

Alessandro Pietro Salerno

LABORATORIO CON CISCO PACKET TRACER

CREAZIONE E CONFIGURAZIONE DI UNA RETE SEGMENTATA

INTRODUZIONE

La rete oggetto del laboratorio della prima settimana di corso è una rete che prevede l'implementazione di una particolare tipologia di reti ovvero le VLAN (virtual local area network) . Ho deciso di implementare la rete di una banca , dunque sarà un contesto lavorativo dove saranno evidenziati i diversi livelli delle VLAN ed anche i livelli fisici dell' edificio per una maggiore chiarezza .

Utilizzando cisco packet tracer ci è richiesto di creare una rete segmentata che rispetti alcuni requisiti come un minimo di 2 switch , host collegati a switch diversi che facciano parte della stessa VLAN , ed anche l' assegnazione di reti diverse alle rispettive VLAN tramite la tecnica del Subnetting , ed eseguire le opportune verifiche di connessioni , verificando in particolar modo la connessione tra 2 switch diversi .

La teoria necessaria per l'implementazione di questa rete fa riferimento ad una parte fondamentale delle tipologie di reti , le VLAN.

VIRTUAL LOCAL AREA NETWORK

Le VLAN sono reti logiche che consentono la segmentazione di una rete fisica in più sottoreti diverse tra loro , migliorandone sotto vari aspetti la gestione del traffico .

Le VLAN sono dunque considerati delle sottoreti indipendenti .

Vantaggi :

- ✓ **SICUREZZA** : il traffico di una VLAN non può essere visto da host di un'altra VLAN senza l'uso esplicito di routing , dunque di un dispositivo di livello 3 (router) .
È più semplice applicare regole d'accesso quando il traffico è ben separato tra le VLAN
- ✓ **FLESSIBILITÀ** : i dispositivi posso essere fisicamente spostati ma rimanere nella stessa VLAN .
- ✓ **OTTIMIZZAZIONE DELLE PERFORMANCE** : il traffico di broadcast viene ridotto in seguito alla segmentazione della rete e dunque il dominio di broadcast è ridotto , ciò fa migliorare il traffico diminuendone il carico e ne migliora le prestazioni .

Svantaggi :

- **COMPLESSITÀ** : la configurazione può diventare complessa , specialmente in reti estese con molti switch .
- **DIPENDENZA DAI TRUNK** : un errore sui trunk può isolare intere VLAN , devono quindi essere ben configurati affinché il traffico passi correttamente
- **ROUTING** : per far sì che 2 VLAN comunichino bisogna aggiungere un router o switch di livello 3 , che possono introdurre un pò di latenza e costi aggiuntivi .

SVOLGIMENTO

Dopo aver implementato la rete su Cisco packet tracer con gli opportuni collegamenti , ho configurato gli host e gli switch , avendo cura di assegnare IP Address differenti al fine di creare reti diverse tra le varie VLAN tramite subnetting come richiesto .

I COLLEGAMENTI : tra i host e switch sono tutti con cavo Copper Straight-through , tra switch tramite cavo Copper Cross-over , poiché dispositivi simili , selezionando opportunamente le porte Gigabit per una velocità superiore , data la maggiore intensità di traffico in quel tratto .

LE CONFIGURAZIONI : agli host sono stati assegnati indirizzi IP privati di classe B , 172.16.0.0 nello specifico .

Ho deciso di creare 7 VLAN , dunque tramite la tecnica di subnetting ho assegnato i vari IP alle diverse VLAN. Ottenendo 7 indirizzi IP diversi :

172.16.0.0 / 19

172.16.32.0 / 19

172.16.64.0 / 19

172.16.96.0 / 19

172.16.128.0 / 19

172.16.160.0 / 19

172.16.192.0 / 19

Ogni subnet ha dunque un incremento di 32 nel terzo byte .

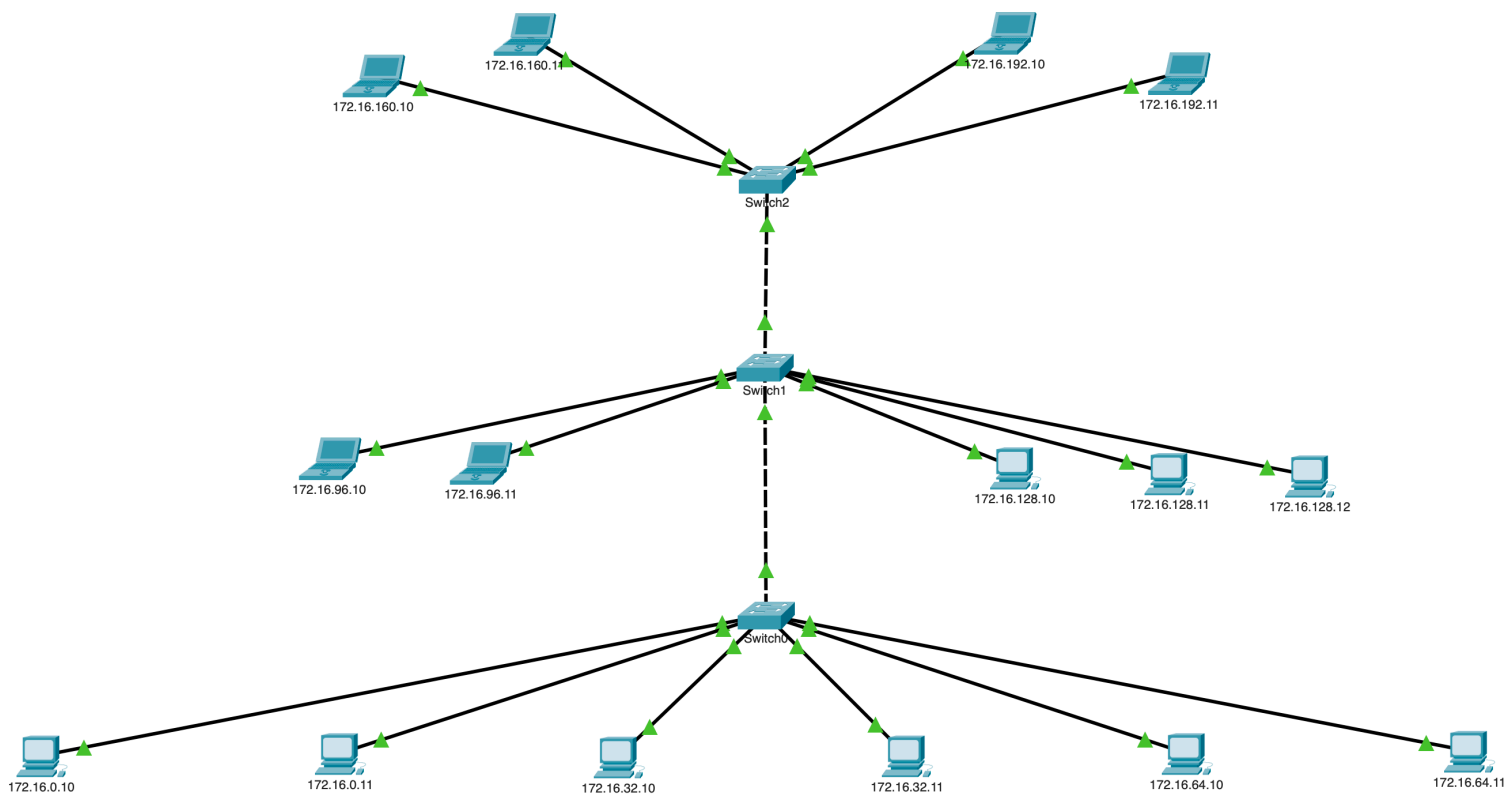
SUBNETTING : pratica che consente di suddividere gli indirizzi IP di una rete in sottoreti più piccole e migliora l'ottimizzazione delle risorse di rete , la gestione degli indirizzi IP , la sicurezza e consente l'implementazione di VLAN come in questo caso .

Procedimento : dato l'indirizzo IP 172.16.0.0 con cidr 16 ho calcolato i bit necessari per ottenere almeno 7 subnet ovvero $2^x \geq \text{numero di subnet desiderate}$, dove $x = 3$.

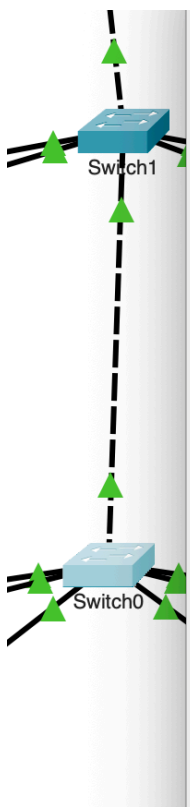
Servono dunque 3 bit , che vengono presi in prestito dagli host , dunque la nuova subnet mask ha CIDR = 19 è nello specifico è 255.255.224.0 così ogni subnet ha a disposizione 2^{13} host , 8192 totali di cui 8190 host utili .

Con il teorema dell'incremento otteniamo $256 - 224$ (ottetto interessato) = 32 , quindi l'incremento è di 32 nel terzo byte . Otteniamo così 8 subnet anche se ne useremo 7 .

STRUTTURA DELLA RETE :



IMPLEMENTAZIONE DELLE VLAN :



Physical Config CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

SWITCHING

- VLAN Database

INTERFACE

- FastEthernet0/1
- FastEthernet0/2
- FastEthernet0/3
- FastEthernet0/4
- FastEthernet0/5
- FastEthernet0/6
- FastEthernet0/7
- FastEthernet0/8

VLAN Configuration

VLAN Number

VLAN Name

Add Remove

VLAN No	VLAN Name
1	default
2	SportelliBancari
3	segreteria
4	Comunicazione
5	OperatoriFinanziari
6	CEO
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1005	trnet-default

Equivalent IOS Commands

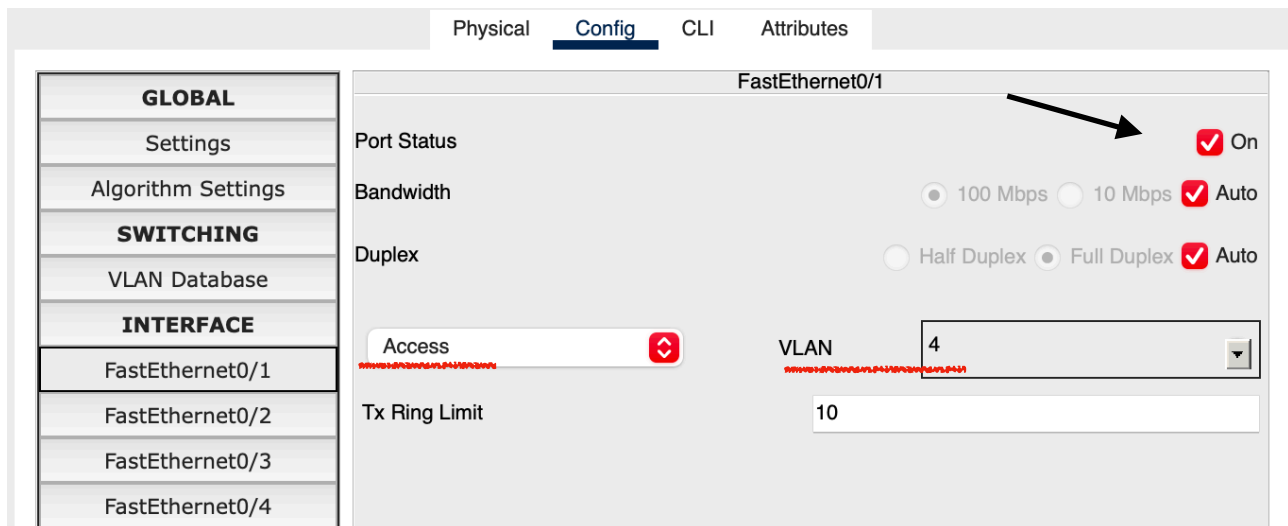
```
Switch(config-vlan)#  
Switch(config-vlan)#end  
Switch#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.
```

I nomi assegnati alle VLAN sono esplicativi , la VLAN 4 è destinata alla comunicazione interna tra host di diversi livello e con mansioni differenti .

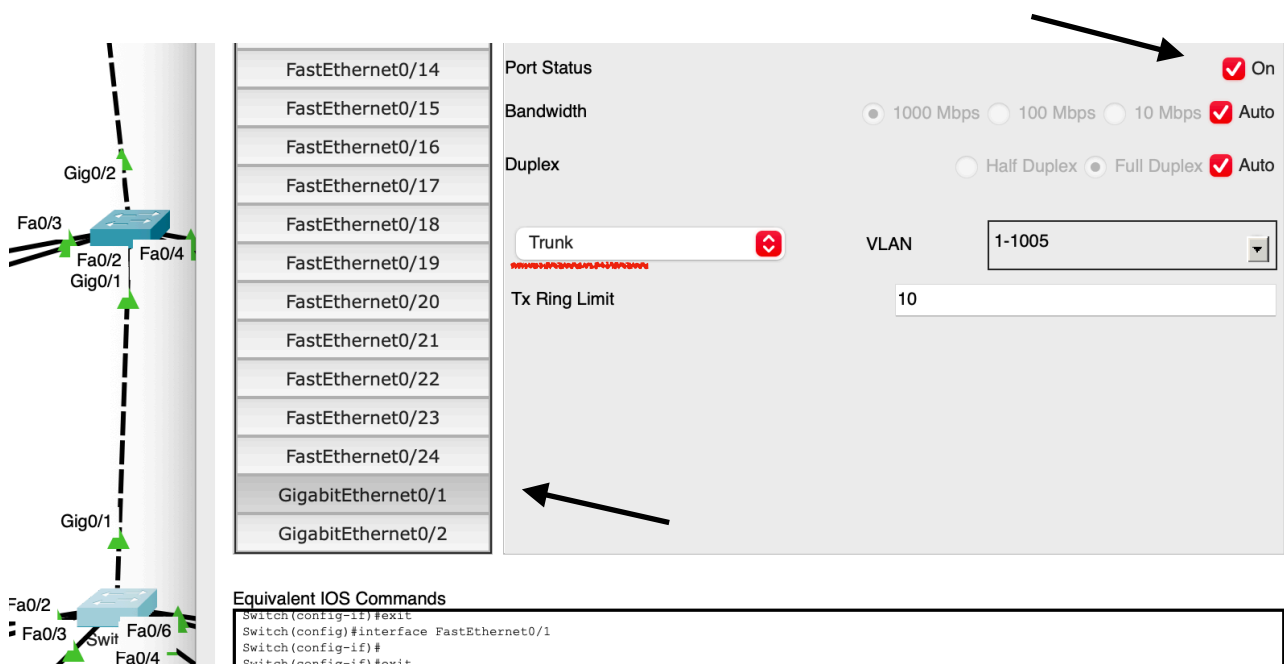
Ad esempio gli operatori finanziari sono situati al secondo piano dell' edificio ed hanno la VLAN 5 dedicata fra loro però ci sono due operatori con due host diversi che appartengono alla VLAN 4 per poter comunicare con il piano superiore , quello dei capi .

ASSEGNAZIONE DELLE VLAN :

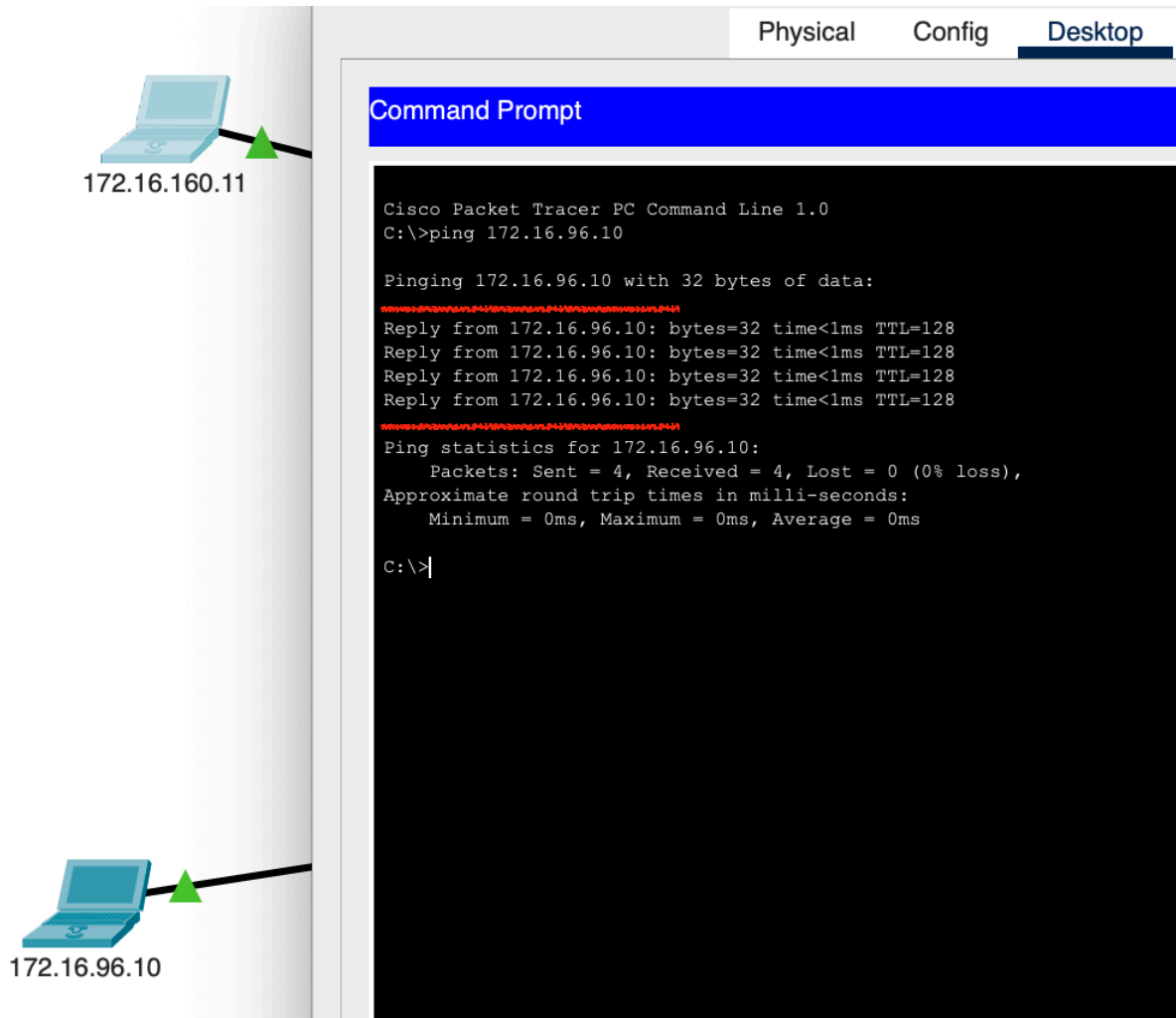
Bisogna configurare lo switch , selezionando la porta relativa all' host che si vuole inserire in una VLAN ed assicurarsi che sia impostata su “access” e che sia accessa , infine selezionare la VLAN desiderata



Per quanto riguarda i collegamenti tra switch assicurarsi di impostare le porte su “trunk” , così da poter comunicare tra switch



Una volta assegnate le VLAN si procede con la verifica del funzionamento del collegamento TRUNK tra gli switch , dunque metto in comunicazione tramite comando “Ping” 2 host appartenenti alla stessa VLAN ma collegati fisicamente a due switch differenti .



L' host 172.16.160.11 ha inviato una richiesta con verifica di raggiungibilità all' host con IP 172.16.96.10 ed ha ricevuto una conferma positiva . I 2 host possono comunicare anche se collegati a 2 switch diversi .

Il comando ping si affida al protocollo ARP per il suo funzionamento , nello specifico il protocollo ARP opera nel secondo livello del modello ISO/OSI ovvero nel livello data.

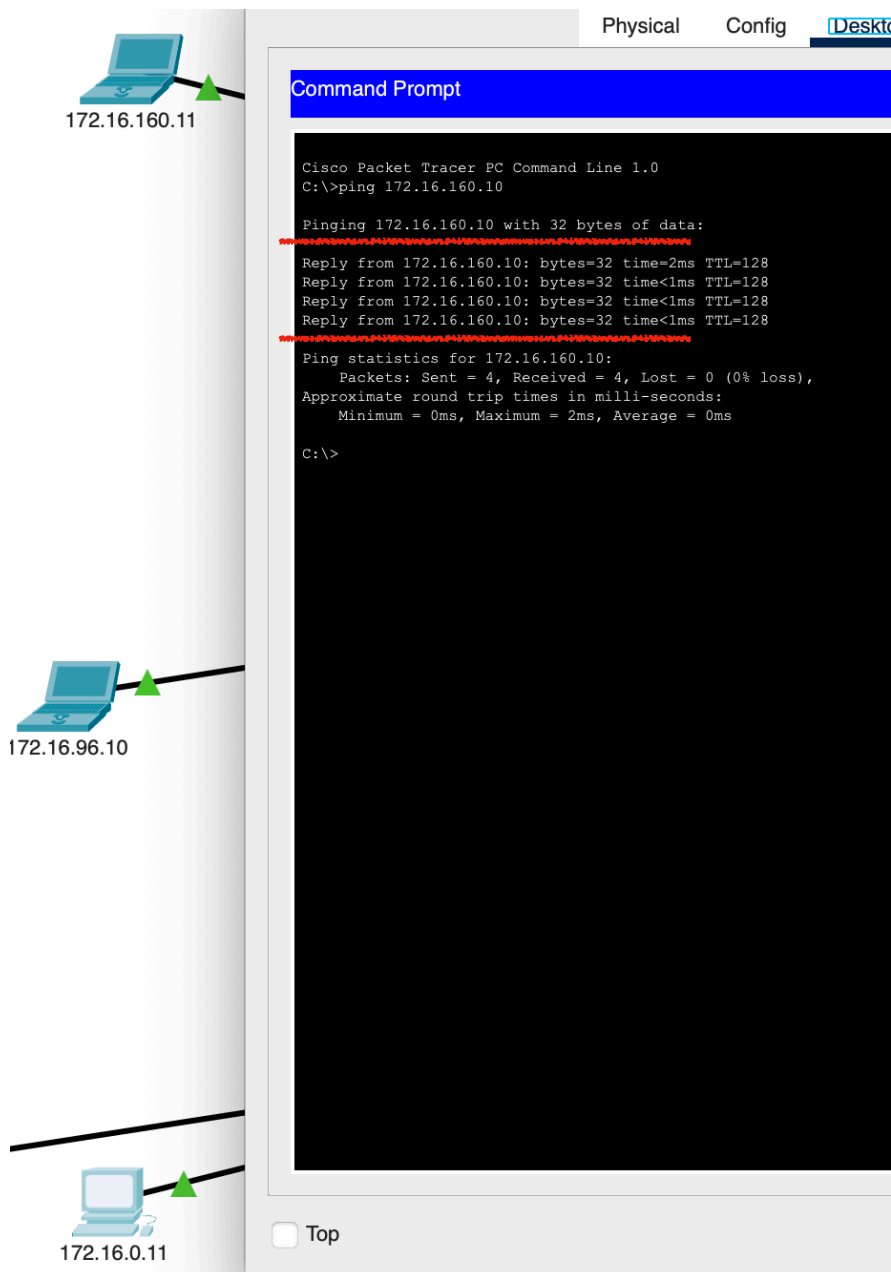
FUNZIONAMENTO PROTOCOLLO ARP

Per poter inviare un pacchetto l' host mittente deve essere a conoscenza del indirizzo MAC del destinatario ma non è un dato noto dunque ARP invia una richiesta, l' ARP request, di conferma dell' indirizzo IP , alla quale rispondere positivamente soltanto l' host con l' IP richiesto , l' ARP reply , in modalità unicast .

L' ARP request è invece spedita in modalità broadcast all' indirizzo MAC FF:FF:FF:FF:FF:FF dello switch .

Infine il mittente aggiorna la sua cache ARP associando a quell' IP il suo rispettivo MAC , così da effettuare la successive comunicazioni in maniera diretta e più velocemente.

Un ulteriore verifica è stata effettuata mettendo in connessione l' host IP 172.16.0.10 del reparto sportelli bancari quindi primo piano con l' host IP 172.16.160.10 del reparto dei capi (CEO) , ultimo piano dell' edificio , però entrambi appartenenti alla VLAN 4 dedicata alla comunicazione interna .



CONCLUSIONI

La rete implementata , secondo le richieste fornite dalla consegna , funziona . Poiché sono state rispettate tutte le regole e le procedure necessarie .

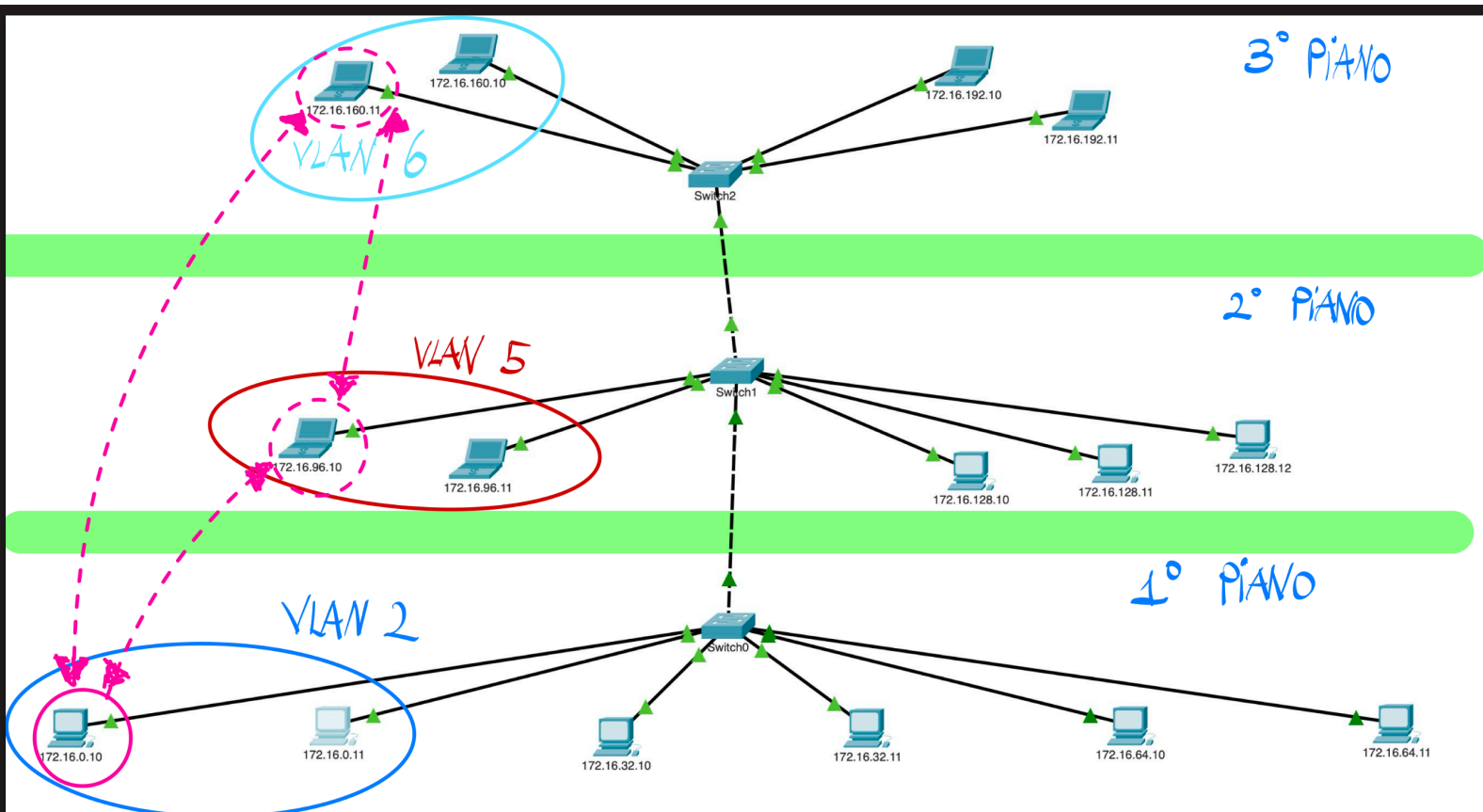
Le verifiche sono state effettuate con successo .

In considerazione ho tenuto il fatto di avere già elaborato dei report in merito l' elaborazione di altre reti più semplici nei quali ho spiegato la teoria necessaria , come ad esempio il

funzionamento dei router o i passaggi che avvengo ai pacchetti quando passano da livello 2 a livello 3 e viceversa o semplicemente gli screenshot delle configurazioni degli IP di ogni singolo host . Argomenti che ho deciso di non riportare per non rendere il report eccessivamente lungo .

Come conclusione personale posso dire che con l' aggiunta di un router la rete sarebbe stata più elaborata ed efficiente poiché avrebbe quasi rispettato le caratteristiche di una reale .

Ad esempio avrei potuto far comunicare un solo host per ogni piano dell' edificio , dedicato all' esclusiva comunicazione tra reparti , con un host di un piano diverso come ad esempio un host della segreteria con un host dei CEO , invece di doverli includere tutti in una VLAN dedicata alla comunicazione e dunque risultare isolati dagli altri host dello stesso piano .



**Un esempio di come potrebbero comunicare i vari reparti dell' edificio.
Con la possibilità di poter creare altre VLAN consentendo sempre ad un
singolo host la possibilità di entrare in comunicazione con gli host degli
altri piani o di altre VLAN e viceversa .
Oppure completarlo creando un' unica VLAN per ogni reparto .**