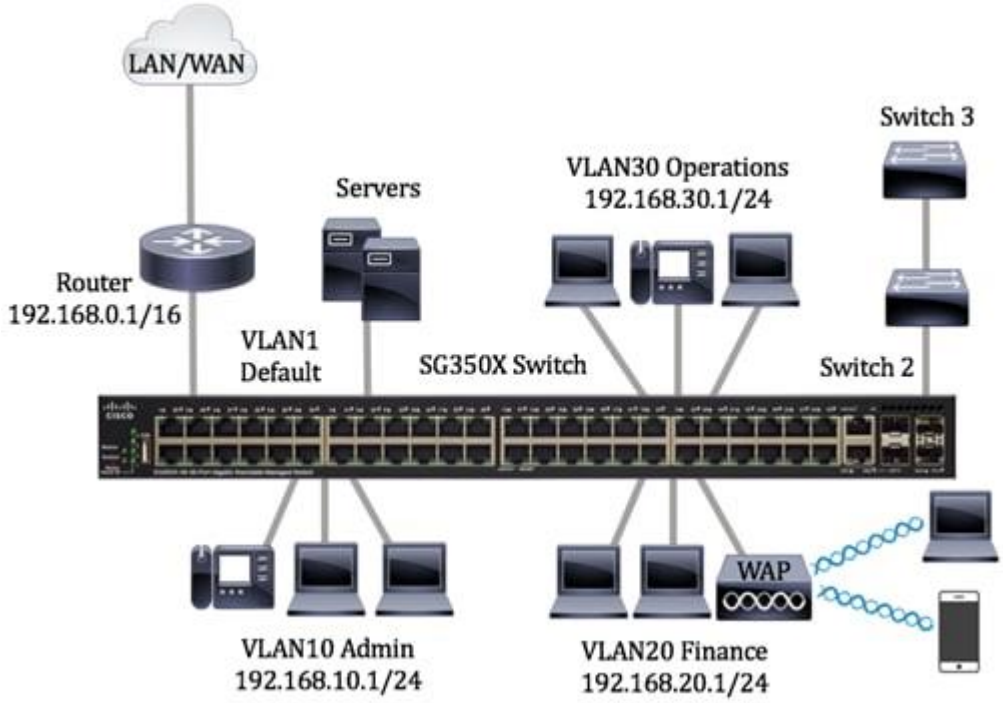
La VLAN è una rete segmentata in genere in base alla funzione o all'applicazione. Il funzionamento di VLAN e LAN fisiche è molto simile, con il vantaggio che sulle VLAN è possibile raggruppare gli host anche se non si trovano fisicamente nella stessa posizione. La porta di uno switch può appartenere a una VLAN. I pacchetti unicast, broadcast e multicast vengono inoltrati e trasmessi a tutte le porte della stessa VLAN.

L'uso delle VLAN inoltre può migliorare le prestazioni in quanto riduce la necessità di inviare pacchetti broadcast e multicast a destinazioni non necessarie. Infine, facilita la configurazione della rete connettendo logicamente i dispositivi senza doverli riposizionare fisicamente.



Una LAN virtuale o VLAN (Virtual Local Area Network) consente di segmentare logicamente una LAN (Local Area Network) in più domini di broadcast. Quando sulla rete vengono trasmessi anche dati sensibili, la creazione di VLAN offre una maggiore sicurezza e il traffico viene quindi indirizzato a VLAN specifiche. Solo gli utenti che appartengono alla VLAN possono accedere e modificare i dati trasmessi su tale rete.

È possibile configurare le porte, specificare se usarle in modalità di accesso o in modalità trunk e scegliere quali porte assegnare alle VLAN. In questo documento viene spiegato come configurare un'interfaccia VLAN come porta di accesso o porta trunk sullo switch tramite l'interfaccia della riga di comando (CLI).

Le VLAN offrono numerosi vantaggi rispetto alle reti locali fisiche tradizionali. Tra i principali vantaggi si annoverano un **aumento delle prestazioni della rete**, poiché la segmentazione riduce il traffico di broadcast e i domini di broadcast diventano più piccoli, limitando anche le collisioni. La sicurezza viene migliorata poiché dispositivi appartenenti a VLAN diverse non possono comunicare direttamente, anche se collegati allo stesso switch, limitando l'accesso alle risorse. Inoltre, la flessibilità è notevole: gli host possono essere spostati da una VLAN all'altra semplicemente modificando la configurazione software dello switch, senza dover ricablare fisicamente la rete.

Tuttavia, le VLAN presentano anche alcuni svantaggi. Un problema significativo è che il traffico tra VLAN richiede il routing, che deve essere gestito da un router o da uno switch livello 3, il che può diventare un collo di bottiglia in reti di grandi dimensioni. Inoltre, se non configurate correttamente, le VLAN possono essere vulnerabili a attacchi informatici, poiché il traffico tra VLAN può essere spoofato o compromesso. Non è possibile inoltrare il traffico di rete da una VLAN a un'altra senza un router aggiuntivo, e in alcuni casi possono verificarsi problemi di interoperabilità tra dispositivi di diversi produttori. Inoltre, un attacco in un singolo sistema può diffondersi rapidamente all'interno di una VLAN, specialmente se non sono implementate politiche di sicurezza adeguate. Per questo motivo, non è consigliabile usare le VLAN come unico mezzo di isolamento critico, come per una DMZ, e si raccomanda l'uso di firewall dedicati.