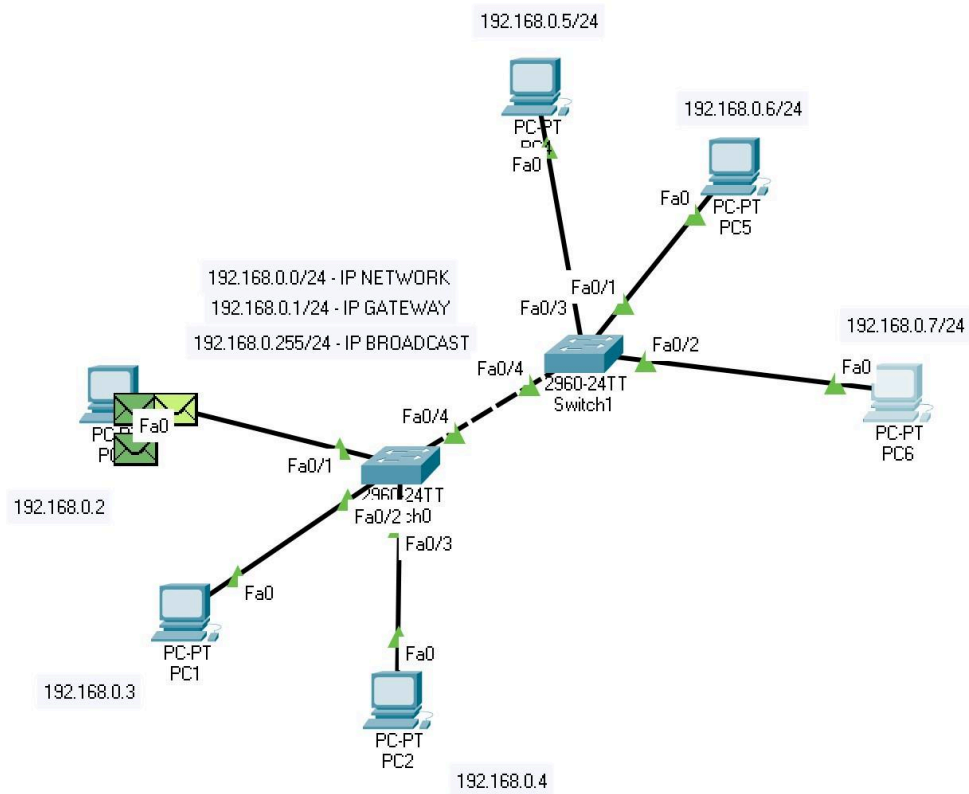


Esercizio S1L3 - Cisco Packet Tracker

Configurazione di rete:



Configurazioni singole dei vari dispositivi:

The image shows a configuration window for a device labeled 'PC0'. The window has four tabs: 'Physical', 'Config', 'Desktop', and 'Attributes'. The 'Config' tab is active, and within it, the 'IP Configuration' sub-tab is selected. The 'Interface' dropdown menu is set to 'FastEthernet0'. The 'IP Configuration' section has two radio buttons: 'DHCP' (unselected) and 'Static' (selected). Below these are input fields for 'IPv4 Address' (192.168.0.2), 'Subnet Mask' (255.255.255.0), 'Default Gateway' (192.168.0.1), and 'DNS Server' (0.0.0.0). The 'IPv6 Configuration' section also has two radio buttons: 'Automatic' (unselected) and 'Static' (selected). It includes input fields for 'IPv6 Address' (empty), 'Link Local Address' (FE80::260:2FFF:FEE4:ADE3), 'Default Gateway' (empty), and 'DNS Server' (empty). The '802.1X' section has a checkbox for 'Use 802.1X Security' (unchecked), a dropdown for 'Authentication' (MD5), and input fields for 'Username' and 'Password' (both empty). A 'Top' button is located at the bottom left of the window.

PC0

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.0.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::260:2FFF:FEE4:ADE3

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

☐ Top

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edi
------	-------------	--------	-------------	------	-------	-----------	----------	-----	-----

PC2

PhysicalConfigDesktopProgrammingAttributes

IP Configuration

X

InterfaceFastEthernet0

IP Configuration

DHCP

Static

IPv4 Address192.168.0.4

Subnet Mask255.255.255.0

Default Gateway192.168.0.1

DNS Server0.0.0.0

IPv6 Configuration

Automatic

Static

IPv6 Address/

Link Local AddressFE80::260:2FFF:FE14:8B32

Default Gateway

DNS Server

802.1X

Use 802.1X Security

AuthenticationMD5

Username

Password

Top

PC4

Physical

Config

Desktop

Programming

Attributes

IP Configuration

InterfaceFastEthernet0

IP Configuration

DHCP

Static

IPv4 Address

192.168.0.5

Subnet Mask

255.255.255.0

Default Gateway

192.168.0.1

DNS Server

0.0.0.0

IPv6 Configuration

Automatic

Static

IPv6 Address

/

Link Local Address

FE80::200:CFF:FE41:B797

Default Gateway

DNS Server

802.1X

Use 802.1X Security

Authentication

MD5

Username

Password

Top

PC5

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.0.6
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.0.1
DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /
Link Local Address: FE80::2E0:A3FF:FE4E:EE41
Default Gateway:
DNS Server:

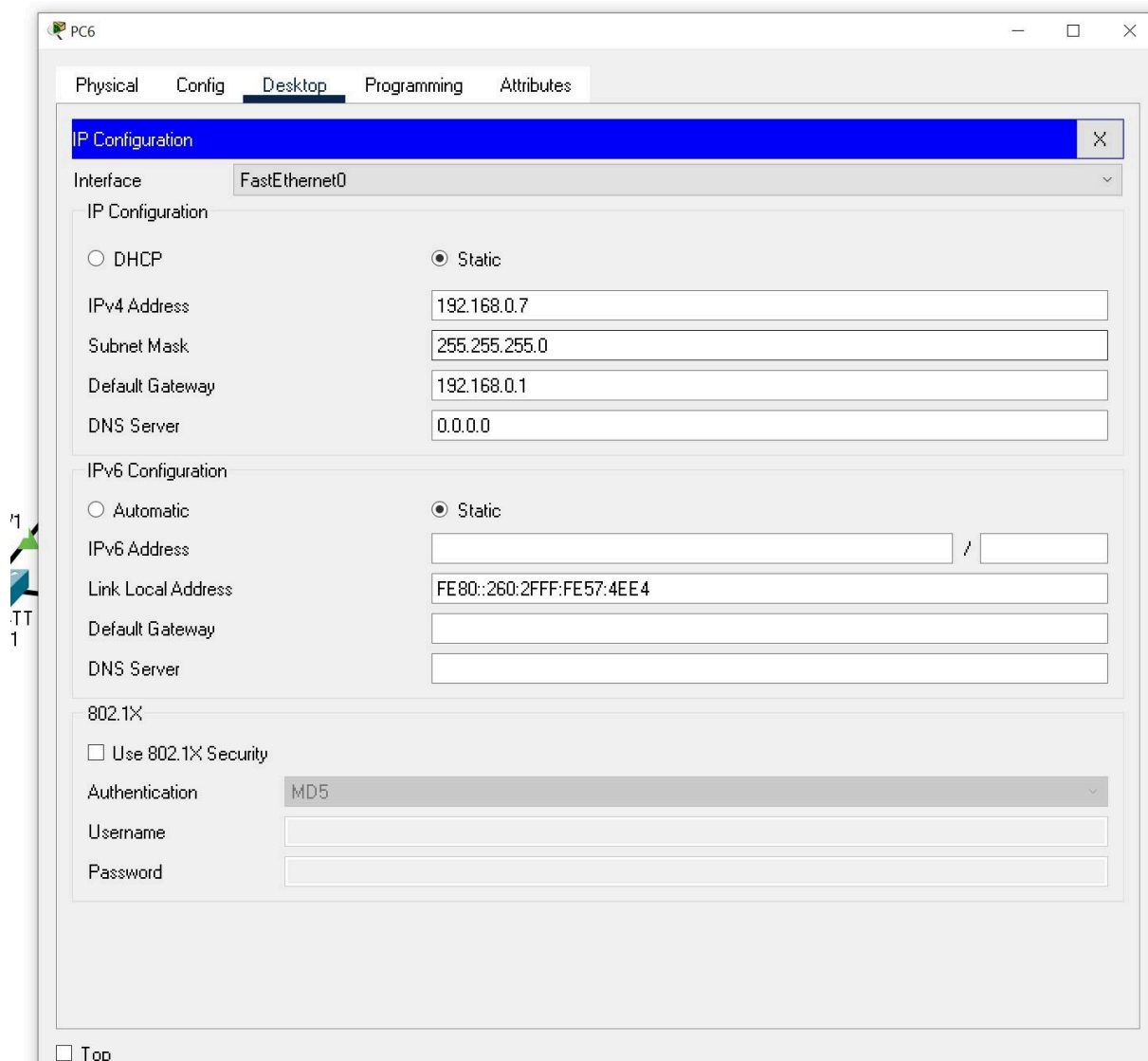
802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:
Password:

☐ Top



L'esercizio si è svolto creando 6 dispositivi finali collegati a due switch differenti divisi per gruppi di tre ma con uno stesso IP Network. Una volta configurati con indirizzi IP Host disponibili, i dispositivi sono pronti per tentare la comunicazione attraverso il ping dal command prompt: il ping, mettendosi in contatto prima con il suo switch di riferimento e successivamente con l'altro switch, richiede di mettersi in contatto con l'altro gruppo di dispositivi (descritto dall'IP già in nostro possesso e a cui indirizziamo il ping stesso), e una volta fatta la richiesta ARP da parte dello switch, vengono restituite le informazioni MAC che identificano la scheda di rete del dispositivo. Una volta assicurato il contatto solo fra i due dispositivi che desideriamo far comunicare, la richiesta ICMP viene trasmessa senza intoppi, come si evince dai risultati ping sotto riportati. Qualora venisse fatta una seconda richiesta di comunicazione, l'ARP non sarà più necessario, in quanto i dati saranno già stati acquisiti dalla rete creando così un "canale" già definito per i dispositivi che hanno inviato i PDU.