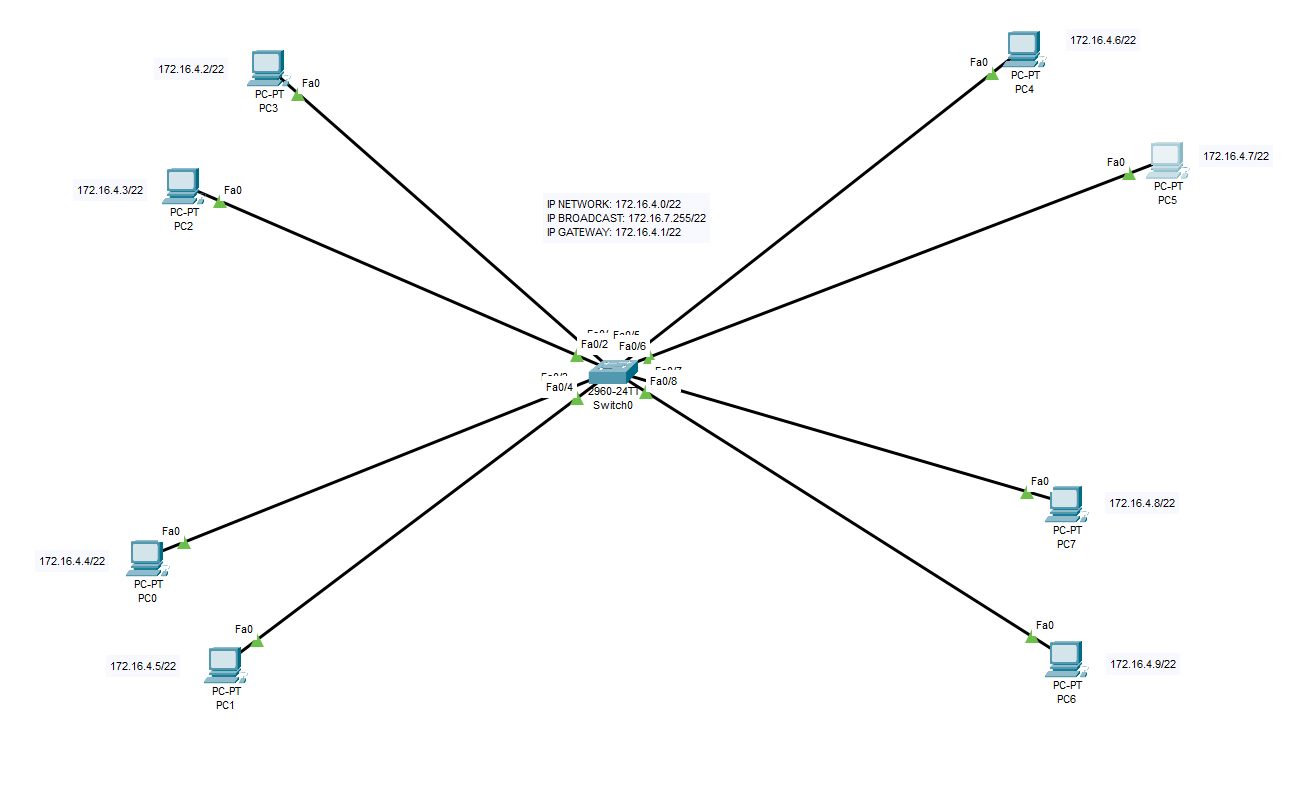
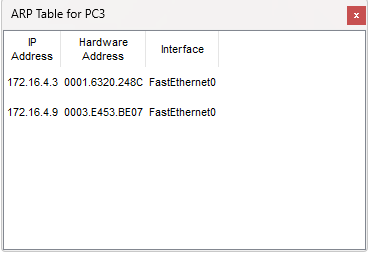
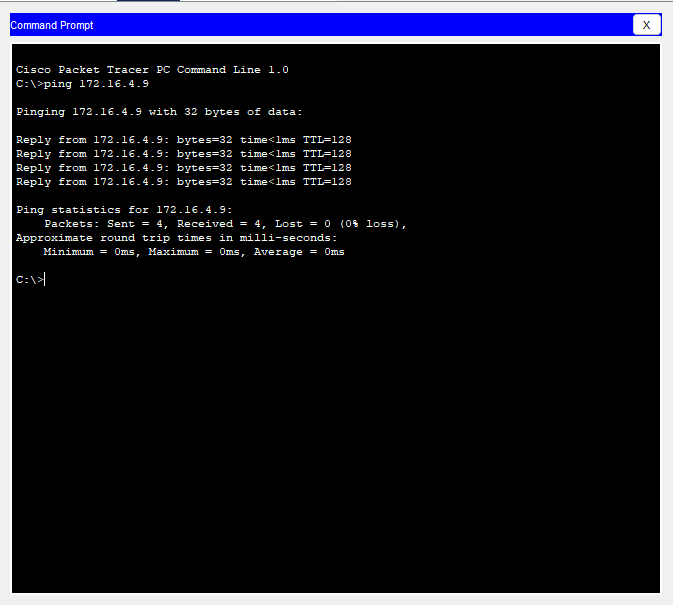
PROGETTO S1/L5

OBIETTIVO: Creare una rete segmentata con quattro VLAN diverse.

STEP 1 Creazione della rete

  
Prendendo in considerazione l’indirizzo IP di CLASSE B 172.16.4.0/22 si procede alla creazione della rete con i seguenti parametri:  
  
IP NETWORK: 172.16.4.0/22  
IP BROADCAST: 172.16.7.255/22  
IP GATEWAY: 172.16.4.1/22

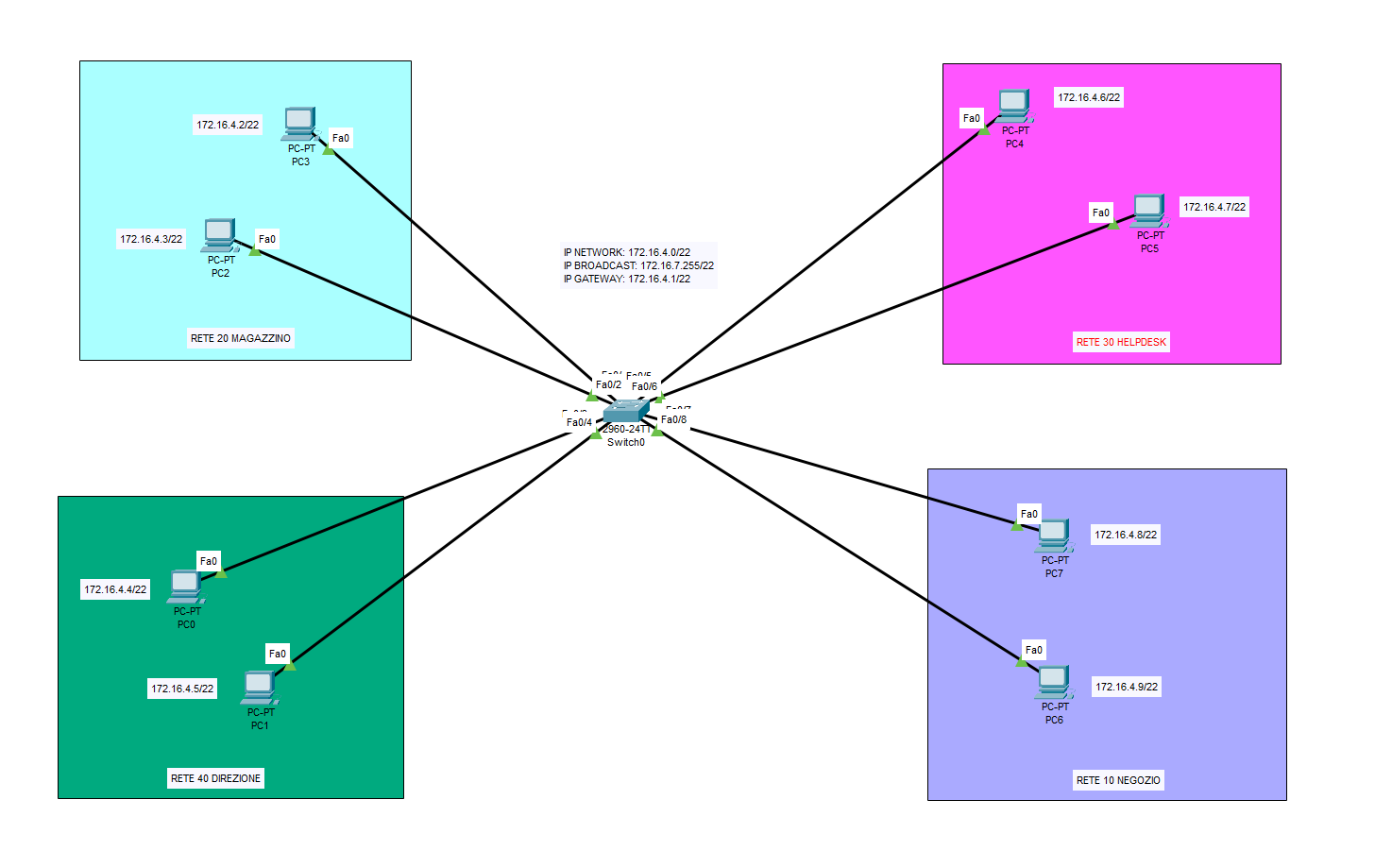
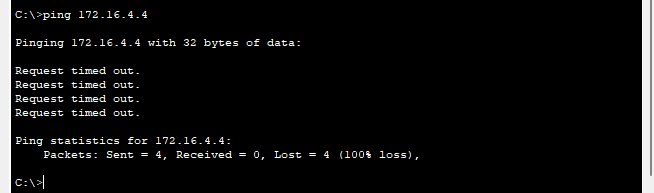
Una volta creata la rete, collegando gli host tramite *switch*(dispositivo di livello 2 nel modello ISO-OSI), bisogna assicurarsi che i dispositivi siano in grado di comunicare tra di loro. Per controllare che i collegamenti siano stati fatti in maniera corretta, si procede ad un tentativo di comunicazione tramite *ping* nel prompt dei comandi.

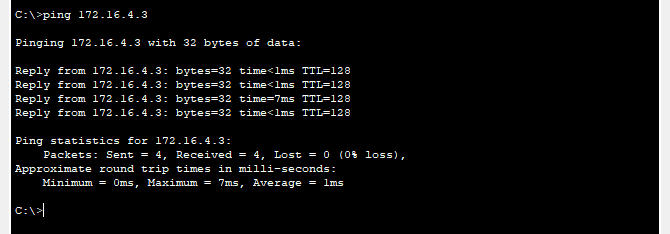
Dimostrazione di host PC-PT PC3 con indirizzo IP 172.16.4.2/22 che comunica con successo con l’host PC-PT PC6 con indirizzo IP 172.16.4.9/22

Tramite questo procedimento, si può affermare che i due host siano collegati alla stessa rete.   
Ma come accade tutto questo? Se i due host non hanno mai comunicato tra loro, o la cache è stata pulita, prima del ping l’host mittente invierà una richiesta di *protocollo ARP*. Ma come funziona nello specifico?  
  
In questo caso PC-PT PC3 (mittente) deve inviare un segnale a PC-PT PC6(destinatario), di cui conosce l’indirizzo IP, perché collegati alla stessa rete tramite switch, ma non l’indirizzo fisico (MAC). Quindi il mittente (PC-PT PC3) invierà una richiesta ARP tramite il broadcast di rete (172.16.7.255/22 in questo caso) a tutti gli host collegati per scoprire qual sarà l’indirizzo fisico (MAC) collegato all’indirizzo IP interessato. Una volta trovato il dispositivo interessato, il destinatario risponderà alla richiesta ARP inviando il proprio indirizzo fisico al dispositivo mittente. Di conseguenza, il mittente (PC-PT PC3) registrerà l’indirizzo fisico del dispositivo destinatario nella propria tabella ARC, permettendo dunque ai due dispositivi di poter comunicare direttamente da quel momento in poi.

STEP 2 Suddivisione della rete in quattro VLAN

Dopo aver creato la rete ed essersi accertati che tutti i dispositivi possano comunicare tra di loro, bisogna aumentarne la sicurezza per proteggersi da eventuali attacchi. Il modo migliore per iniziare è suddividere le reti tramite VLAN (Virtual Local Area Network) che permette di segmentare la rete, aumentando l’efficienza e la sicurezza dell’intero network.   
  
Con un singolo *switch* è possibile creare svariate VLAN, rendendo impossibile la comunicazione tra host appartenenti a VLAN diverse, se non tramite *router* (dispositivo di livello 3 nel modello ISO-OSI). Grazie a questo semplice procedimento, le possibilità di un attaccante di trovare il suo obiettivo vengono dimezzate.

Ecco come si mostra una rete dopo essere stata suddivisa in 4 VLAN:  
  
  
Ma sarà dunque veramente impossibile per PC-PT PC3 che adesso fa parte della VLAN 20 MAGAZZINO comunicare con un dispositivo non facente parte della stessa VLAN in mancanza di un router? Ecco la dimostrazione:  


In questo esempio, PC-PT PC3 (IP 172.16.4.2/22) ha provato senza successo a comunicare con PC-PT PC0 (IP 172.16.4.4/22), facente parte della VLAN 40 DIREZIONE, una VLAN diversa.   
  
Quindi ogni dispositivo adesso è isolato e non potrà più comunicare con nessuno? Sbagliato.  
I dispositivi che si trovano all’interno della stessa VLAN saranno in grado di comunicare tra di loro grazie alla sola presenza di uno switch come da esempio, con PC-PT PC3 (IP 172.16.4.2/22) e PC-PT PC2 (IP 172.16.4.3/22) che fanno parte della VLAN 20 MAGAZZINO:  
  


In sintesi, le VLAN sono il primo passo verso la sicurezza del proprio network. Grazie ad esse è possibile suddividere in compartimenti virtuali svariati dispositivi, mettendo dunque in sicurezza i dati sensibili di un’azienda che altrimenti potrebbe essere sottratti con facilità da qualsiasi attaccante, esperto o principiante che sia. Un procedimento, a mio avviso, standard che dovrebbe essere preso in considerazione da qualsiasi azienda che vuole proteggere i propri interessi.