Nel progetto, era stato richiesto di progettare una rete IP Net locale, in cui siano presenti 8 dispositivi connessi ad uno Switch (dispositivo di livello 2 modello ISO OSI) successivamente segmentati con 4 VLAN (Virtual Local Area Network) differenti. Dopo aver impostato i parametri della rete, quali IP di rete (192.168.1.0/24), l'indirizzo IP dei dispositivi e le relative Subnetmask, è stata effettuato un controllo, tramite il comando "ping" per verificare se i dispositivi presenti nella rete fossero in grado di comunicare tra loro.

Poiché i dispositivi, non conoscono l'indirizzo MAC dei destinatari, entra in funzione il protocollo ARP (Address Resolution Protocol) il quale funziona seguendo due fasi, ARP Request ed ARP Reply. Il mittente invia quindi un pacchetto contente il suo indirizzo IP, e MAC, e avrà come destinatario l'indirizzo IP del dispositivo che dovrà ricevere il pacchetto e come indirizzo MAC FF.FF.FF.FF.FF.FF. Questo pacchetto giungerà allo Switch, il quale non avendo l'indirizzo MAC destinatario, ma soltanto le 12 F, invierà una richiesta in broadcast a tutti i dispositivi connessi alla rete, ARP Request. In seguito, mentre i dispositivi non interessati cestineranno la richiesta, il dispositivo interessato, risponderà con una ARP Reply, rispondendo con un messaggio unicast contente il proprio indirizzo MAC allo Switch, il quale verrà a sua volta inviato al dispositivo mittente. Si potrà quindi procedere tramite il comando ping verificare se le macchine siano in grado di comunicare.

Prima della segmentazione, è stato quindi verificato che i dispositivi fossero in grado di comunicare tra loro, per cui, allo scopo di creare una rete più sicura e con una miglior gestione è stato fatto ricorso alle VLAN. Si sceglie di utilizzare questo tipo di segmentazione (VLAN), una tecnica informatica nata appositamente per questo scopo, segmentare il dominio di broadcast (a differenza del subnetting che utilizza invece una tecnica matematica agendo direttamente sulle subnetmask (CIDR), la cui origine è dovuta alla risoluzione del problema degli IPv4 oramai terminati), poiché questo processo rende le reti molto più sicure e difficili da attaccare, garantendo una migliore gestione dei dati riducendo la trasmissione di pacchetti inutili.

Sono state configurate tramite lo Switch, 4 VLAN differenti (10 Direction – 20 Employees – 30 Segretary – 40 Data management), e successivamente gli 8 dispositivi sono stati suddivisi in gruppi da 2 per rete VLAN. È stato successivamente effettuato un check tramite il comando ping, prima tra 2 dispositivi appartenenti alla stessa rete VLAN, i quali hanno comunicato tra loro con successo, e dopodiché è stato effettuato lo stesso controllo, tra dispositivi di VLAN differenti, i quali invece, non hanno potuto comunicare tra loro, come previsto. La segmentazione è stata quindi effettuata in modo efficace, ed è stata creata una rete più sicura. Una modifica che potrebbe essere eseguita, potrebbe essere la rimozione dei nominativi delle VLAN, utilizzando soltanto la numerazione di queste ultime, in modo tale da migliorare ancor di più la sicurezza in caso un attaccante cerchi di penetrare la rete, soluzione però non molto efficace in caso si parli di un'azienda all'interno della quale non sia presente un sistemista di rete.