

# Projeto rede Wi-Fi - SecurityPro

## (Configuração da rede)

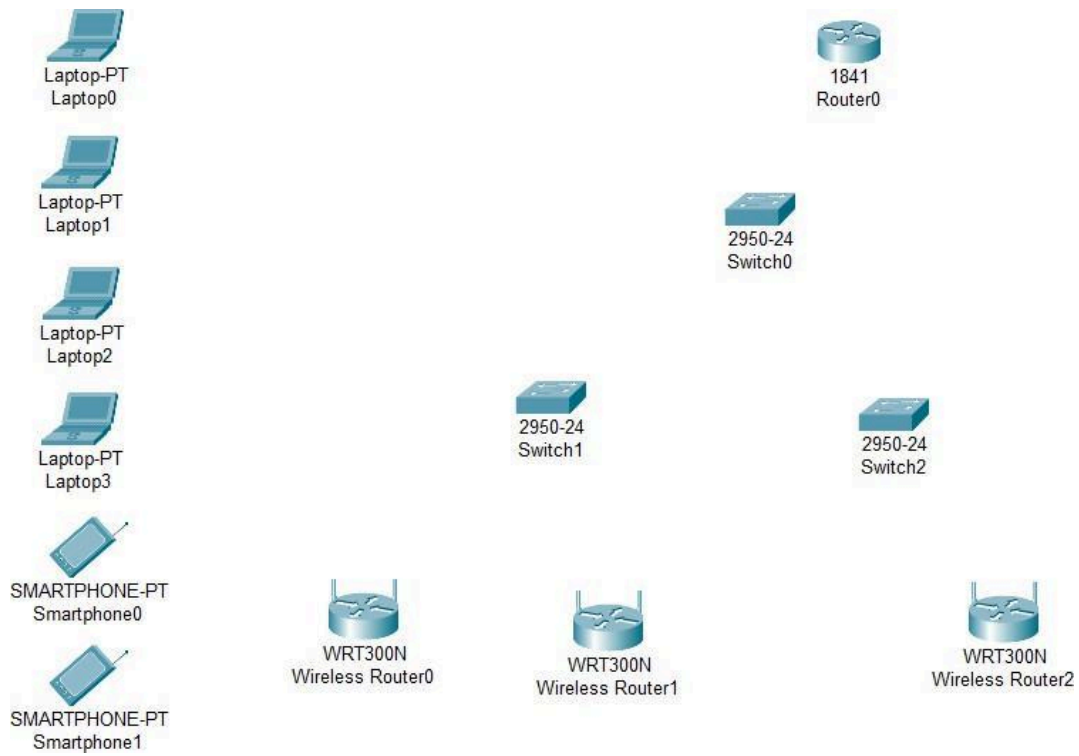
### Índice:

1ª Etapa: Escolha e posicionamento dos dispositivos a serem utilizados na rede:.....	4
2ª Etapa: Renomear os dispositivos na rede:.....	4
3ª Etapa: Conectar fisicamente os dispositivos via cabo:.....	7
4ª Etapa: Ativar a interface do roteador SecurityPro-Router:.....	8
5ª Etapa: Criar as Vlans nos switches SW-1, SW-2 e SW-3:.....	9
6ª Etapa: Configurar o DHCP pool vlan no roteador SecurityPro-Router e realizar o encapsulamento das vlans nas sub interfaces do roteador:.....	11
7ª Etapa: Configurar o SSID em cada Ponto de Acesso (AP):.....	12
8ª Etapa: Adicionar um servidor EAP, desabilitar os serviços que não serão utilizados e ativar o serviço de autenticação AAA:.....	13
9ª Etapa: Configurar o IP do servidor EAP Radius de forma estática, seguindo a documentação da topologia lógica:.....	14
10ª Etapa: Configurar o servidor EAP para autenticação dos usuários com os dispositivos corporativos, criar usuário e senha:.....	15
11ª Etapa: Configurar o AP-Corporativo com IP estático, desabilitar o DHCP interno, pois a rede já está configurada para entrega de DHCP e conectar o AP-Corporativo para autenticação no servidor EAP, desabilitar o SSID Broadcast para evitar fácil identificação da rede:.....	16
12ª Etapa: No SecurityPro-Router, fazer a exclusão dos endereços de IP que foram setados de forma estática para o servidor EAP e o Ponto de Acesso da rede, do dhcp pool vlan100 para não ocorrer conflito de IP:.....	19
13ª Etapa: Configurar os clientes para se conectarem à rede. Instalar placa de rede em dispositivos que necessitem, e configurar o acesso à rede:.....	19
14ª Etapa: Ativar o recebimento de IP dinâmico via DHCP e realizar o teste de conectividade com ICMP (ping):.....	22
15ª Etapa: Configurar o AP-Dispositivos-Pessoais com IP estático, desabilitar o DHCP interno, pois a rede já está configurada para entrega de DHCP e configurar o canal para:.....	25
16ª Etapa: No SecurityPro-Router, fazer a exclusão dos endereços de IP que foram setados de forma estática para o AP da rede, do dhcp pool vlan200 para não ocorrer conflito de IP:.....	27
17ª Etapa: Configurar o acesso à rede com SSID e PSK nos endpoints de usuários:.....	28
18ª Etapa: Configurar o recebimento de IP dinâmico via DHCP do endpoint de usuário da rede vlan200 Dispositivos-Pessoais:.....	29
19ª Etapa: Conectar demais dispositivos e realizar o teste de conectividade com o a subinterface do gateway padrão da rede vlan 200:.....	30
20ª Etapa: Configurar o AP-Convidados com IP estático, desabilitar o DHCP interno, pois a rede já está configurada para entrega de DHCP e desativar o SSID Broadcast semelhantes às etapas nos outros Pontos de Acesso:.....	31
21ª Etapa: No SecurityPro-Router, fazer a exclusão dos endereços de IP que foram setados de forma estática para o AP da rede, do dhcp pool vlan300 Convidados para não ocorrer conflito de IP:.....	32
22ª Etapa: Configurar os clientes para se conectarem à rede. Instalar placa de rede WPC300N em dispositivos que necessitem, e configurar o acesso à rede:.....	33
23ª Etapa: Configurar o recebimento de IP dinâmico via DHCP do endpoint do convidado da rede vlan300 Convidados:.....	35
24ª Etapa: Conectar demais dispositivos e realizar o teste de conectividade com o a subinterface	

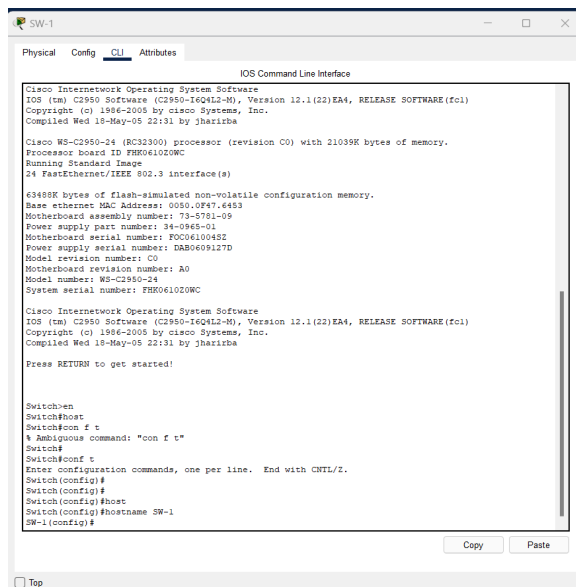
do gateway padrão da rede vlan 300:.....	36
25ª Etapa: Configurar no SecurityPro-Router as listas de acesso para bloquear o acesso ao servidor EAP das vlan 200 e vlan 300 - permitindo somente o tráfego da vlan 100 no servidor:.....	38
26ª Etapa: Configurar as listas de acesso para bloquear o acesso entre vlans:.....	40
27ª Etapa: No SecurityPro-Router realizar escrita em memória para salvar todas as configurações feitas usando os seguintes comandos:.....	41
28ª Etapa: Após salvar as configurações desligar o roteador e instalar a placa serial WC-1T para conexão com outro roteador (que será a simulação da internet):.....	42
29ª Etapa: Interconectar via cabo serial o roteador da rede SecurityPro com o roteador da internet e configurar uma lista de acesso para o protocolo NAT, a fim de evitar exposição de IP privado para a rede externa, sendo realizado a tradução de IP privado para IP público configurado no roteador SecurityPro- Router:.....	43
30ª Etapa: Posicionar os dispositivos:.....	44
31ª Etapa: Configurando as vlans nos switches:.....	45
32ª Etapa: Configurar as vlans 10 DNS e 20 WEB no roteador RouterInternet seguindo os seguintes comandos:.....	46
33ª Etapa: Configurar os servidores com IP Estático de acordo com cada rede criada em nas respectivas Vlans 10 e 20 e conforme documentação de topologia lógica:.....	49
34ª Etapa: Configurar os servidores com os seus respectivos serviços e desabilitar demais serviços que não serão utilizados:.....	51
35ª Etapa: No SecurityPro-Router configurar dentro do dhcp pool vlan, o servidor DNS:.....	55
36ª Etapa: Confirmar entrega de DNS via DHCP em cada end devices das redes nas vlans 100, 200 e 300:.....	56
37ª Etapa: Configurar a tabela de roteamento de SecurityRouter-Pro para que a rede interna envie o tráfego e consiga acessar por padrão a rede serial (internet) e o OSPF para anúncio de rede:.....	57
38ª Etapa: Realizar o teste de conectividade no servidor DNS e WEB.....	58
39ª Etapa - Após todas as configurações de rede WLAN e WAN, realizar a escrita na memória nos dispositivos de roteadores e switches com o comando wr (write).....	60
40ª Etapa: Acessar a web através dos dispositivos finais em cada uma das rede vlans 100, 200 e 300 para verificar todo o acesso na internet, conforme o objetivo inicial da WLAN:.....	60

# Processo de configuração da rede

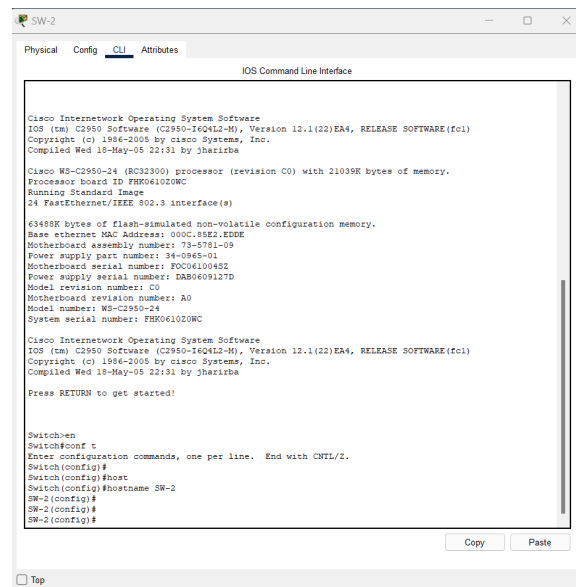
**1ª Etapa: Escolha e posicionamento dos dispositivos a serem utilizados na rede:**



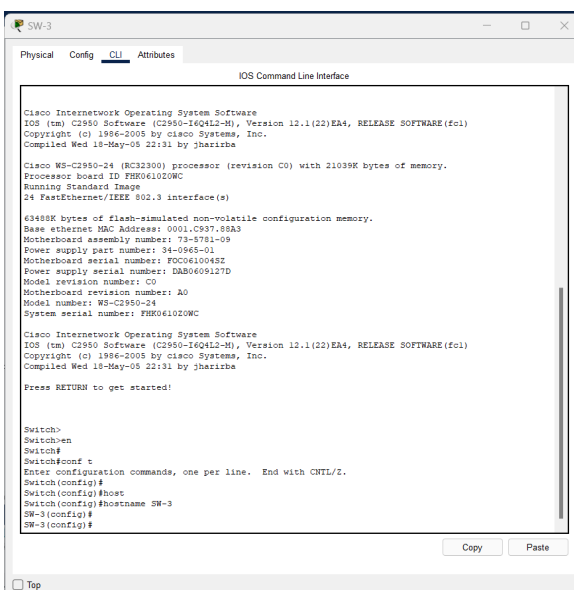
## 2ª Etapa: Renomear os dispositivos na rede:



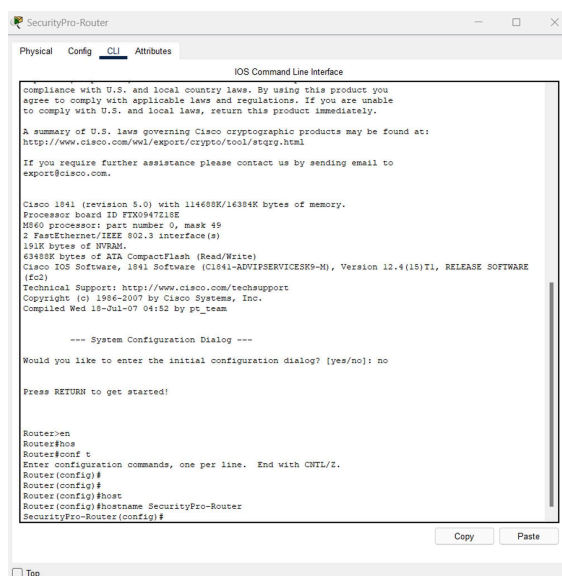
## Renomeando o SW-1



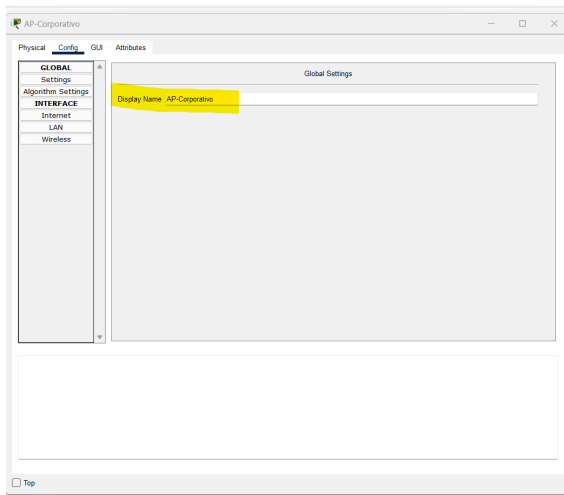
## Renomeando o SW-2



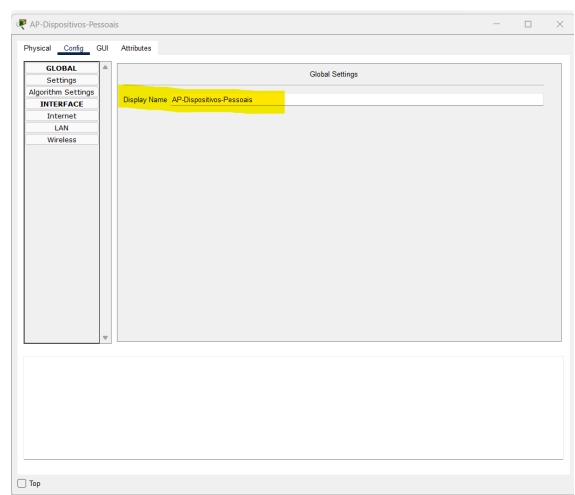
## Renomeando o SW-3



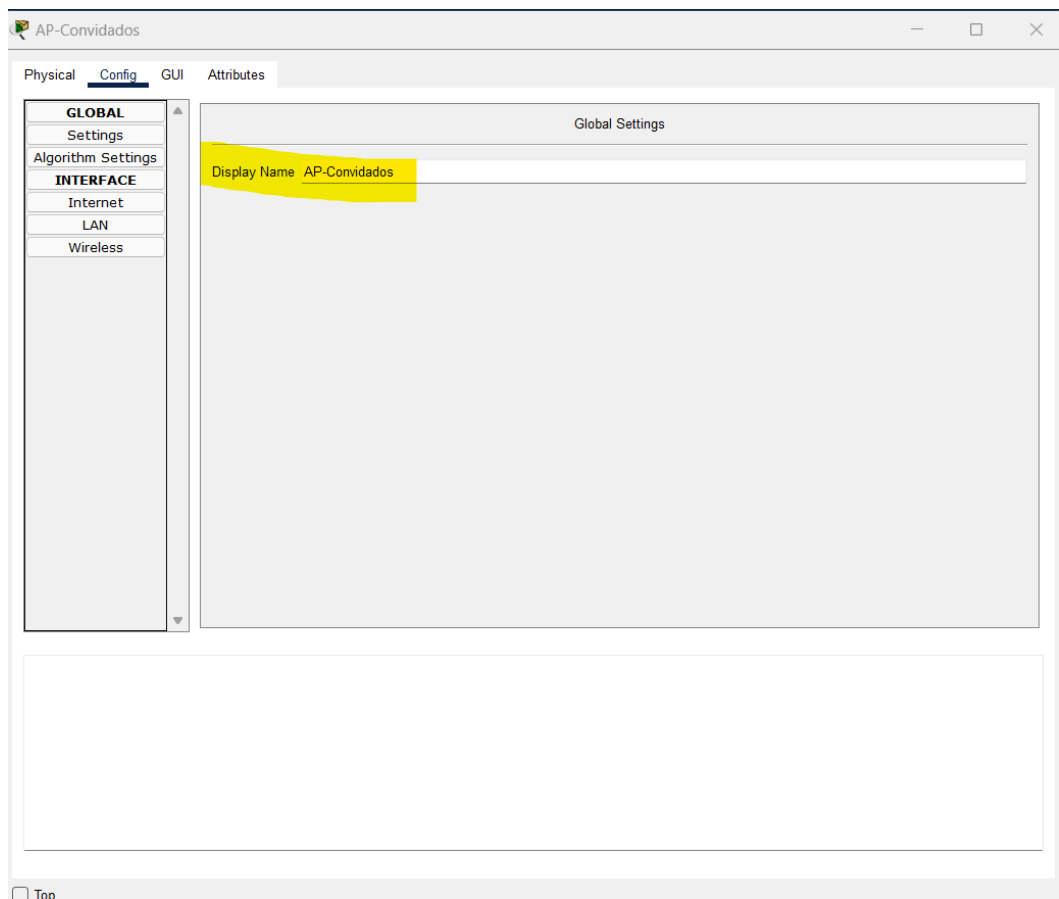
## Renomeando o roteador para SecurityPro- Router



Renomeando o AP-Corporativo

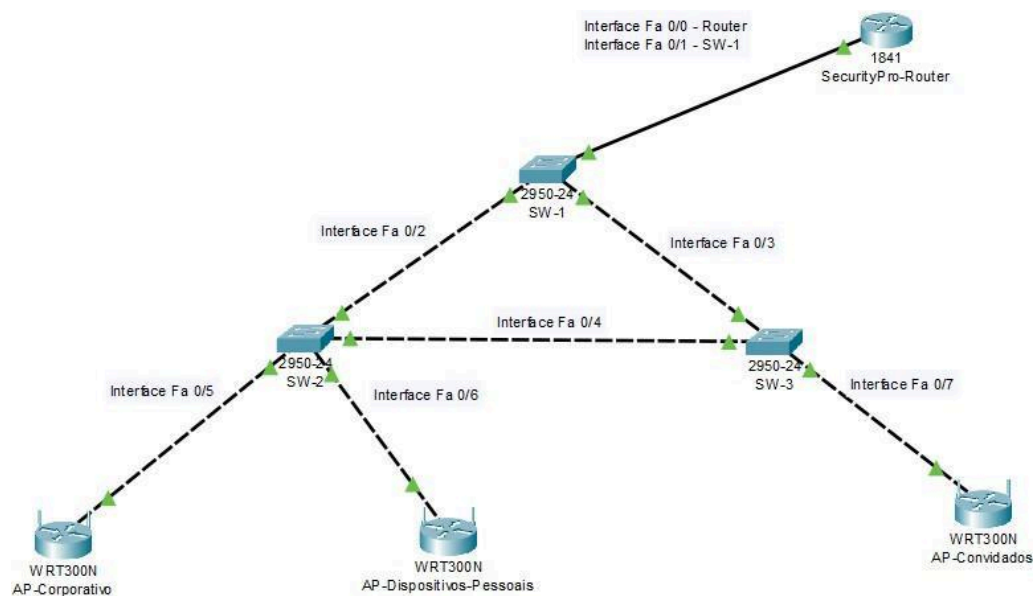


Renomeando o AP-Dispositivos-Pessoais

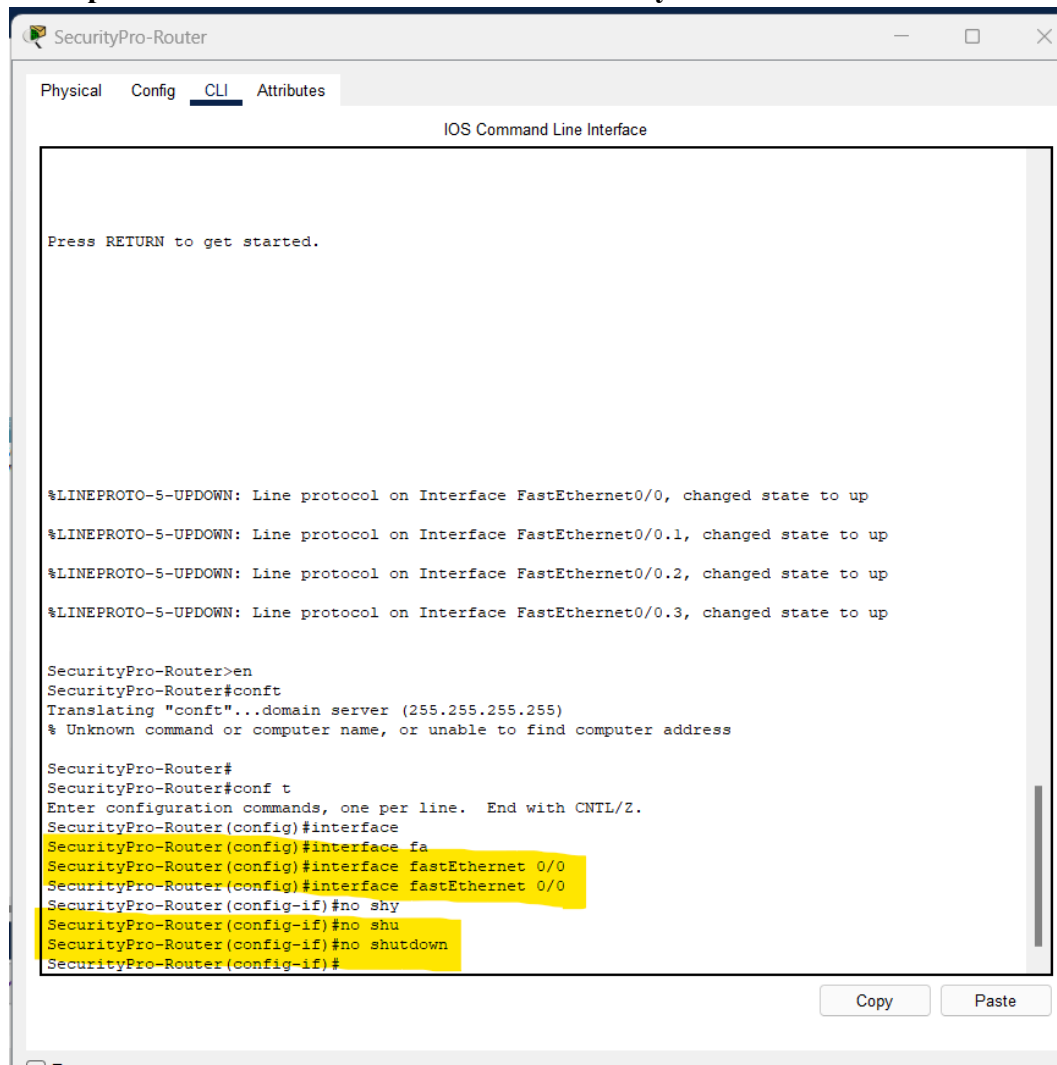


Renomeando o AP-Convidados

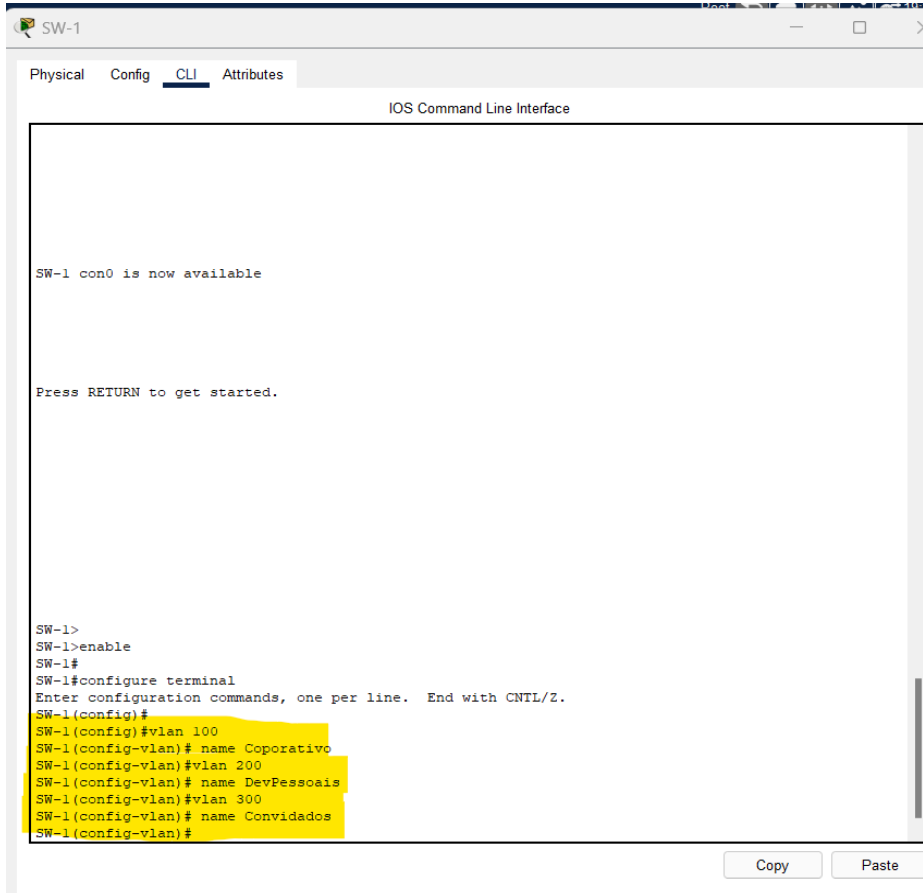
### 3ª Etapa: Conectar fisicamente os dispositivos via cabo:



#### 4ª Etapa: Ativar a interface do roteador SecurityPro-Router:



## 5ª Etapa: Criar as Vlans nos switches SW-1, SW-2 e SW-3:



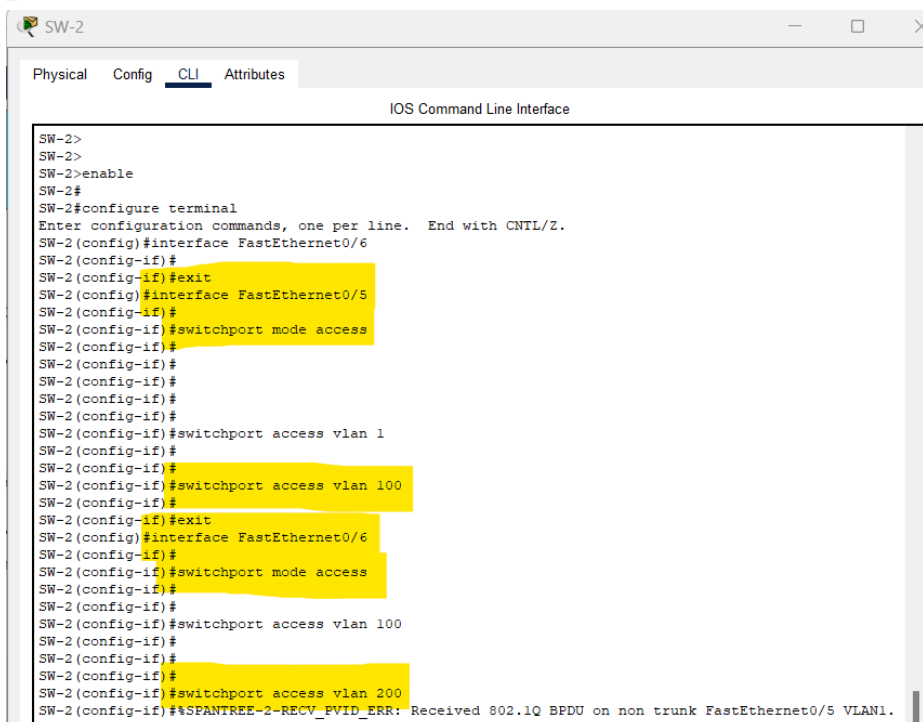
The screenshot shows the CLI interface for switch SW-1. The interface has tabs for Physical, Config, CLI (selected), and Attributes. The title bar says "SW-1" and the window title is "IOS Command Line Interface". The main area displays the following text:

```
SW-1 con0 is now available

Press RETURN to get started.

SW-1>
SW-1>enable
SW-1#
SW-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-1(config)#
SW-1(config)#vlan 100
SW-1(config-vlan)# name Coporativo
SW-1(config-vlan)#vlan 200
SW-1(config-vlan)# name DevPessoais
SW-1(config-vlan)#vlan 300
SW-1(config-vlan)# name Convidados
SW-1(config-vlan)#
```

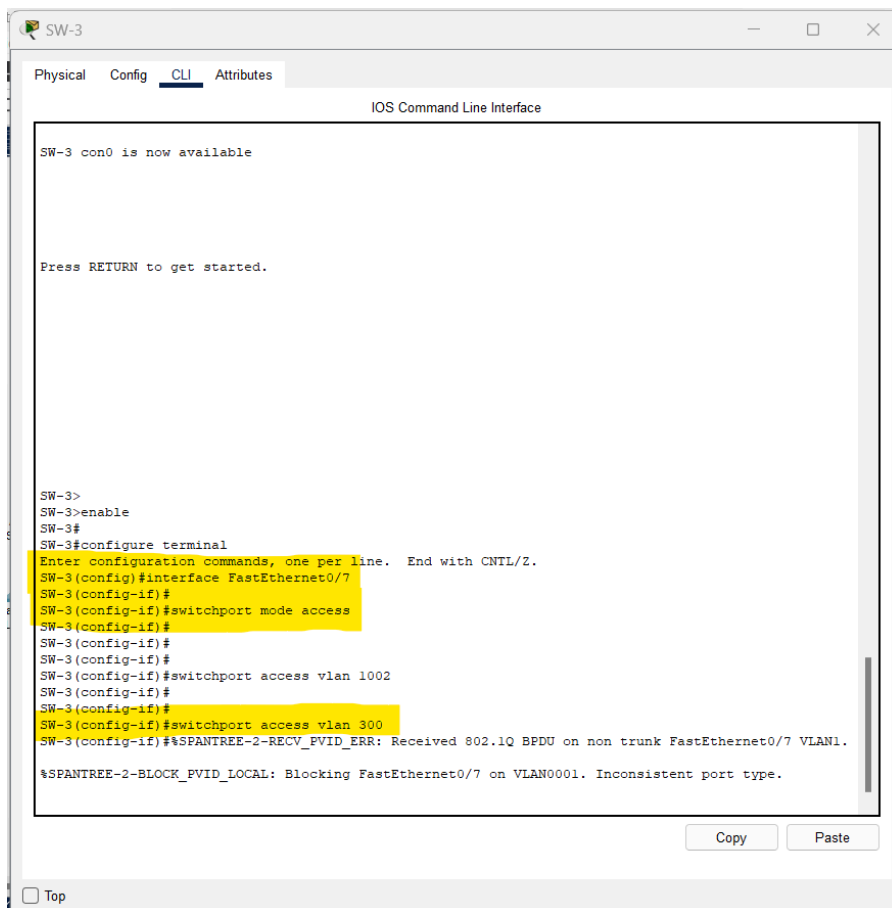
At the bottom right, there are "Copy" and "Paste" buttons.



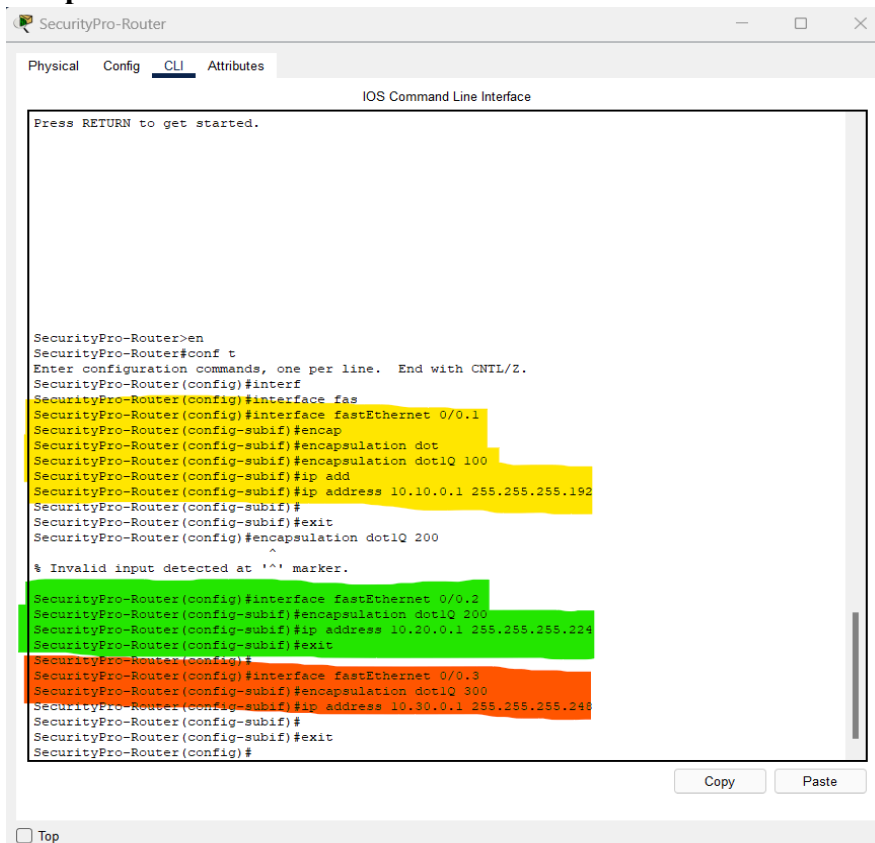
The screenshot shows the CLI interface for switch SW-2. The interface has tabs for Physical, Config, CLI (selected), and Attributes. The title bar says "SW-2" and the window title is "IOS Command Line Interface". The main area displays the following text:

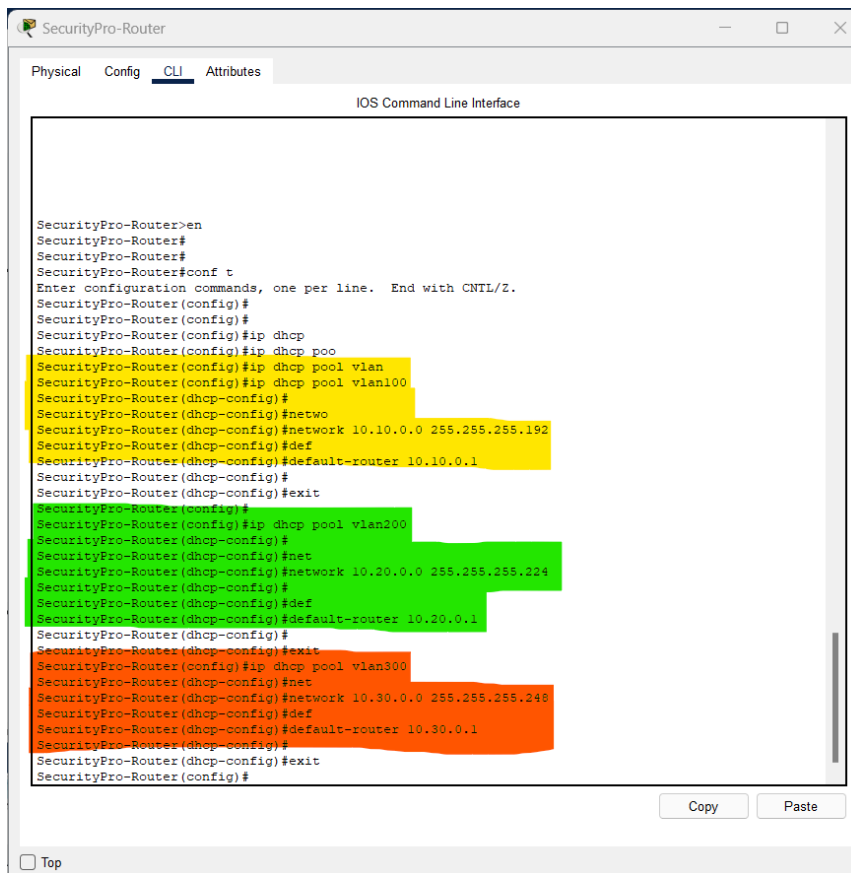
```
SW-2>
SW-2>
SW-2>enable
SW-2#
SW-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-2(config)#interface FastEthernet0/6
SW-2(config-if)#
SW-2(config-if)#exit
SW-2(config)#interface FastEthernet0/5
SW-2(config-if)#
SW-2(config-if)#switchport mode access
SW-2(config-if)#
SW-2(config-if)#
SW-2(config-if)#
SW-2(config-if)#
SW-2(config-if)#switchport access vlan 1
SW-2(config-if)#
SW-2(config-if)#
SW-2(config-if)#switchport access vlan 100
SW-2(config-if)#
SW-2(config-if)#exit
SW-2(config)#interface FastEthernet0/6
SW-2(config-if)#
SW-2(config-if)#switchport mode access
SW-2(config-if)#
SW-2(config-if)#
SW-2(config-if)#switchport access vlan 100
SW-2(config-if)#
SW-2(config-if)#
SW-2(config-if)#
SW-2(config-if)#switchport access vlan 200
SW-2(config-if)##SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/5 VLAN1.
```



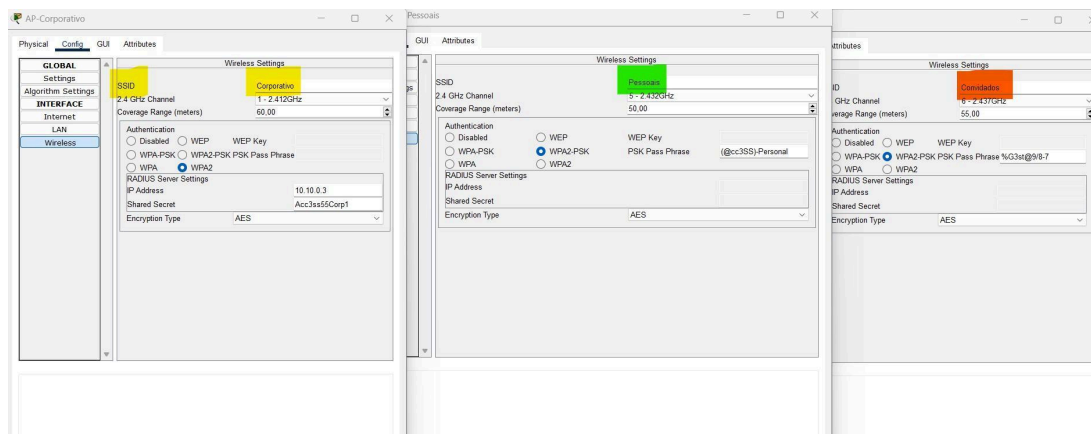


## 6ª Etapa: Configurar o DHCP pool vlan no roteador SecurityPro-Router e realizar o encapsulamento das vlans nas sub interfaces do roteador.

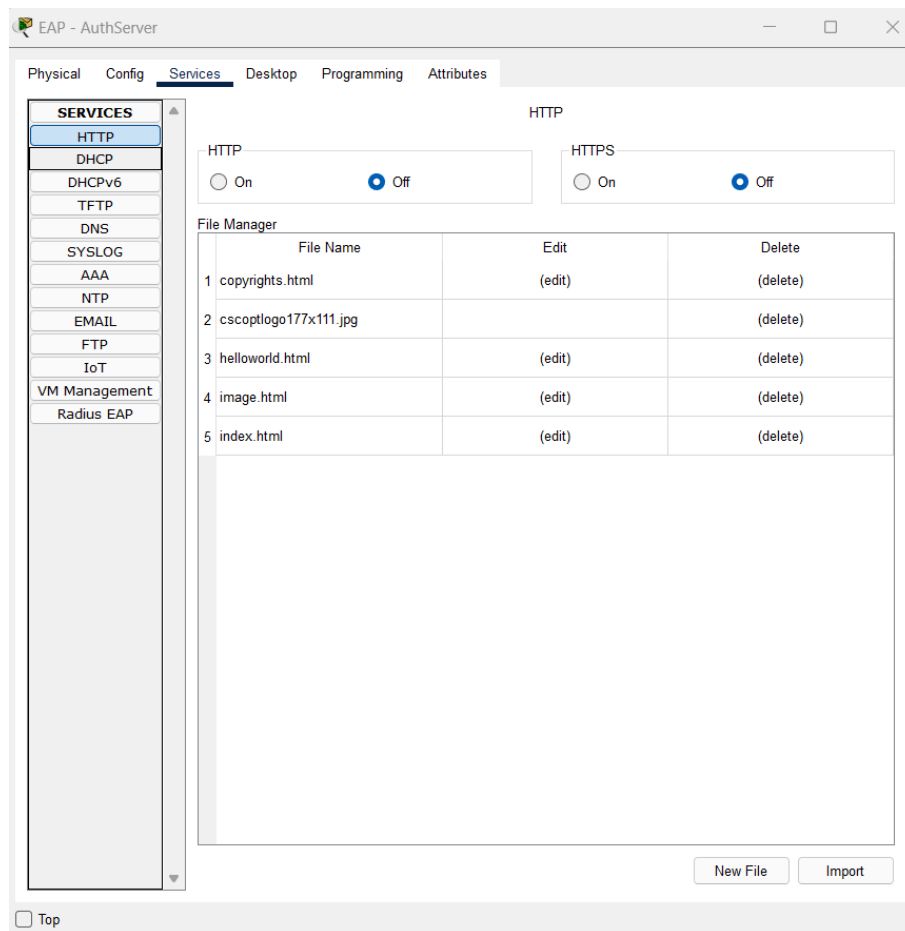




## 7ª Etapa: Configurar o SSID em cada Ponto de Acesso (AP):



**8ª Etapa: Adicionar um servidor EAP, desabilitar os serviços que não serão utilizados e ativar o serviço de autenticação AAA:**



## 9ª Etapa: Configurar o IP do servidor EAP Radius de forma estática, seguindo a documentação da topologia lógica:

The screenshot shows the 'EAP - AuthServer' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing settings for both IPv4 and IPv6. The IPv4 configuration is set to 'Static' with an IP address of 10.10.0.3, subnet mask of 255.255.255.192, default gateway of 10.10.0.1, and DNS server of 0.0.0.0. The IPv6 configuration is also set to 'Static' with a link local address of FE80::240:BFF:FEBD:E290. The '802.1X' section is collapsed, showing options for 'Use 802.1X Security', 'Authentication' (MD5), 'Username', and 'Password'.

Section	Option	Value
IP Configuration	Static	<input checked="" type="radio"/>
	IPv4 Address	10.10.0.3
	Subnet Mask	255.255.255.192
	Default Gateway	10.10.0.1
	DNS Server	0.0.0.0
IPv6 Configuration	Static	<input checked="" type="radio"/>
	IPv6 Address	
	Link Local Address	FE80::240:BFF:FEBD:E290
	Default Gateway	
	DNS Server	
802.1X	Use 802.1X Security	<input type="checkbox"/>
	Authentication	MD5
	Username	
	Password	

☐ Top

10ª Etapa: Configurar o servidor EAP para autenticação dos usuários com os dispositivos corporativos, criar usuário e senha:

EAP - AuthServer

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

**AAA**

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

AAA

Service ☒ On ☐ Off Radius Port 1645

Network Configuration

Client Name Client IP

Secret ServerType Radius

	Client Name	Client IP	Server Type	Key	
1	AP-Corporativo	10.10.0.2	Radius	Acc3ss55Corp1	Add
					Save
					Remove

User Setup

Username Password

	Username	Password	
1	UserCorp01	C0nTroll?1Y3s	Add
2	UserCorp02	F0r@cc3ss/10	
3	UserCorp03	T3nt@(100)2	Save
4	UserCorp04	T3nt@(2)-100:	
5	UserCorp05	FF/05-Auth01	Remove

☐ Top

**11ª Etapa: Configurar o AP-Corporativo com IP estático, desabilitar o DHCP interno, pois a rede já está configurada para entrega de DHCP e conectar o AP-Corporativo para autenticação no servidor EAP, desabilitar o SSID Broadcast para evitar fácil identificação da rede:**

AP-Corporativo

Physical Config **GUI** Attributes

Wireless-N Broadband Router Firmware Version: v0.93.3

**Setup** Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing

**Internet Setup**

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers):

Host Name:

Domain Name:

MTU:  Size: 1500

**Network Setup**

Router IP: IP Address: 10 . 10 . 0 . 2 Subnet Mask: 255.255.255.192

DHCP Server Settings: DHCP Server: ☐ Enabled ☒ Disabled DHCP Reservation

Start IP Address: 10.10.0.1

Maximum number of Users: 50

IP Address Range: 10.10.0.1 - 50

Client Lease Time: 0 minutes (0 means one day)

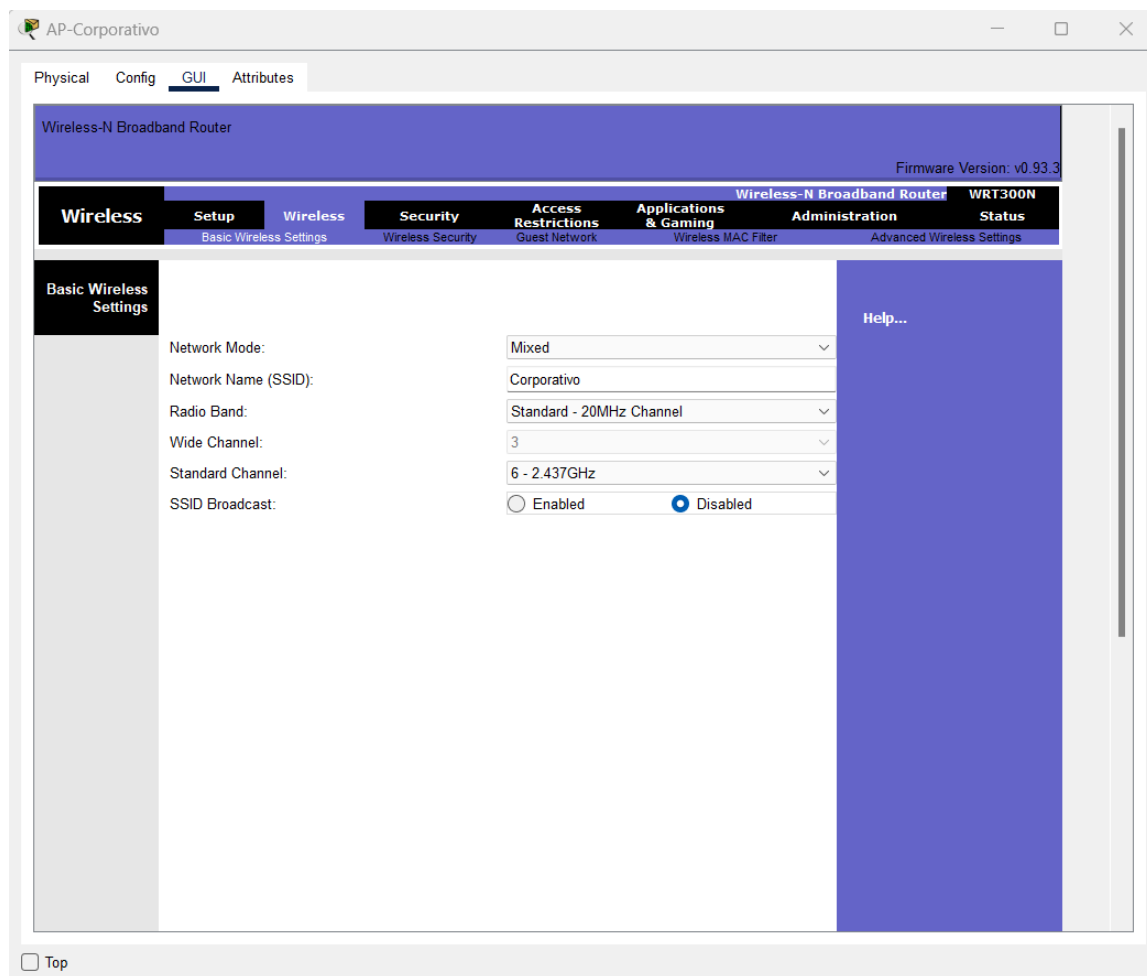
Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

☐ Top



Desabilitar o SSID para evitar reconhecimento na rede.

AP-Corporativo

Physical **Config** GUI Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

Internet

LAN

**Wireless**

**Wireless Settings**

SSID: Corporativo

2.4 GHz Channel: 1 - 2.412GHz

Coverage Range (meters): 60,00

Authentication:

☐ Disabled ☐ WEP ☐ WPA-PSK ☐ WPA2-PSK ☒ WPA2

WEP Key:

PSK Pass Phrase:

RADIUS Server Settings

IP Address: 10.10.0.3

Shared Secret: Acc3ss55Corp1

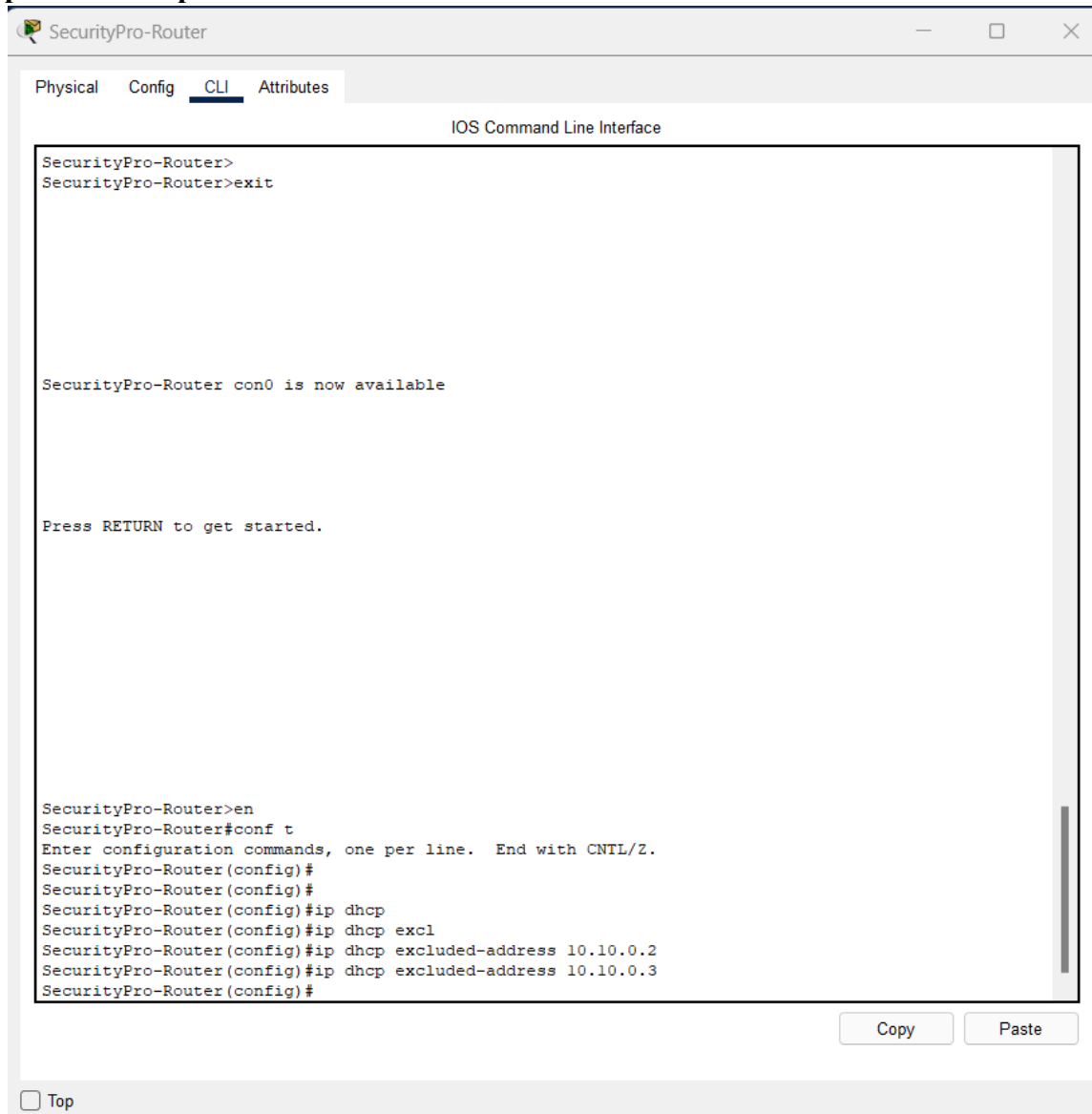
Encryption Type: AES

☐ Top

Configurar para acesso a rede com IP do Servidor de autenticação e senha.

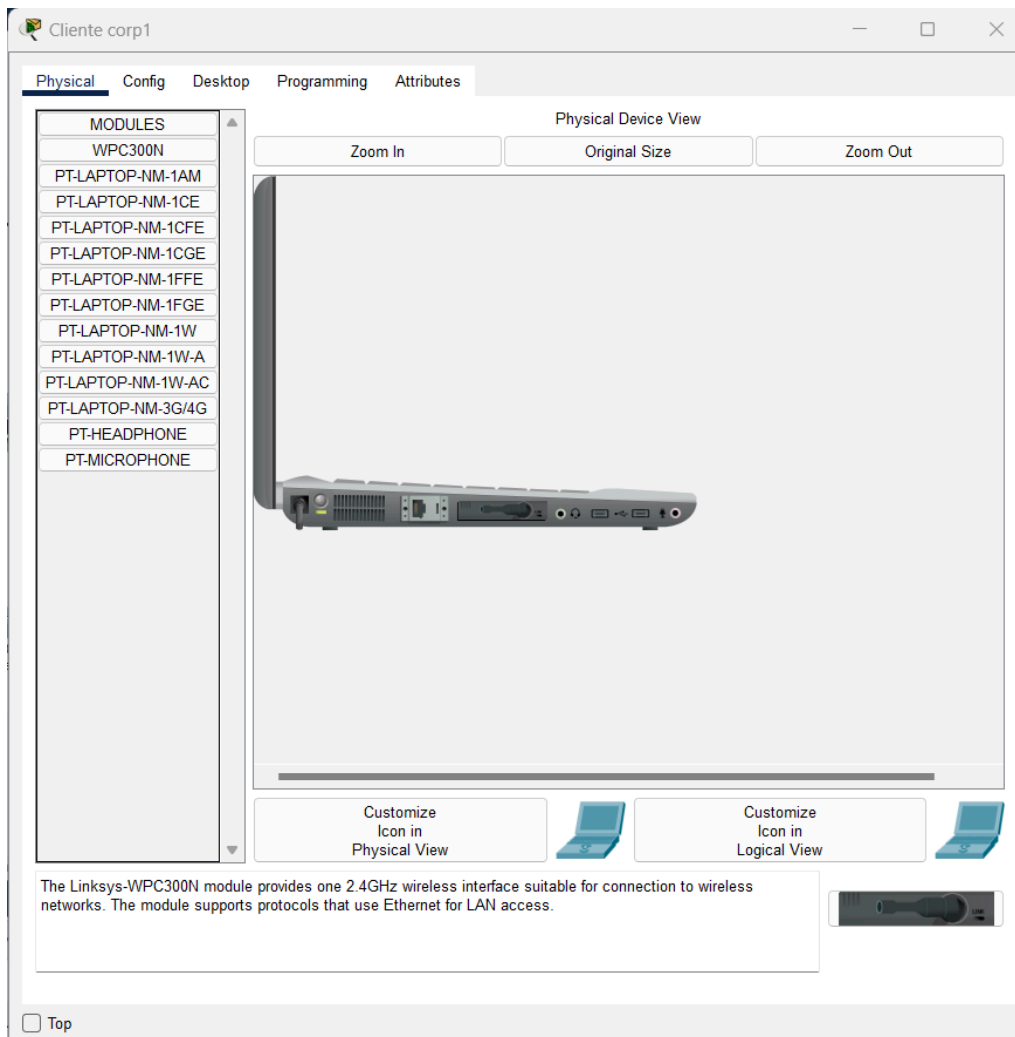


**12ª Etapa: No SecurityPro-Router, fazer a exclusão dos endereços de IP que foram setados de forma estática para o servidor EAP e o Ponto de Acesso da rede, do dhcp pool vlan100 para não ocorrer conflito de IP:**



**13ª Etapa: Configurar os clientes para se conectarem à rede. Instalar placa de rede em dispositivos que necessitem, e configurar o acesso à rede:**

- Desligue o laptop, e faça a troca escolhendo nas opções ao lado a placa WPC300N. Depois ligue o laptop novamente.



Instalar placa de rede WPC300N .

Cliente corp1

Physical **Config** Desktop Programming Attributes

**GLOBAL**

Settings

Algorithm Settings

**INTERFACE**

Wireless0

Bluetooth

**Wireless0**

Port Status ☒ On

Bandwidth 300 Mbps

MAC Address 00D0.BCEC.10E2

SSID Corporativo

Authentication

☐ Disabled ☐ WEP ☐ WPA-PSK ☐ WPA ☐ 802.1X ☒ WPA2

Method: WEP Key PSK Pass Phrase User ID Password User Name Password

MD5 C0nTroll?1Y3s

Encryption Type AES

IP Configuration

☒ DHCP ☐ Static

IPv4 Address 10.10.0.4

Subnet Mask 255.255.255.192

IPv6 Configuration

☒ Automatic ☐ Static

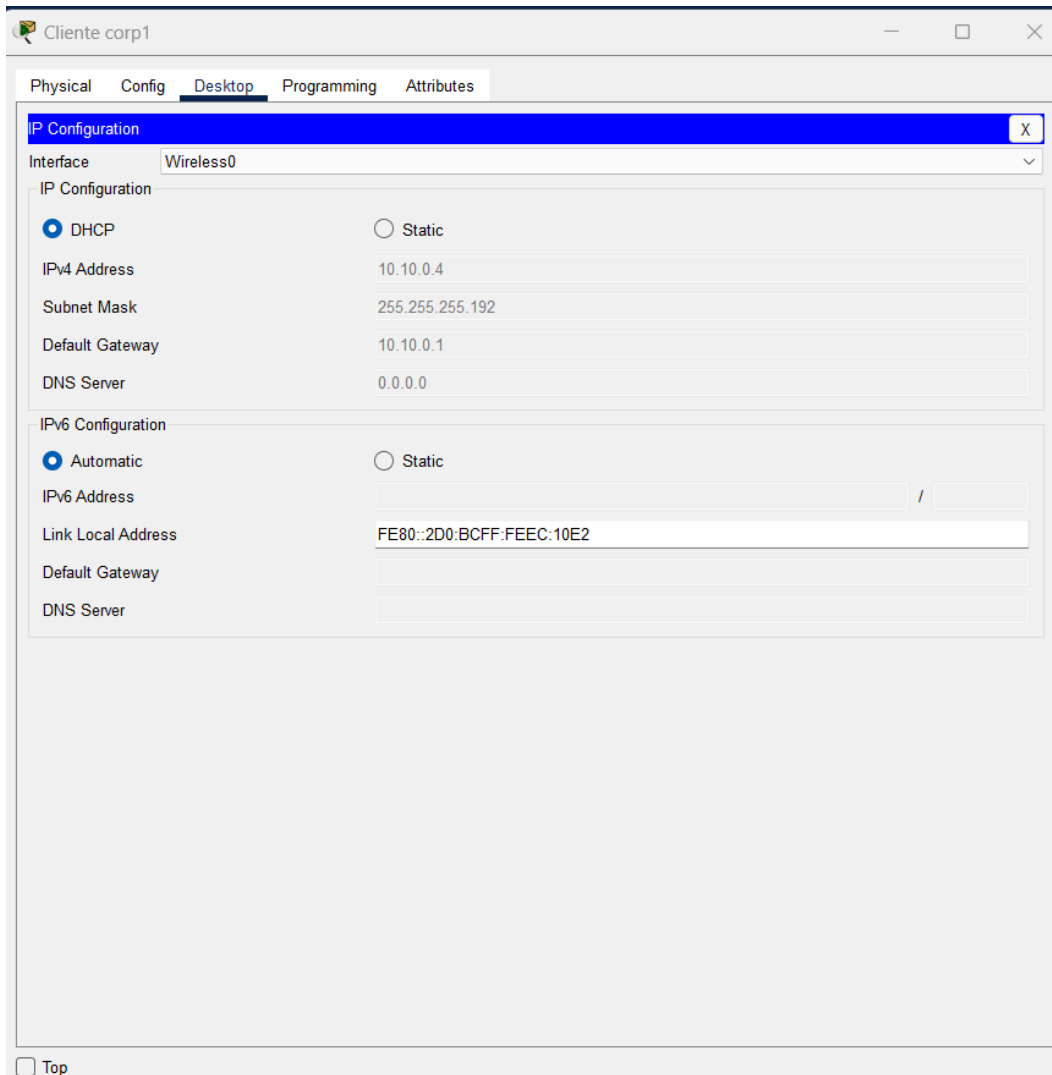
IPv6 Address /

Link Local Address FE80::2D0:BCFF:FEEC:10E2

☐ Top

Configurar a rede com o SSID, UserID e Password, que foram configurados também no servidor EAP para autenticação.

**14ª Etapa: Ativar o recebimento de IP dinâmico via DHCP e realizar o teste de conectividade com ICMP (ping):**



Cliente corp1

Physical Config **Desktop** Programming Attributes

**IP Configuration** [X]

Interface: Wireless0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 10.10.0.4

Subnet Mask: 255.255.255.192

Default Gateway: 10.10.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address: /

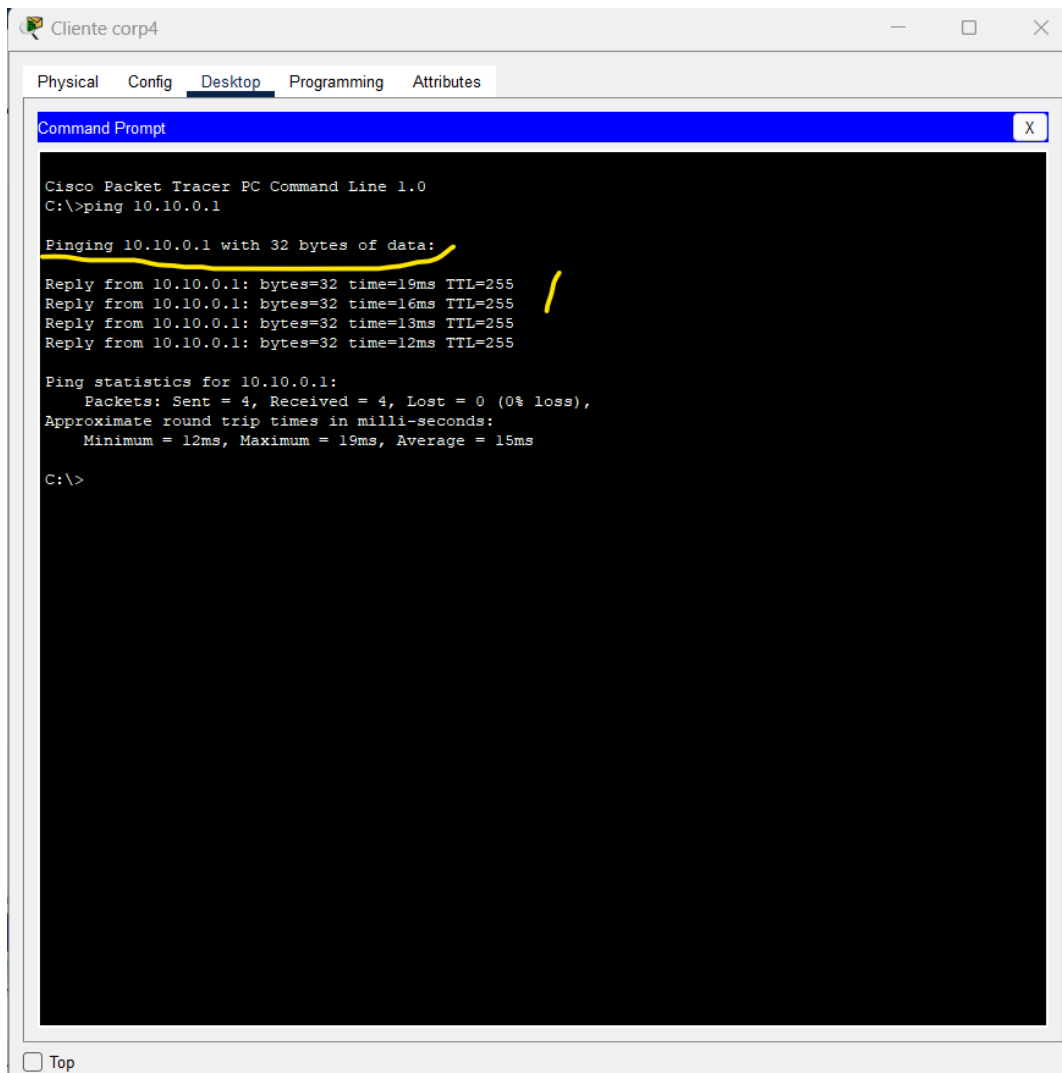
Link Local Address: FE80::2D0:BCFF:FEEC:10E2

Default Gateway:

DNS Server:

☐ Top

Recebimento de IP dinâmico via DHCP.



Teste de conectividade com a sub interface do roteador da vlan100 Corporativo - sucesso!

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.0.1

Pinging 10.10.0.1 with 32 bytes of data:

Reply from 10.10.0.1: bytes=32 time=19ms TTL=255
Reply from 10.10.0.1: bytes=32 time=16ms TTL=255
Reply from 10.10.0.1: bytes=32 time=13ms TTL=255
Reply from 10.10.0.1: bytes=32 time=12ms TTL=255

Ping statistics for 10.10.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 19ms, Average = 15ms

C:\>ping 10.10.0.3

Pinging 10.10.0.3 with 32 bytes of data:
Reply from 10.10.0.3: bytes=32 time=25ms TTL=128
Reply from 10.10.0.3: bytes=32 time=12ms TTL=128
Reply from 10.10.0.3: bytes=32 time=17ms TTL=128
Reply from 10.10.0.3: bytes=32 time=12ms TTL=128

Ping statistics for 10.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 25ms, Average = 16ms

C:\>
```

Teste de conectividade com o servidor EAP - sucesso!

*Após os testes realizados com sucesso, conectar demais dispositivos na rede da vlan100 Corporativo, seguindo os mesmos passos anteriores.*

**15ª Etapa: Configurar o AP-Dispositivos-Pessoais com IP estático, desabilitar o DHCP interno, pois a rede já está configurada para entrega de DHCP e configurar o canal para:**

The screenshot shows the 'Setup' page of a TP-Link WRT300N router. The 'Network Setup' tab is selected, and the 'DHCP Server Settings' section is expanded. The DHCP Server is set to 'Disabled'. The Router IP is set to 10.20.0.2. The Subnet Mask is 255.255.255.224. The DHCP Server Start IP Address is 10.20.0.1, and the Maximum number of Users is 29. The IP Address Range is 10.20.0.1 - 29. The Client Lease Time is 0 minutes. Static DNS 1, 2, and 3 are all set to 0.0.0.0. The WINS section is also visible at the bottom.

Physical Config **GUI** Attributes

Wireless-N Broadband Router Firmware Version: v0.93.3

**Setup** Setup **Wireless** Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing

**Internet Setup**

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers):

Host Name: Domain Name: MTU: Size: 1500

**Network Setup**

Router IP: IP Address: 10 . 20 . 0 . 2 Subnet Mask: 255.255.255.224

DHCP Server Settings: DHCP Server: ☐ Enabled ☒ Disabled DHCP Reservation

Start IP Address: 10.20.0.1

Maximum number of Users: 29

IP Address Range: 10.20.0.1 - 29

Client Lease Time: 0 minutes (0 means one day)

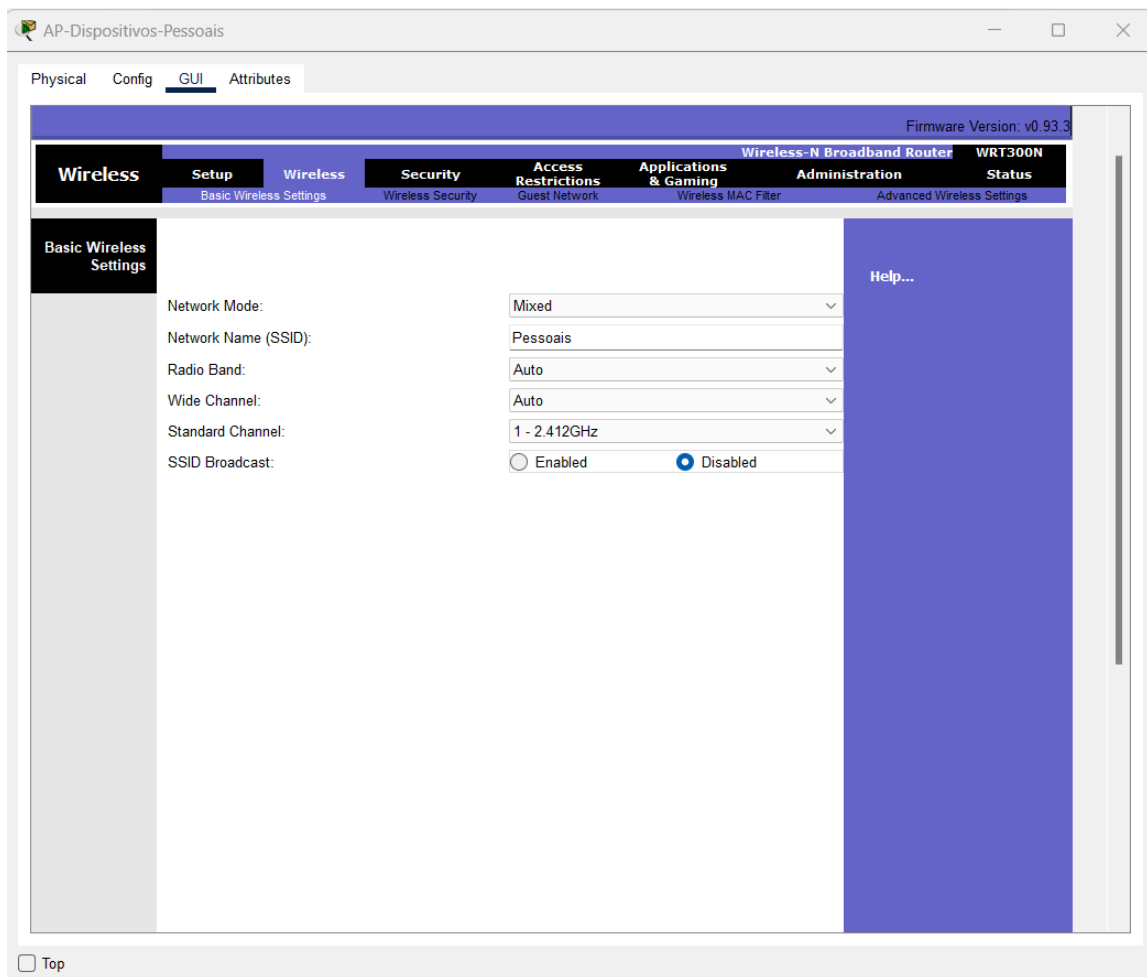
Static DNS 1: 0 . 0 . 0 . 0

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

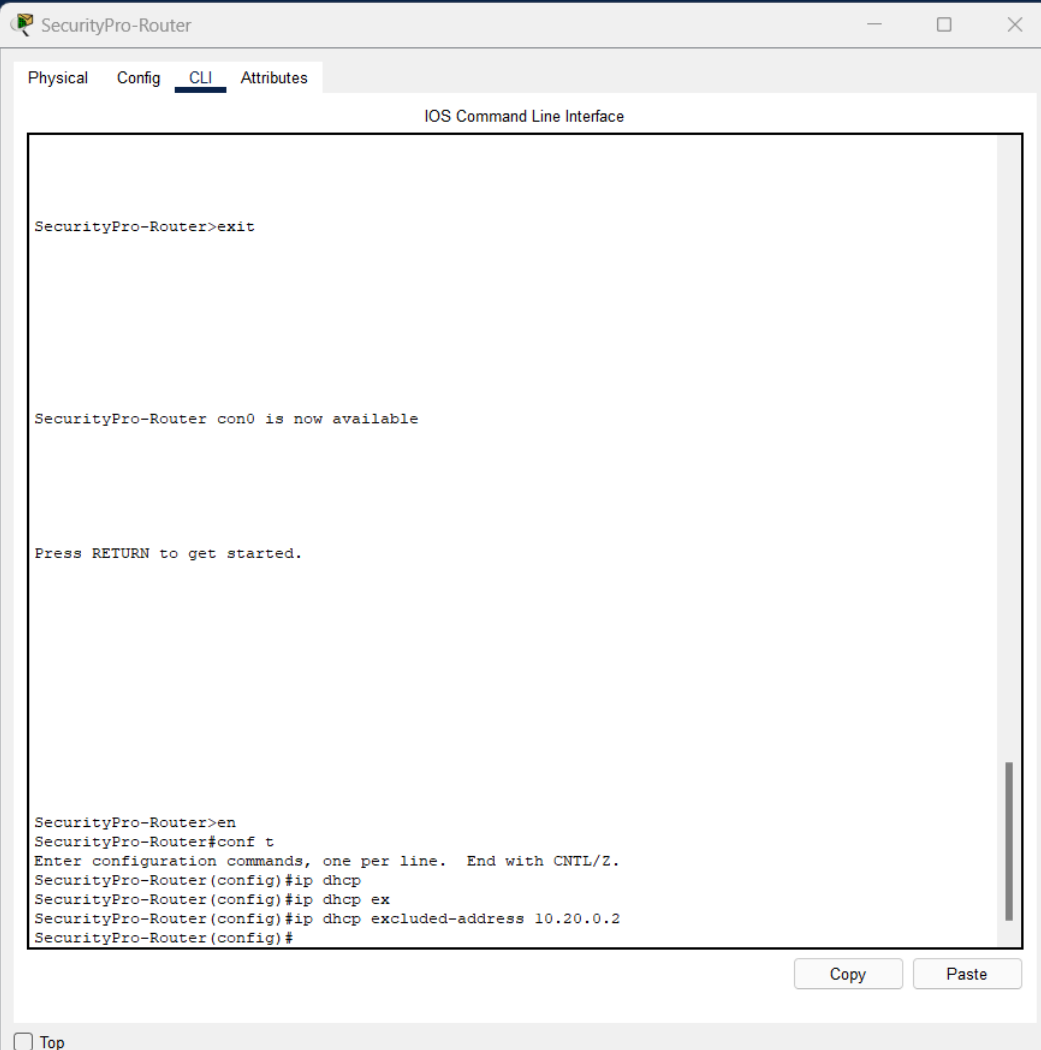
☐ Top



Desabilitar o SSID para evitar reconhecimento na rede.



**16ª Etapa: No SecurityPro-Router, fazer a exclusão dos endereços de IP que foram setados de forma estática para o AP da rede, do dhcp pool vlan200 para não ocorrer conflito de IP:**



The screenshot shows a web-based interface for the SecurityPro-Router. At the top, there are tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' being the active tab. Below the tabs, the title 'IOS Command Line Interface' is displayed. The main area contains a text box with the following text:

```
SecurityPro-Router>exit

SecurityPro-Router con0 is now available

Press RETURN to get started.

SecurityPro-Router>en
SecurityPro-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecurityPro-Router(config)#ip dhcp
SecurityPro-Router(config)#ip dhcp ex
SecurityPro-Router(config)#ip dhcp excluded-address 10.20.0.2
SecurityPro-Router(config)#
```

At the bottom right of the text box, there are 'Copy' and 'Paste' buttons. At the bottom left of the interface, there is a 'Top' link.

## 17ª Etapa: Configurar o acesso à rede com SSID e PSK nos endpoints de usuários:

The screenshot shows the configuration window for the 'Smartphone Bianca' device. The 'Config' tab is selected, and the 'Wireless0' interface is chosen from the left sidebar. The main configuration area is divided into several sections:

- Wireless0**
  - Port Status: ☒ On
  - Bandwidth: 300 Mbps
  - MAC Address: 000C.8537.C0B1
  - SSID: Pessoais
- Authentication**
  - ☐ Disabled
  - ☐ WEP
  - ☒ WPA-PSK
  - ☐ WPA
  - ☐ WPA2
  - ☐ 802.1X
  - Method: MD5
  - WEP Key: [empty]
  - PSK Pass Phrase: (@cc3SS)-Personal
  - User ID: [empty]
  - Password: [empty]
  - User Name: [empty]
  - Password: [empty]
  - Encryption Type: AES
- IP Configuration**
  - ☒ DHCP
  - ☐ Static
  - IPv4 Address: 10.20.0.3
  - Subnet Mask: 255.255.255.224
- IPv6 Configuration**
  - ☒ Automatic
  - ☐ Static
  - IPv6 Address: [empty]
  - Link Local Address: FE80::20C:85FF:FE37:C0B1

At the bottom left, there is a 'Top' button.

## 18ª Etapa: Configurar o recebimento de IP dinâmico via DHCP do endpoint de usuário da rede vlan200 Dispositivos-Pessoais:

Smartphone Bianca

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: Wireless0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address: 10.20.0.3

Subnet Mask: 255.255.255.224

Default Gateway: 10.20.0.1

DNS Server: 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address: /

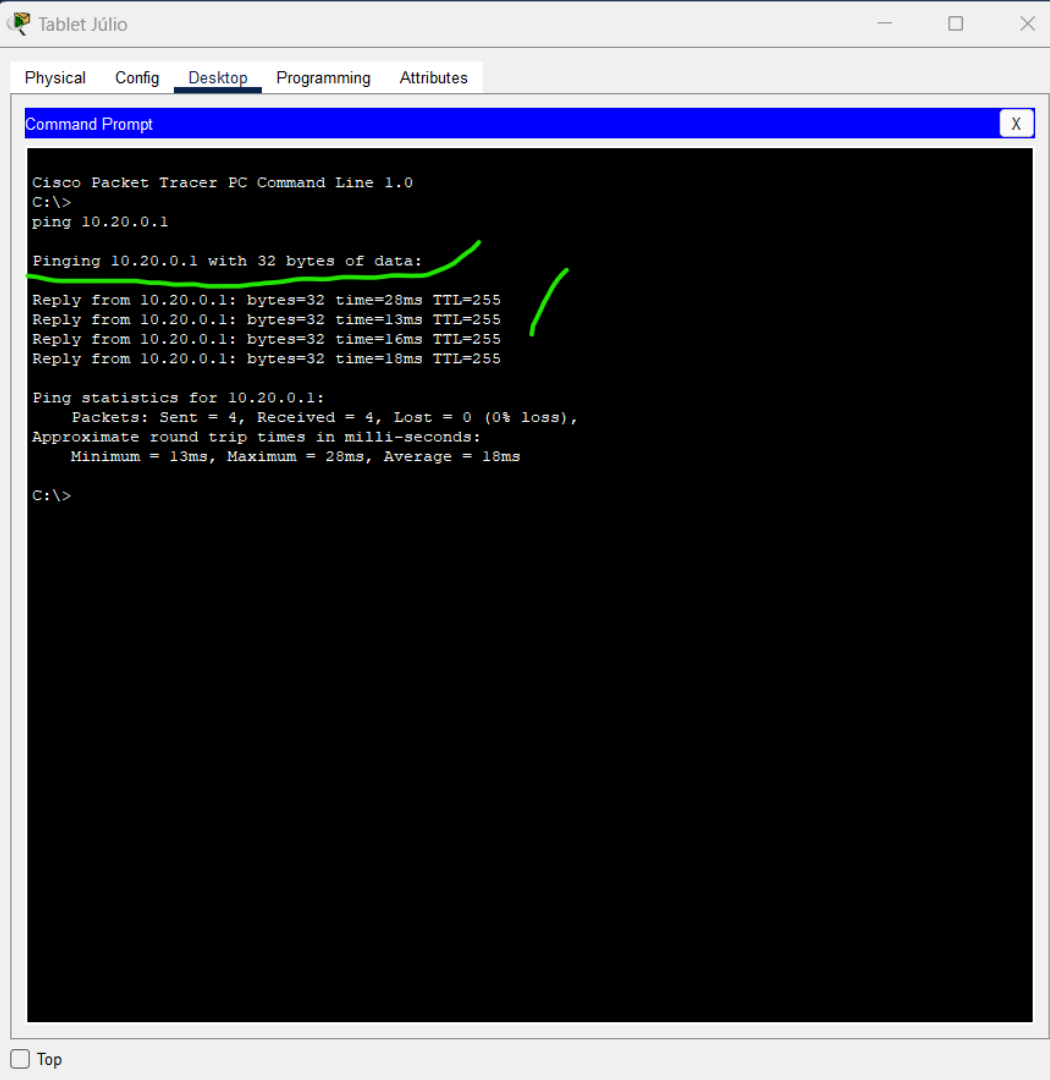
Link Local Address: FE80::20C:85FF:FE37:C0B1

Default Gateway:

DNS Server:

☐ Top

**19ª Etapa: Conectar demais dispositivos e realizar o teste de conectividade com o a subinterface do gateway padrão da rede vlan 200:**



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named 'Tablet Júlio'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' currently selected. The command prompt shows the following text:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 10.20.0.1

Pinging 10.20.0.1 with 32 bytes of data:

Reply from 10.20.0.1: bytes=32 time=28ms TTL=255
Reply from 10.20.0.1: bytes=32 time=13ms TTL=255
Reply from 10.20.0.1: bytes=32 time=16ms TTL=255
Reply from 10.20.0.1: bytes=32 time=18ms TTL=255

Ping statistics for 10.20.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 28ms, Average = 18ms

C:\>
```

Hand-drawn green annotations are present: a horizontal line under 'Pinging 10.20.0.1 with 32 bytes of data:', a vertical line to the right of the four 'Reply from' lines, and a diagonal line to the right of the 'Ping statistics' section.

At the bottom left of the window, there is a checkbox labeled 'Top' which is currently unchecked.

Teste de conectividade(ping) com o gateway padrão - sucesso!

*Após os testes realizados com sucesso, conectar demais dispositivos na rede da vlan200 Pessoais, seguindo os mesmos passos anteriores.*

**20ª Etapa: Configurar o AP-Convidados com IP estático, desabilitar o DHCP interno, pois a rede já está configurada para entrega de DHCP e desativar o SSID Broadcast semelhantes às etapas nos outros Pontos de Acesso:**

The screenshot shows the configuration interface for a Wireless-N Broadband Router (WRT300N) with firmware version v0.93.3. The 'Setup' tab is active, and the 'Network Setup' section is expanded. The 'Internet Setup' section shows 'Automatic Configuration - DHCP' selected. The 'Network Setup' section shows the 'Router IP' set to 10.30.0.2 with a subnet mask of 255.255.255.248. The 'DHCP Server Settings' section shows the DHCP server disabled, with a start IP address of 10.30.0.1, a maximum number of users of 5, and an IP address range of 10.30.0.1 - 5. The client lease time is set to 0 minutes. Static DNS settings are also visible.

Physical Config **GUI** Attributes

Wireless-N Broadband Router Firmware Version: v0.93.3

**Setup** Setup **Wireless** Security Access Restrictions Applications & Gaming Administration Status

Basic Setup DDNS MAC Address Clone Advanced Routing

**Internet Setup**

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers):

Host Name: Domain Name: MTU: Size: 1500

**Network Setup**

Router IP: IP Address: 10 . 30 . 0 . 2 Subnet Mask: 255.255.255.248

DHCP Server: ☐ Enabled ☒ Disabled DHCP Reservation

Start IP Address: 10.30.0.1

Maximum number of Users: 5

IP Address Range: 10.30.0.1 - 5

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: 0 . 0 . 0 . 0

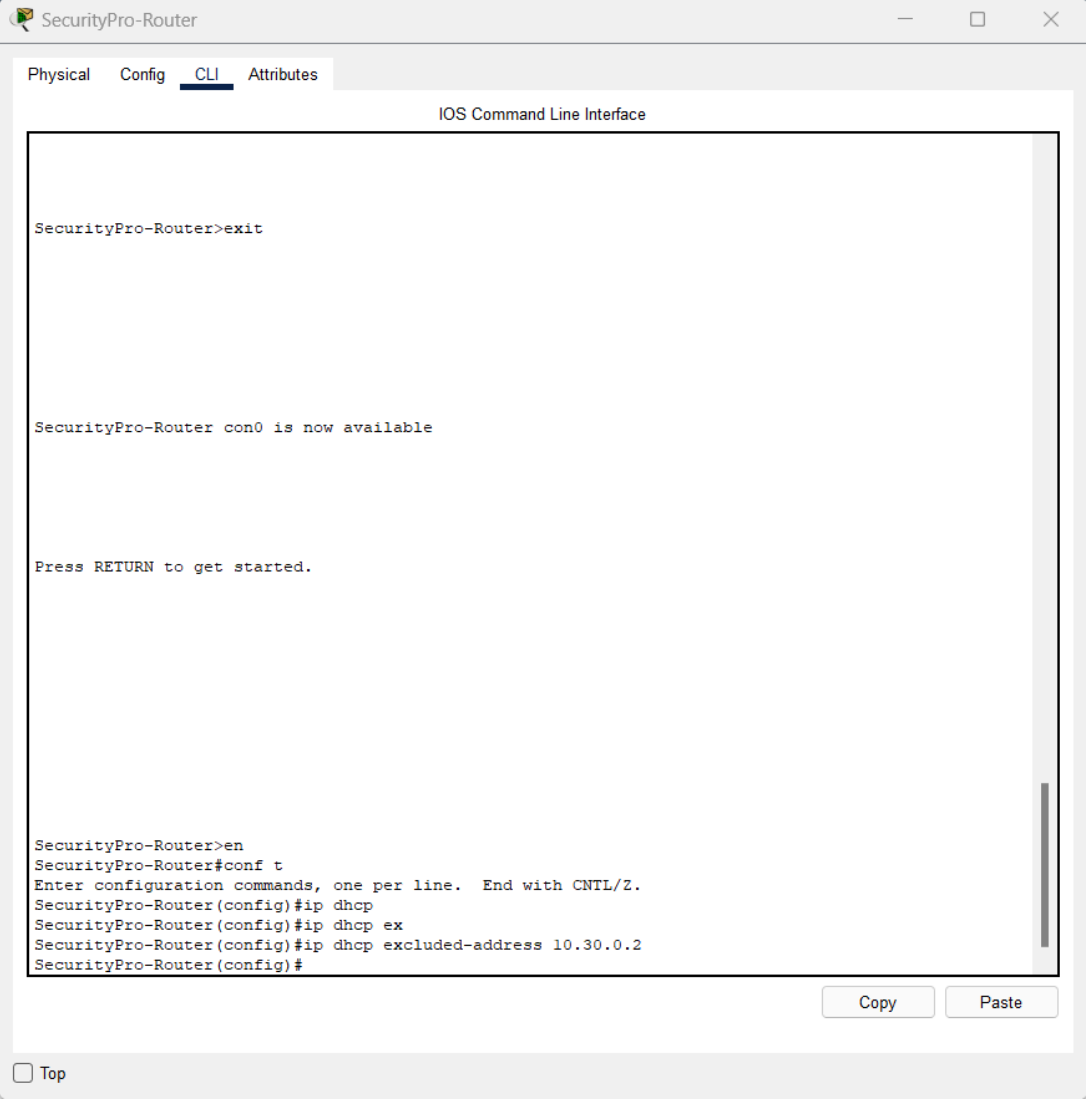
Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

WINS: 0 . 0 . 0 . 0

☐ Top

**21ª Etapa: No SecurityPro-Router, fazer a exclusão dos endereços de IP que foram setados de forma estática para o AP da rede, do dhcp pool vlan300 Convidados para não ocorrer conflito de IP:**



The screenshot shows a web-based interface for the SecurityPro-Router. At the top, there are tabs for 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs is a header for the 'IOS Command Line Interface'. The main area is a text box containing the following text:

```
SecurityPro-Router>exit

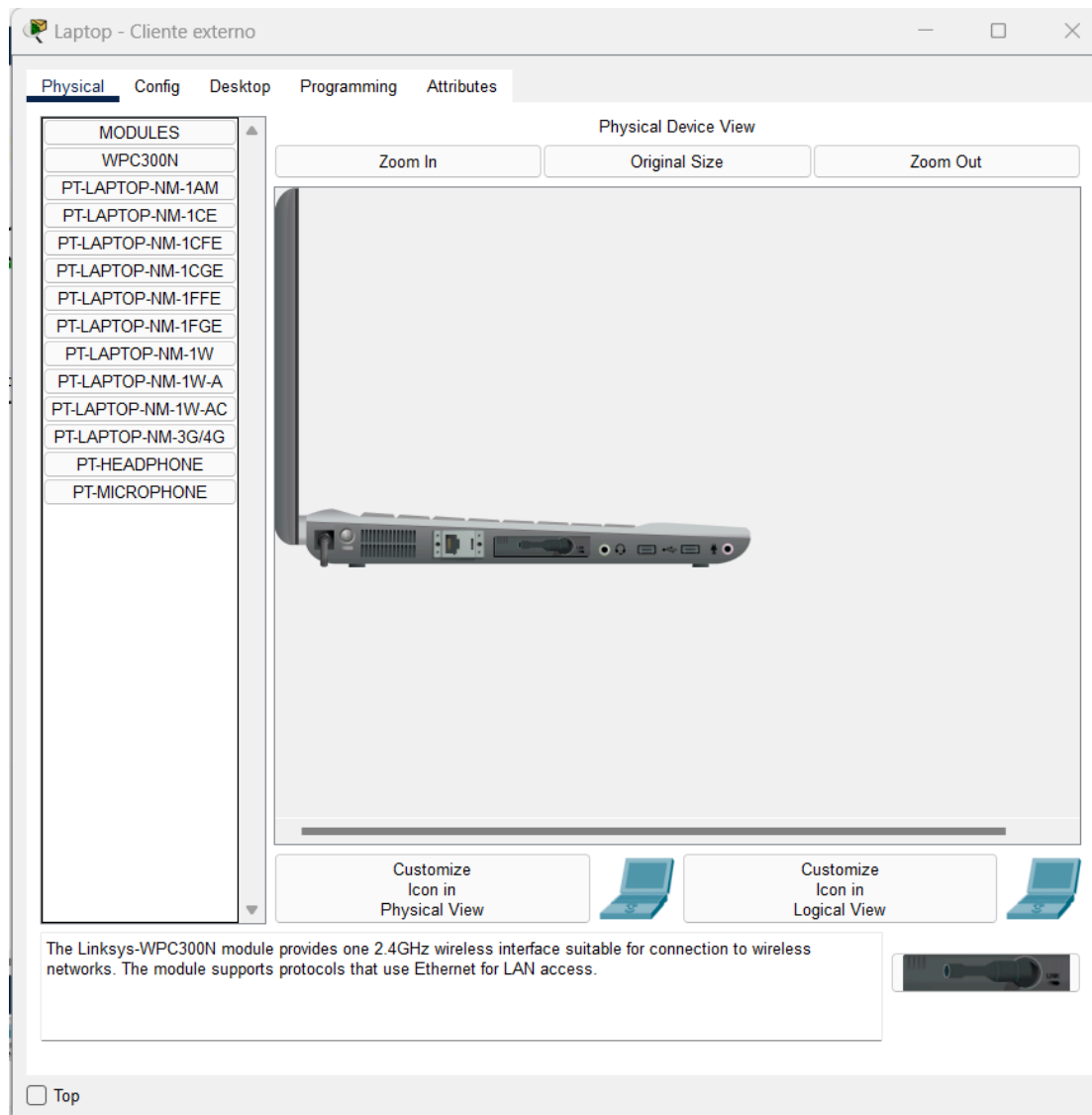
SecurityPro-Router con0 is now available

Press RETURN to get started.

SecurityPro-Router>en
SecurityPro-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecurityPro-Router(config)#ip dhcp
SecurityPro-Router(config)#ip dhcp ex
SecurityPro-Router(config)#ip dhcp excluded-address 10.30.0.2
SecurityPro-Router(config)#
```

At the bottom right of the text box, there are 'Copy' and 'Paste' buttons. At the bottom left of the interface, there is a 'Top' link.

**22ª Etapa: Configurar os clientes para se conectarem à rede. Instalar placa de rede WPC300N em dispositivos que necessitem, e configurar o acesso à rede:**



Laptop - Cliente externo

PhysicalConfigDesktopProgrammingAttributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

Bluetooth

Wireless0

Port Status

On

Bandwidth

300 Mbps

MAC Address

00E0.A3C5.62B5

SSID

Convidados

Authentication

Disabled

WPA-PSK

WPA

802.1X

WEP

WPA2-PSK

WPA2

Method:

WEP Key

PSK Pass Phrase

%G3st@9/8-7

User ID

Password

MD5

User Name

Password

Encryption Type

AES

IP Configuration

DHCP

Static

IPv4 Address

10.30.0.3

Subnet Mask

255.255.255.248

IPv6 Configuration

Automatic

Static

IPv6 Address

/

Link Local Address

FE80::2E0:A3FF:FEC5:62B5

Top



**23ª Etapa: Configurar o recebimento de IP dinâmico via DHCP do endpoint do convidado da rede vlan300 Convidados:**

Laptop - Cliente externo

Physical Config **Desktop** Programming Attributes

**IP Configuration** [X]

Interface: Wireless0

IP Configuration

☒ DHCP ☐ Static

IPv4 Address:

Subnet Mask:

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address:  /

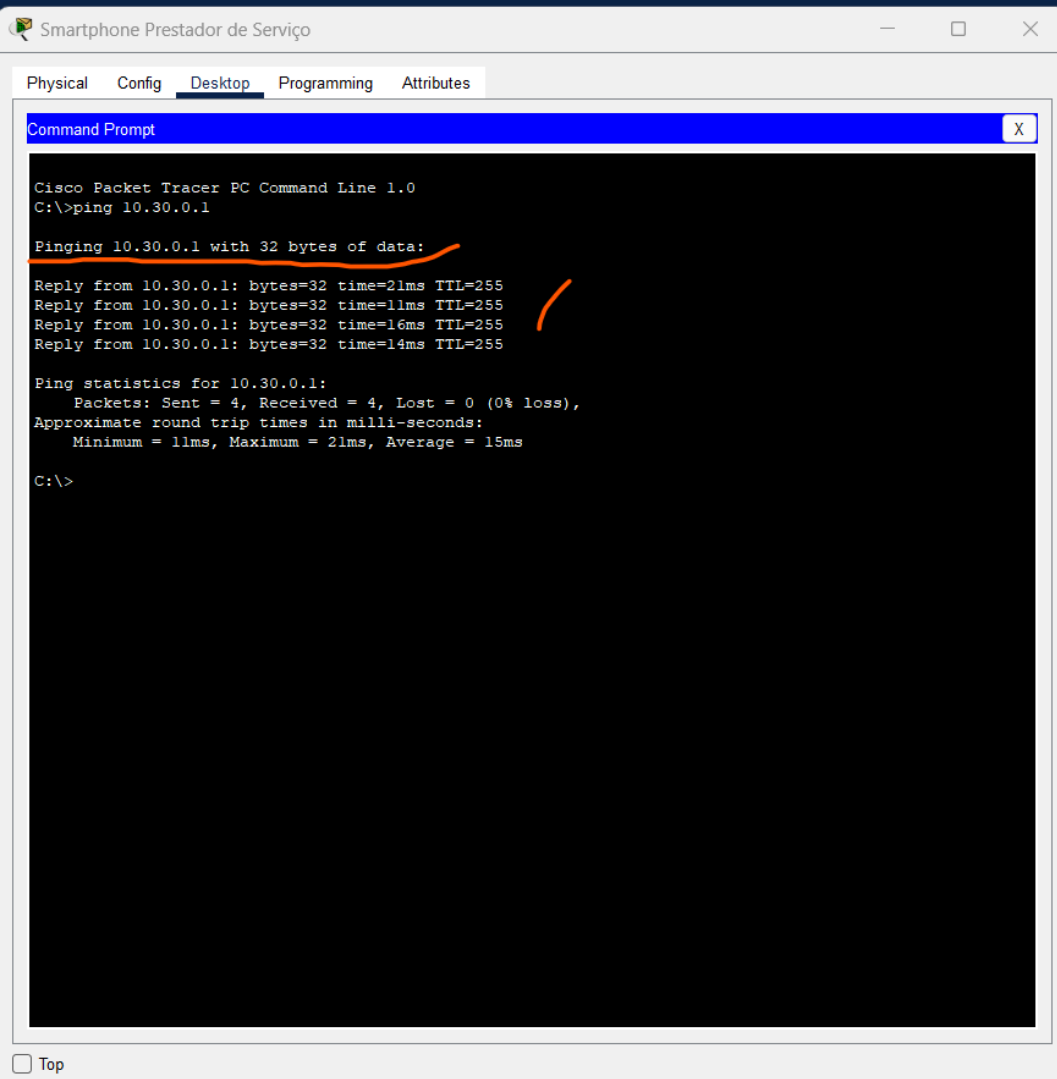
Link Local Address: FE80::2E0:A3FF:FEC5:62B5

Default Gateway:

DNS Server:

☐ Top

**24ª Etapa: Conectar demais dispositivos e realizar o teste de conectividade com o a subinterface do gateway padrão da rede vlan 300:**



The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named 'Smartphone Prestador de Serviço'. The window has tabs for Physical, Config, Desktop, Programming, and Attributes, with 'Desktop' selected. The Command Prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.30.0.1

Pinging 10.30.0.1 with 32 bytes of data:
Reply from 10.30.0.1: bytes=32 time=21ms TTL=255
Reply from 10.30.0.1: bytes=32 time=11ms TTL=255
Reply from 10.30.0.1: bytes=32 time=16ms TTL=255
Reply from 10.30.0.1: bytes=32 time=14ms TTL=255

Ping statistics for 10.30.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 21ms, Average = 15ms

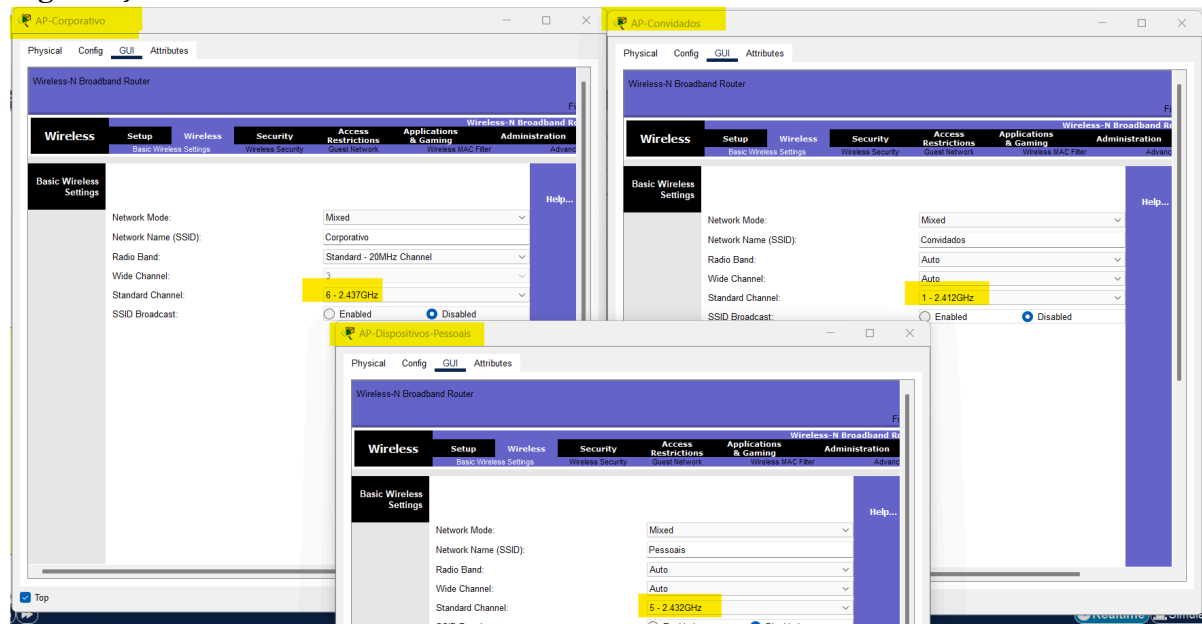
C:\>
```

Hand-drawn orange annotations are present: a line under 'Pinging 10.30.0.1 with 32 bytes of data:', a bracket on the right side of the four 'Reply' lines, and a bracket on the right side of the 'Ping statistics' block.

Teste de conectividade(ping) subinterface do gateway padrão da rede vlan 300 - sucesso!

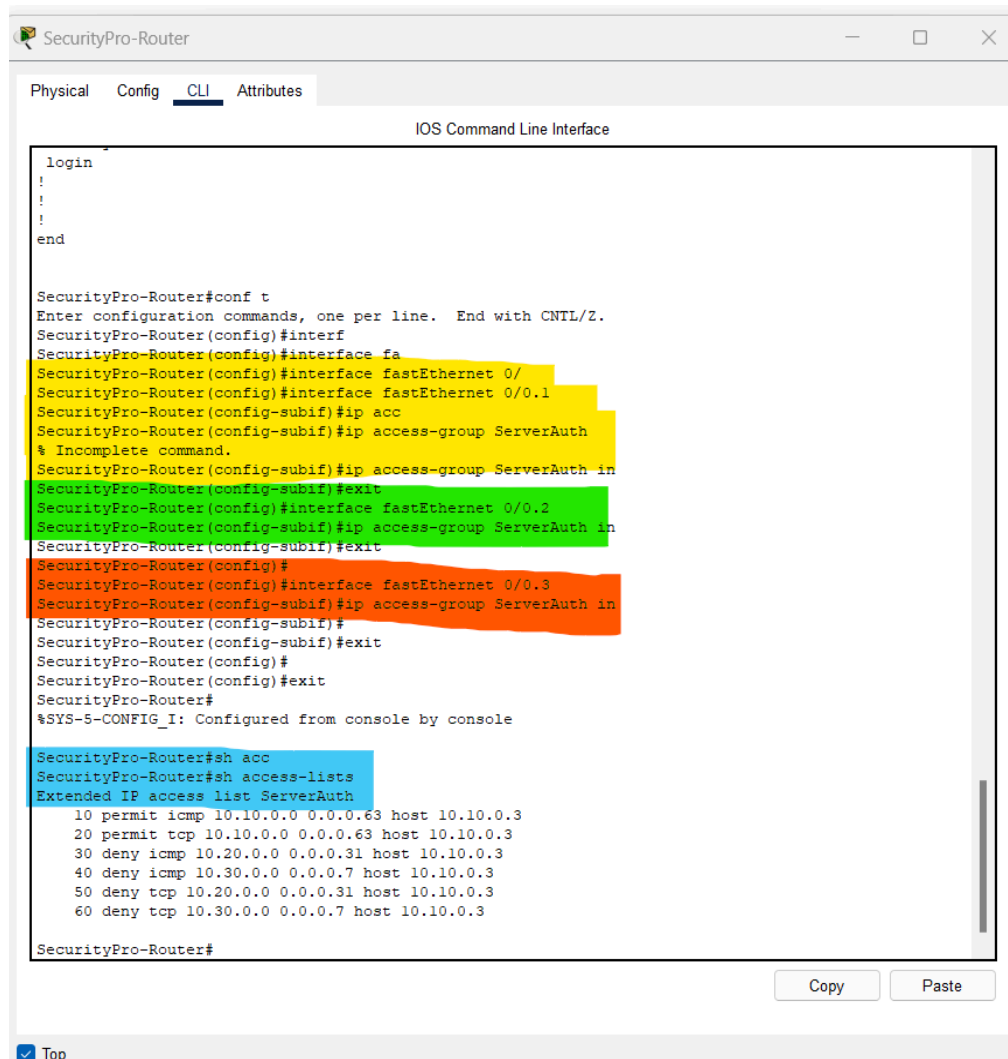
*Após os testes realizados com sucesso, conectar demais dispositivos na rede da vlan300 Convidados, seguindo os mesmos passos anteriores.*

**Configurar os canais e a frequência nos Pontos de Acesso para evitar interferência de sinal, seguindo o planejamento da rede e a Política de Segurança:**



Após todos os teste de conectividade da rede WLAN realizados com sucesso, configurar as listas de acesso para evitar que o tráfego não autorizado seja efetuado na rede.

**25ª Etapa: Configurar no SecurityPro-Router as listas de acesso para bloquear o acesso ao servidor EAP das vlan 200 e vlan 300 - permitindo somente o tráfego da vlan 100 no servidor:**



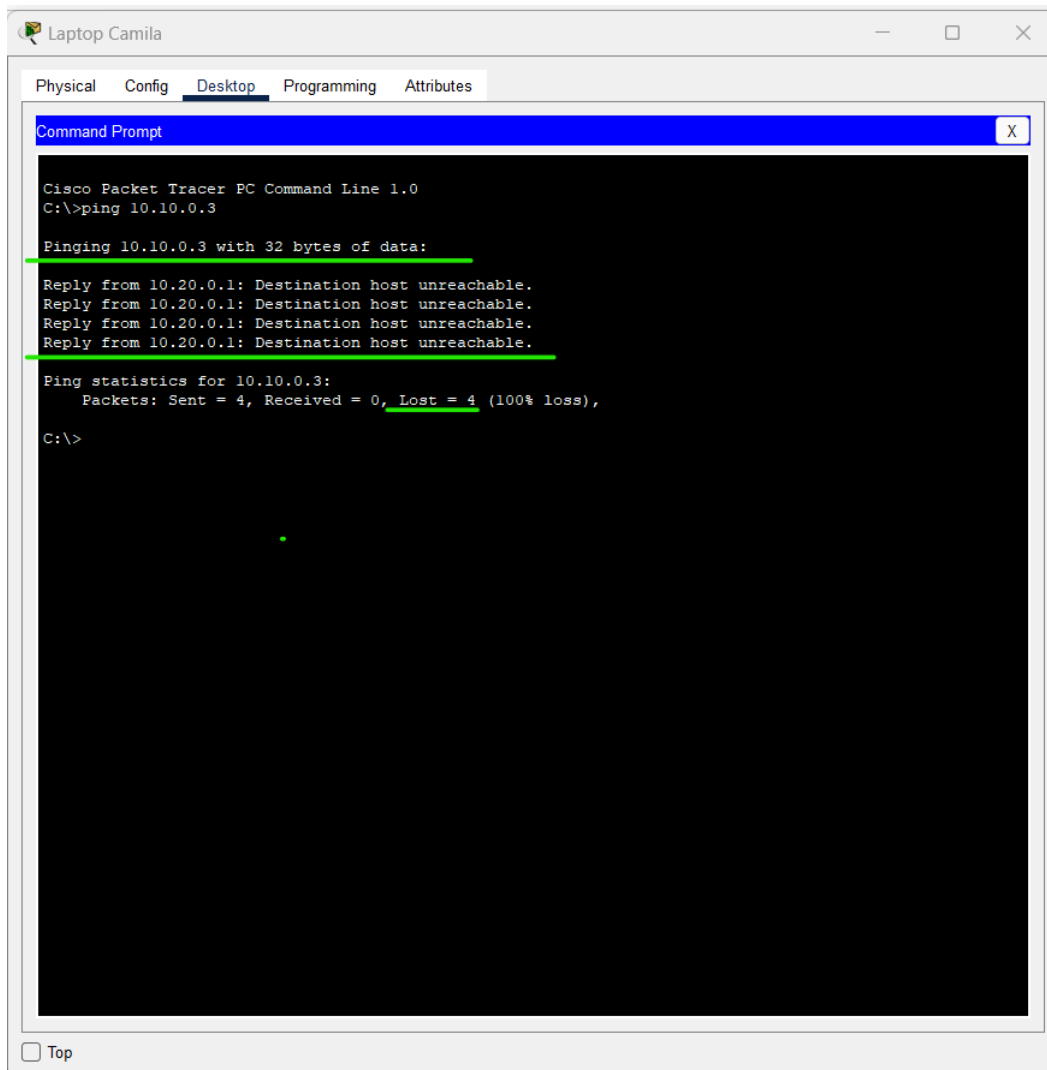
```
login
!!
end

SecurityPro-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecurityPro-Router(config)#interf
SecurityPro-Router(config)#interface fa
SecurityPro-Router(config)#interface fastEthernet 0/
SecurityPro-Router(config)#interface fastEthernet 0/0.1
SecurityPro-Router(config-subif)#ip acc
SecurityPro-Router(config-subif)#ip access-group ServerAuth
% Incomplete command.
SecurityPro-Router(config-subif)#ip access-group ServerAuth in
SecurityPro-Router(config-subif)#exit
SecurityPro-Router(config)#interface fastEthernet 0/0.2
SecurityPro-Router(config-subif)#ip access-group ServerAuth in
SecurityPro-Router(config-subif)#exit
SecurityPro-Router(config)#
SecurityPro-Router(config)#interface fastEthernet 0/0.3
SecurityPro-Router(config-subif)#ip access-group ServerAuth in
SecurityPro-Router(config-subif)#
SecurityPro-Router(config-subif)#exit
SecurityPro-Router(config)#
SecurityPro-Router#
%SYS-5-CONFIG_I: Configured from console by console

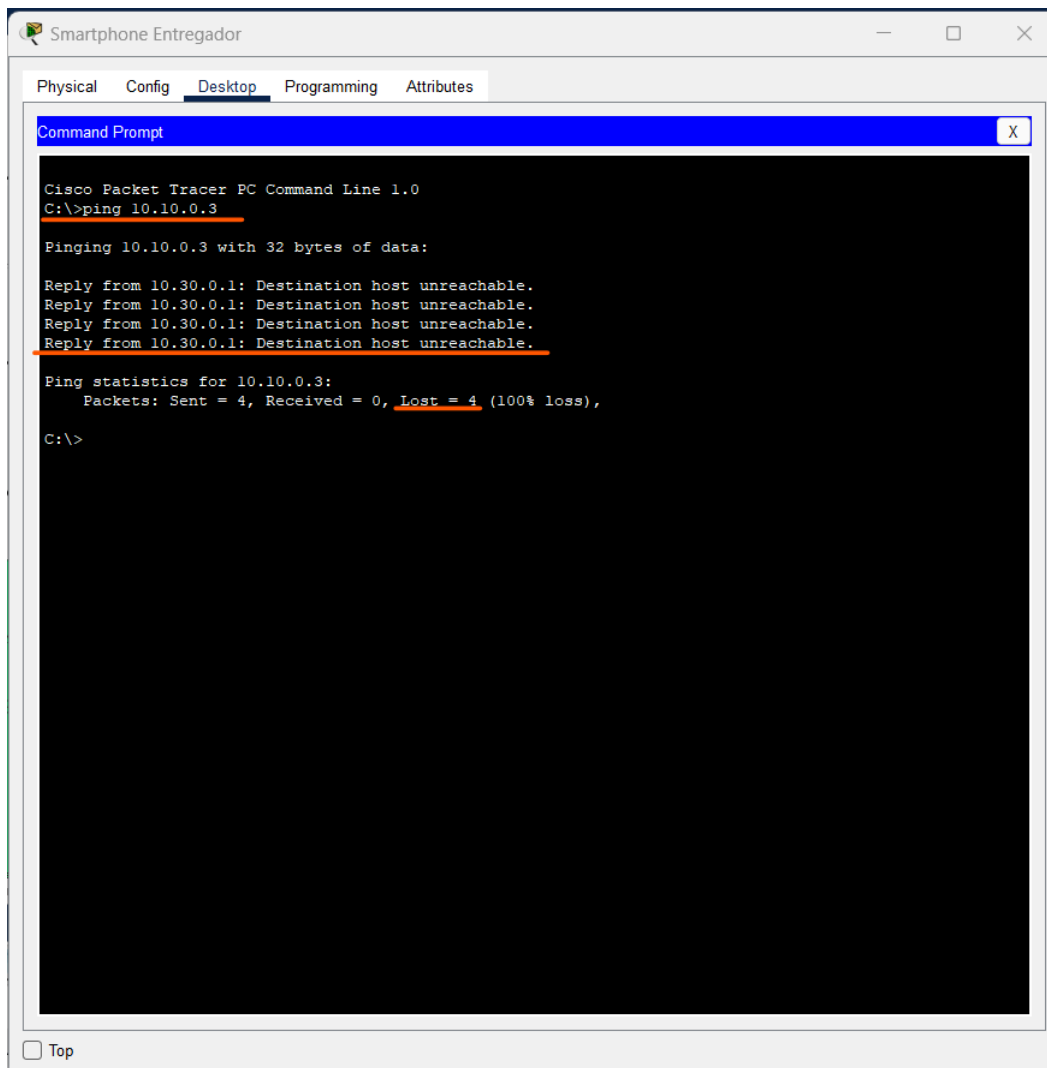
SecurityPro-Router#sh acc
SecurityPro-Router#sh access-lists
Extended IP access list ServerAuth
 10 permit icmp 10.10.0.0 0.0.0.63 host 10.10.0.3
 20 permit tcp 10.10.0.0 0.0.0.63 host 10.10.0.3
 30 deny icmp 10.20.0.0 0.0.0.31 host 10.10.0.3
 40 deny icmp 10.30.0.0 0.0.0.7 host 10.10.0.3
 50 deny tcp 10.20.0.0 0.0.0.31 host 10.10.0.3
 60 deny tcp 10.30.0.0 0.0.0.7 host 10.10.0.3

SecurityPro-Router#
```

Lista de acesso ServerAuth configurada para bloquear tráfego de rede da rede 10.20.0.0 e da rede 10.30.0.0, ao acessar o servidor.



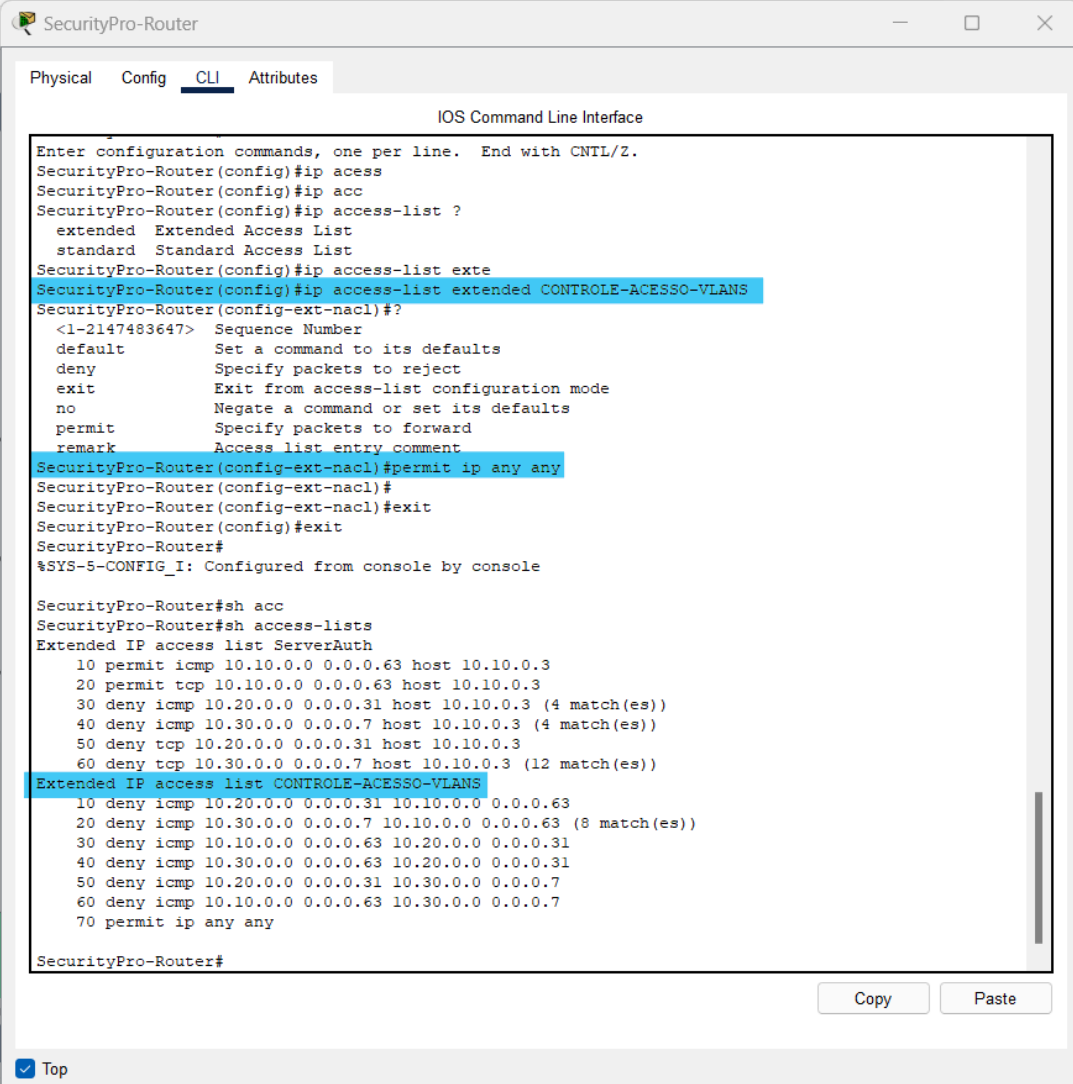
Falha no teste de ping para o servidor EAP 10.10.0.3 de origem da vlan200 na rede 10.20.0.0.  
Devido à lista de acesso configurada com sucesso!



Falha no teste de ping para o servidor EAP 10.10.0.3 de origem da vlan300 na rede 10.30.0.0.  
Devido à lista de acesso configurada com sucesso!

## 26ª Etapa: Configurar as listas de acesso para bloquear o acesso entre vlans:

Obs. Essa lista de acesso impede que dispositivos de vlan diferente, encontrem e vejam outros dispositivos e bloqueiam de realizar o ping (teste de conectividade via ICMP):

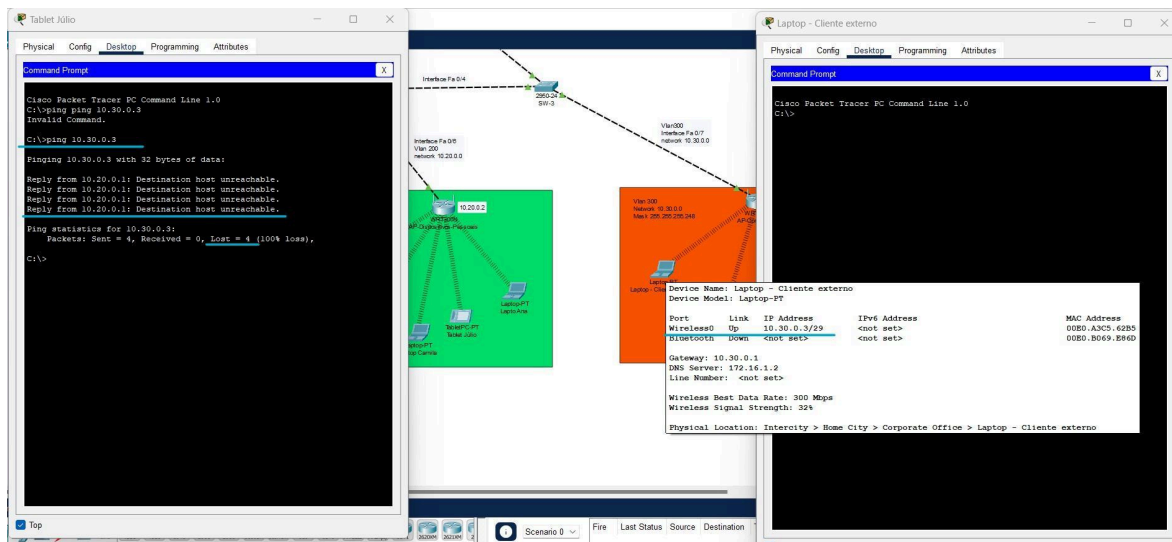


```
SecurityPro-Router
Physical Config CLI Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTRL/Z.
SecurityPro-Router(config)#ip access
SecurityPro-Router(config)#ip acc
SecurityPro-Router(config)#ip access-list ?
    extended Extended Access List
    standard Standard Access List
SecurityPro-Router(config)#ip access-list exte
SecurityPro-Router(config)#ip access-list extended CONTROLE-ACESSO-VLANS
SecurityPro-Router(config-ext-nacl)#?
    <1-2147483647> Sequence Number
    default Set a command to its defaults
    deny Specify packets to reject
    exit Exit from access-list configuration mode
    no Negate a command or set its defaults
    permit Specify packets to forward
    remark Access list entry comment
SecurityPro-Router(config-ext-nacl)#permit ip any any
SecurityPro-Router(config-ext-nacl)#
SecurityPro-Router(config-ext-nacl)#exit
SecurityPro-Router(config)#exit
SecurityPro-Router#
%SYS-5-CONFIG_I: Configured from console by console

SecurityPro-Router#sh acc
SecurityPro-Router#sh access-lists
Extended IP access list ServerAuth
  10 permit icmp 10.10.0.0 0.0.0.63 host 10.10.0.3
  20 permit tcp 10.10.0.0 0.0.0.63 host 10.10.0.3
  30 deny icmp 10.20.0.0 0.0.0.31 host 10.10.0.3 (4 match(es))
  40 deny icmp 10.30.0.0 0.0.0.7 host 10.10.0.3 (4 match(es))
  50 deny tcp 10.20.0.0 0.0.0.31 host 10.10.0.3
  60 deny tcp 10.30.0.0 0.0.0.7 host 10.10.0.3 (12 match(es))
Extended IP access list CONTROLE-ACESSO-VLANS
  10 deny icmp 10.20.0.0 0.0.0.31 10.10.0.0 0.0.0.63
  20 deny icmp 10.30.0.0 0.0.0.7 10.10.0.0 0.0.0.63 (8 match(es))
  30 deny icmp 10.10.0.0 0.0.0.63 10.20.0.0 0.0.0.31
  40 deny icmp 10.30.0.0 0.0.0.63 10.20.0.0 0.0.0.31
  50 deny icmp 10.20.0.0 0.0.0.31 10.30.0.0 0.0.0.7
  60 deny icmp 10.10.0.0 0.0.0.63 10.30.0.0 0.0.0.7
  70 permit ip any any

SecurityPro-Router#
```

Configurada lista de acesso CONTROLE-ACESSO-VLANS para bloqueio de tráfego entre dispositivos de vlans diferentes.



Falha no teste de conectividade entre vlans. Devido à lista de acesso configurada com sucesso!

Com a rede toda configurada com autenticação, criptografia, segmentação entre vlans, ocultação de SSID Broadcast, entrega de IP dinâmico via DHCP e teste de de conectividade realizado com sucesso e garantindo o bom desempenho da rede. Configurar a rede externa para acesso à internet.

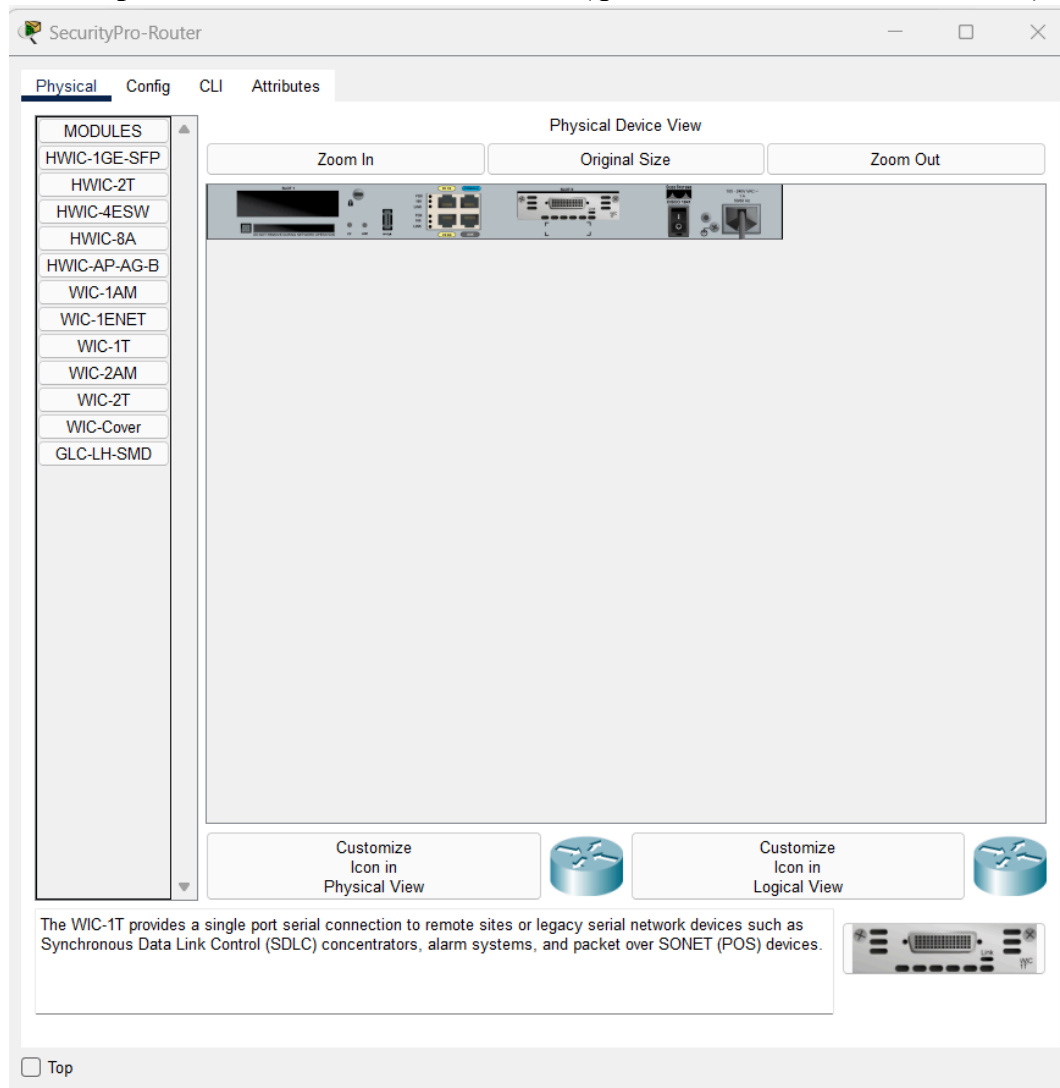
**27ª Etapa: No SecurityPro-Router realizar escrita em memória para salvar todas as configurações feitas usando os seguintes comandos:**

enable

wr (abreviação de write)



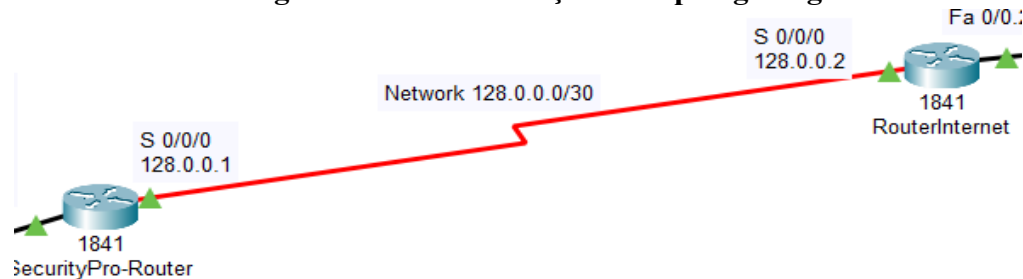
**28ª Etapa: Após salvar as configurações desligar o roteador e instalar a placa serial WC-1T para conexão com outro roteador (que será a simulação da internet):**



Placa de rede serial instalada.

**29ª Etapa: Interconectar via cabo serial o roteador da rede SecurityPro com o roteador da internet e configurar uma lista de acesso para o protocolo NAT, a fim de evitar exposição de IP privado para a rede externa, sendo realizado a tradução de IP privado para IP público configurado no roteador SecurityPro- Router:**

**Interconectar e configurar a rede 128.0.0.0 entres os roteadores nas respectivas interfaces seriais seguindo a documentação da topologia lógica:**



```
SecurityPro-Router>en
SecurityPro-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecurityPro-Router(config)#ip acc
SecurityPro-Router(config)#ip access-list stad
SecurityPro-Router(config)#ip access-list stan
SecurityPro-Router(config)#ip access-list standard NAT
SecurityPro-Router(config-std-nacl)#permit 10.10.0.0 0.0.0.63
SecurityPro-Router(config-std-nacl)#permit 10.20.0.0 0.0.0.31
SecurityPro-Router(config-std-nacl)#permit 10.30.0.0 0.0.0.7
SecurityPro-Router(config-std-nacl)#exit
SecurityPro-Router(config)#interf
SecurityPro-Router(config)#interface fas
SecurityPro-Router(config)#interface fastEthernet 0/
SecurityPro-Router(config)#interface fastEthernet 0/0.1
SecurityPro-Router(config-subif)#ip nat inside
SecurityPro-Router(config-subif)#exit
SecurityPro-Router(config)#interface fastEthernet 0/0.2
SecurityPro-Router(config-subif)#ip nat ins
SecurityPro-Router(config-subif)#ip nat inside
SecurityPro-Router(config-subif)#
SecurityPro-Router(config-subif)#exit
SecurityPro-Router(config)#
SecurityPro-Router(config)#interface fastEthernet 0/0.3
SecurityPro-Router(config-subif)#ip na
SecurityPro-Router(config-subif)#ip nat in
SecurityPro-Router(config-subif)#ip nat inside
SecurityPro-Router(config-subif)#
SecurityPro-Router(config-subif)#exit
SecurityPro-Router(config)#interf
SecurityPro-Router(config)#interface se
SecurityPro-Router(config)#interface serial 0/0/0
SecurityPro-Router(config)#interface serial 0/0/0
SecurityPro-Router(config-if)#ip nat ou
SecurityPro-Router(config-if)#ip nat outside
SecurityPro-Router(config-if)#
SecurityPro-Router(config-if)#exit
SecurityPro-Router(config)#ip nat insi
SecurityPro-Router(config)#ip nat inside sour
SecurityPro-Router(config)#ip nat inside source li
SecurityPro-Router(config)#ip nat inside source list NAT interf
SecurityPro-Router(config)#ip nat inside source list NAT interface serial 0/0/0 overl
SecurityPro-Router(config)#ip nat inside source list NAT interface serial 0/0/0 overload
SecurityPro-Router(config)#
```

Lista de acesso NAT configurada, para habilitar tradução de endereços IP privados para público para acesso a internet, utilizando o IP configurado na interface serial do roteador.

### 30ª Etapa: Posicionar os dispositivos:

- 01 roteador
- 02 Switches
- 01 Servidor web
- 01 Servidor DNS

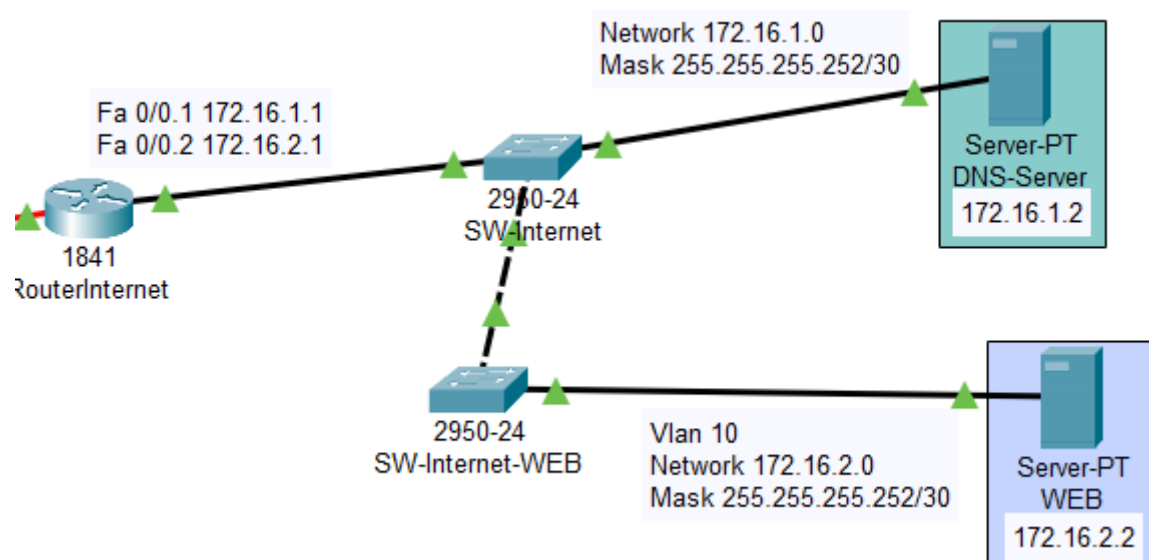
Após instalados e conectados via cabo, realizar a alteração do nome dos dispositivos com o comando:

```
en
```

```
hostname RouterInternet #(para o roteador)
```

```
hostname SW-Internet-WEB #(para o switch do servidor WEB)
```

```
hostname SW-Internet #(para o switch do servidor DNS)
```



### 31ª Etapa: Configurando as vlans nos switches:

SW-Internet-WEB

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch(config-vlan)#
Switch(config-vlan)#exit
Switch(config)#sh vl
Switch(config)#do sh vlan b
Switch(config)#do sh vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
10 DNS	active	
20 WEB	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch(config)#hostname
Switch(config)#hostname SW-Intenet-WEB
SW-Intenet-WEB(config)#
SW-Intenet-WEB(config)#
SW-Intenet-WEB(config)#interf
SW-Intenet-WEB(config)#interface fas
SW-Intenet-WEB(config)#interface fastEthernet 0/1
SW-Intenet-WEB(config-if)#sw
SW-Intenet-WEB(config-if)#switchport mo
SW-Intenet-WEB(config-if)#switchport mode acc
SW-Intenet-WEB(config-if)#switchport mode access
SW-Intenet-WEB(config-if)#sw
SW-Intenet-WEB(config-if)#switchport acc
SW-Intenet-WEB(config-if)#switchport access vlan
SW-Intenet-WEB(config-if)#switchport access vlan 20
SW-Intenet-WEB(config-if)#exit
SW-Intenet-WEB(config)#
```

Copy Paste

☒ Top

SW-Internet-WEB

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
Switch(config)#vlan 10
Switch(config-vlan)#name DNS
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name WEB
Switch(config-vlan)#
Switch(config-vlan)#exit
Switch(config)#sh vl
Switch(config)#do sh vlan b
Switch(config)#do sh vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
10 DNS	active	
20 WEB	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
Switch(config)#hostname
Switch(config)#hostname SW-Intenet-WEB
SW-Intenet-WEB(config)#
```

Copy Paste

☐ Top

Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch(config)#vlan
Switch(config)#vlan 10
Switch(config-vlan)#ne
Switch(config-vlan)#?
VLAN configuration commands:
  exit      Apply changes, bump revision number, and exit mode
  name      Ascii name of the VLAN
  no        Negate a command or set its defaults
  remote-span Add the Remote Switched Port Analyzer (RSPAN) feature to the VLAN
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name WEB
Switch(config-vlan)#exit
Switch(config)#vlan 10
Switch(config-vlan)#name DNS
Switch(config-vlan)#
Switch(config-vlan)#exit
Switch(config)#exit
Switch#sh vlan
Switch#sh vlan br
Switch#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/4, Fa0/5, Fa0/6 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
10	DNS	active	
20	WEB	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

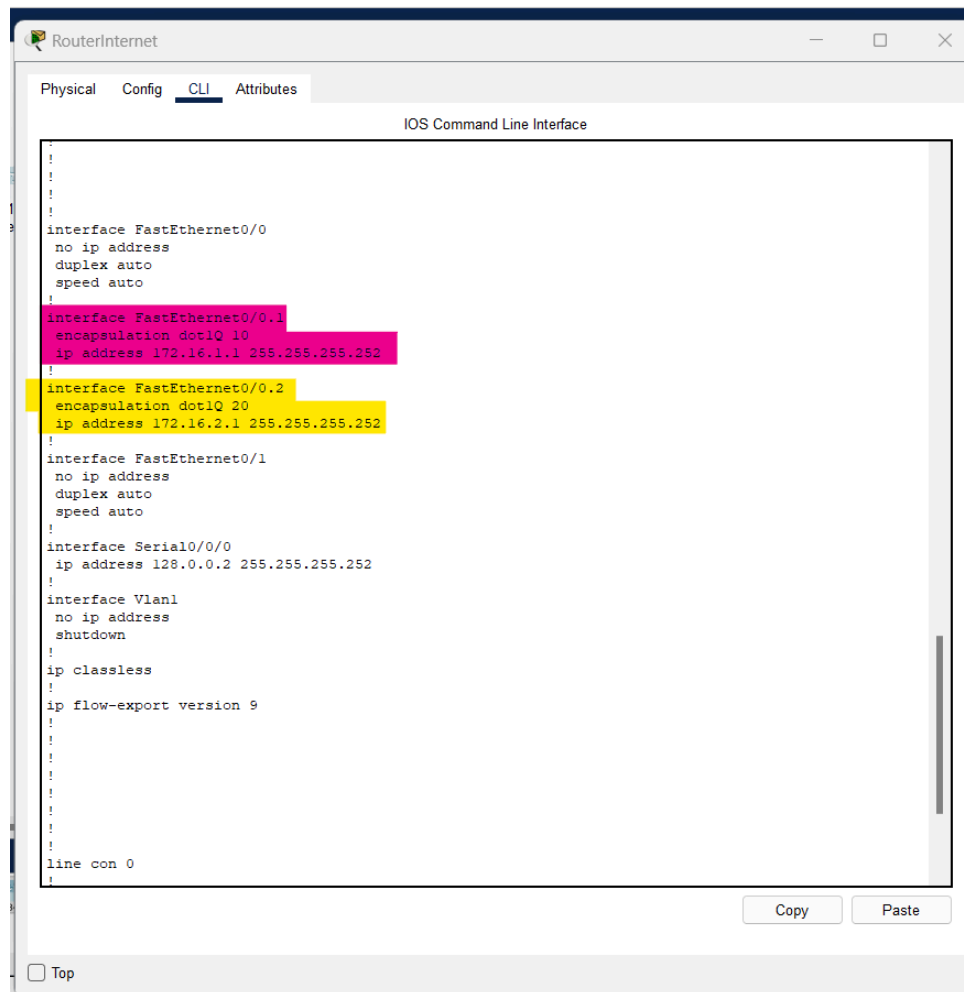
Switch#

Copy Paste

☐ Top

**32ª Etapa: Configurar as vlans 10 DNS e 20 WEB no roteador RouterInternet seguindo os seguintes comandos:**

```
RouterInternet>en
RouterInternet#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RouterInternet(config)#interf
RouterInternet(config)#interface fast
RouterInternet(config)#interface fastEthernet 0/0.1
RouterInternet(config-subif)#enc
RouterInternet(config-subif)#encapsulation do
RouterInternet(config-subif)#encapsulation dot1Q 10
RouterInternet(config-subif)#ip add
RouterInternet(config-subif)#ip address 172.16.1.1 255.255.255.252
RouterInternet(config-subif)#exit
RouterInternet(config)#interface fastEthernet 0/0.2
RouterInternet(config-subif)#enc
RouterInternet(config-subif)#encapsulation do
RouterInternet(config-subif)#encapsulation dot1Q 20
RouterInternet(config-subif)#ip add
RouterInternet(config-subif)#ip address 172.16.2.1 255.255.255.252
RouterInternet(config-subif)#
RouterInternet(config-subif)#
```



**33ª Etapa: Configurar os servidores com IP Estático de acordo com cada rede criada em nas respectivas Vlans 10 e 20 e conforme documentação de topologia lógica:**

The screenshot shows the 'DNS-Server' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is active, showing settings for both IPv4 and IPv6. The IPv4 configuration is set to 'Static' with an IP address of 172.16.1.2, a subnet mask of 255.255.255.252, a default gateway of 172.16.1.1, and a DNS server of 0.0.0.0. The IPv6 configuration is also set to 'Static' with a link local address of FE80::201:43FF:FE16:15EA. The 802.1X section is visible but not configured, showing 'Use 802.1X Security' as unchecked, 'Authentication' as MD5, and empty fields for 'Username' and 'Password'. A 'Top' button is located at the bottom left of the window.

IP Configuration	
<b>IP Configuration</b>	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	172.16.1.2
Subnet Mask	255.255.255.252
Default Gateway	172.16.1.1
DNS Server	0.0.0.0
<b>IPv6 Configuration</b>	
<input type="radio"/> Automatic	<input checked="" type="radio"/> Static
IPv6 Address	/
Link Local Address	FE80::201:43FF:FE16:15EA
Default Gateway	
DNS Server	
<b>802.1X</b>	
<input type="checkbox"/> Use 802.1X Security	
Authentication	MD5
Username	
Password	

☐ Top

IP estático no servidor DNS na rede 172.16.1.0 e o gateway padrão na subinterface do roteador de internet.

WEB

Physical Config Services **Desktop** Programming Attributes

**IP Configuration** X

IP Configuration

☐ DHCP ☒ Static

IPv4 Address 172.16.2.2

Subnet Mask 255.255.255.252

Default Gateway 172.16.2.1

DNS Server 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address /

Link Local Address FE80::201:C7FF:FE46:8E4D

Default Gateway

DNS Server

802.1X

☐ Use 802.1X Security

Authentication MD5

Username

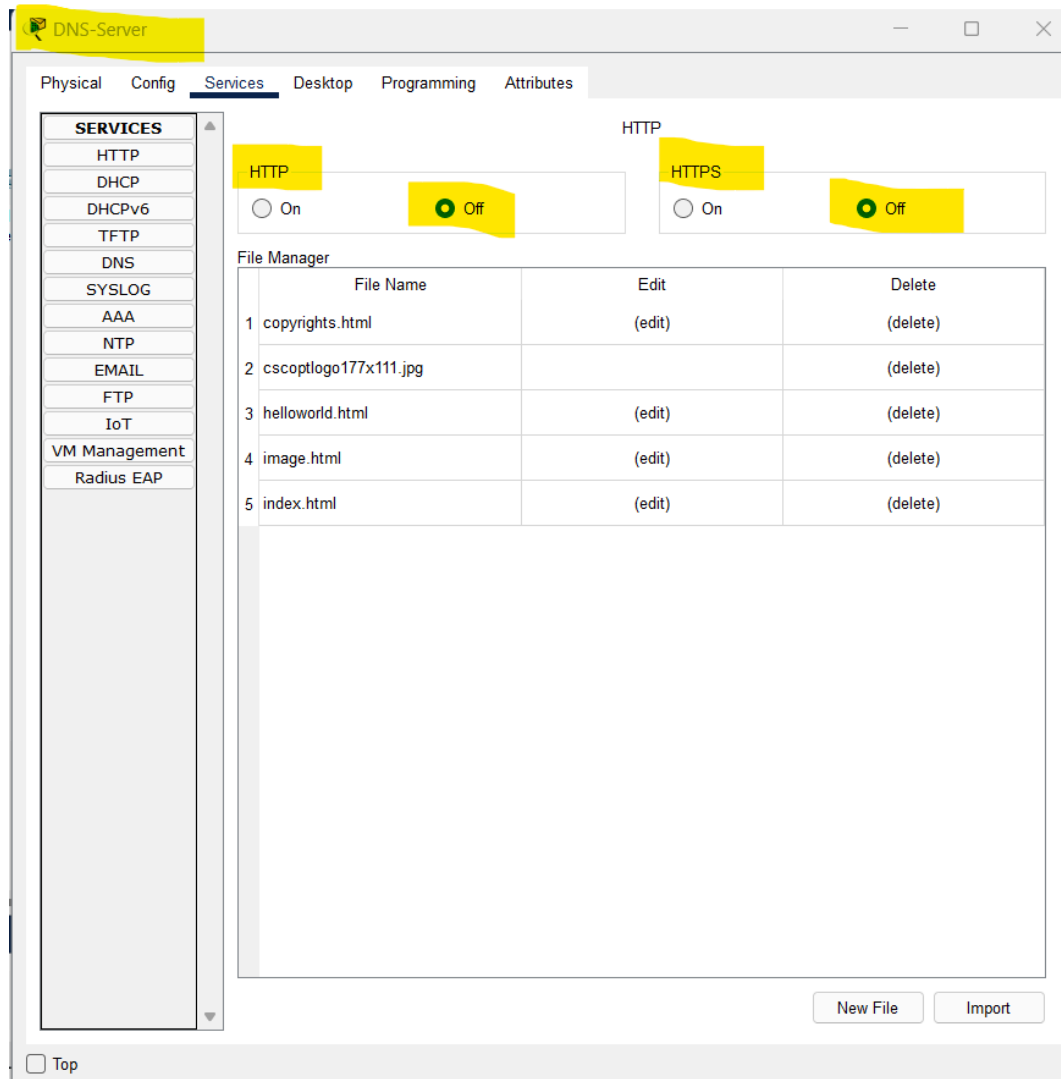
Password

☐ Top

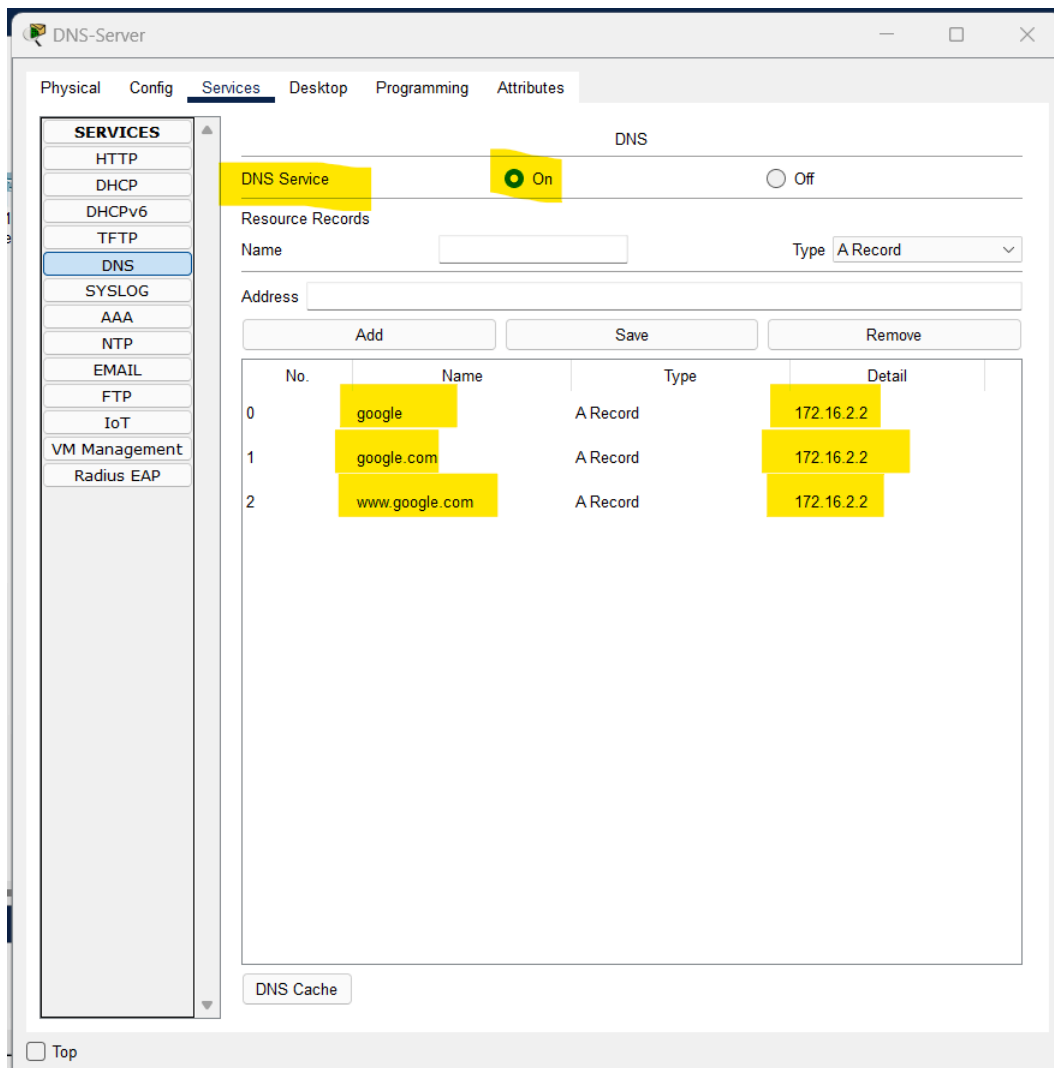
IP estático no servidor WEB na rede 172.16.2.0 e o gateway padrão na subinterface do roteador de internet.



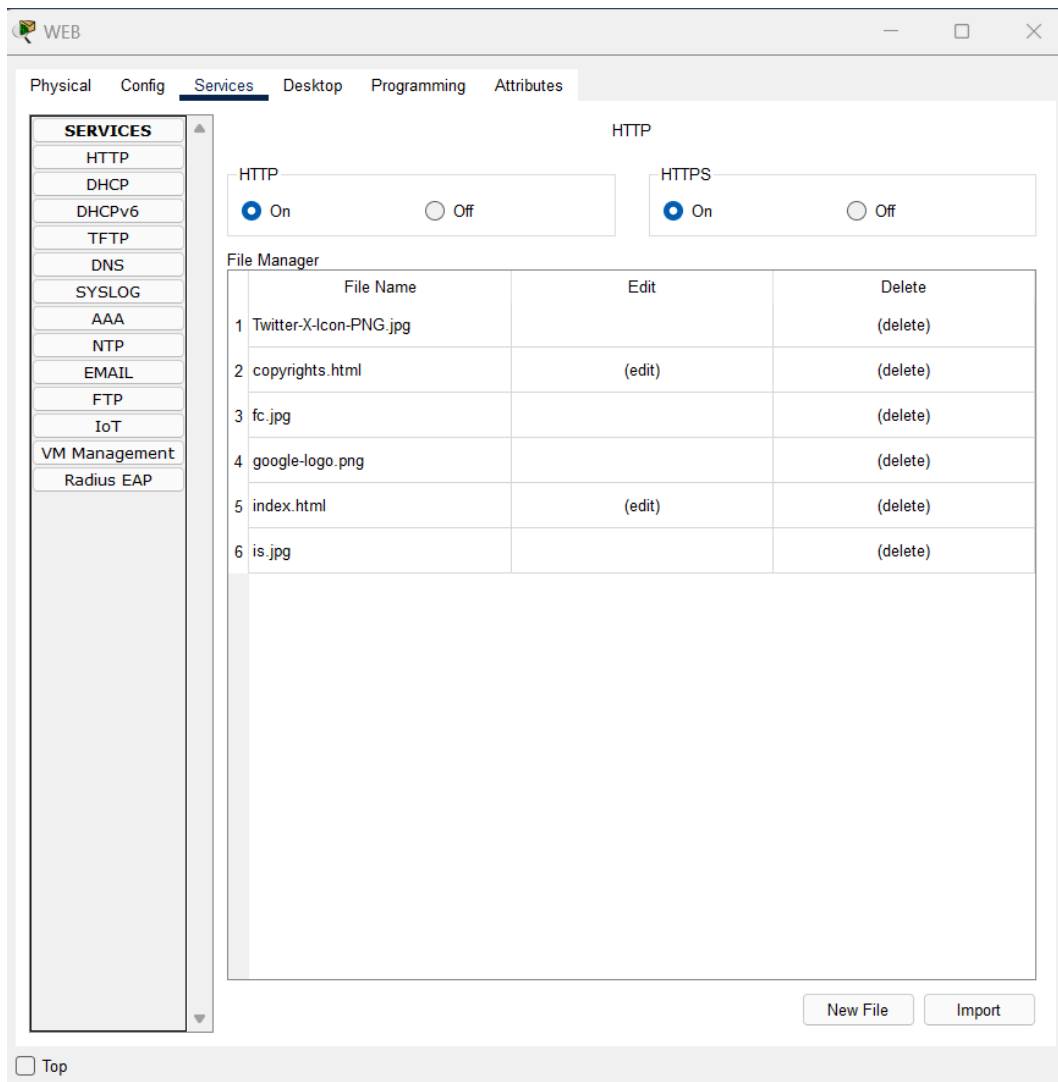
**34ª Etapa: Configurar os servidores com os seus respectivos serviços e desabilitar demais serviços que não serão utilizados:**



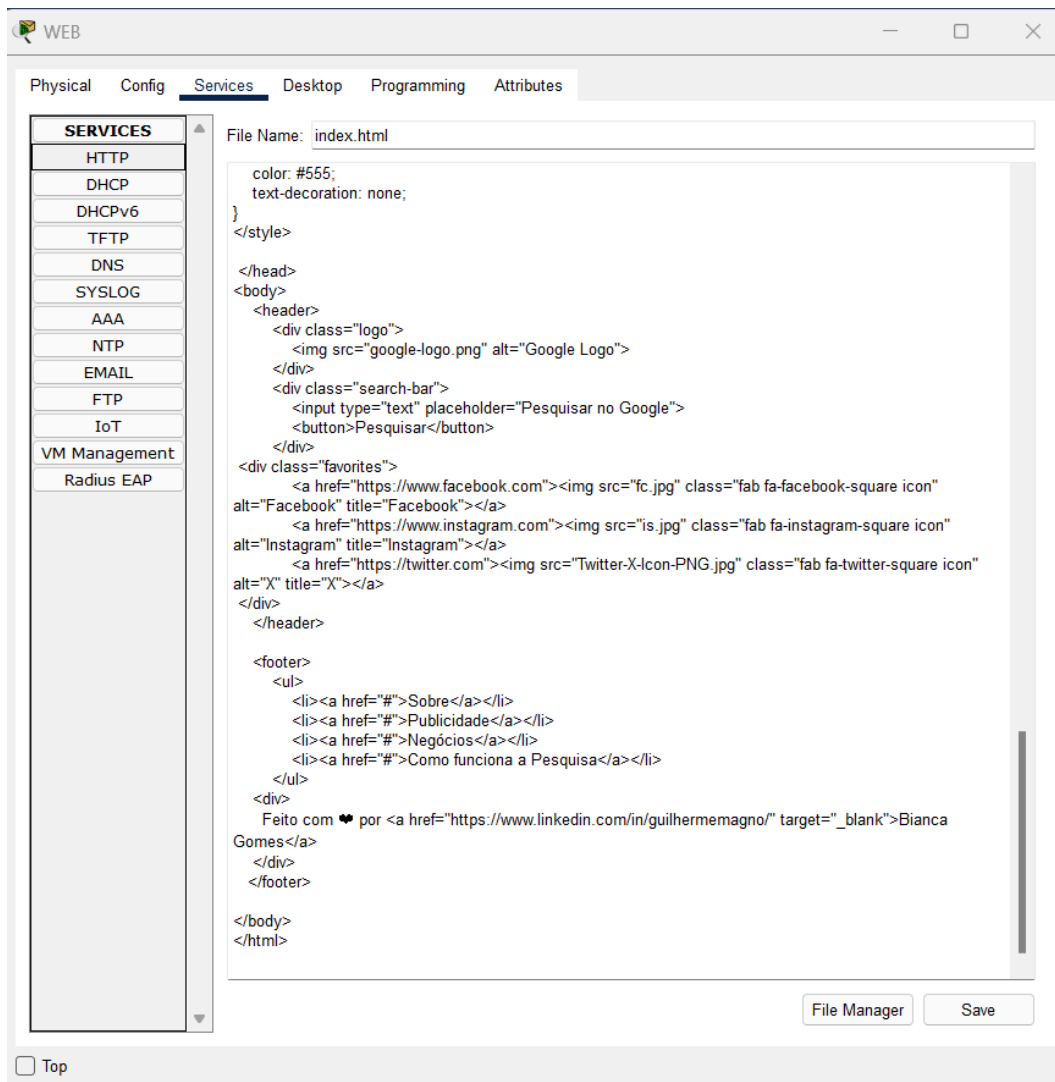
Serviço HTTP e HTTPS desabilitados no servidor DNS.



Serviço de DNS habilitado com o endereço do servidor WEB.

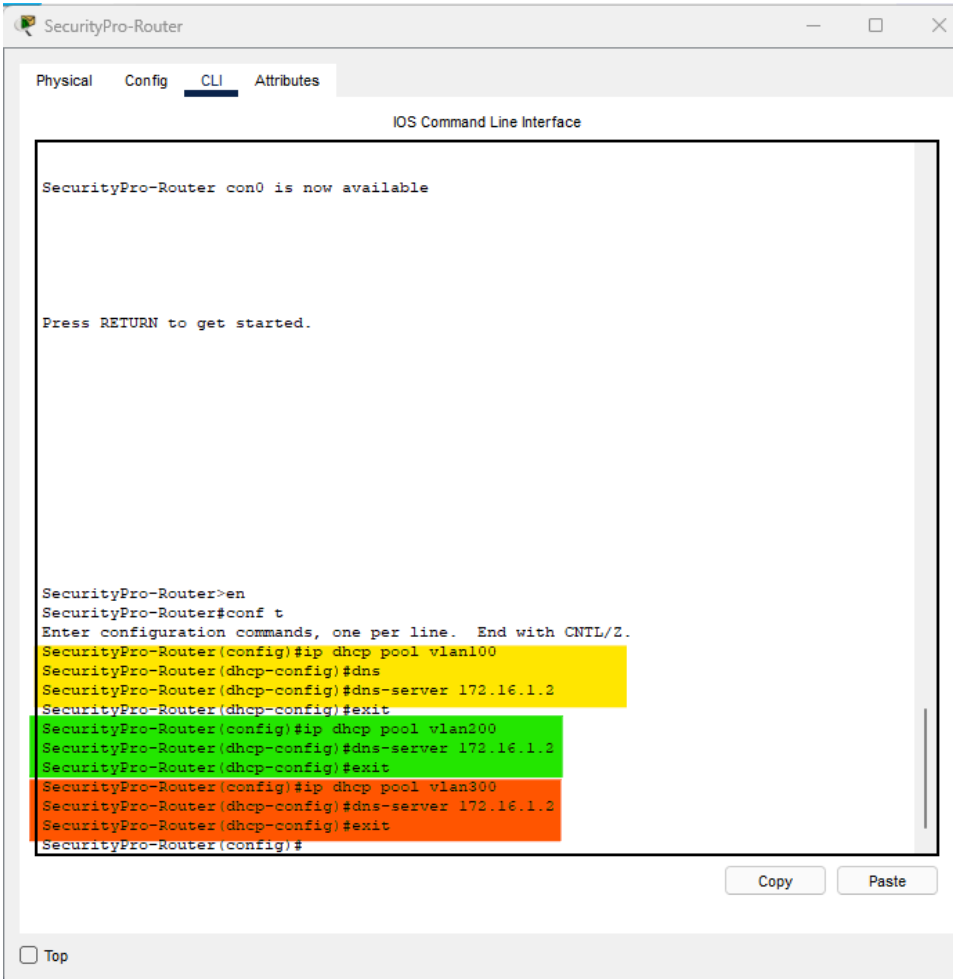


Configuração do serviço de HTTP e HTTPS no servidor web.



Página index.html configurada no servidor WEB.

### 35ª Etapa: No SecurityPro-Router configurar dentro do dhcp pool vlan, o servidor DNS:



The screenshot shows the SecurityPro-Router CLI interface. The window title is "SecurityPro-Router". The tabs are "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is selected, and the title bar says "IOS Command Line Interface". The main text area shows the following commands and output:

```
SecurityPro-Router con0 is now available

Press RETURN to get started.

SecurityPro-Router>en
SecurityPro-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecurityPro-Router(config)#ip dhcp pool vlan100
SecurityPro-Router(dhcp-config)#dns
SecurityPro-Router(dhcp-config)#dns-server 172.16.1.2
SecurityPro-Router(dhcp-config)#exit
SecurityPro-Router(config)#ip dhcp pool vlan200
SecurityPro-Router(dhcp-config)#dns-server 172.16.1.2
SecurityPro-Router(dhcp-config)#exit
SecurityPro-Router(config)#ip dhcp pool vlan300
SecurityPro-Router(dhcp-config)#dns-server 172.16.1.2
SecurityPro-Router(dhcp-config)#exit
SecurityPro-Router(config)#
```

At the bottom right of the CLI window, there are "Copy" and "Paste" buttons. At the bottom left, there is a "Top" button.

**36ª Etapa: Confirmar entrega de DNS via DHCP em cada end device das redes nas vlans 100, 200 e 300:**

Cliente corp1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface Wireless0

IP Configuration

☒ DHCP ☐ Static DHCP request successful.

IPv4 Address 10.10.0.4

Subnet Mask 255.255.255.192

Default Gateway 10.10.0.1

DNS Server 172.16.1.2

IPv6 Configuration

☒ Automatic ☐ Static ipv6 request failed.

IPv6 Address /

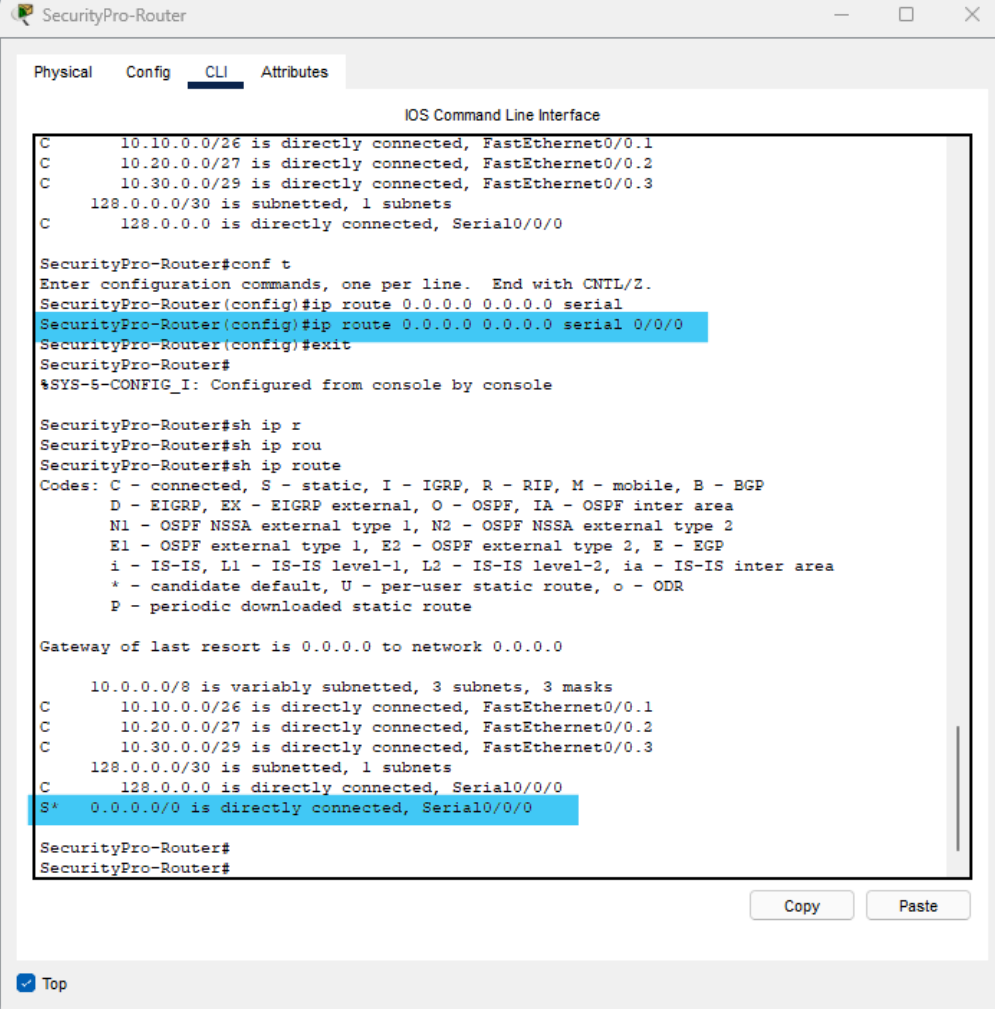
Link Local Address FE80::2D0:BCFF:FEEC:10E2

Default Gateway

DNS Server

☐ Top

**37ª Etapa: Configurar a tabela de roteamento de SecurityRouter-Pro para que a rede interna envie o tráfego e consiga acessar por padrão a rede serial (internet) e o OSPF para anúncio de rede:**



The screenshot shows the SecurityPro-Router CLI interface with the following content:

```
SecurityPro-Router
Physical Config CLI Attributes

IOS Command Line Interface

C 10.10.0.0/26 is directly connected, FastEthernet0/0.1
C 10.20.0.0/27 is directly connected, FastEthernet0/0.2
C 10.30.0.0/29 is directly connected, FastEthernet0/0.3
C 128.0.0.0/30 is subnetted, 1 subnets
C 128.0.0.0 is directly connected, Serial0/0/0

SecurityPro-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecurityPro-Router(config)#ip route 0.0.0.0 0.0.0.0 serial
SecurityPro-Router(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/0
SecurityPro-Router(config)#exit
SecurityPro-Router#
*SYS-5-CONFIG_I: Configured from console by console

SecurityPro-Router#sh ip r
SecurityPro-Router#sh ip rou
SecurityPro-Router#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

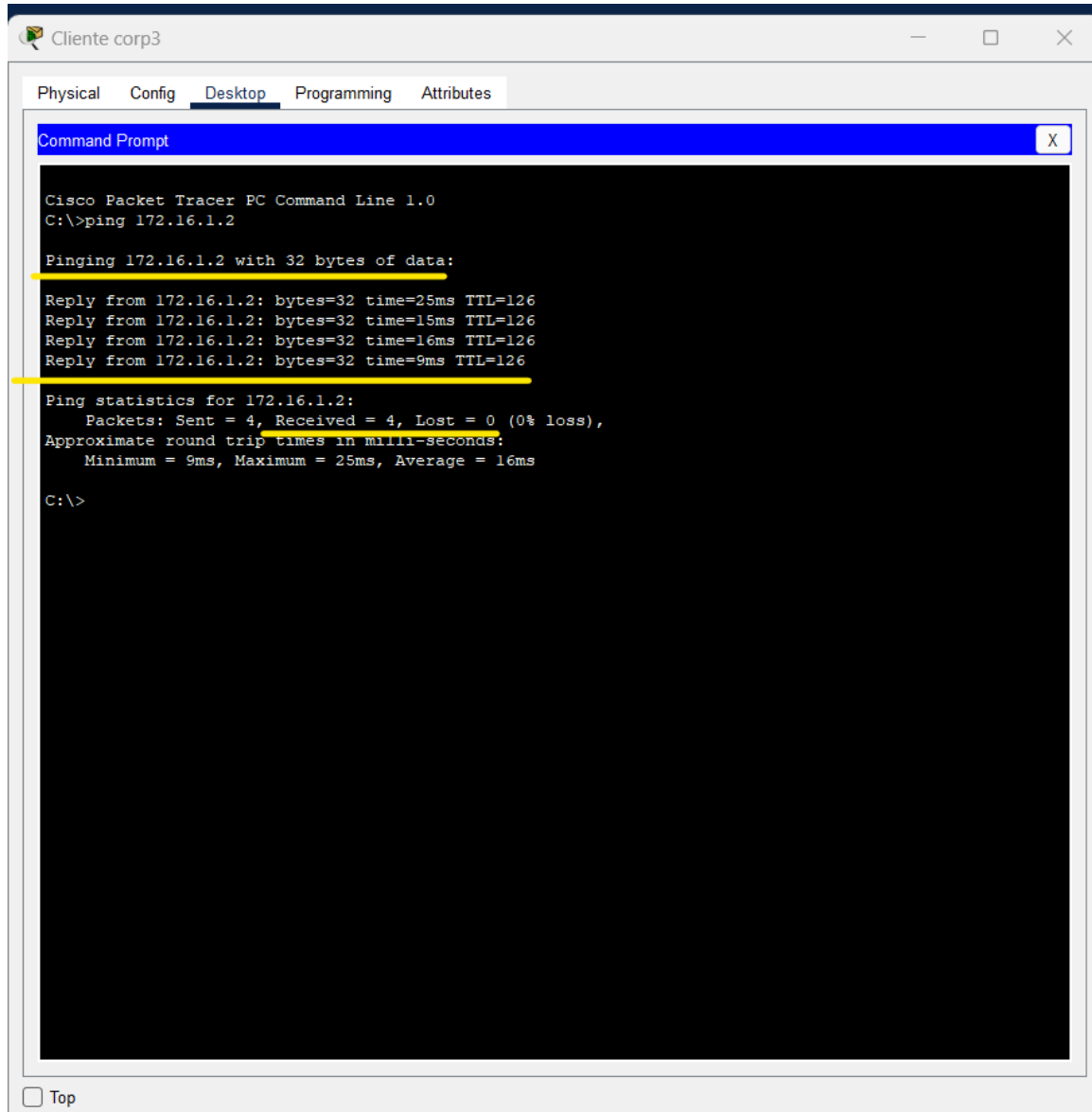
10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C 10.10.0.0/26 is directly connected, FastEthernet0/0.1
C 10.20.0.0/27 is directly connected, FastEthernet0/0.2
C 10.30.0.0/29 is directly connected, FastEthernet0/0.3
C 128.0.0.0/30 is subnetted, 1 subnets
C 128.0.0.0 is directly connected, Serial0/0/0
S* 0.0.0.0/0 is directly connected, Serial0/0/0

SecurityPro-Router#
SecurityPro-Router#
```

Buttons: Copy Paste

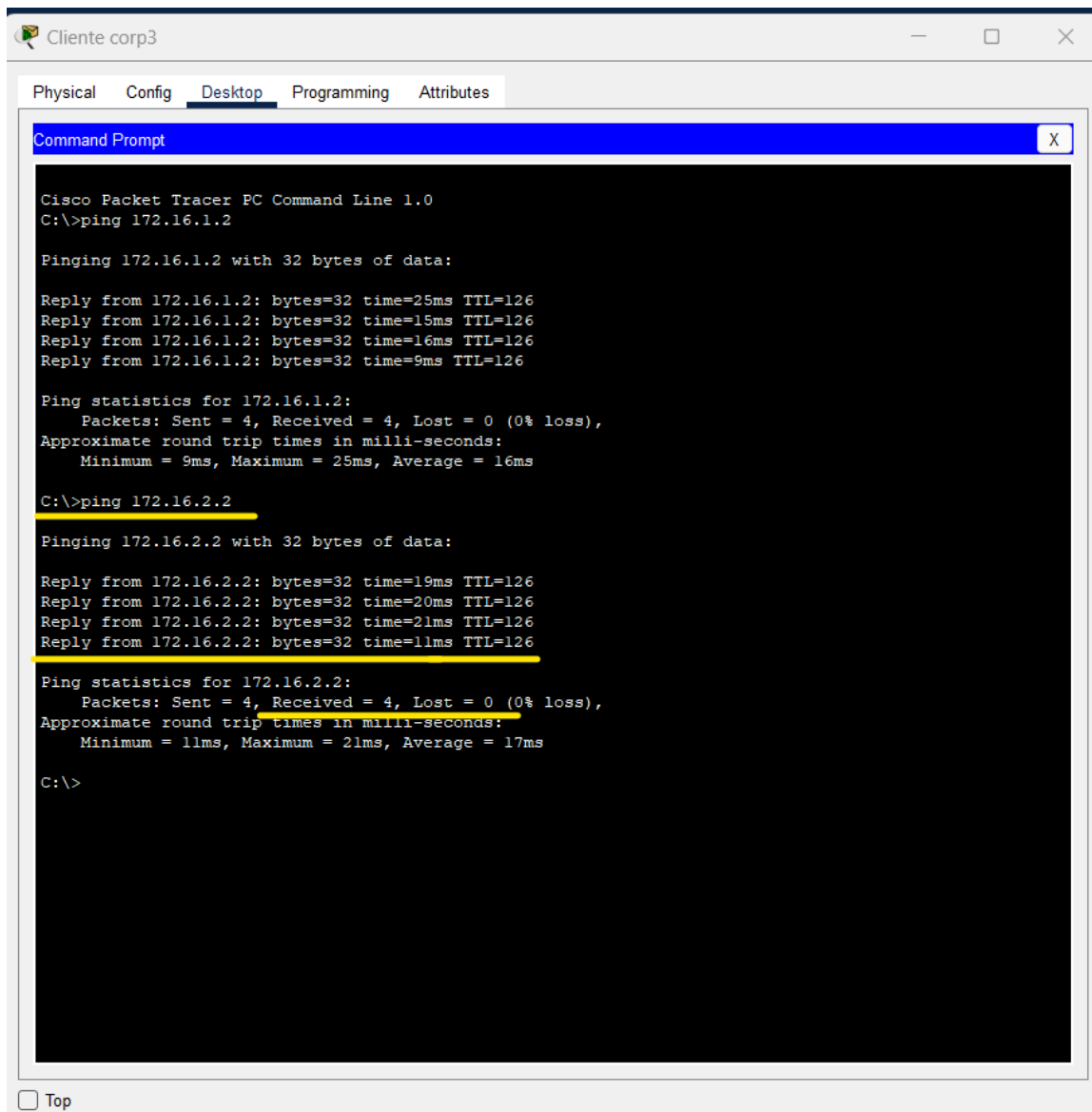
☒ Top

### 38ª Etapa: Realizar o teste de conectividade no servidor DNS e WEB



Teste de conectividade servidor DNS - origem rede vlan 100 - Corporativo - sucesso!





The screenshot shows a Cisco Packet Tracer PC Command Line window for a device named 'Cliente corp3'. The window has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' currently selected. The command prompt shows the following output:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.1.2

Pinging 172.16.1.2 with 32 bytes of data:

Reply from 172.16.1.2: bytes=32 time=25ms TTL=126
Reply from 172.16.1.2: bytes=32 time=15ms TTL=126
Reply from 172.16.1.2: bytes=32 time=16ms TTL=126
Reply from 172.16.1.2: bytes=32 time=9ms TTL=126

Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 25ms, Average = 16ms

C:\>ping 172.16.2.2

Pinging 172.16.2.2 with 32 bytes of data:

Reply from 172.16.2.2: bytes=32 time=19ms TTL=126
Reply from 172.16.2.2: bytes=32 time=20ms TTL=126
Reply from 172.16.2.2: bytes=32 time=21ms TTL=126
Reply from 172.16.2.2: bytes=32 time=11ms TTL=126

Ping statistics for 172.16.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 21ms, Average = 17ms

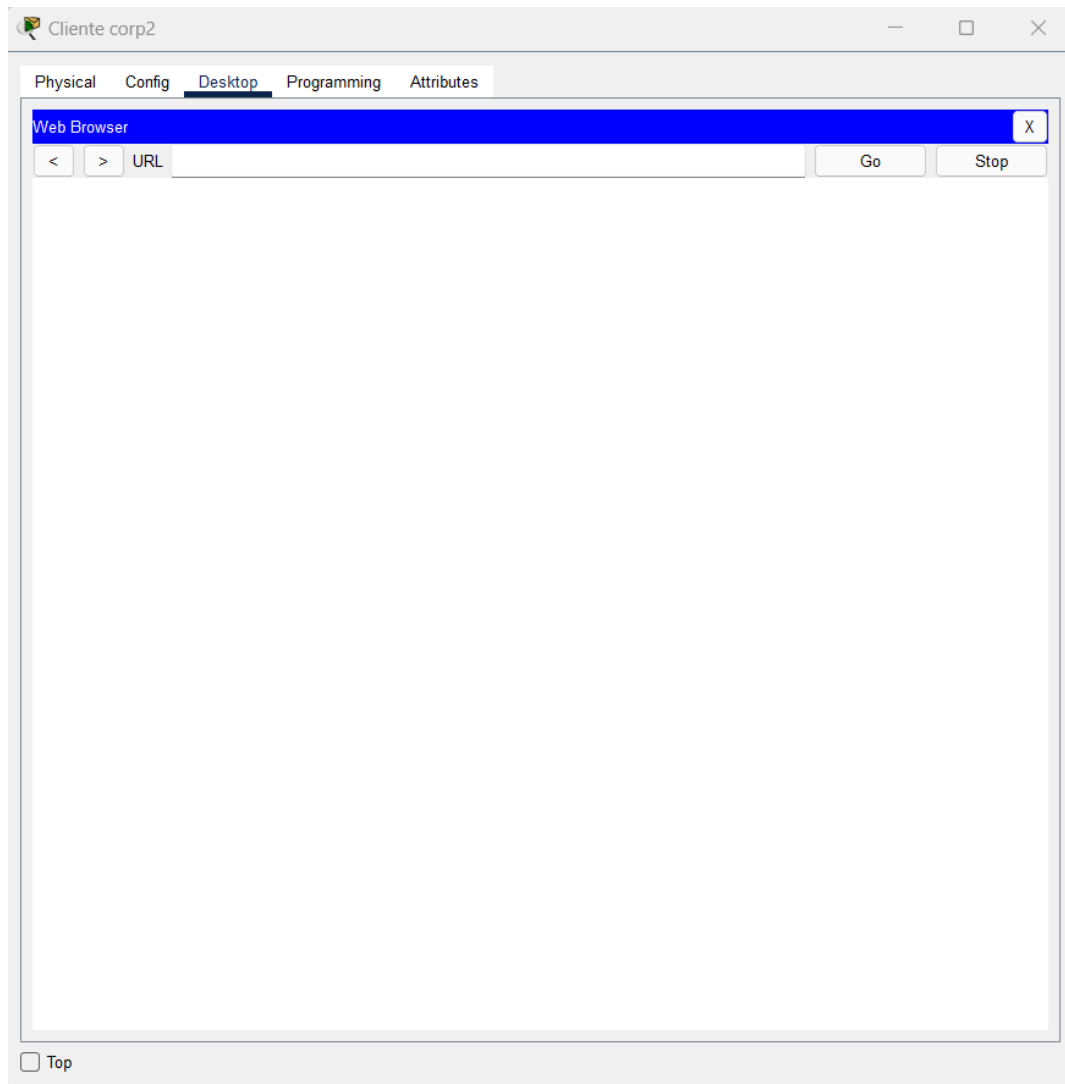
C:\>
```

At the bottom of the window, there is a 'Top' button.

Teste de conectividade servidor WEB - origem rede vlan 100 - Corporativo - sucesso!

**39ª Etapa - Após todas as configurações de rede WLAN e WAN, realizar a escrita na memória nos dispositivos de roteadores e switches com o comando wr (write)**

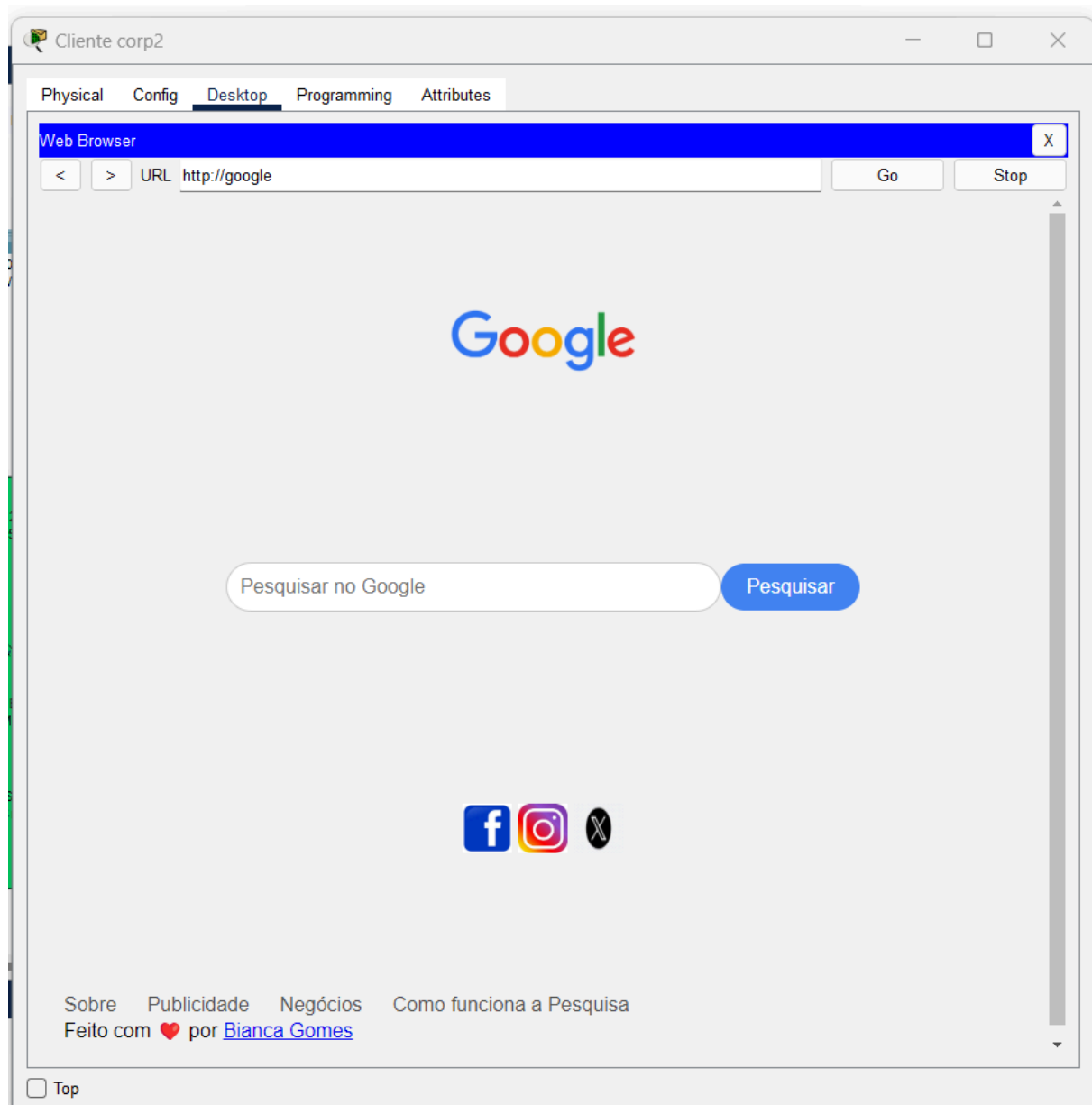
**40ª Etapa: Acessar a web através dos dispositivos finais em cada uma das redes VLANs 100, 200 e 300 para verificar todo o acesso na internet, conforme o objetivo inicial da WLAN:**



No dispositivo do Cliente corp 2, vá até a aba Desktop e clique em Web Browser:

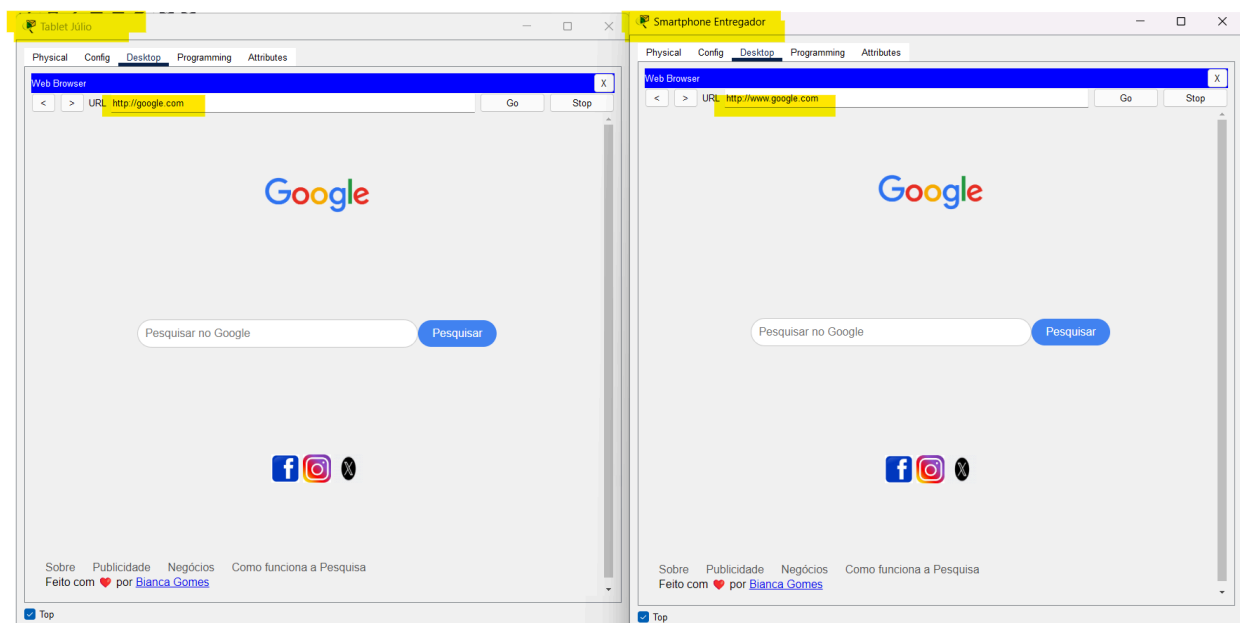
Digite o site que deseja acessar conforme configurado no servidor DNS nesse caso:

Aguarde alguns instantes até que a página seja carregada.



Acesso realizado com sucesso à internet.

Realize o teste dos os demais dispositivos da outras vlans:





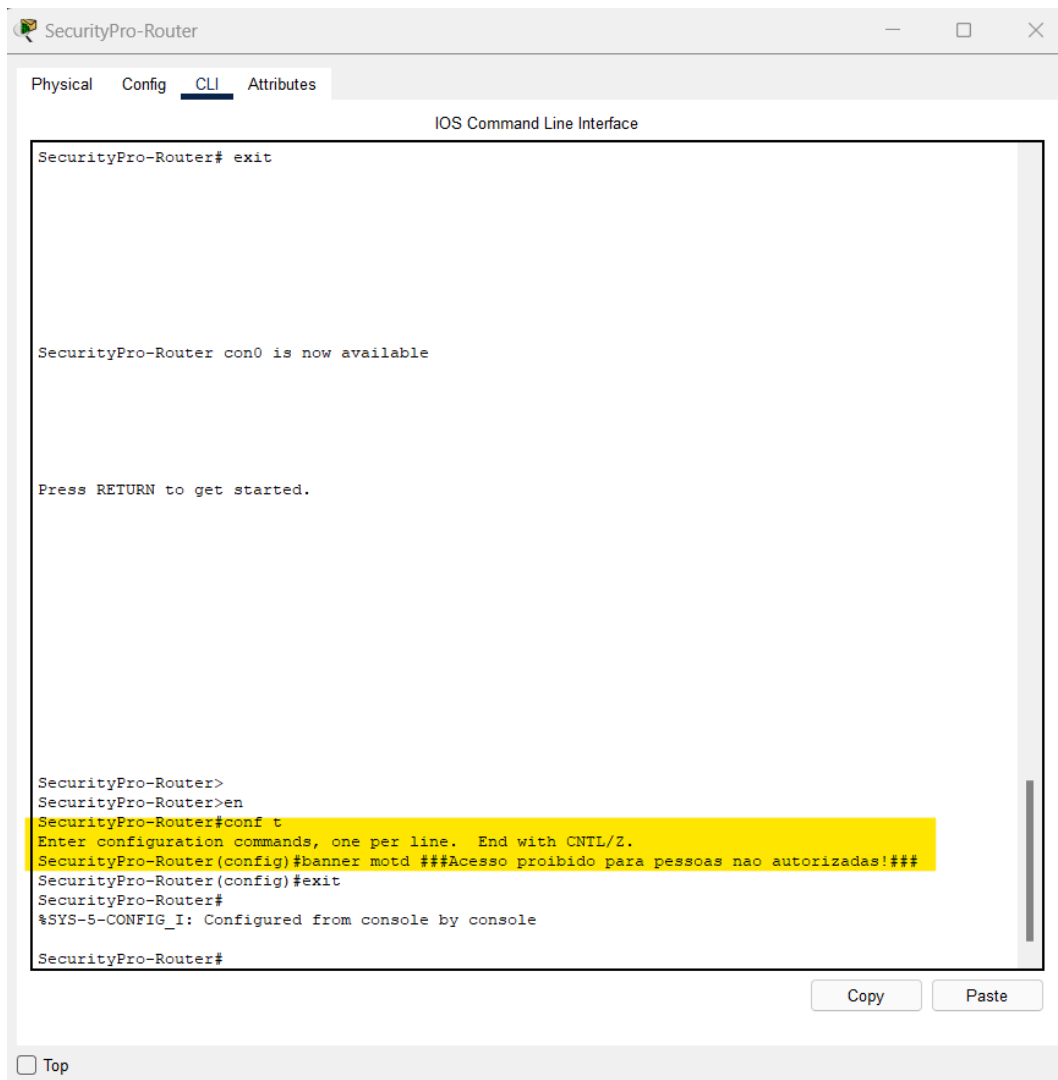
Rede configurada com sucesso! 😊

Todos os colaboradores autorizados poderão agora em seu horário de descanso acessar a internet via Wi-Fi quando estiverem no refeitório e no pátio!

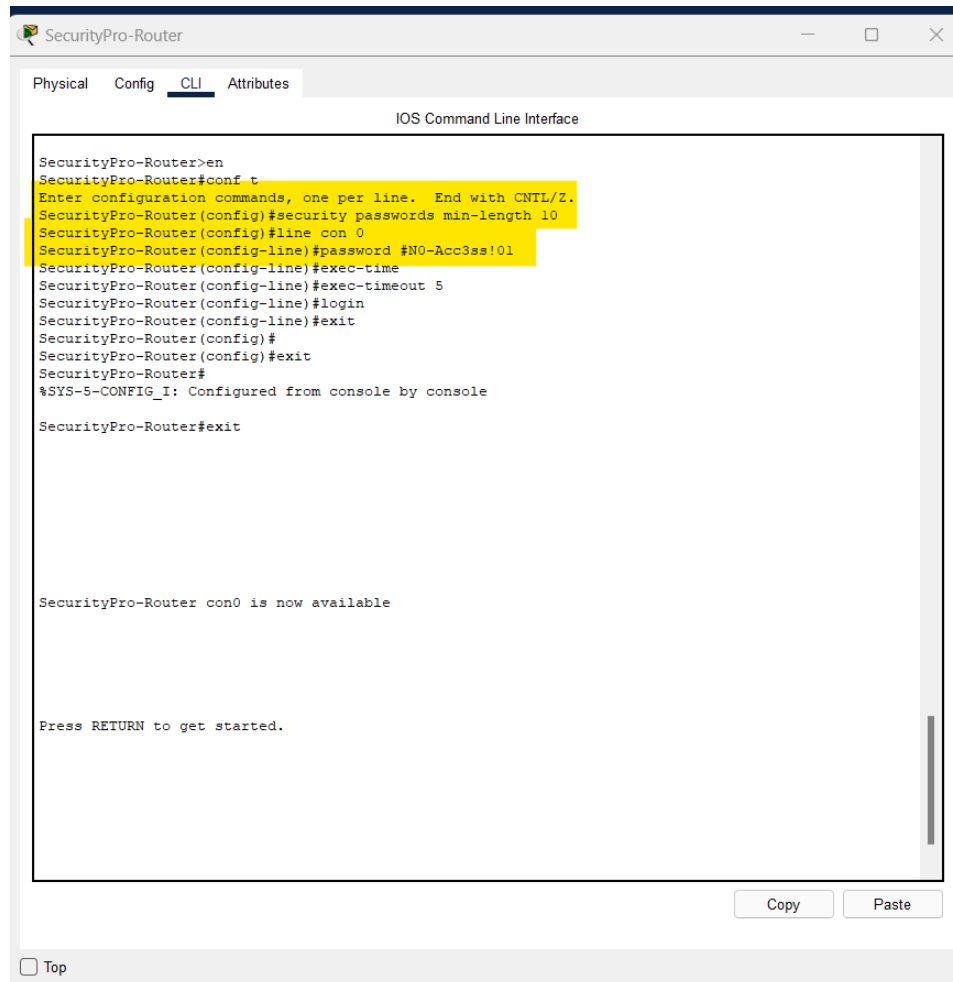
## Outras configurações importantes:

### 1. Configuração de um banner para aviso de acesso proibido ao roteador e à rede:

```
RouterInternet#  
  
RouterInternet con0 is now available  
  
Press RETURN to get started.  
  
RouterInternet>en  
RouterInternet#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
RouterInternet(config)#banner mo  
RouterInternet(config)#banner motd ###Acesso proibido para pessoas nao autorizadas###  
RouterInternet(config)#exit  
RouterInternet#  
%SYS-5-CONFIG_I: Configured from console by console  
RouterInternet#
```



2. Configurar tamanho mínimo de senha no roteador, e adicionar senha para acesso a console 0 e exigirá uma senha antes de permitir o acesso ao modo EXEC do usuário:



The screenshot shows a web-based interface for a SecurityPro-Router. The 'CLI' tab is selected, displaying the 'IOS Command Line Interface'. The terminal window shows the following commands and output:

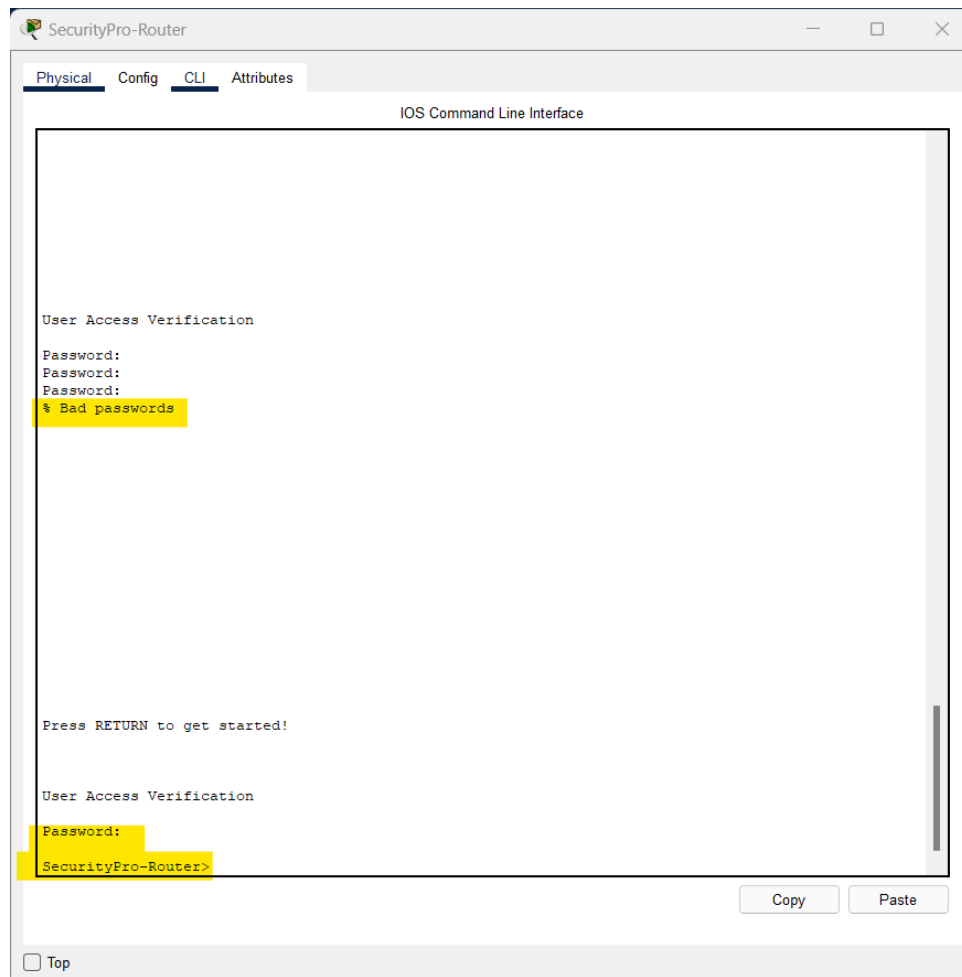
```
SecurityPro-Router>en
SecurityPro-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecurityPro-Router(config)#security passwords min-length 10
SecurityPro-Router(config)#line con 0
SecurityPro-Router(config-line)#password #N0-Acc3ss!01
SecurityPro-Router(config-line)#exec-time
SecurityPro-Router(config-line)#exec-timeout 5
SecurityPro-Router(config-line)#login
SecurityPro-Router(config-line)#exit
SecurityPro-Router(config)#
SecurityPro-Router(config)#exit
SecurityPro-Router#
%SYS-5-CONFIG_I: Configured from console by console

SecurityPro-Router#exit

SecurityPro-Router con0 is now available

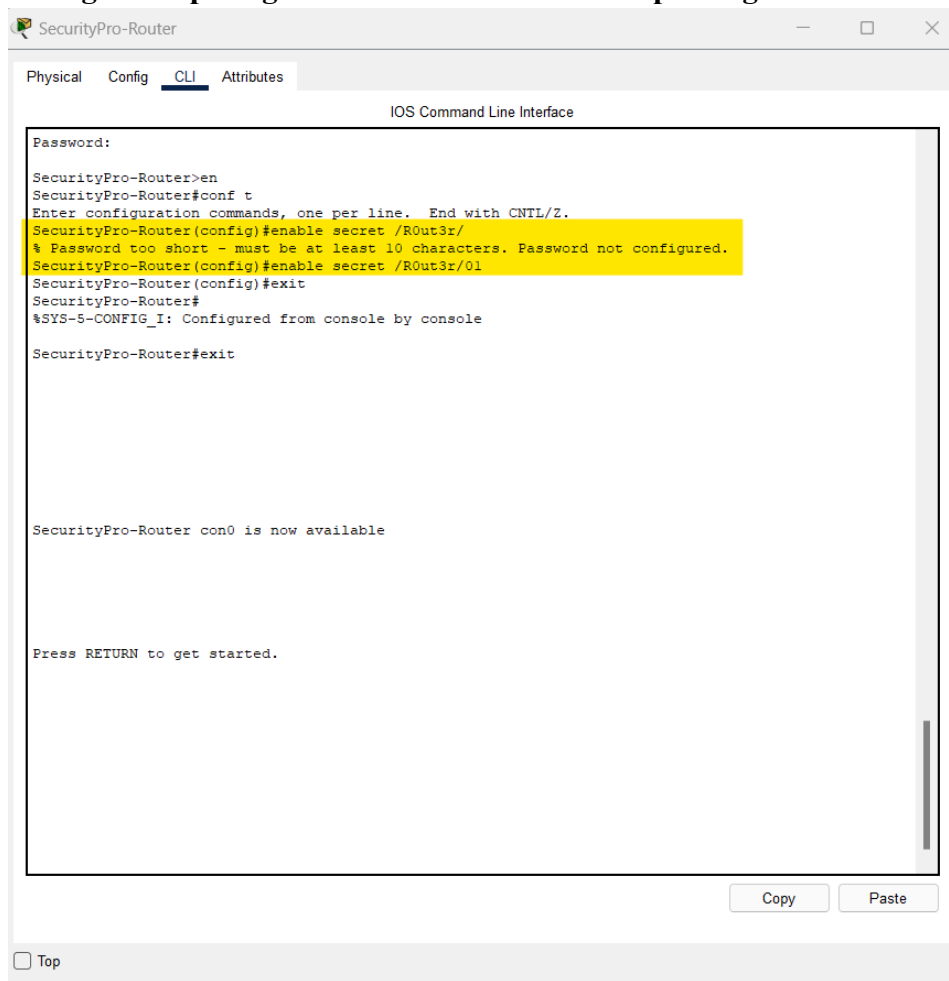
Press RETURN to get started.
```

At the bottom of the terminal window, there are 'Copy' and 'Paste' buttons. Below the terminal window, there is a 'Top' button.



Acesso ao console somente com senha!

### 3. Configurar e proteger o modo de acesso EXEC privilegiado:



The screenshot shows a terminal window titled "SecurityPro-Router" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
SecurityPro-Router>en
SecurityPro-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecurityPro-Router(config)#enable secret /R0ut3r/
% Password too short - must be at least 10 characters. Password not configured.
SecurityPro-Router(config)#enable secret /R0ut3r/01
SecurityPro-Router(config)#exit
SecurityPro-Router#
%SYS-5-CONFIG_I: Configured from console by console
SecurityPro-Router#exit
```

Below the terminal output, the message "SecurityPro-Router con0 is now available" is displayed, followed by "Press RETURN to get started." At the bottom right of the terminal area, there are "Copy" and "Paste" buttons. At the bottom left of the window, there is a "Top" button.



SecurityPro-Router

PhysicalConfigCLIAttributes

IOS Command Line Interface

SecurityPro-Router#exit

SecurityPro-Router con0 is now available

Press RETURN to get started.

User Access Verification

Password:

SecurityPro-Router>en

Password:

Password:

SecurityPro-Router#conf t

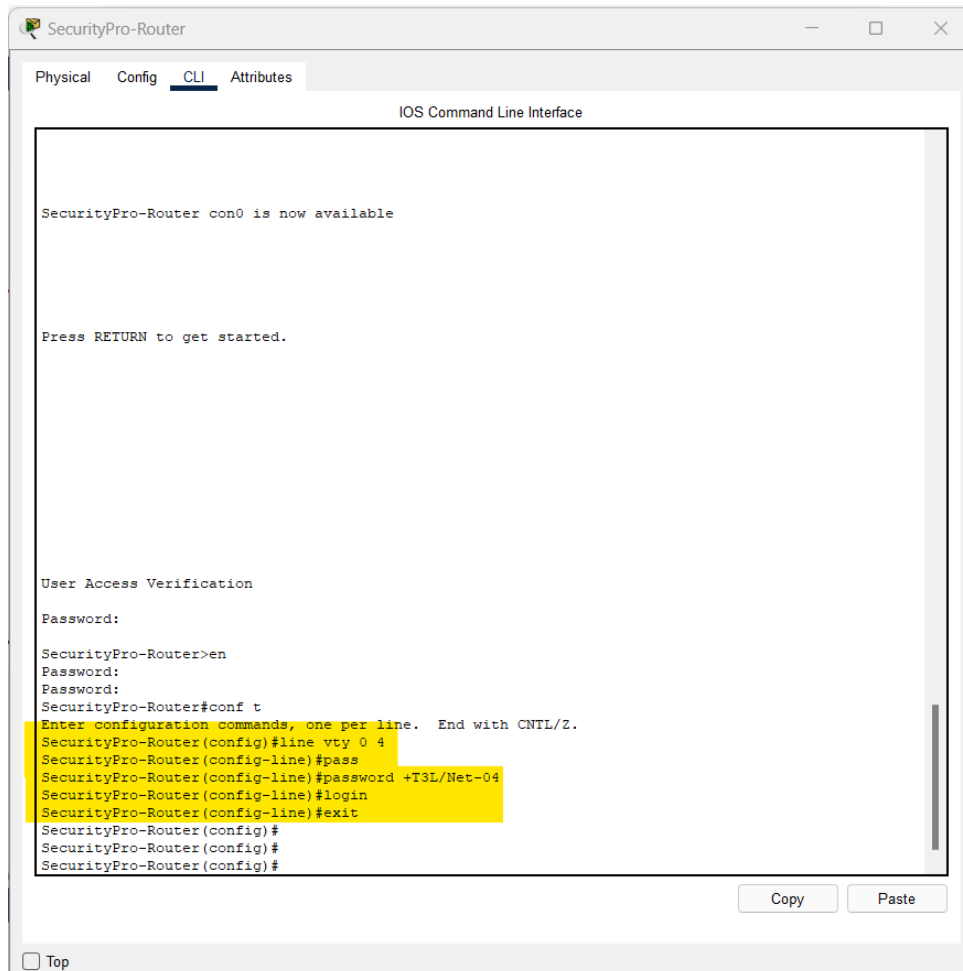
Enter configuration commands, one per line. End with CNTL/Z.

SecurityPro-Router(config)#

CopyPaste

☐ Top

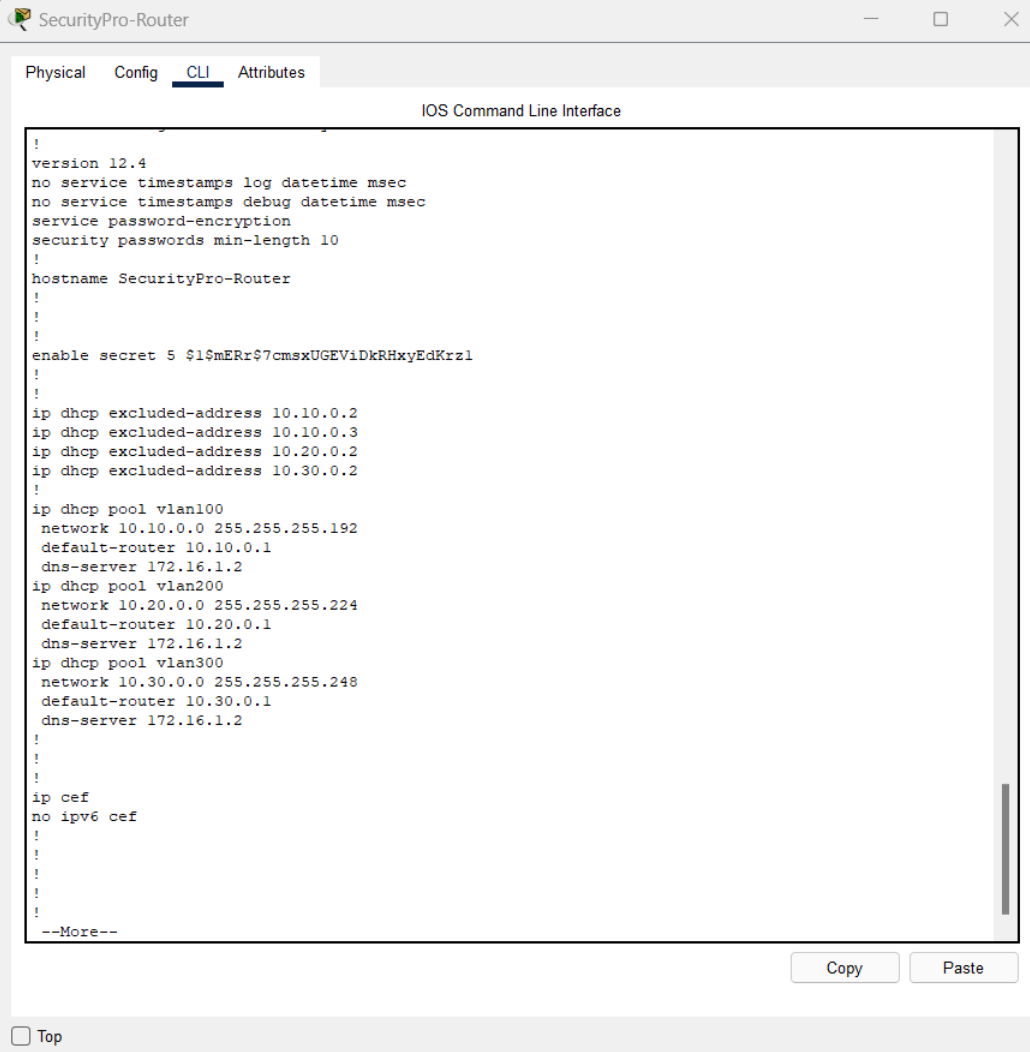
**4. Configurar senha para as linhas VTY (que permitem acesso remoto aos dispositivos usando telnet ou ssh):**



**5. Criptografar todas as senhas no roteador:**

```
SecurityPro-Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SecurityPro-Router(config)#service pass
SecurityPro-Router(config)#service password-encryption
SecurityPro-Router(config)#exit
SecurityPro-Router#
%SYS-5-CONFIG_I: Configured from console by console
```

## Verifique todas as configurações no SecurityPro-Router:



The screenshot shows the SecurityPro-Router interface with the CLI tab selected. The CLI window displays the following configuration:

```
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname SecurityPro-Router
!
!
enable secret 5 $l$mERr$7cmsxUGEViDkRHxyEdKrz1
!
!
ip dhcp excluded-address 10.10.0.2
ip dhcp excluded-address 10.10.0.3
ip dhcp excluded-address 10.20.0.2
ip dhcp excluded-address 10.30.0.2
!
ip dhcp pool vlan100
network 10.10.0.0 255.255.255.192
default-router 10.10.0.1
dns-server 172.16.1.2
ip dhcp pool vlan200
network 10.20.0.0 255.255.255.224
default-router 10.20.0.1
dns-server 172.16.1.2
ip dhcp pool vlan300
network 10.30.0.0 255.255.255.248
default-router 10.30.0.1
dns-server 172.16.1.2
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
--More--
```

At the bottom of the CLI window, there are "Copy" and "Paste" buttons. Below the CLI window, there is a "Top" button with a checkbox.

SecurityPro-Router

PhysicalConfigCLIAttributes

IOS Command Line Interface

```
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.1
encapsulation dot1Q 100
ip address 10.10.0.1 255.255.255.192
ip access-group CONTROLE-ACESSO-VLANS in
ip nat inside
!
interface FastEthernet0/0.2
encapsulation dot1Q 200
ip address 10.20.0.1 255.255.255.224
ip access-group CONTROLE-ACESSO-VLANS in
ip nat inside
!
interface FastEthernet0/0.3
encapsulation dot1Q 300
ip address 10.30.0.1 255.255.255.248
ip access-group CONTROLE-ACESSO-VLANS in
ip nat inside
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
--More--
```

CopyPaste

☐ Top

SecurityPro-Router

PhysicalConfigCLIAttributes

IOS Command Line Interface

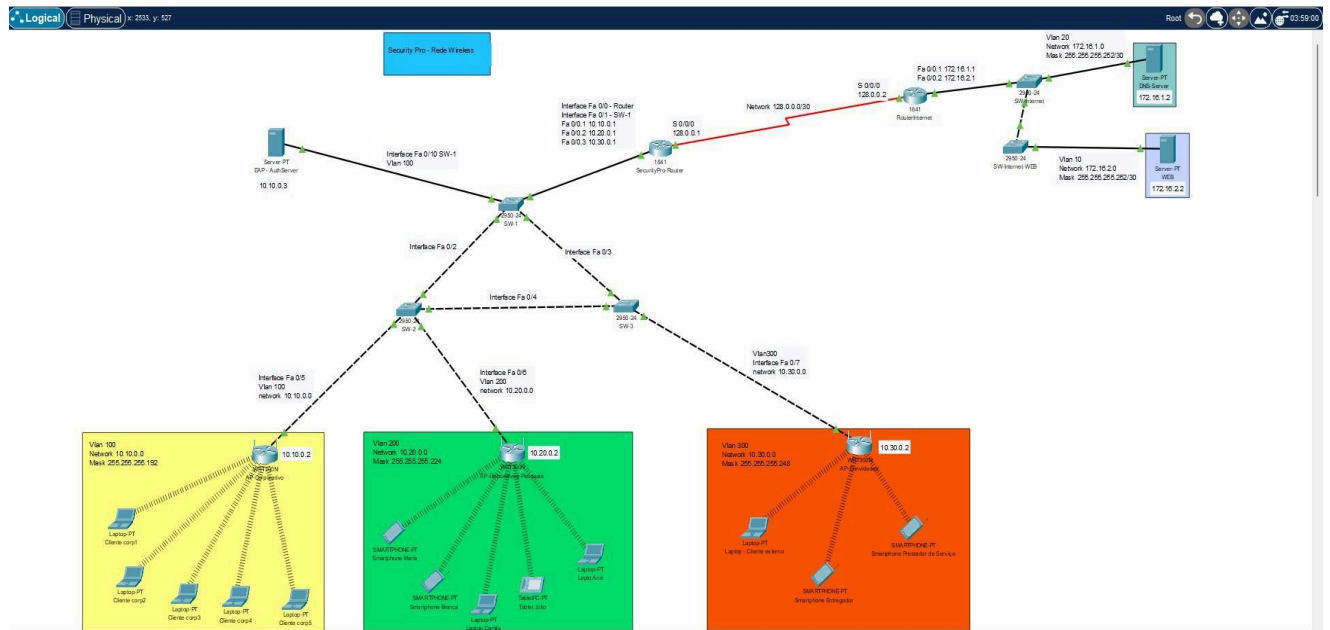
```
deny icmp 10.20.0.0 0.0.0.31 host 10.10.0.3
deny icmp 10.30.0.0 0.0.0.7 host 10.10.0.3
deny tcp 10.20.0.0 0.0.0.31 host 10.10.0.3
deny tcp 10.30.0.0 0.0.0.7 host 10.10.0.3
ip access-list extended CONTROLE-ACESSO-VLANS
deny icmp 10.20.0.0 0.0.0.31 10.10.0.0 0.0.0.63
deny icmp 10.30.0.0 0.0.0.7 10.10.0.0 0.0.0.63
deny icmp 10.10.0.0 0.0.0.63 10.20.0.0 0.0.0.31
deny icmp 10.30.0.0 0.0.0.63 10.20.0.0 0.0.0.31
deny icmp 10.20.0.0 0.0.0.31 10.30.0.0 0.0.0.7
deny icmp 10.10.0.0 0.0.0.63 10.30.0.0 0.0.0.7
permit ip any any
ip access-list standard NAT
permit 10.10.0.0 0.0.0.63
permit 10.20.0.0 0.0.0.31
permit 10.30.0.0 0.0.0.7
!
banner motd ^C
##### Acesso proibido para pessoas nao autorizadas!#####
^C
!
!
!
!
!
line con 0
exec-timeout 5 0
password 7 0862621E4438061441181F457A7A
login
!
line aux 0
!
line vty 0 4
password 7 086A781D25562B1206465C50
login
!
!
!
end

SecurityPro-Router#
```

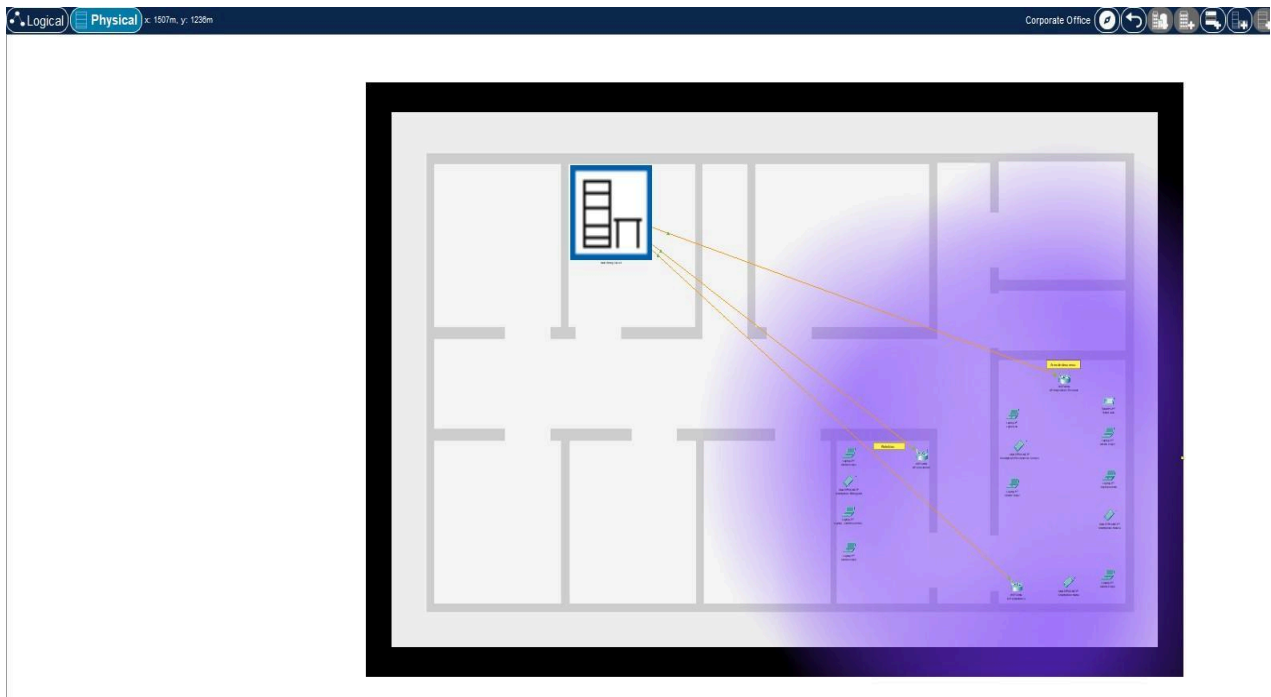
CopyPaste

☐ Top

# Visão lógica da rede:



# Visão física da rede



**Não esqueça de rever as Políticas de Segurança da rede e o planejamento.**