

VLAN

Le VLAN (Virtual Local Area Network) é una segmentazione virtuale di una rete in modo tale da avere diverse sottoreti senza però cambiare la configurazione fisica di tutta la rete. Questa configurazione è interamente gestita dagli switch di rete.

Le VLAN hanno molti benefici, tra cui la sicurezza, diminuzione del carico del traffico, gestione più semplice e flessibilità nella configurazione.

Esistono due tipi di VLAN

Access port collegano dispositivi finali e appartengono a una singola VLAN.

Trunk Ports: Collegano gli switch tra loro e possono trasportare il traffico di più VLAN usando il tagging VLAN per identificare il traffico di ciascuna VLAN.

All'interno dei pacchetti di una VLAN viene inserito un tag che serve per riconoscere la VLAN stessa.

Per la configurazione delle VLAN, alcuni switch hanno due tipi di porte:

Access Ports che collegano i dispositivi finali come computer, stampanti, ecc.

Trunk Ports che servono per collegare due switch tra loro permettendogli di trasportare il traffico di più VLAN usando il tagging VLAN

Tipi di vlan

VLAN di default: ogni switch ha una VLAN di default a cui appartengono tutte le porte non configurate per altre VLAN.

VLAN di accesso: sono VLAN standard utilizzate per segmentare il traffico di rete. (reparto vendite/IT)

VLAN di Management: è dedicata alla gestione dei dispositivi di rete

VLAN di voce: specifiche per il traffico VoIP (Voice over IP) e generalmente hanno una priorità più alta per garantire la qualità di servizio

VLAN di Rete: utilizzate per il Routing tra VLAN diverse

TCP

Il protocollo TCP è un protocollo orientato alla connessione e garantisce la trasmissione affidabile e ordinata dato che prima di effettuare uno scambio di pacchetti viene effettuata una comunicazione tra i due dispositivi (three-way-handshake)

SYN: il mittente invia un pacchetto (SYN) al destinatario

SYN-ACK: il destinatario risponde con un pacchetto

SYN-ACK

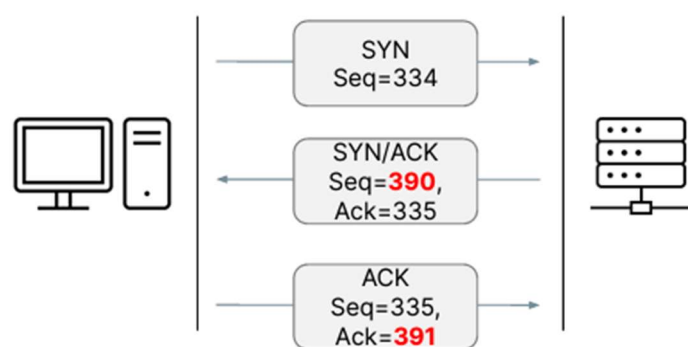
ACK: il mittente risponde con un pacchetto ACK stabilendo così la connessione

Questo scambio avviene tramite dei flag dove:

il mittente usa un numero generato casualmente e lo usa come flag SYN

successivamente, il destinatario prende quel numero, lo incrementa di uno e lo usa come flag di ACK e genera un altro SYN casuale.

Infine, il mittente incrementerà a sua volta il SYN flag ricevuto e invertirà i codici SYN e ACK. Da ora in poi i due dispositivi comunicheranno usando questi due codici



UDP

Il protocollo UDP è senza connessione e offre una maggiore velocità e minori overhead sacrificando l'ordinamento e l'affidabilità dei dati.

DNS (Domain Name System)

Opera al livello 7 della pila (Application Layer) e si occupa di convertire i nomi dei domini, come www.google.com in indirizzo IP.



I server DNS generalmente sono messi a disposizione dai provider.

DHCP (Dynamic Host Configuration Protocol)

Si occupa di assegnare a un dispositivo automaticamente tutte le informazioni che servono per poter comunicare sotto una determinata rete, come ad esempio indirizzo IP e Subnet Mask

Le porte

Una porta è un particolare codice che serve per indentificare le applicazioni specifiche o servizi in esecuzione su un particolare server.

Mentre l'indirizzo IP identifica la macchina di destinazione, la porta fornisce informazioni sul servizio specifico.

Categorie di porte

Well-Known: da 0 a 1023 e sono riservate per i server (http 80, https 443, FTP 21)

Registered: da 1024 a 49151 utilizzate per applicazioni e servizi registrati.

Dynamic or Private: da 49152 a 65535 utilizzate temporaneamente da applicazioni per comunicazioni private e dinamiche.

NAT e PAT

NAT è una tecnica di traduzione degli indirizzi e va a modificare gli indirizzi IP é uno dei pochissimi momenti dove l'indirizzo IP viene modificato

Viene usato per fare da ponte tra rete privata e rete pubblica.

Esistono due tipi di NAT

Static NAT dove viene mappato un indirizzo IP pubblico fisso con uno privato

Dynamic NAT mappa un IP privato ad indirizzo IP pubblico tra degli indirizzi pubblici stabiliti (pool di indirizzi).

PAT (Port Address Translation) non traduce solo gli indirizzi ip ma anche I numeri di porta