo
- Creare domini di collisione più piccoli

Un **dominio di collisione** è l'area in cui possono verificarsi collisioni di dati. Se cinque computer condividono lo stesso mezzo, i dati inviati da uno possono collidere con quelli di un altro.

L'uso di switch migliora l'efficienza della rete rispetto ai router, poiché gli switch operano a livello 2 (MAC address) mentre i router operano a livello 3 (IP address), richiedendo più tempo per elaborare le trasmissioni.

2. STP: Spanning Tree Protocol

Le reti con switch spesso prevedono percorsi ridondanti per garantire affidabilità e fault tolerance. Tuttavia, questa ridondanza può causare **loop di rete**, generando il fenomeno del **broadcast storm**, che satura la rete e ne impedisce il funzionamento.

Per evitare i loop, gli switch utilizzano **STP (Spanning Tree Protocol)**, definito dallo standard IEEE 802.1D. STP crea una **topologia ad albero**, mantenendo attivi solo alcuni percorsi e mettendo gli altri in standby.

Funzionamento di STP

1. Identifica i percorsi ridondanti e li mette in **standby**.
2. Attiva solo un percorso alla volta tra due dispositivi della rete.
3. In caso di guasto, riattiva automaticamente un percorso in standby.
4. Se STP non fosse attivo, si creerebbero loop infiniti che congestionerebbero la rete.

Componenti di STP

- **Root Bridge**: switch principale da cui parte l'albero dello spanning tree.
- **Root Port**: porta dello switch con il percorso più breve verso la root.
- **Designated Port**: porta attiva per ogni segmento di rete.
- **Blocking Port**: porta inattiva per prevenire i loop.

Stati delle porte in STP

1. **Blocking**: riceve solo BPDU, non inoltra dati.
2. **Listening**: verifica l'assenza di percorsi ridondanti.
3. **Learning**: costruisce la tabella di bridging.
4. **Forwarding**: trasmette e riceve dati.
5. **Disabled**: porta disabilitata dall'amministratore.

3. Evoluzione di STP: Rapid Spanning Tree Protocol (RSTP)

Nel 2001, IEEE ha introdotto **RSTP (IEEE 802.1w)** per migliorare la convergenza della rete in caso di cambiamenti topologici.

Differenze principali tra STP e RSTP:

- **Convergenza più veloce**: RSTP impiega da 3 a 6 secondi, contro i 30-50 secondi di STP.
- **Nuove porte alternate e backup**: consentono una ripresa più rapida in caso di guasto.
- **Funziona meglio in reti full-duplex con switch moderni**.

4. VLAN: Le Reti Locali Virtuali

Le **VLAN** (Virtual Local Area Network) sono una tecnologia di rete che permette di creare **reti locali virtuali** all'interno di una rete fisica, separando il traffico di dati in segmenti logici indipendenti. Questo significa che anche se i dispositivi sono fisicamente connessi alla stessa infrastruttura di rete, possono essere suddivisi in **gruppi separati**, come se appartenessero a reti fisiche diverse.

Funzioni e Vantaggi delle VLAN

1. **Segmentazione della rete**:
    - Le VLAN consentono di **segmentare** una rete fisica in più **sottoreti logiche**. Ogni VLAN ha il suo dominio di broadcast, il che significa che i dispositivi all'interno della stessa VLAN possono comunicare tra loro senza influenzare altri dispositivi nelle altre VLAN.
2. **Maggiore sicurezza**:
    - Separando il traffico delle diverse VLAN, si riduce il rischio che dispositivi non autorizzati possano accedere a dati sensibili di altre VLAN. Ad esempio, puoi separare il traffico della rete amministrativa da quello della rete degli utenti.
3. **Ottimizzazione del traffico**:
    - Le VLAN permettono di ridurre il **traffico di broadcast**, poiché i messaggi di broadcast (come ARP) rimangono limitati a ciascuna VLAN. Questo migliora le prestazioni della rete, riducendo la congestione e aumentando l'efficienza.
4. **Facilità di gestione**:
    - Le VLAN semplificano la gestione della rete. Ad esempio, se un dipendente cambia ufficio, può essere semplicemente assegnato a una VLAN diversa senza dover modificare fisicamente le connessioni di rete.
5. **Supporto per la mobilità dei dispositivi**:
    - Dispositivi che si spostano fisicamente in diverse posizioni della rete possono mantenere la loro configurazione VLAN, migliorando la **mobilità** senza cambiare la loro configurazione IP.

Come si crea una VLAN?

La creazione di una VLAN avviene solitamente tramite la configurazione degli switch di rete. Ogni dispositivo collegato alla rete (come computer, stampanti, server) può essere assegnato a una VLAN specifica, che viene identificata da un **VLAN ID (**un numero che identifica univocamente la VLAN).

1. Assegnazione delle porte agli switch

La configurazione di una VLAN può avvenire raggruppando le **porte degli switch**. Ogni porta di uno switch può essere assegnata a una VLAN specifica. In questo caso, i dispositivi collegati a una porta dello switch fanno parte della stessa VLAN, anche se fisicamente si trovano su switch diversi.

Ad esempio, se uno switch ha le porte 1-10 assegnate alla VLAN 10 (ad esempio per il reparto vendite), i dispositivi collegati a queste porte saranno trattati come appartenenti alla VLAN 10, indipendentemente da dove si trovano fisicamente.

2. Assegnazione per utenti (indirizzo MAC)

Un altro metodo è l'assegnazione della VLAN in base **all'indirizzo MAC** del dispositivo. Ogni dispositivo sulla rete ha un indirizzo MAC univoco, e una VLAN può essere creata associando un determinato indirizzo MAC a una VLAN specifica.

Tuttavia, questa modalità è meno comune perché è più complessa da gestire. Inoltre, se un dispositivo cambia porta, potrebbe essere necessario riconfigurare manualmente la VLAN, rendendo difficile la gestione dinamica della rete.

3. Assegnazione tramite protocolli (indirizzo IP)

Le VLAN possono anche essere configurate utilizzando indirizzi logici come gli indirizzi IP. Una volta che i dispositivi ottengono un **indirizzo IP** tramite il **DHCP** (Dynamic Host Configuration Protocol), lo switch può assegnarli alla VLAN corrispondente in base all'indirizzo IP.

Questo metodo è diventato meno comune poiché il DHCP è ampiamente utilizzato e semplifica l'assegnazione dinamica degli indirizzi IP, rendendo più semplice la gestione delle VLAN tramite l'indirizzo IP.

Funzionamento delle VLAN

Quando un dispositivo in una VLAN invia un messaggio di broadcast, questo messaggio viene trasmesso solo ai dispositivi appartenenti alla stessa VLAN, non a tutta la rete. Questo aiuta a ridurre il traffico di rete e a migliorare le prestazioni.

Se un dispositivo appartenente a una VLAN deve comunicare con un dispositivo in un'altra VLAN, è necessario un **router** o uno **switch Layer-3** (switch che ha capacità di routing) per instradare i pacchetti tra le VLAN.

Funzionamento:

2.4 VLAN Trunking

Il trunking è un metodo per consentire la comunicazione tra host appartenenti a VLAN diverse. Consiste in un collegamento tra switch e router (o tra switch) in grado di trasportare il traffico di più VLAN contemporaneamente. Solitamente, per i trunk si utilizzano porte ad alta velocità, poiché devono gestire volumi elevati di traffico.

Due tipi di collegamenti nelle VLAN:

- **Access link**: collega un dispositivo a una sola VLAN. Il dispositivo non è consapevole della VLAN, poiché lo switch rimuove le informazioni VLAN prima di inoltrare i pacchetti.
- **Trunk link**: connessione punto-punto che trasporta il traffico di più VLAN, usata tra switch, switch-server o switch-router.

Poiché il frame Ethernet originale non prevede un campo per il tagging VLAN, sono stati sviluppati diversi protocolli per gestire questa funzione. Lo standard internazionale più utilizzato è **IEEE 802.1Q**, che aggiunge un campo di 4 byte ai frame Ethernet per l'identificazione della VLAN.

VLAN Trunking Protocol (VTP)

In reti complesse, la gestione manuale delle VLAN può essere complessa e soggetta a errori. Il **VLAN Trunking Protocol (VTP)**, sviluppato da Cisco, semplifica questa gestione centralizzando la configurazione delle VLAN. Gli switch si dividono in:

- **VTP Server**: permette di creare, modificare ed eliminare VLAN.
- **VTP Client**: riceve e applica le configurazioni propagate dal server.
- **VTP Transparent**: inoltra gli aggiornamenti senza applicarli.

L'uso del VTP riduce il rischio di errori e facilita la gestione delle VLAN in reti di grandi dimensioni.

IL FIREWALL E LE ACL

3.1 Firewall

Il firewall è un componente essenziale per la sicurezza delle reti informatiche. Il suo nome deriva dal termine inglese che significa "muro tagliafuoco", e il suo compito è proprio quello di proteggere una rete aziendale o domestica da accessi non autorizzati provenienti dall'esterno. Agisce come una barriera tra la rete interna (LAN) e il mondo esterno, come Internet (WAN), controllando e filtrando i pacchetti di dati che entrano e escono dalla rete secondo regole predefinite (policy).

Tipologie di firewall

Un firewall può essere implementato in diversi modi:

- **Software**: può essere installato su un computer o un router, agendo a livello logico per filtrare i pacchetti.
- **Hardware**: un dispositivo fisico dedicato che offre maggiore sicurezza rispetto a una soluzione puramente software.

I firewall possono essere configurati per bloccare traffico dannoso, filtrare le connessioni e garantire che solo i dispositivi e le applicazioni autorizzate possano comunicare con l'esterno. Questo è particolarmente utile nelle aziende, dove la protezione dei dati è fondamentale.

Importanza del firewall

Non avere un firewall espone la rete a numerosi attacchi e tentativi di intrusione. Mentre in un ambiente domestico il danno potrebbe essere minimo, in un'azienda un attacco potrebbe comportare perdite di dati e costi elevati. I firewall permettono di stabilire regole precise, come ad esempio limitare l'accesso a Internet solo a determinati dispositivi o impedire l'uso di protocolli non sicuri.

I firewall moderni possono proteggere le reti anche da attacchi sofisticati come:

- **ARP Spoofing**
- **Port Scanning**
- **Denial of Service (DoS)**
- **Worms e malware (Blaster, Sasser, SQL Slammer, ecc.)**

3.2 Categorie di firewall

I firewall possono essere suddivisi in tre categorie principali in base al livello dello stack TCP/IP in cui operano:

1. **Application Level Firewall**

    - Opera al livello **Application** dello stack TCP/IP.
    - Analizza il contenuto dei pacchetti a livello applicativo, riconoscendo protocolli come HTTP, FTP, SMTP.
    - Blocca attacchi come virus o worm presenti nelle sessioni HTTP o SMTP.
    - Appartengono a questa categoria i **proxy**, che agiscono come intermediari tra i computer interni e Internet. Un proxy può limitare l'accesso a determinati siti e migliorare la sicurezza impedendo connessioni dirette tra la rete interna e Internet.
    - Vantaggi: sicurezza elevata.
    - Svantaggi: può rallentare la rete.
2. **Packet Filter Firewall**
    - Opera ai livelli **Network e Transport**.
    - Analizza i pacchetti solo in base agli **header IP e TCP/UDP**, senza ispezionare il contenuto.
    - Parametri controllati:
        - **Indirizzo IP di origine e destinazione**
        - **Porta TCP/UDP di origine e destinazione**
        - **Protocollo di livello superiore (es. HTTP, FTP, etc.)**
    - È veloce e non introduce latenza significativa, ma ha lo svantaggio di non poter analizzare il contenuto del traffico, quindi non può fermare virus o malware trasmessi tramite e-mail o altri protocolli.
3. **Stateful Packet Inspection Firewall**
    - Opera a livello **Transport** e offre un controllo più avanzato rispetto ai Packet Filter Firewall.
    - Analizza non solo gli header, ma anche lo **stato della connessione**, creando una tabella di stato per tenere traccia delle connessioni attive.
    - Permette di bloccare pacchetti non autorizzati basandosi sulla logica della connessione, rendendo il filtraggio più sicuro rispetto a un semplice controllo degli indirizzi IP.
    - Vantaggi: miglior sicurezza rispetto al Packet Filter Firewall.
    - Svantaggi: ha una complessità di configurazione maggiore.

3.3 Le ACL (Access Control List)

Le **ACL (Access Control List)** sono una serie di regole applicate ai firewall o ai router per controllare il traffico di rete. Consentono di definire quali pacchetti possono attraversare una determinata interfaccia, filtrando quelli in entrata e in uscita.

Motivi per usare le ACL

Le ACL vengono utilizzate per diversi scopi:

- **Migliorare la sicurezza**: possono restringere gli accessi a determinate reti o sottoreti.
- **Ottimizzare le prestazioni**: limitando il traffico inutile si riducono i carichi sulla rete.
- **Controllare il tipo di traffico consentito**: ad esempio, permettere solo l'invio di e-mail ma bloccare il protocollo Telnet.

Le ACL vengono eseguite in **sequenza**: appena un pacchetto soddisfa una regola, viene elaborato senza verificare le regole successive. Questo significa che l'ordine delle regole è fondamentale: è buona pratica inserire le regole più restrittive all'inizio.

Se una ACL non contiene alcuna regola, di default ne viene applicata una **implicita di blocco totale** (deny all), che impedisce il passaggio di qualsiasi pacchetto.

Tipologie di ACL

Le ACL si dividono in due categorie principali:

1. **Standard ACL**: filtra i pacchetti considerando solo l'indirizzo IP di origine. Devono essere posizionate il più vicino possibile alla destinazione finale.
2. **Extended ACL**: permette di applicare regole più specifiche, basandosi su parametri come:
    - **Indirizzo IP di origine e destinazione**
    - **Protocollo utilizzato (TCP, UDP, ICMP, ecc.)**
    - **Numero di porta utilizzata**
    - **Tipo di servizio richiesto**
    - Devono essere posizionate il più vicino possibile alla sorgente del traffico.

Le **ACL estese** offrono maggiore flessibilità e precisione nel filtraggio del traffico, ma sono più complesse da configurare.