**Escola Superior de Tecnologia e Gestão**

**Licenciatura em Engenharia Informática**

**Tecnologias de Computadores**

**Ano Letivo 2023/24**

**Trabalhos Laboratoriais de Redes de Computadores II**

**Elaborado em: 27/10/23**

**Guilherme Rodrigues a2020154390**

**Índice**

[1. Introdução 1](#_Toc149476114)

[2. Fichas Laboratoriais 1](#_Toc149476115)

[2.1. 01.1.7\_Lab\_-\_Basic\_Switch\_Configuration 1](#_Toc149476116)

[2.2. 01.6.2 Lab - Configure Basic Router Settings 17](#_Toc149476117)

[2.3. 04.5.2 Lab - Implement Inter-VLAN Routing 32](#_Toc149476118)

[2.4. Physical Layer **Erro! Marcador não definido.**](#_Toc149476119)

[2.5. Number Systems **Erro! Marcador não definido.**](#_Toc149476120)

[2.6. Data Link Layer **Erro! Marcador não definido.**](#_Toc149476121)

[3. Conclusion 61](#_Toc149476122)

[4. References Erro! Marcador não definido.](#_Toc149476123)

# Introdução

Neste relatório, examinaremos em detalhes as fichas laboratoriais realizadas ao longo do semestre, destacando as lições aprendidas e as habilidades adquiridas em cada uma delas. O objetivo é não apenas relatar nossas experiências, mas também destacar como essas atividades práticas são cruciais para a nossa formação e como estão alinhadas com os objetivos da disciplina de Redes de Computadores 2.

# Fichas Laboratoriais

## 01.1.7\_Lab\_-\_Basic\_Switch\_Configuration

**Objetivos**

Esta primeira ficha tem os seguintes objetivos:

* **Parte 1: Conectar a Rede e Verificar a Configuração Padrão do Switch**

Nesta parte, o objetivo é realizar a conexão física dos dispositivos de rede e verificar a configuração padrão do **switch**.

* **Parte 2: Configurar as Definições Básicas dos Dispositivos de Rede**

Nesta etapa, iremos configurar as definições básicas dos dispositivos de rede. Isso inclui a configuração das definições essenciais do **switch** e a atribuição do endereço IP ao computador.

* **Parte 3: Verificar e Testar a Conexão de Rede**

Nesta parte, iremos verificar as configurações dos dispositivos. Em seguida, faremos testes de conexão para garantir que os dispositivos se estejam a comunicar corretamente. Iremos utilizar comandos como "**ping**" para verificar a conexão **end-to-end** e "**Telnet**" para testar as capacidades de gerenciamento remoto.

* **Parte 4: Gerenciar a Tabela de Endereços MAC**

Nesta última parte, registamos o endereço MAC do host. Além disso, identificamos os endereços MAC aprendidos pelo **switch**. Iremos explorar as opções do comando "**show mac address-table**" e configurar um endereço MAC estático quando necessário.

**Requisitos**

* + 1 switch (Cisco 2960 com imagem lanbasek9 do Cisco IOS versão 15.2(2) ou comparável)
  + 1 PC (Windows com um programa de emulação de terminal, como **Tera Term**)
  + 1 Cabo de consola para configurar o dispositivo Cisco IOS através da porta de consola
  + 1 cabo Ethernet conforme mostrado na topologia

**Parte 1**

Nesta parte foi feito o esquema da rede utilizado o programa “**Cisco Packet Tracer**” este programa permite emular uma situação real de configuração de rede.

Assim o esquema de rede ficou da seguinte maneira:

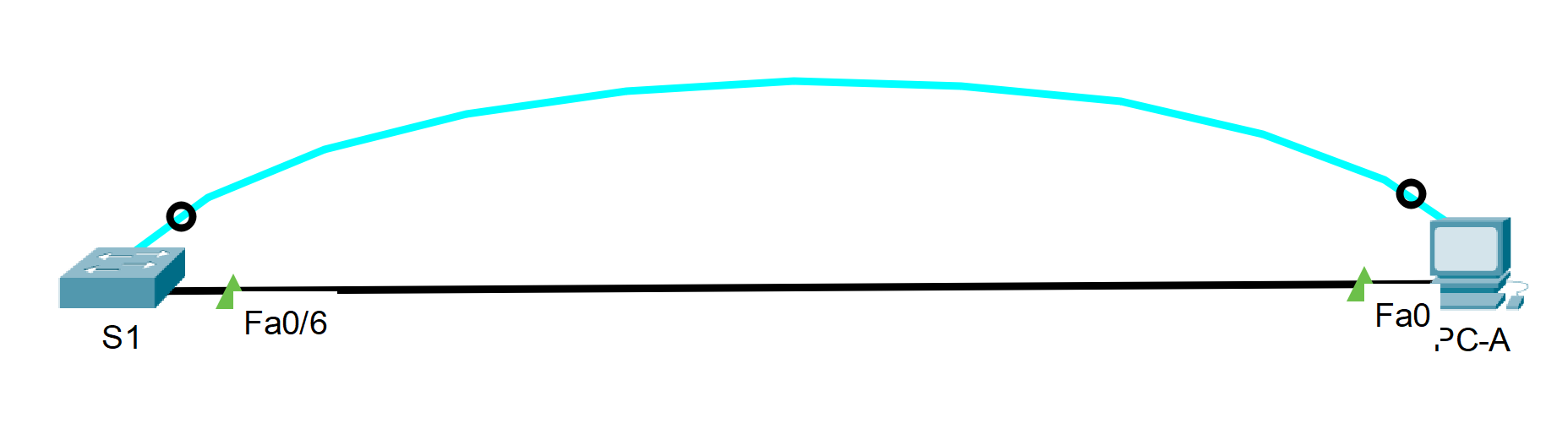


Ilustração : Esquema de rede 1

Usamos um **Switch 2960** e um PC **windows,** o cabo azul representa o cabo de consola e o cabo preto representa o cabo de conexão direta.

As portas onde foi conectado o cabo de ligação direta foi a Fa0/6 no **Switch** e a Fa0 no PC.

Como ainda não foram configurados endereços de IP ainda não existe rede configurada pelo que não é possível fazer uma conexão via **SSH** ou **Telnet**.

**Parte 2**

Supondo que o **switch** não tem um arquivo de configuração armazenado na memória **NVRAM**, vamos usar o comando **enable (en)** para entrar no modo privilegiado do **switch**.

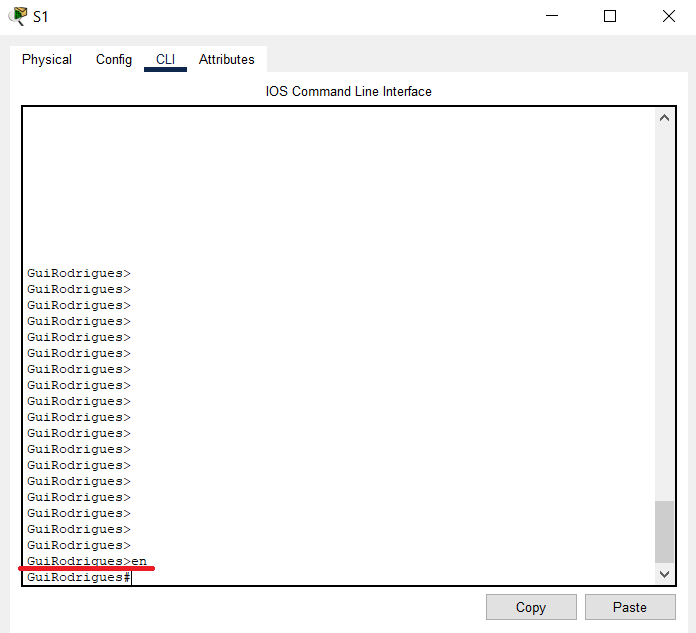


Ilustração : Entrada no modo privilegiado com o comando **enable**

O nome do switch foi previamente alterado com o comando “**hostname**”, para o nome do aluno que realizou a ficha.

Para verificar se há um arquivo de configuração padrão no **switch** usamos o comando “**show running-config**” comando do modo privilegiado do **switch**.

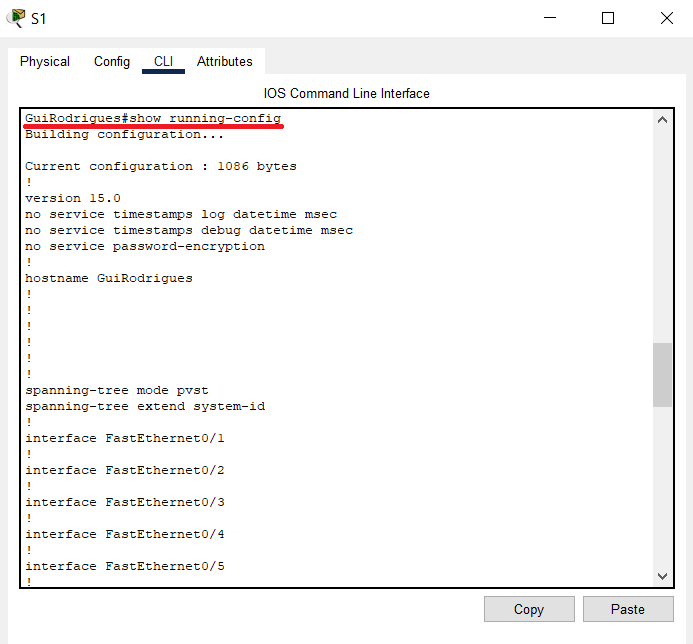


Ilustração : Verificação da existência de um arquivo de configuração

Com este comando também podemos verificar as seguintes informações:

* Existem 24 interfaces de **FastInternet**
* Existem 2 interfaces de **Gibit Ethernet**

Em seguida iremos analisar a configuração dentro da **NVRAM,** para isso usamos o comando “**show start-up-config**” (**show start**).

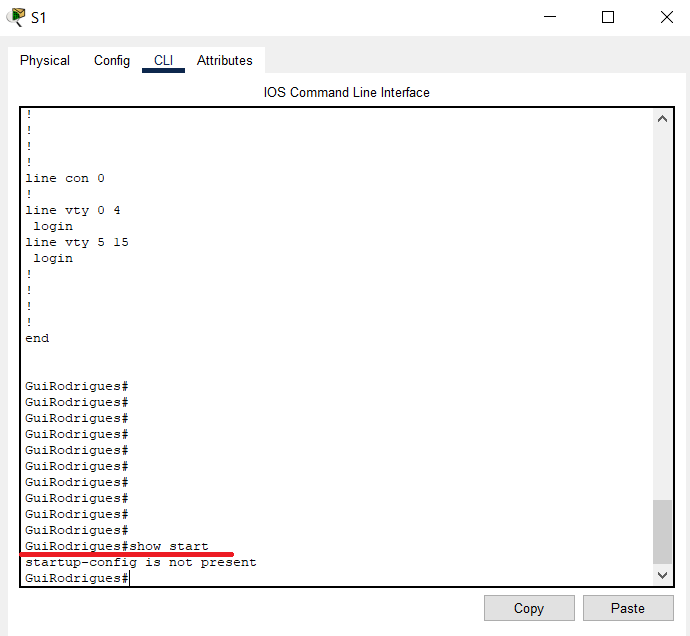


Ilustração : Observar se existe uma configuração inicial

Como podemos observar não existe qualquer tipo de configuração devido ao facto de termos acabado de montar o sistema.

Em seguida veremos as características do **SVI** do **VLAN1**. Conseguimos esta informação através do comando “**show int vlan 1**”

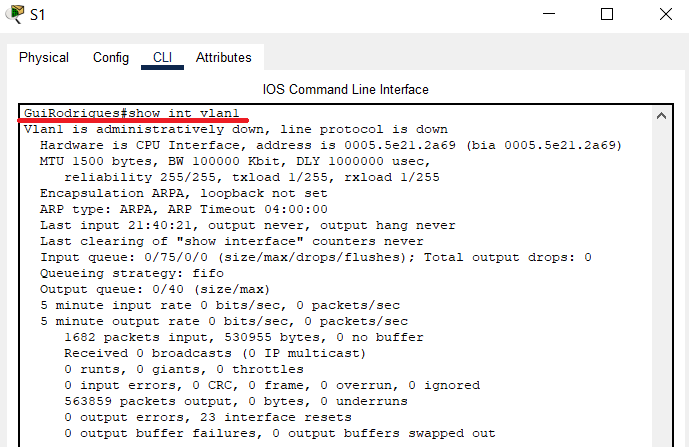


Ilustração : Caraterísticas da VLAN1

Por padrão, a **VLAN 1** está ativada nos **switches Cisco**, mas não estará operacional até que uma porta seja atribuída a ela e esta porta esteja **up**. Se nenhuma porta estiver **up** na **VLAN 1**, a interface da **VLAN 1** estará **up**, mas o protocolo de linha estará **down**. Todas as portas são atribuídas inicialmente à **VLAN 1**.

Podemos também percebem que não existem qualquer endereço de IP direcionado para a **VLAN1**

Se usarmos o comando “**show ip interface VLAN1**”, podemos observar o falado anteriormente.

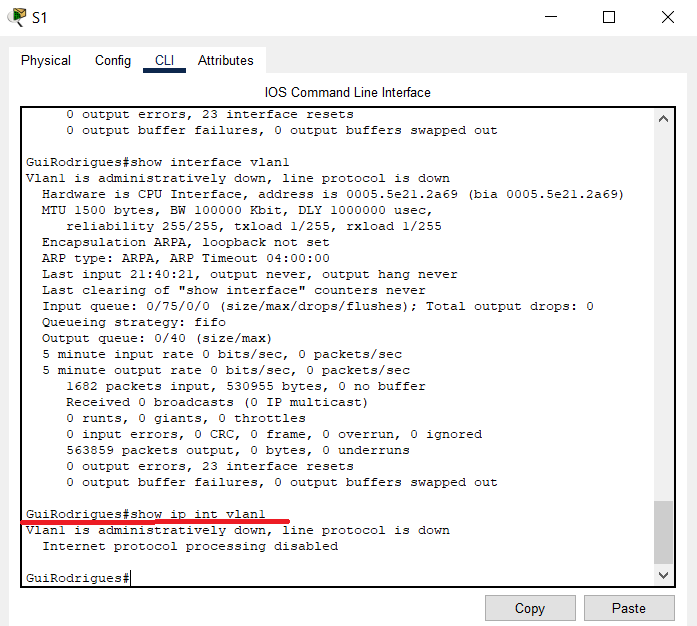


Ilustração : Show ip int vlan1

Conseguimos então observar que a **VLAN1** está ativa, o protocolo de linha está inativo e o processamento de protocolo de Internet está desativado.

Em seguida observaremos a versão do sistema do **switch** para isso usamos o comando “**show version**”

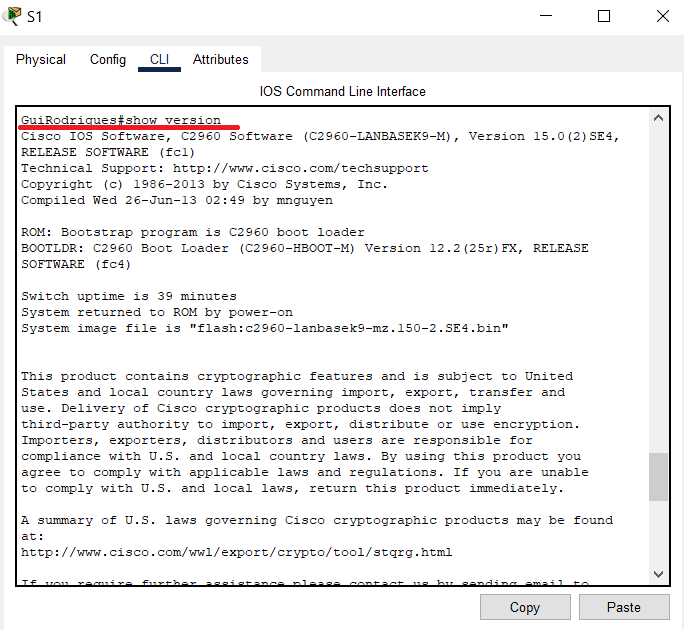


Ilustração : Versão do sistema do switch

A partir deste comando obtemos a informação de que o sistema se encontra na versão 15.0.

Verificamos também as definições padrão da interface á qual conectamos o cabo de conexão direta, o comando utilizado foi “**show int f0/6**”.

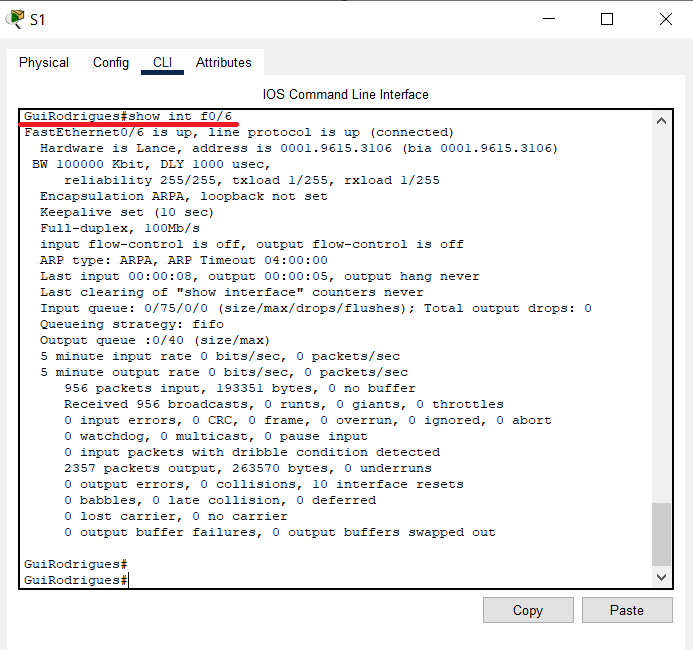


Ilustração : Definição padrão da interface f0/6

Podemos observar então que a interface está **up,** o contrário só aconteceria caso houvesse um problema de cabeamento.

Conseguimos verificar que a definição duplex da interface está em **Full-Duplex** e a velocidade maxima está em 100Mb/s

Para verificar as definições padrão da **VLAN** devemos usar o comando “**show vlan**”

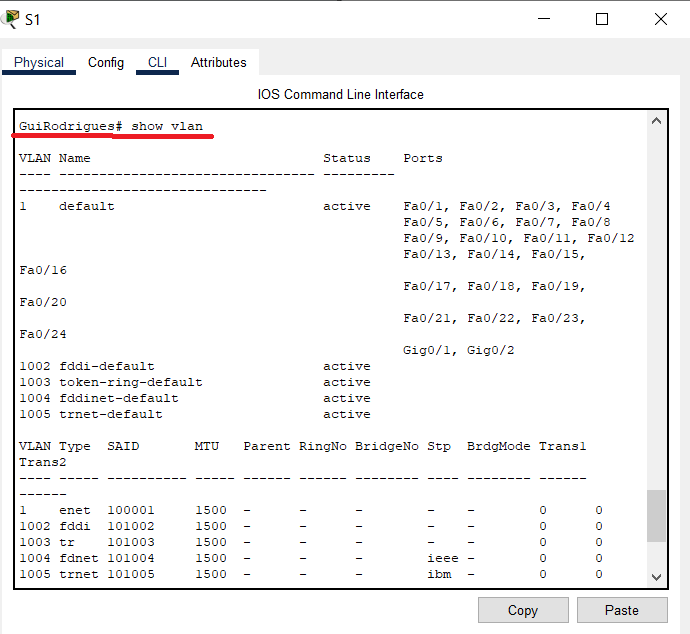


Ilustração : Definição padrão da VLAN

A partir deste comando conseguimos extrair o nome padrão da interface “**default**”, se está ativa, o número de portas associadas e o seu tipo.

Por fim usamos os comandos “**show flash**” e “**dir flash**” para ver o conteúdo e da memória flash.

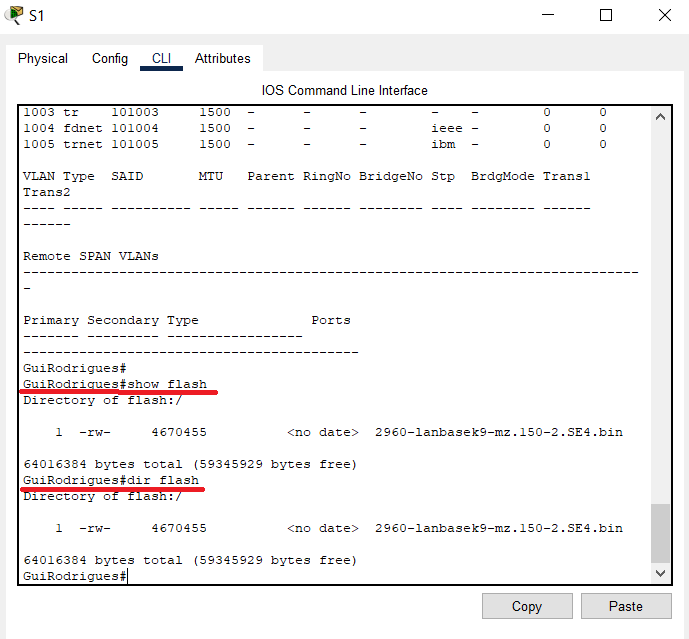


Ilustração : conteudo da memória flash

**Parte 2**

Começamos então a configuração básica do switch. Em primeiro colocamos a seguinte configuração:

* no ip domain-lookup
* hostname S1
* service password-encryption
* enable secret class
* banner motd #Apenas pessoal Autorizado #

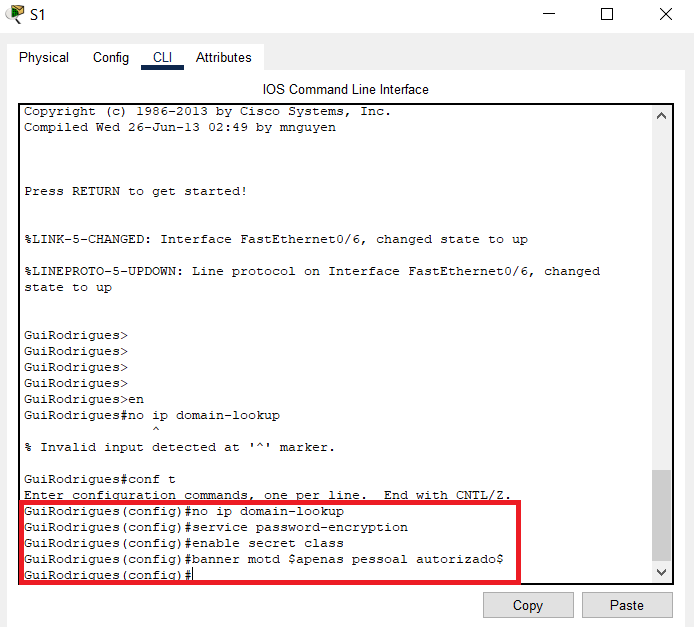


Ilustração : Configuração simples

Em segundo foi defenido o endereço IP SVI do **switch,** isto permite configurar e acessar o **switch** remotamente.

Para começar, criamos uma **VLAN 99** no **switch**. Em seguida, defenimos o endereço IP do **switch** para 192.168.1.2 com uma máscara de sub-rede 255.255.255.0 na interface virtual interna **VLAN 99**. O endereço IPv6 também pode ser configurado na interface **SVI**.

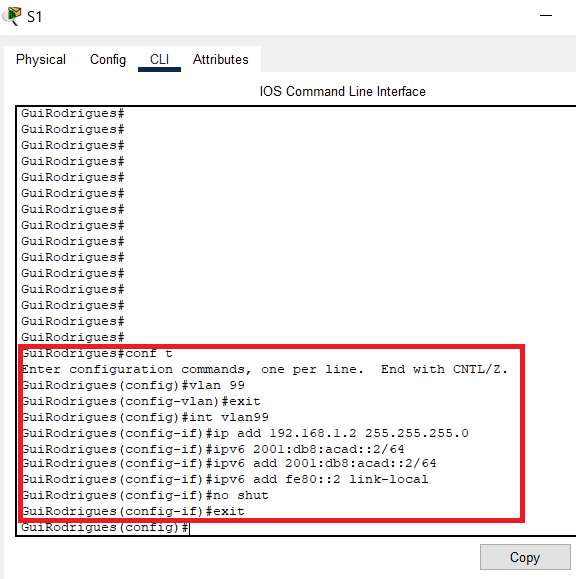


Ilustração : Configuração da VLAN99

Em seguida iremos atribuir portos a **VLAN 99**. Usamos então os comandos “**interface range f0/1 – 24,g0/1 -2”** e“**switchport access vlan 99”,** a confirmação é feita através do comando “**show vlan brief**”.

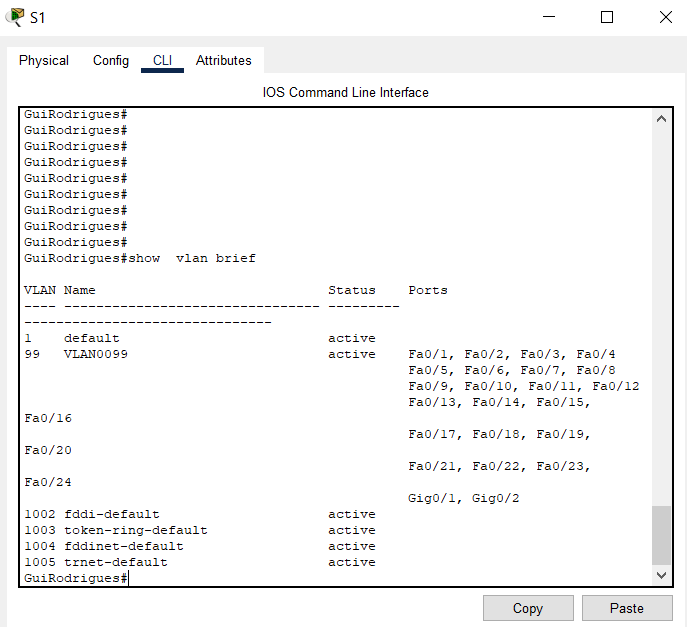


Ilustração : Atribuição das portas

O acesso à porta da consola também deve ser restrito com uma senha. Usamos cisco como senha de login da consola. A configuração padrão é permitir todas as conexões de console sem necessidade de senha. Para evitar que mensagens do console interrompam comandos, usamos a opção de registo síncrono.

Foram configuradas também as linhas do terminal virtual (**vty**) do **switch** para permitir acesso **telnet**.

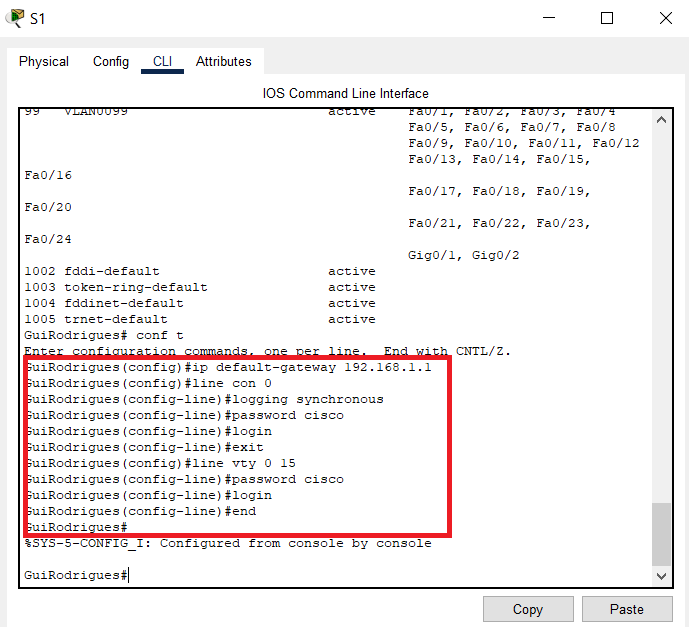


Ilustração : Segurança da porta da consola

Em seguida foi feita a configuração do PC.

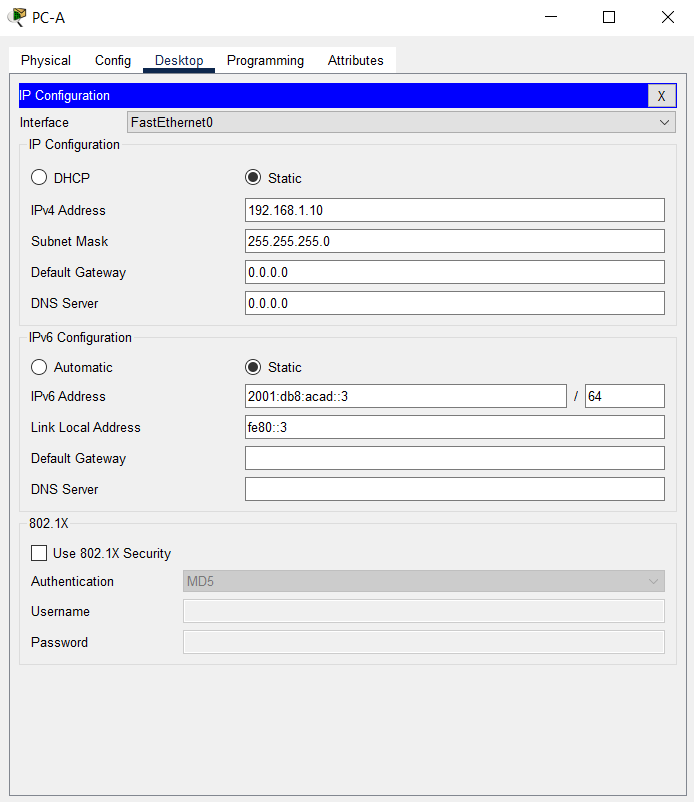


Ilustração : Configuração do PC.

**Parte 3**

Na terceira parte vamos mostrar toda a configuração feita até agora.

Começando pelo **switch**. Para observar a configuração em execução usamos o comando “**show run**”.

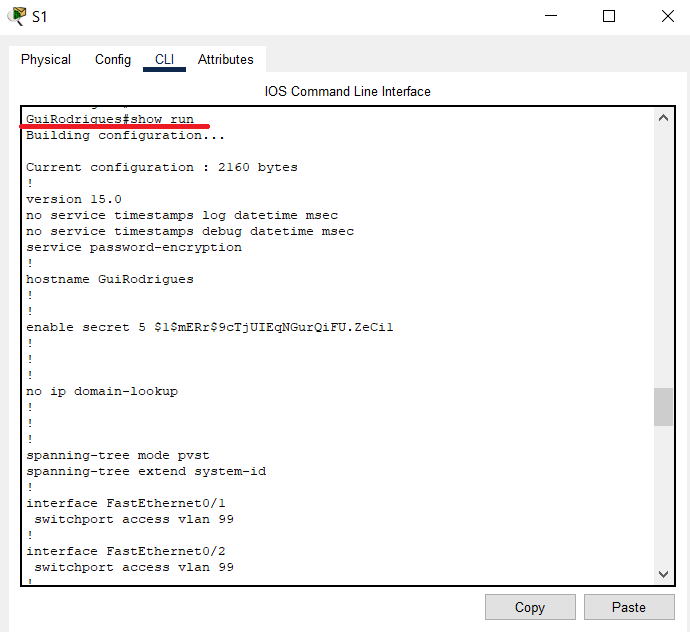


Ilustração : Configuração em execução

Uma imagem com texto, captura de ecrã, ecrã, software

Descrição gerada automaticamente

Ilustração : Configuração em execução 2

Em seguida podemos ver também a configuração da **VLAN 99** que criamos anteriormente. Ao executar o comando “**show interface vlan99**”.

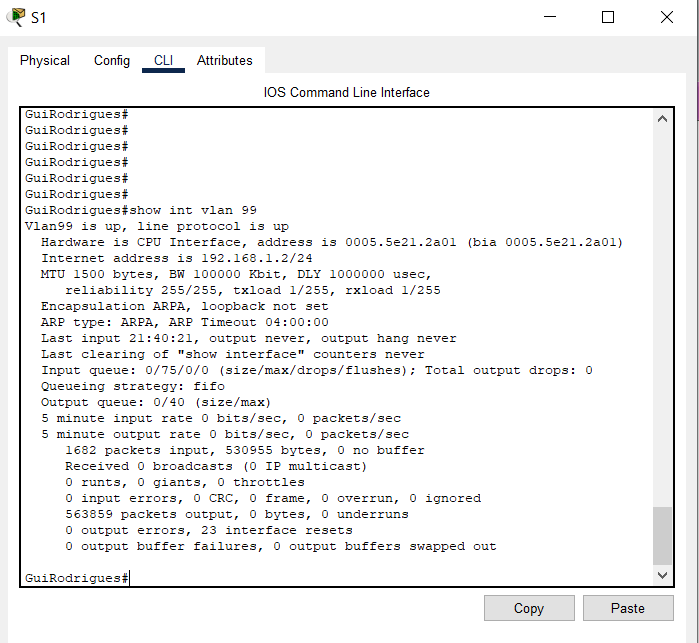


Ilustração : Configuração da vlan 99

A partir deste comando podemos observar que a largura de banda da interface é de 1000000 Kb/s e que o estado da **vlan** é **up**.

Por fim verificaremos se é possível realizar a comunicação entre o PC e o switch. Para isso usamos o comando “**ping**” juntamente do IP do dispositivo que pretendemos comunicar.

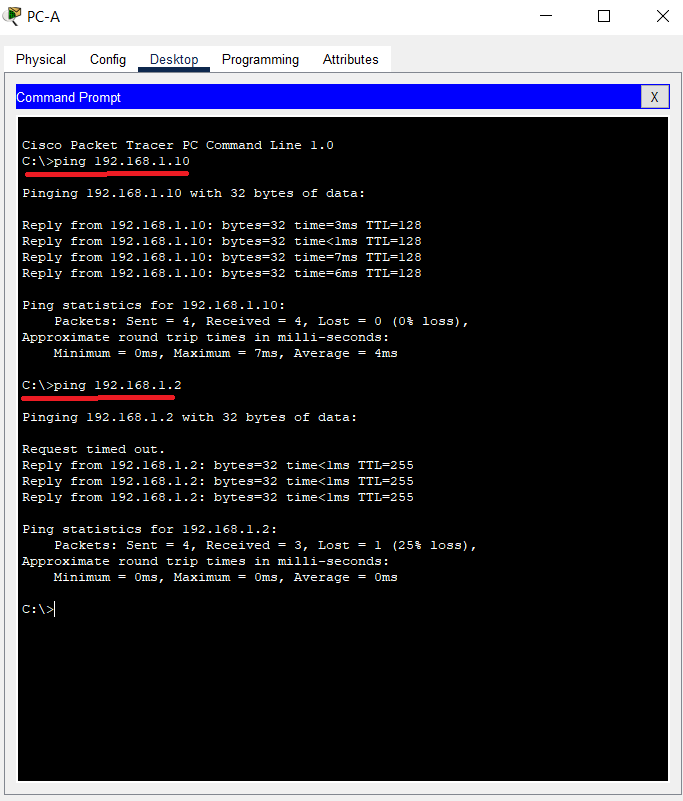


Ilustração : Ping dos dispositivos

Ante de terminarmos todos os testes é necessário copiar a configuração atual para a configuração de arranque, para esse efeito usamos o comando “**cp run start**” assim a próxima vez que iniciarmos o switch este será iniciado com a configuração que temos neste momento a ser executada.

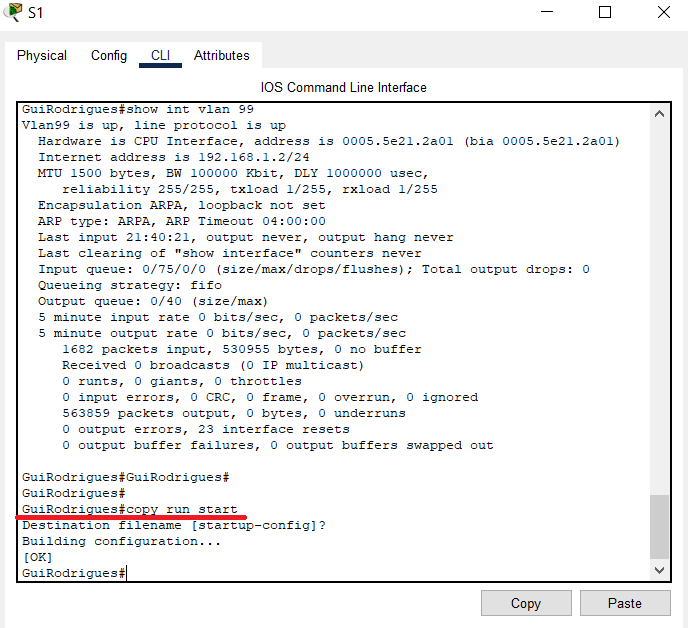


Ilustração : Copia da configuração

Em seguida apartir do PC iremos verificar o endereço **mac** do host, usando o comando “**ipconfig /all**”

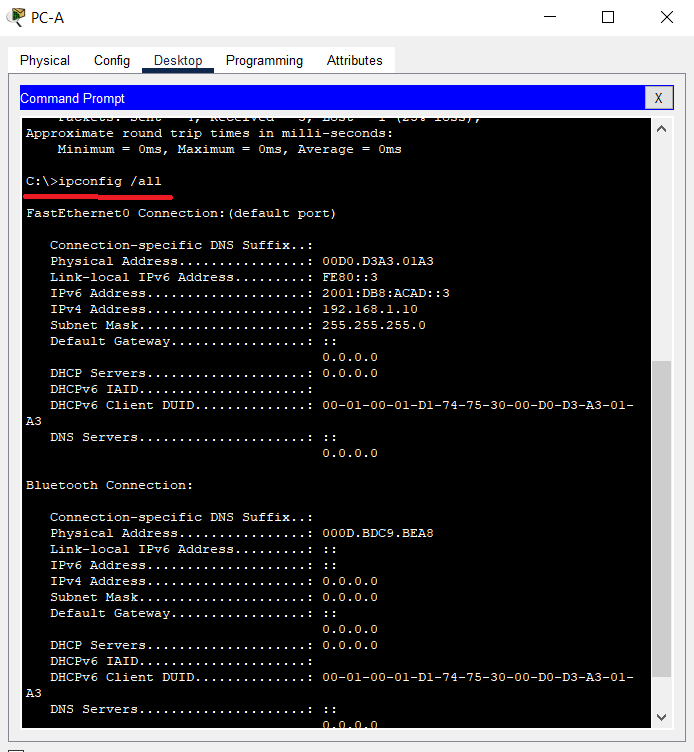


Ilustração : ipconfig /all

Em seguida conseguimos determinar o que é que o switch aprendeu com as configurações que foram efetuadas usando o comando “**show mac address-table**”. Este comando possui algumas variações que são observáveis quando ao comando é acrescentada a opção “**?**”. Esta opção irá mostrar todas as variações possíveis do comando.

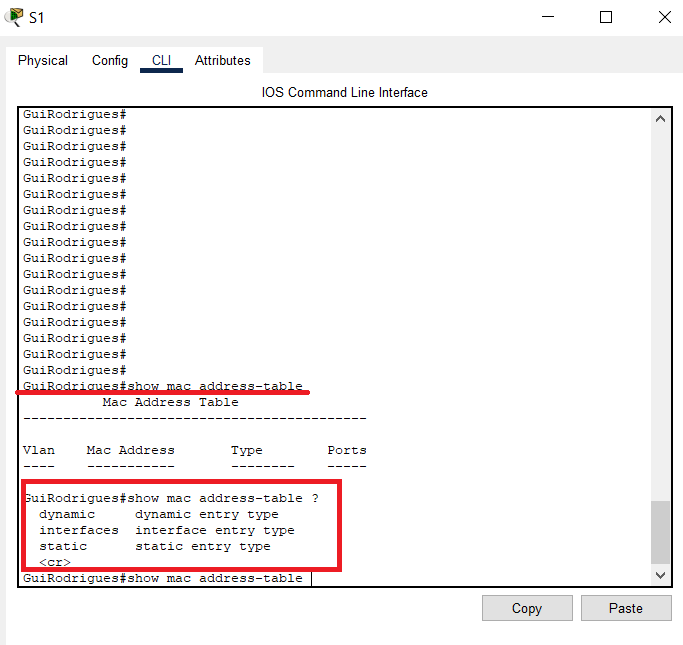


Ilustração : Show mac address-table

## 01.6.2 Lab - Configure Basic Router Settings

**Objetivos**

* **Parte 1: Configurar a Topologia e Inicializar Dispositivos**

Nesta etapa, a configuração da topologia de rede é realizada, e os dispositivos são inicializados de acordo com a topologia.

* **Parte 2: Configurar Dispositivos e Verificar a Conexão**

Aqui, as interfaces dos PC’s recebem informações IPv4 e IPv6 estáticas. Além disso, as configurações básicas do router são realizadas, incluindo a configuração do SSH para o router. Após as configurações, a conexão de rede é verificada.

* **Parte 3: Exibir Informações do Router**

Nesta etapa, informações relevantes, como dados de hardware e software do router, são coletadas. A saída da configuração de inicialização e da tabela de rotas é interpretada para verificar o estado das interfaces.

**Requisitos**

* 1 Router (Cisco 4221 com Cisco IOS XE Release 16.9.4 na imagem universal ou equivalente)
* • 1 Comutador (Cisco 2960 com Cisco IOS Release 15.2(2) na imagem lanbasek9 ou equivalente)
* • 2 PC’s (Windows com um programa de emulação de terminal, como o Tera Term)
* • Cabos de consola para configurar os dispositivos Cisco IOS através das portas de consola
* • Cabos Ethernet conforme mostrado na topologia

**Parte 1**

Primeiro e em semelhança a fixa anterior foi feito o esquema da rede utilizado o programa “**Cisco Packet Tracer**”.

Assim o esquema de rede ficou da seguinte maneira:

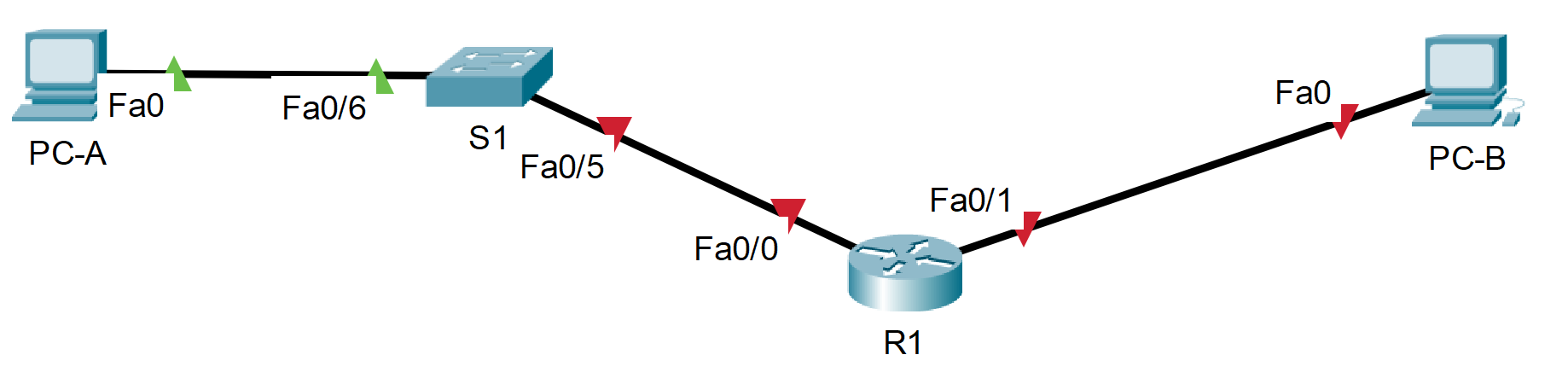


Ilustração : Esquema de rede ficha 2

Usamos um **Switch 2960**, dois PC’s **Windows** e um **router** cisco 2960**,** o cabo preto representa o cabo de conexão direta entre todos os dispositivos.

As portas onde foram conectados os cabos de ligação direta são as seguintes: Fa0 no PC-A e PC-B, as Fa0/6 e Fa0/5 no **switch** e no **router** foram as Fa0/0 e Fa0/2.

**Parte 2**

Na segunda parte foi feita a configuração dos PC’s com IPv4 e IPv6 e dos restantes dispositivos da rede.

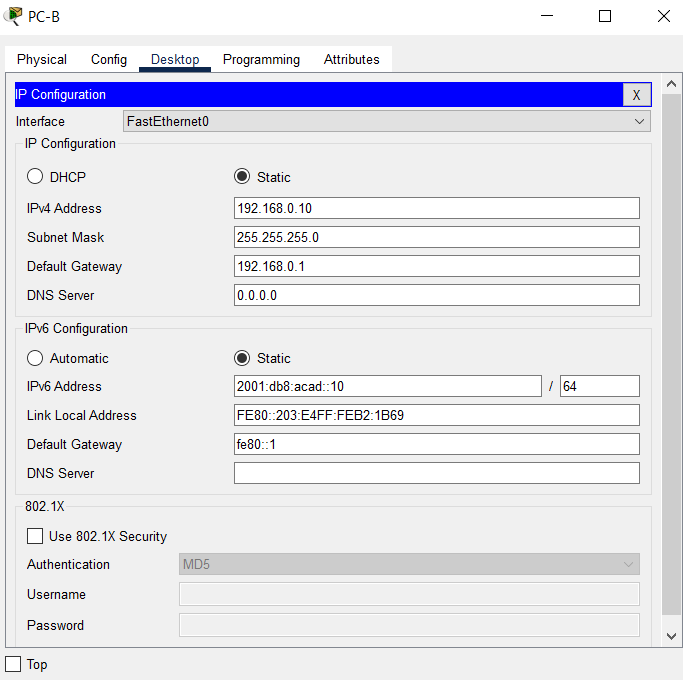


Ilustração : Configuração PC-B

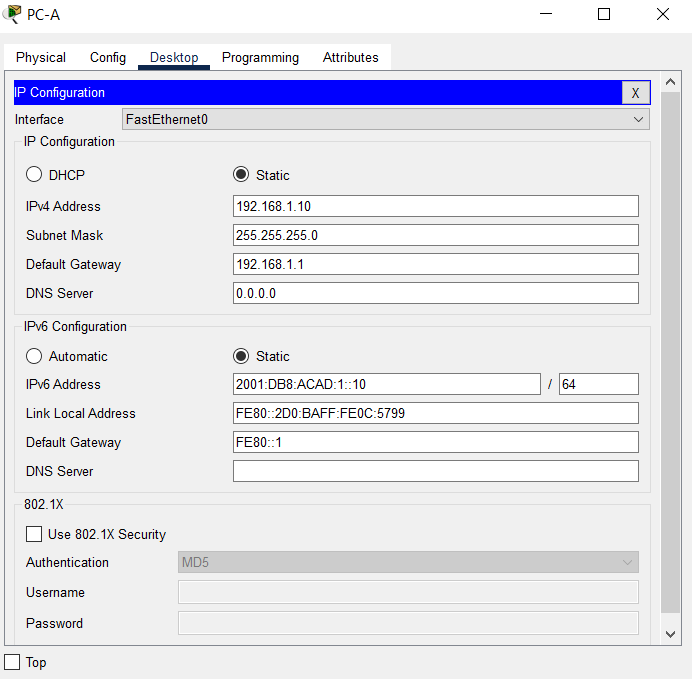


Ilustração : Configuração PC-A

No **router** foiconfigurado um “**hostname”** através do comando “**hostname**”, configurado o nome de domínio do router como “**ccna-lab.com**” através do comando “**ip domain name ccna-lab.com**”, em seguida desativada a pesquisa de DNS para evitar que o router tente traduzir comandos incorretamente inseridos com o comando “**no ip domain lookup**”, depois foram criptografadas todas as passwords “**service password-encryption**”, ainda relativamente as passwords foi configurado para que o sistema exija sempre uma password com um mínimo de 12 caracteres com o comando “**security passwords min-length 12**”. Por fim foi configurado o nome de utilizador “**SSHadmin”** com uma senha criptografada de “**55Hadm!n2020”** e gerado um conjunto de chaves criptográficas com um módulo de 1024 bits com os respetivos comandos “**username SSHadmin secret 55Hadm!n2020**” “**crypto key generate rsa modulus 1024**”.

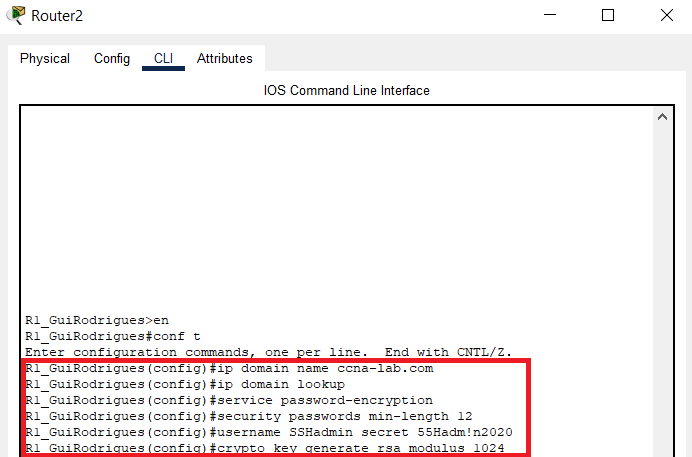


Ilustração : Configuração do router

Em seguida, atribuida a senha de execução privilegiada como “**123456789123**” com o comando “**enable** **secret**”.

Para a atribuição da senha “**123456789123**” para a consola e as sessões desconectarem-se após quatro minutos de inatividade usamos o seguinte grupo de comandos:

* **line console 0**
* **password $cisco!!CON\***
* **exec-timeout 4 0**
* **login**

A mesma senha foi atribuída como a password VTY, foram configuradas as linhas VTY para aceitar apenas conexões SSH e as sessões para desconectar após quatro minutos de inatividade.

* **line vty 0 4**
* **password $cisco!!VTY\***
* **exec-timeout 4 0**
* **transport input ssh**
* **login local**

O banner “Apenas pessoal autorizado” foi criado para avisar que acesso não autorizado não é permitido “**banner motd $(frase desejada)$”.**

Por fim foi ativado o encaminhamento IPv6 “**ipv6 unicast-routing**”.

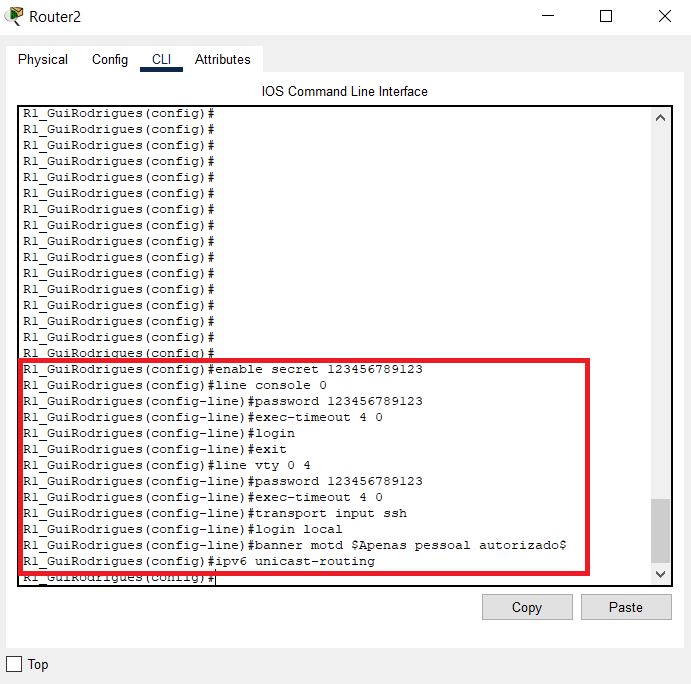


Ilustração : Segunda parte da configuração do router

No próximo passo as três interfaces do router foram configuradas com informações de endereço IPv4 e IPv6. Além disso, cada interface recebeu uma descrição identificativa, e todas as três interfaces foram ativadas para permitir a comunicação.

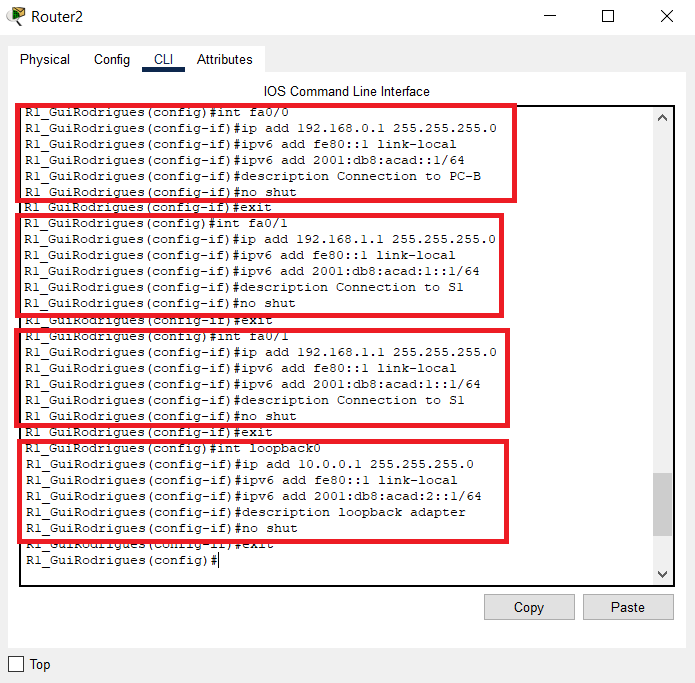


Ilustração : Configuração das portas

Foi configurado para que q router não permitisse logins **vty** por dois minutos se ocorrerem três tentativas de login falhadas dentro de 60 segundos, configurado o relógio e salva a configuração em execução no arquivo de iniciação.

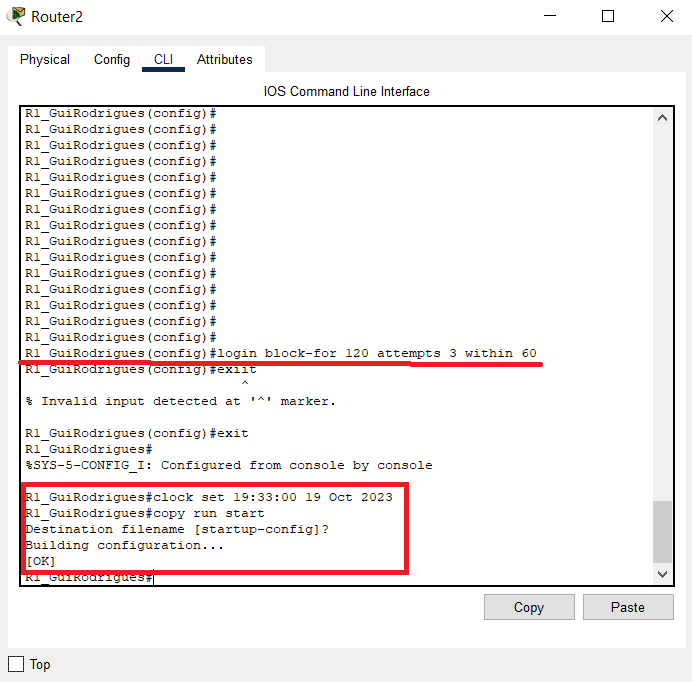


Ilustração : última configuração

No próximo passo a partir do PC-A foi feita a tentativa de **ping**  para o PC-B utilizando o IPv4 e o IPv6.

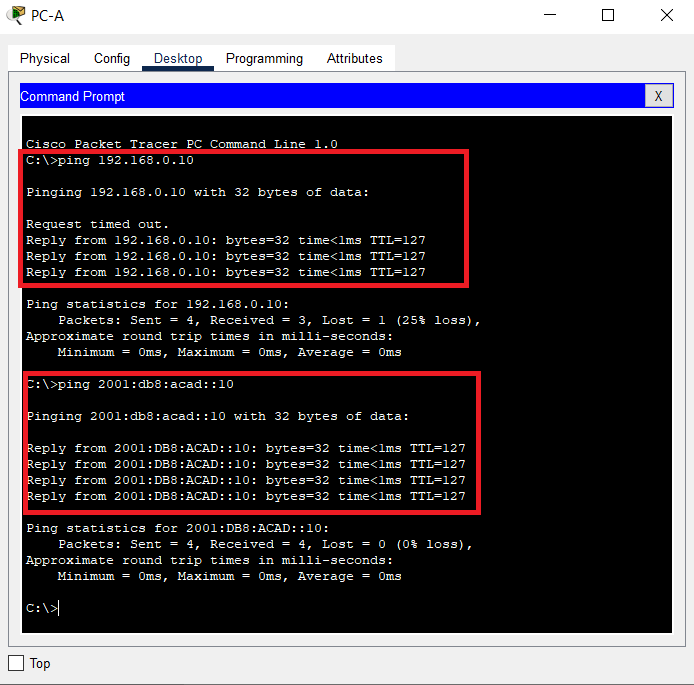


Ilustração : Ping do PC-B atraves do PC-A

**Parte 3**

Nesta parte iremos retirar informação de **software** e **hadrware** usando o comando “**show version**”

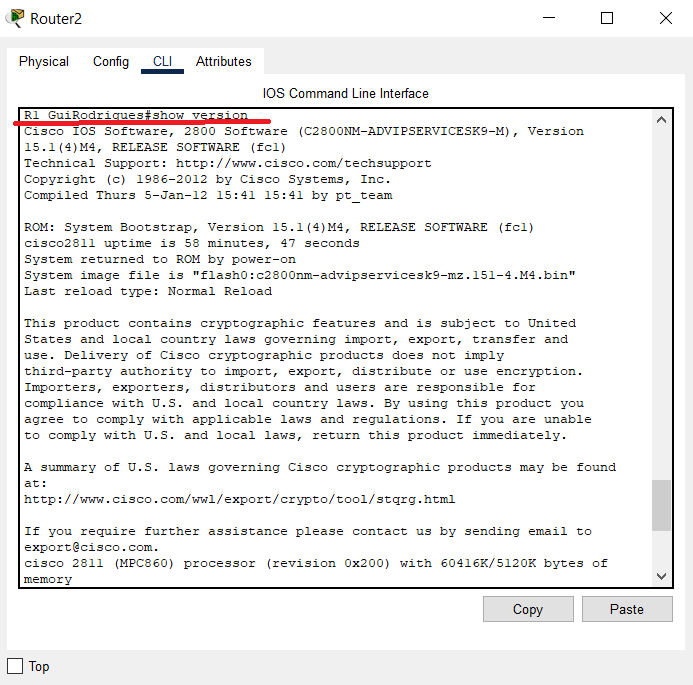


Ilustração : Informação do router

O comando "show" fornece várias telas de saída. Filtrar essa saída permite que se exiba seções específicas da saída. Sendo assim filtramos o comando "**show version**", usando "**show version | include register**".

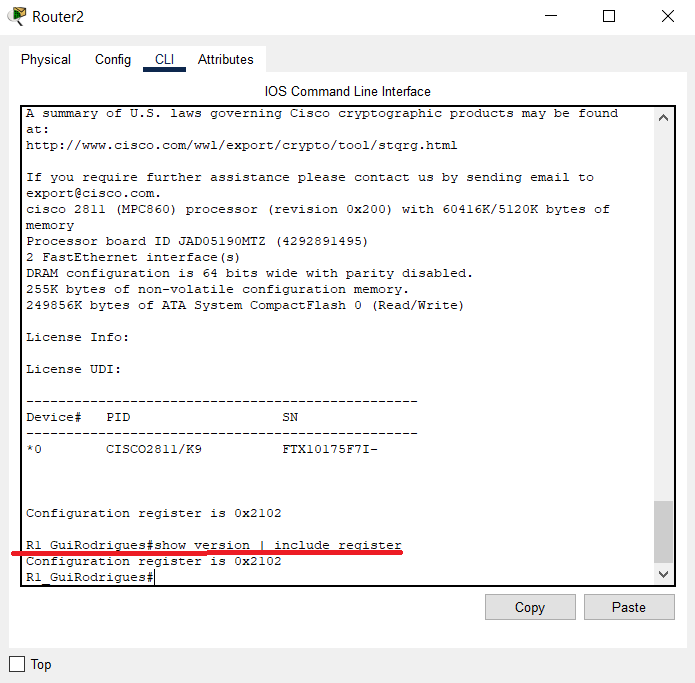


Ilustração : Filtragem do comando show version

Para mostrar a configuração de iniciação usamos o comando “**show start**”**.**



Ilustração : Comando show start

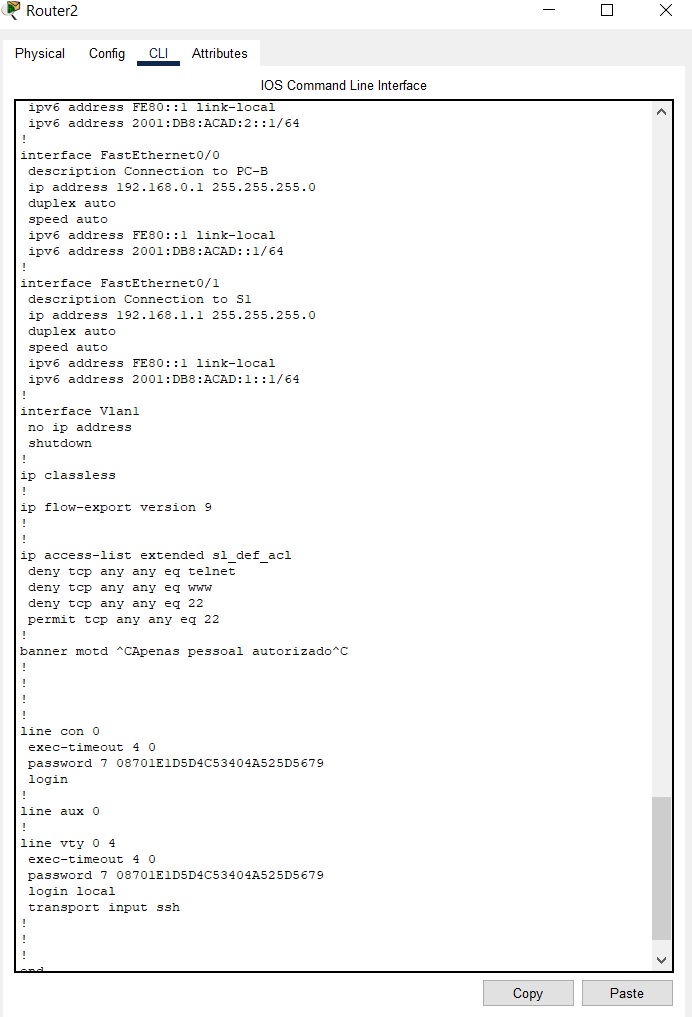


Ilustração : Comando show start parte 2

Para mostrar a tabela de routeamento usamos o comando “**show ip route”**.

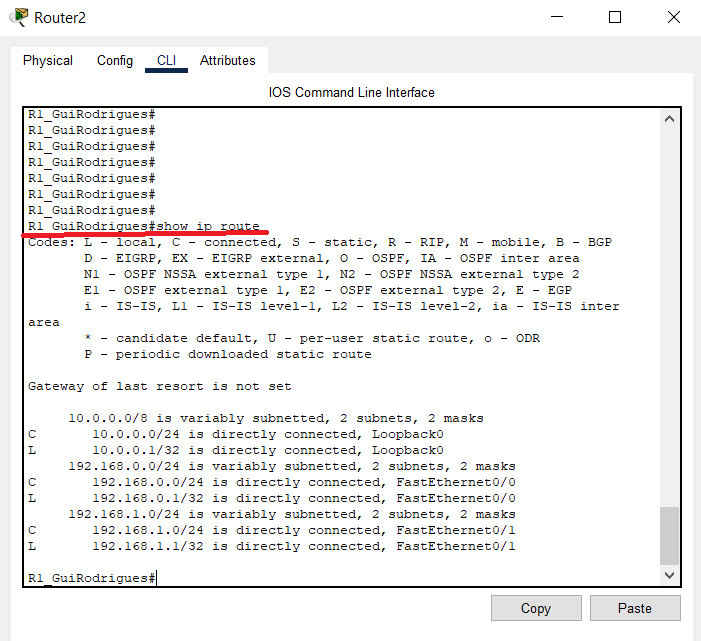


Ilustração : listagem da tabela de roteamento

Para ver a lista de interfaces no router usamos co comando “**show ip int brief**”.

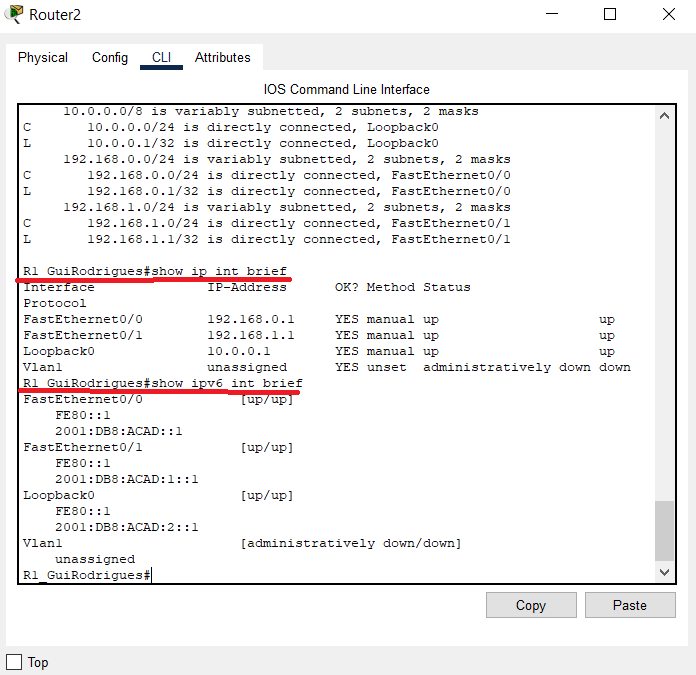


Ilustração : Show ip int brief

Por fim voltamos a reconfigurar o PC-B para possuir um endereço de IP estático e verificamos usando o comando “**ipconfig**”.

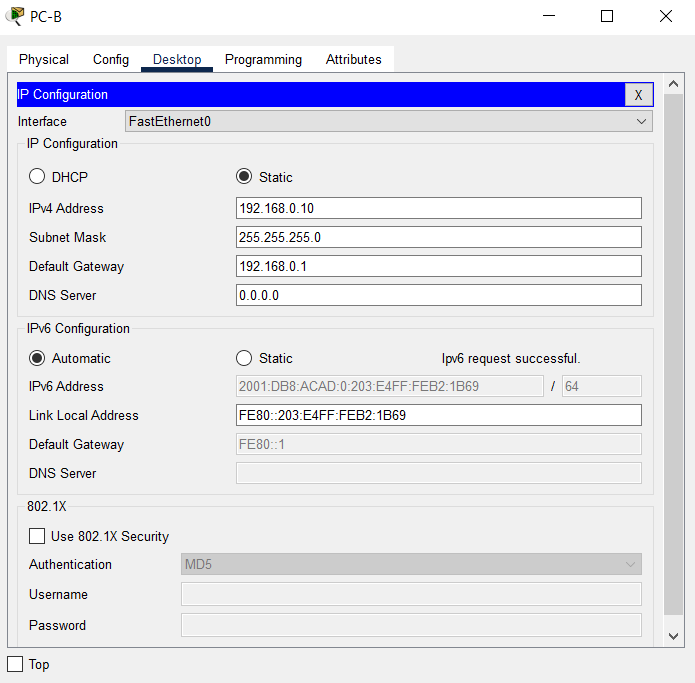


Ilustração : PC-B ip estatico

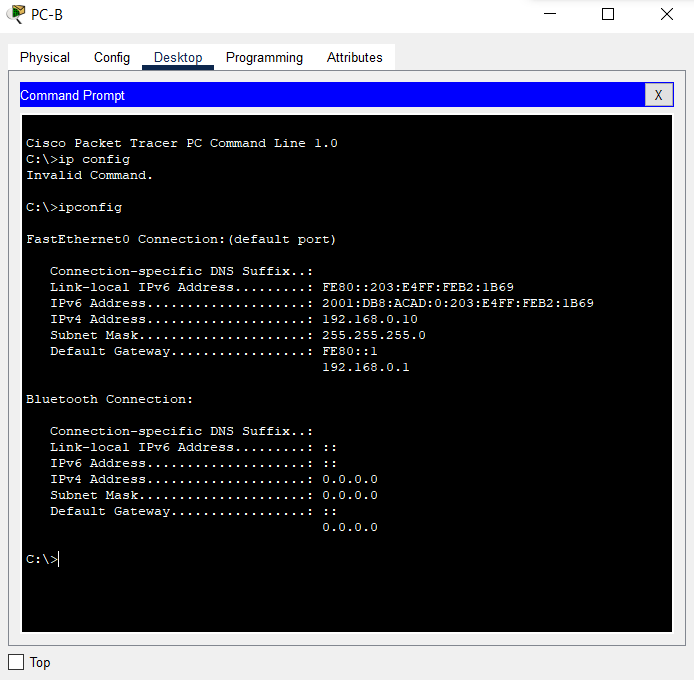


Ilustração : Confirmação da configuração

## 04.5.2 Lab - Implement Inter-VLAN Routing

**Objetivos**

* **Parte 1: Construir a Rede e Realizar Configurações Básicas dos Dispositivos.**
* **Parte 2: Criar VLANs e Atribuir Portas do Switch.**
* **Parte 3: Configurar um Trunk 802.1Q entre os Switches.**
* **Parte 4: Configurar Roteamento Inter-VLAN no Roteador.**
* **Parte 5: Verificar se o Roteamento Inter-VLAN Funciona.**

**Requisitos**

* **1 Router (Cisco 4221 com Cisco IOS XE Release 16.9.4 imagem universal ou equivalente)**
* **2 Switches (Cisco 2960 com Cisco IOS Release 15.2(2) imagem lanbasek9 ou equivalente)**
* **2 PCs (Windows com um programa de emulação de terminal, como o Tera Term)**
* **Cabos de consola para configurar os dispositivos Cisco IOS através das portas de consola**
* **Cabos Ethernet conforme mostrado na topologia**

**Parte 1**

Na primeira parte desta ficha iremos configurar a topologia da rede e definir as configurações básicas dos PCs e switches.

Sendo assim o esquema da rede é o seguinte.

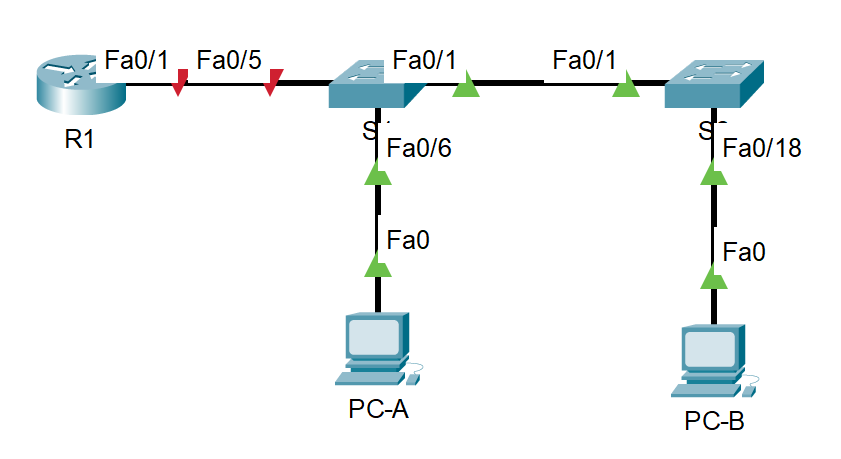


Ilustração : Esquema de rede da ficha 3

Foi realizado primeiramente a configuração router.

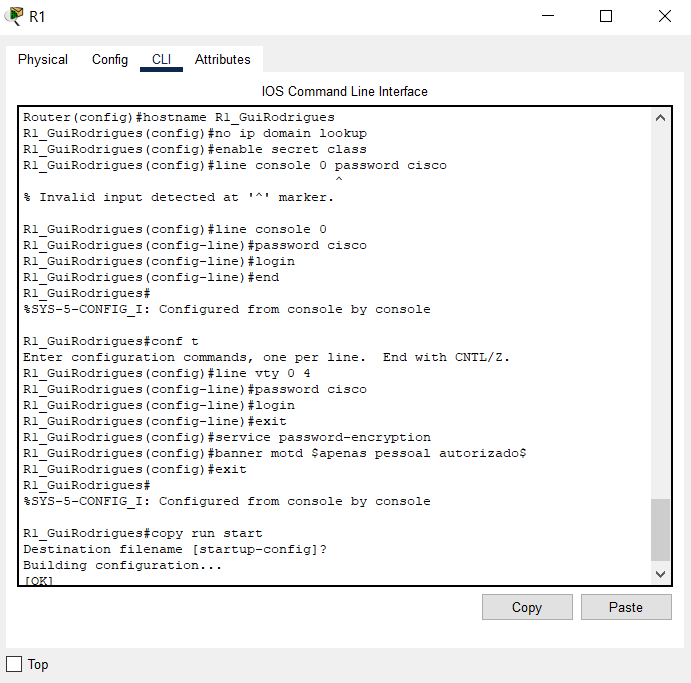


Ilustração : Configuração Basica do router

Nesta configuração foi desativada a pesquisa DNS para evitar traduções incorretas de comandos atribuída a password "**class**" como a senha de acesso privilegiado criptografada e “**cisco**” como a senha da console e do **VTY** e ativado o login. Por fim foi criado um **banner** que avisa que o acesso não autorizado é proibido e guardada a configuração em execução no arquivo de configuração inicial.

Seguidamente foram configurados os **switches** 1 e 2.

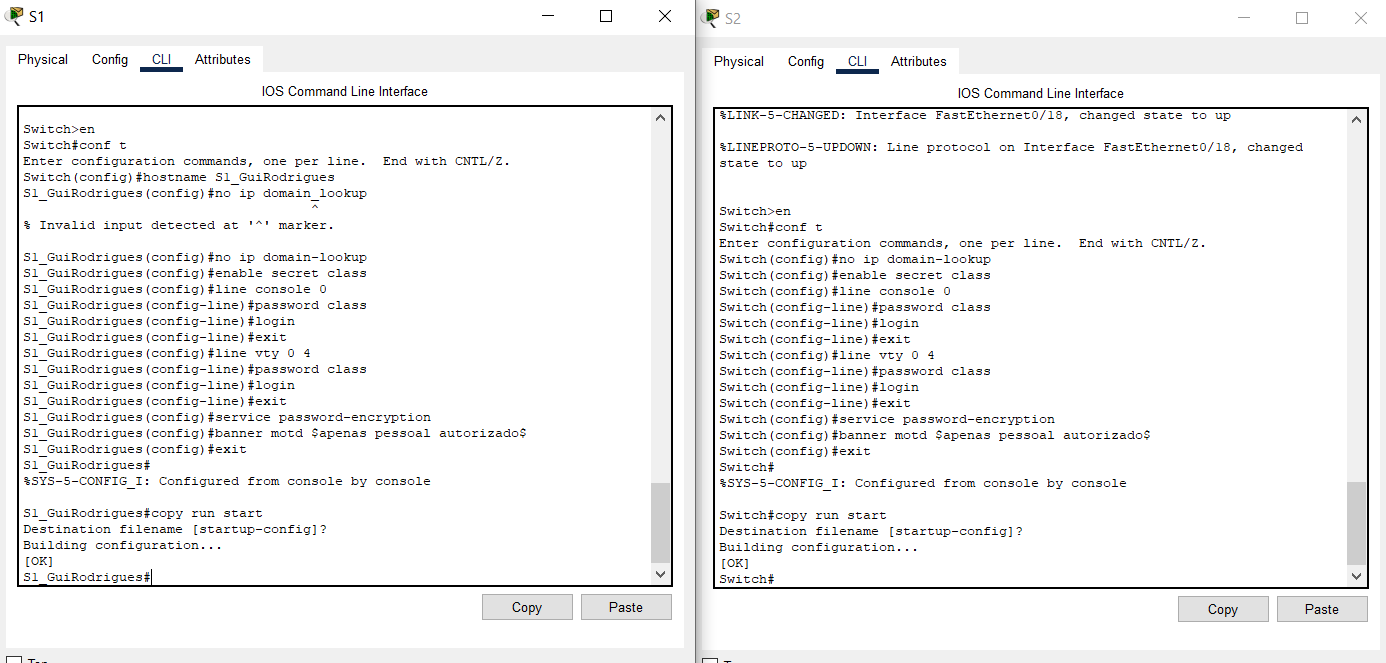


Ilustração : Configuração dos switches

A configuração dos switches é igual a configuração básica do router.

Por fim foi feita a configuração de ambos os PC’s

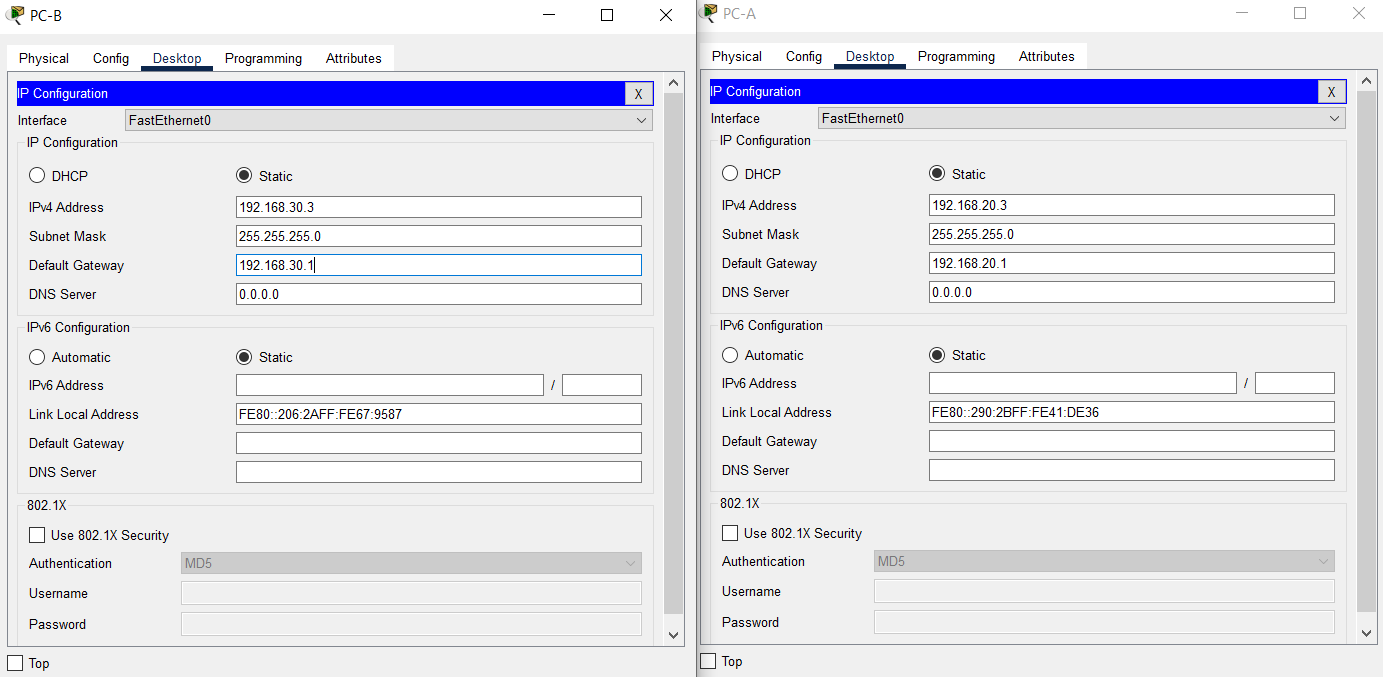


Ilustração : Configuração dos PC's

A seguinte configuração é a configuração e atribuição de nomes às **VLANs** necessárias em cada **switch**.

**Parte 2**

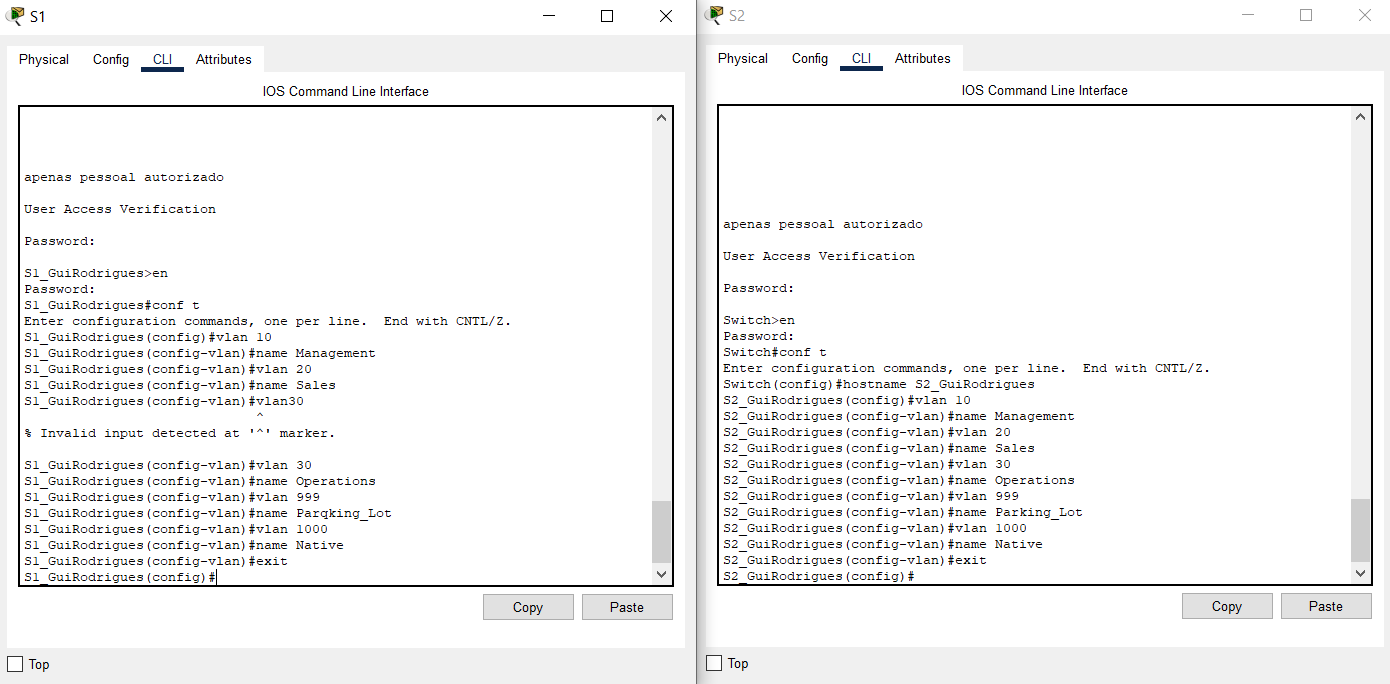


Ilustração : Criação das VLAN's S1

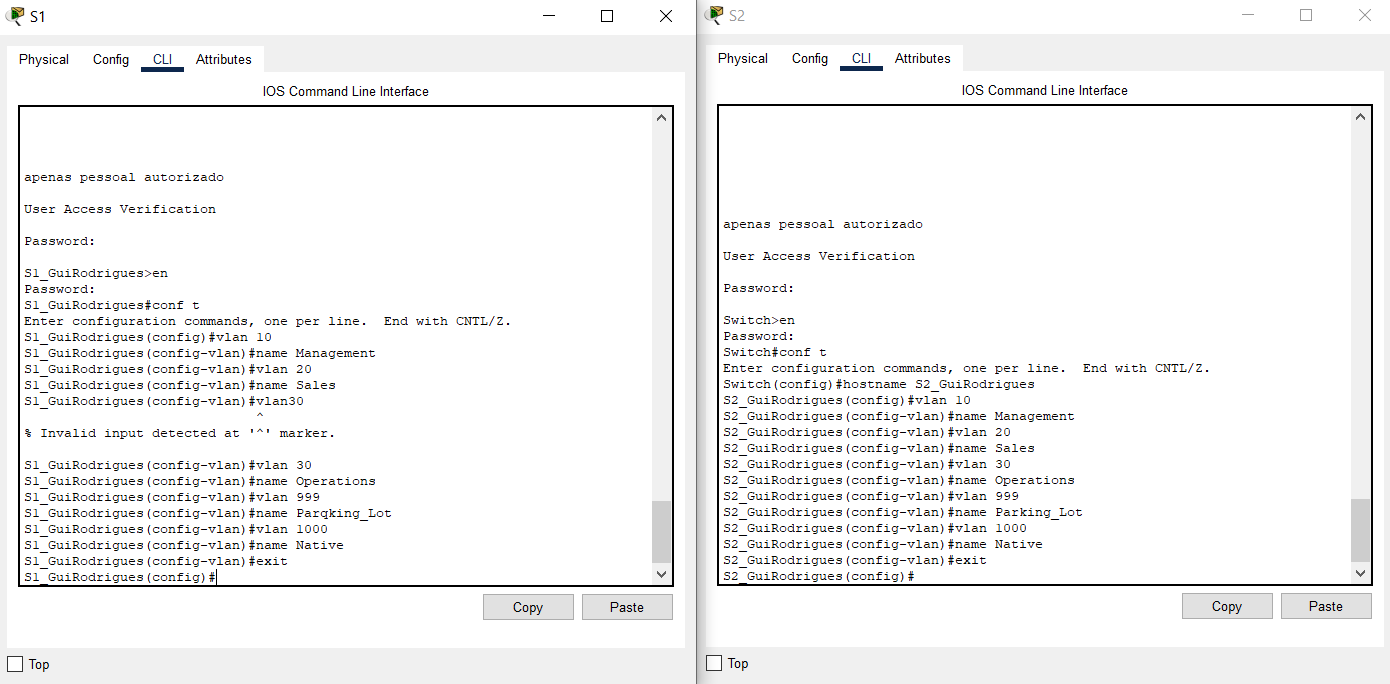


Ilustração : Criação das VLAN's S2

Foram então criadas as **VLAN’s** 10, 20, 30, 999 e 1000 com os nomes “**Management”, “sales”, “Operations”, “Parking\_Lot”** e **“Native**” respetivamente.

Depois foi realizada a configuração da interface de gestão e o “**gateway”** padrão em cada **switch** usando as informações de endereço de IP da Tabela de Endereçamento.

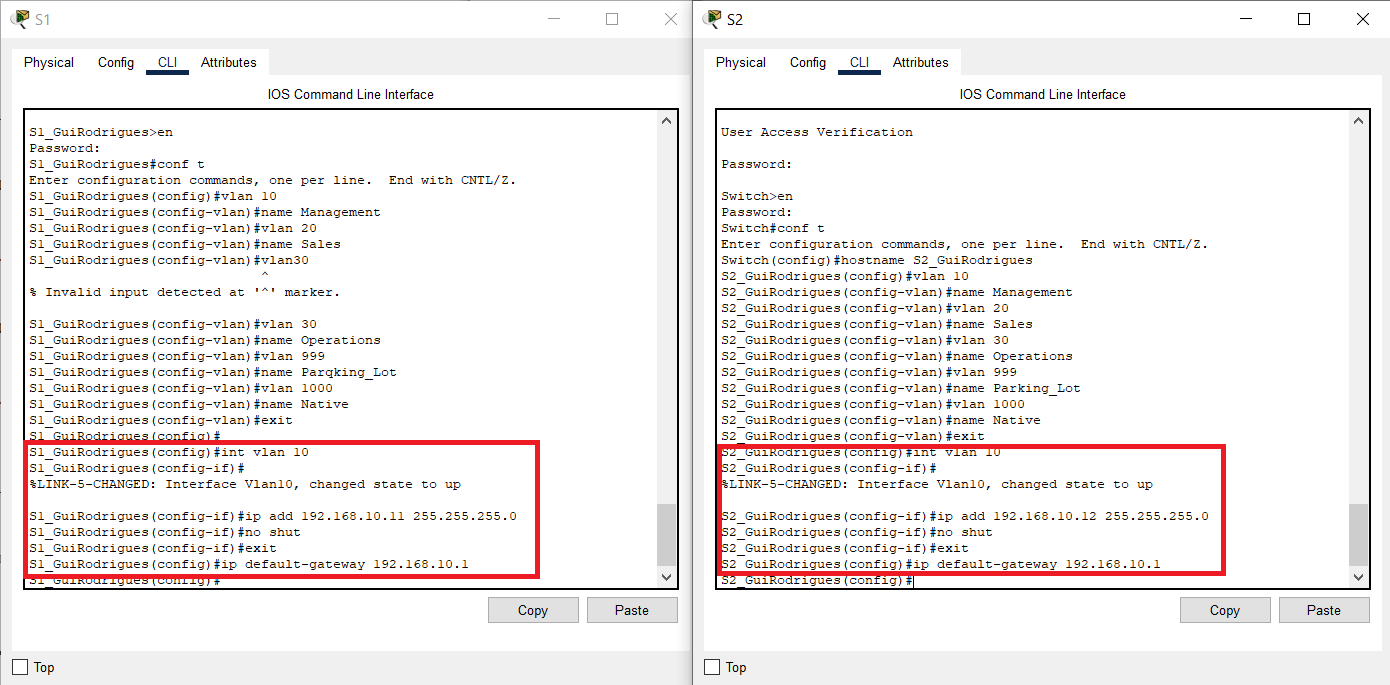


Ilustração : Configuração do Gateway S1

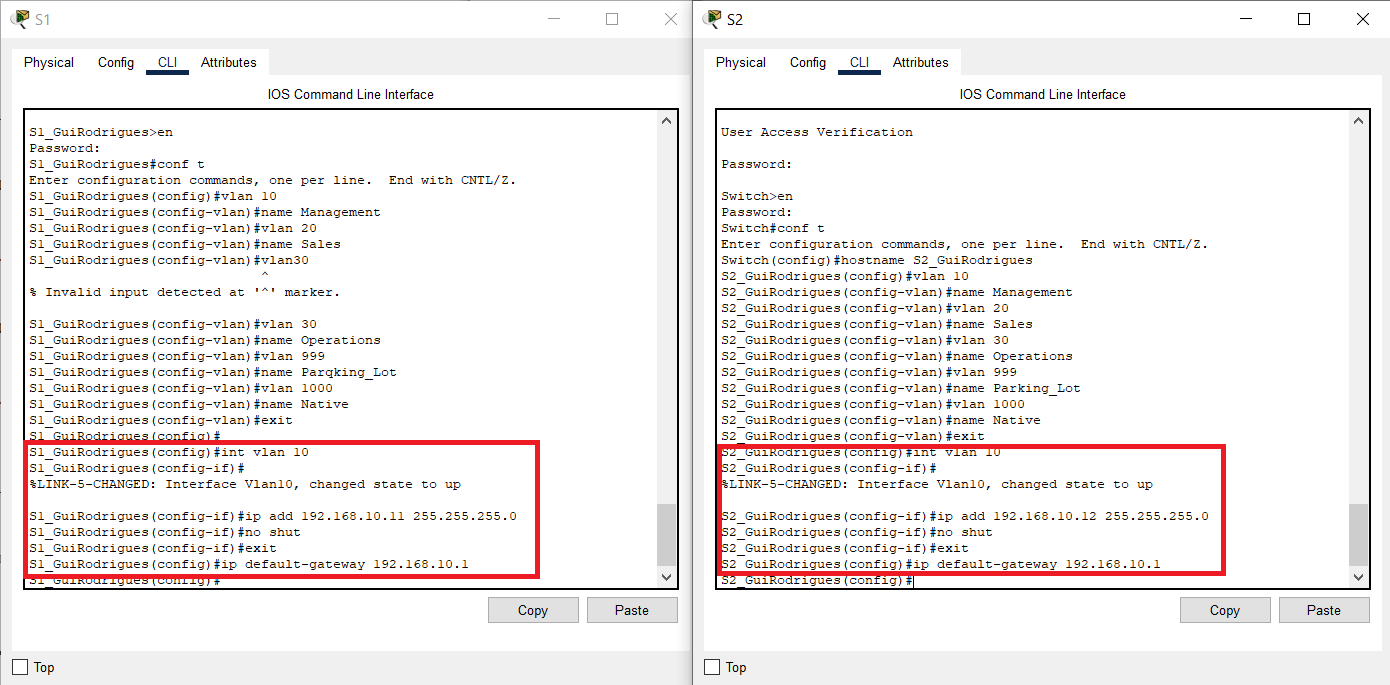


Ilustração : Configuração do Gateway S2

Por fim a todas as portas não utilizadas no switch foram atribuidas à **VLAN** “**Parking**\_**Lot**”, foram configuradas para o modo de acesso estático e desativadas administrativamente.

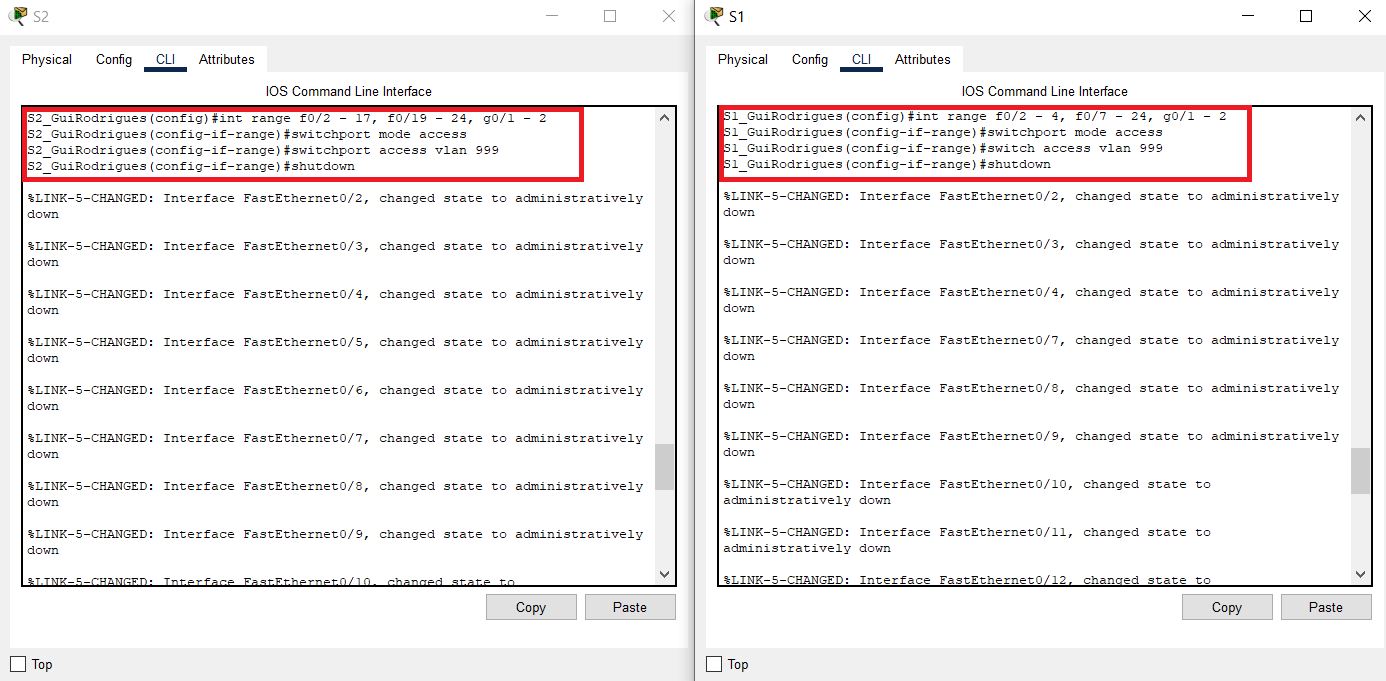


Ilustração : Configuração das portas nao utilizadas

Em seguida foi feito o processo contrário atribuindo as portas usadas á **VLAN 20** e **VLAN 30** no switch 1 e switch 2 respetivamente.

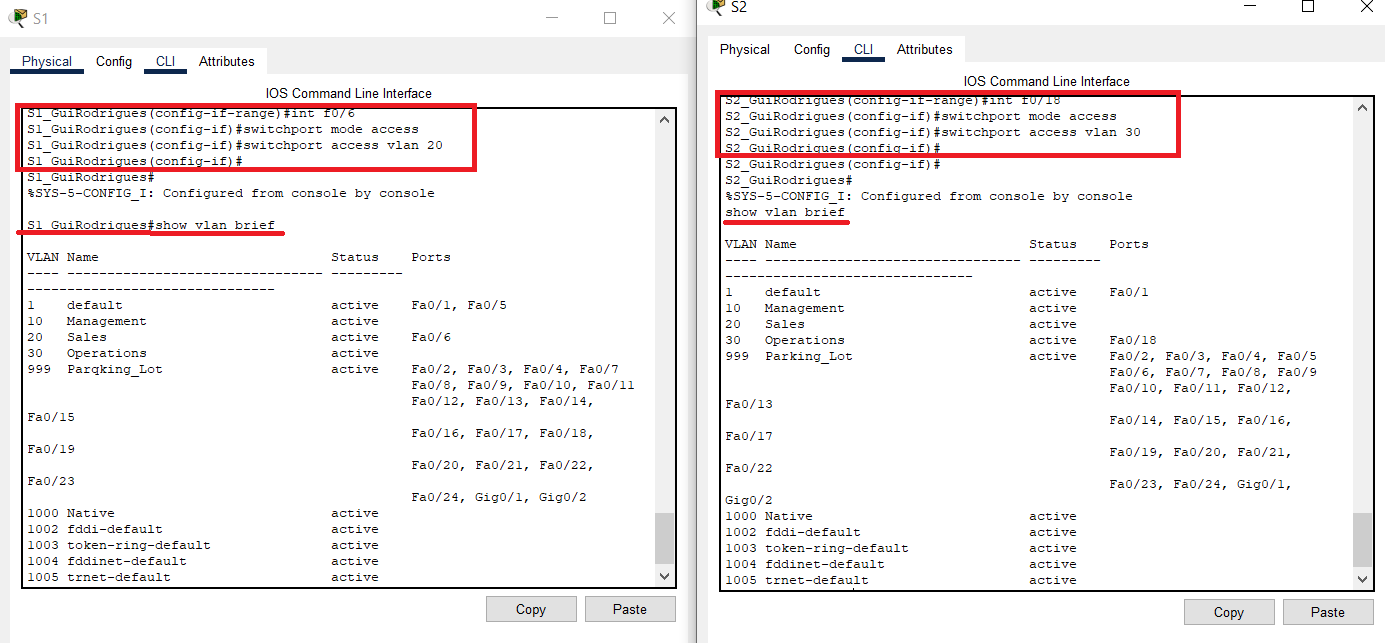


Ilustração : Atribuição a Vlan 20

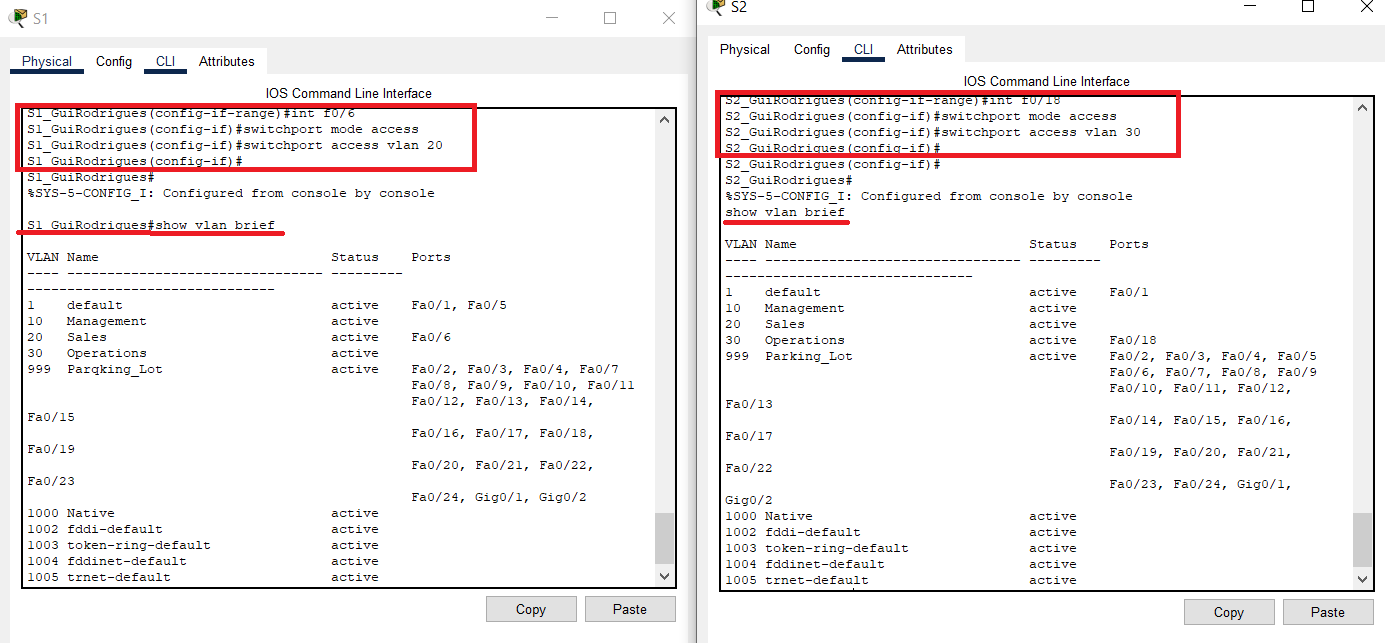


Ilustração : Atribuição a Vlan 30

**Parte 3**

Na Parte 3, ireos configurar manualmente a interface F0/1 como um “**trunk”** em ambos os switches**.**

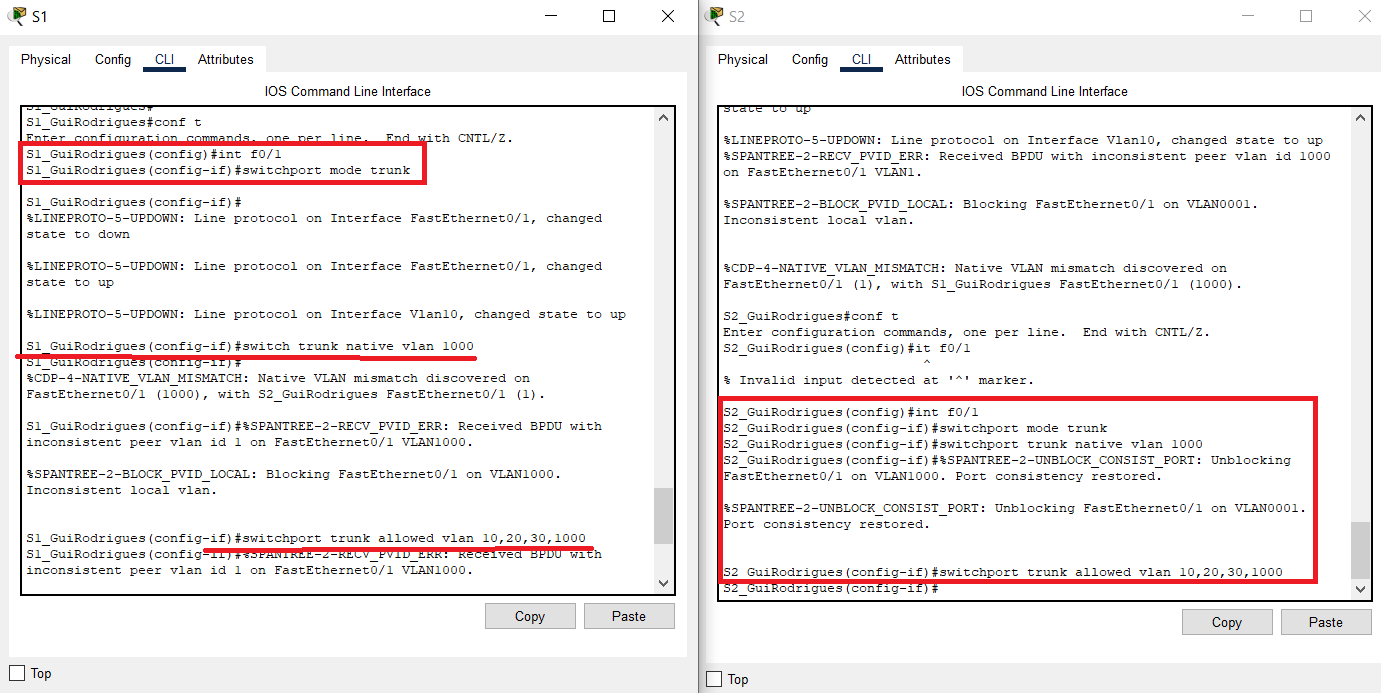


Ilustração : Trunk no switch 1

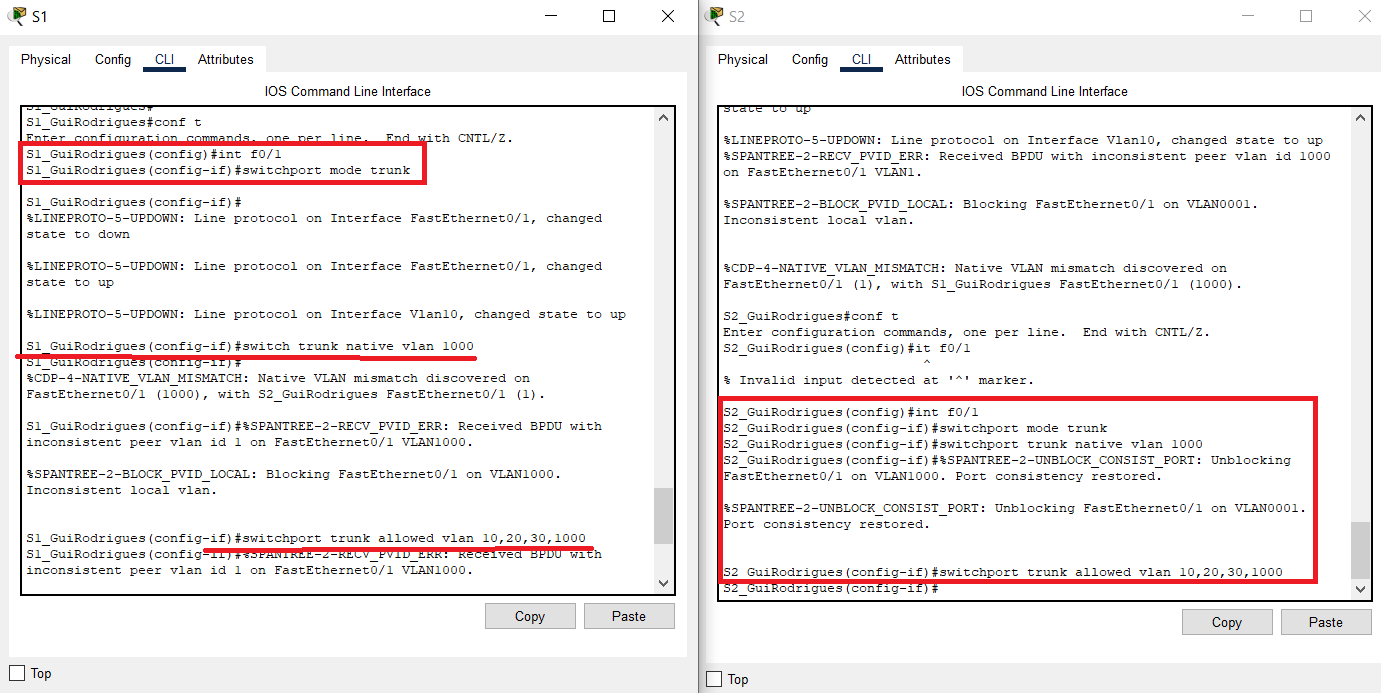


Ilustração : Trunk no switch 2

Em seguida foi feita a confirmação da confirmação.

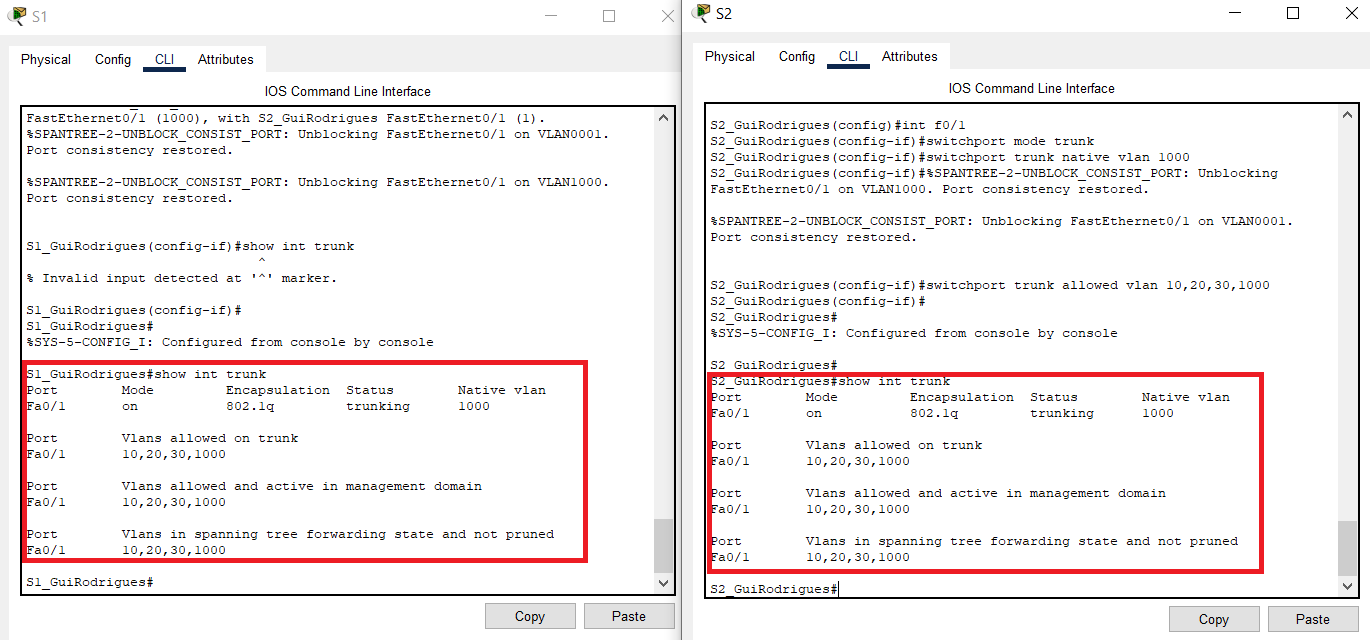


Ilustração : Confirmação da configuração

Em seguida foi feita a ativação da porta Fa0/1 no router.

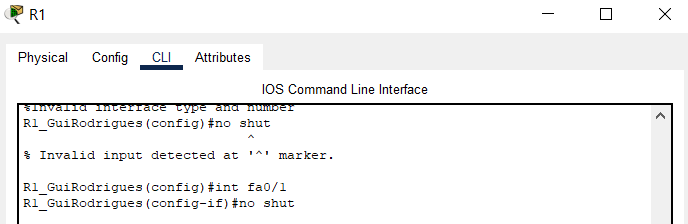


Ilustração : Ativação da porta Fa0/1

Ainda no router foram configuradas as subinterfaces para cada VLAN conforme especificado na tabela de endereçamento IP. Todas essas subinterfaces usam Encapsulamento 802.1Q.

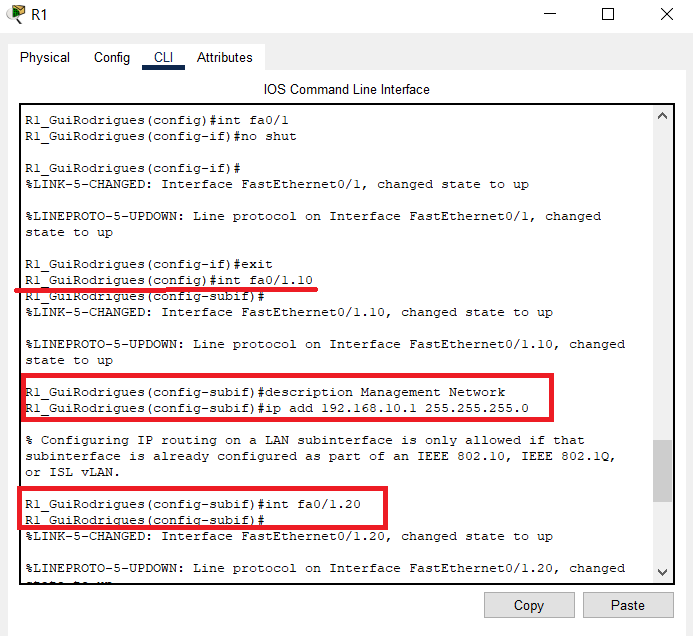


Ilustração : Primeira parte da configuração

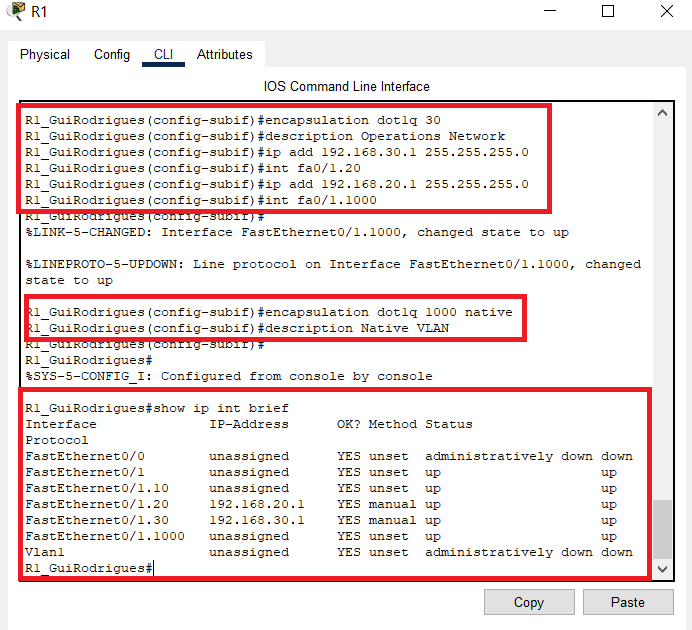


Ilustração : segunda parte da configuração e confirmação da mesma

Por fim testamos a conectividade da rede pingando a partir do PC-A, o “**default gateway”,** o PC-B e o switch 2.

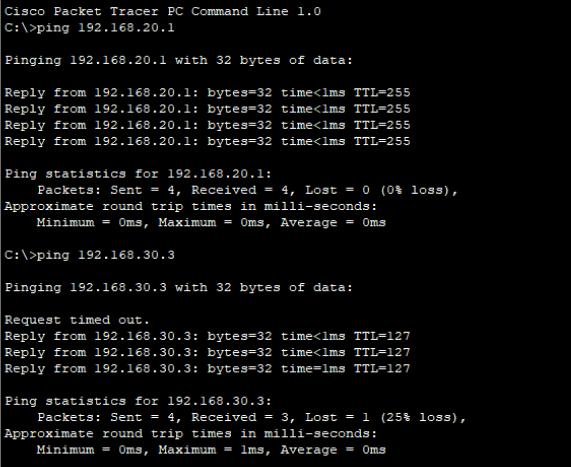


Ilustração : Confirmação da conectividade

## 06.4.2 Lab - Implement Etherchannel

**Objetivos**

* **Parte 1: Construir a rede e configurar as definições básicas do dispositivo**
* **Parte 2: Criar VLANs e atribuir portas de switch**
* **Parte 3: Configurar troncos 802.1Q entre os switches**
* **Parte 4: Implementar e verificar um EtherChannel entre os switches**

**Requisitos**

* **2 Switches (Cisco 2960 com imagem Cisco IOS Release 15.2(2) lanbasek9 ou comparável)**
* **2 PCs (Windows com um programa de emulação de terminal, como Tera Term)**
* **Cabos de consola para configurar os dispositivos Cisco IOS através das portas de consola**
* **Cabos Ethernet conforme mostrado na topologia**

**Parte 1**

Primeira parte iremos realizar o esquema de rede e configurar cada switch.

Assim sendo o esquema de rede é o seguinte:

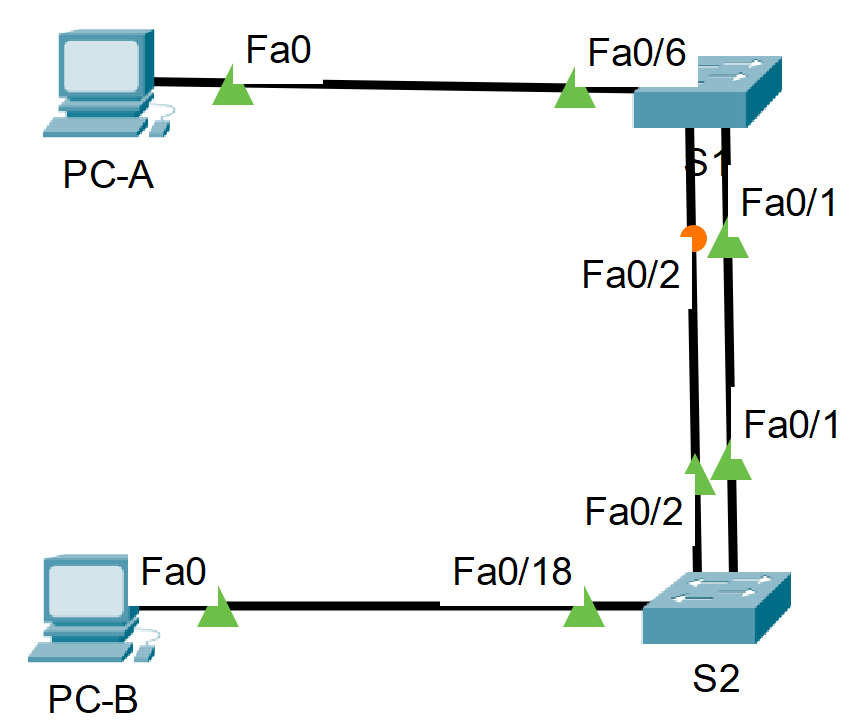


Ilustração : Esquema de rede

Em seguida segue a configuração dos switches. A configuração foi a mesma para ambos o switches.

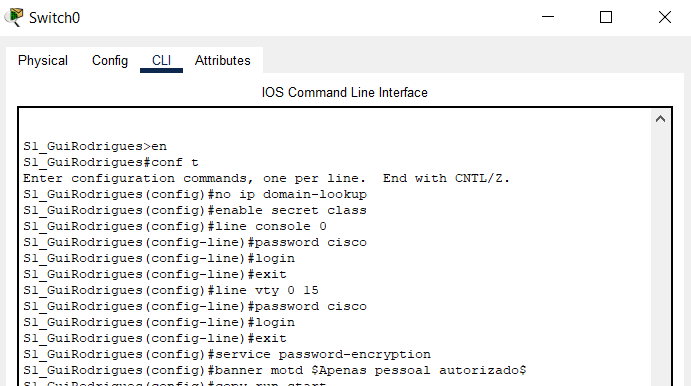


Ilustração : Configuração dos switches

Para os **switches** foram atribuídos um nome de dispositivo, desativada a pesquisa **DNS**, atribuída uma senha criptografada **EXEC** privilegiada e uma senha de consola e realizada a ativação o **login**, o mesmo foi feito para o **VTY**, as senhas foram criptografadas e um **banner** que avisa sobre acesso não autorizado foi criado, por fim a configuração em execução foi guardada no arquivo de configuração de inicialização.

O PC’s foram configurado em seguida:

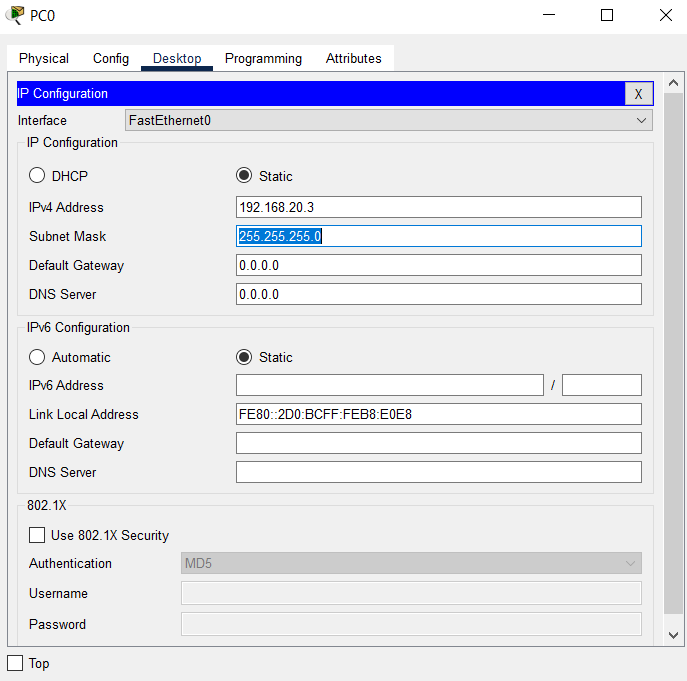


Ilustração : Configuração do PC-A

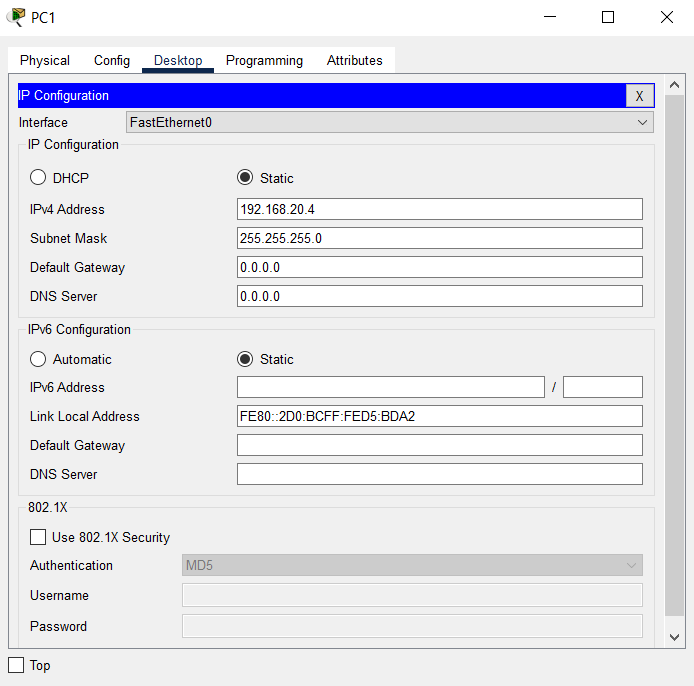


Ilustração : Configuração do PC-B

**Parte 2**

Na segunda parte foram criadas a **VLAN’s** e atribuídas as respetivas portas dos switches.

As **VLAN’s** criadas foram as seguintes 10, 20, 999, 1000 com os respetivos nomes **“Managements”, “Clients”, “Parking\_Lot”** e **“Native**”.

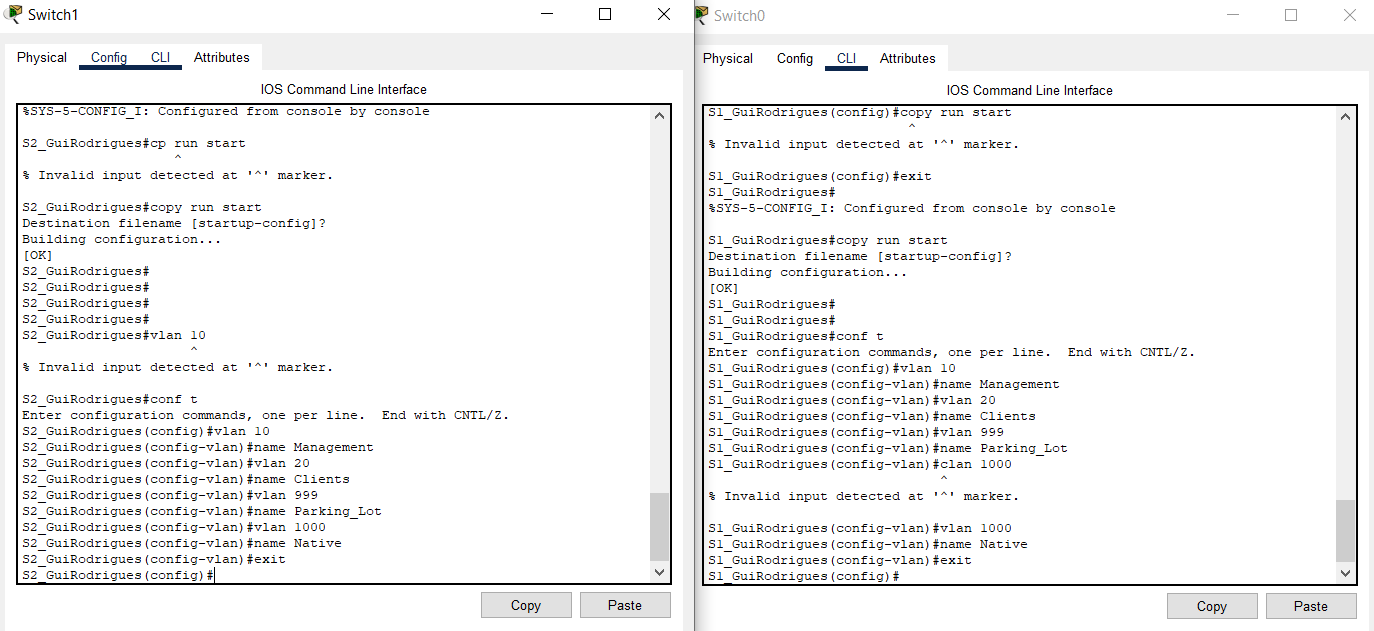


Ilustração : Criação das VLAN's

A mesma configuração repete-se para o **switch** 2.

Em seguida foi atribuído o endereço de IPv4 a **VLAN 10.** No **switch** 1 o ip atribuído foi “**192.168.10.11”**  e no **switch 2** foi ” **192.168.10.12**”.

Foram atribuídas todas as portas não utilizadas no **switch** à **VLAN** **Parking\_Lot**, mudadas para o modo de acesso estático e desativadas administrativamente.

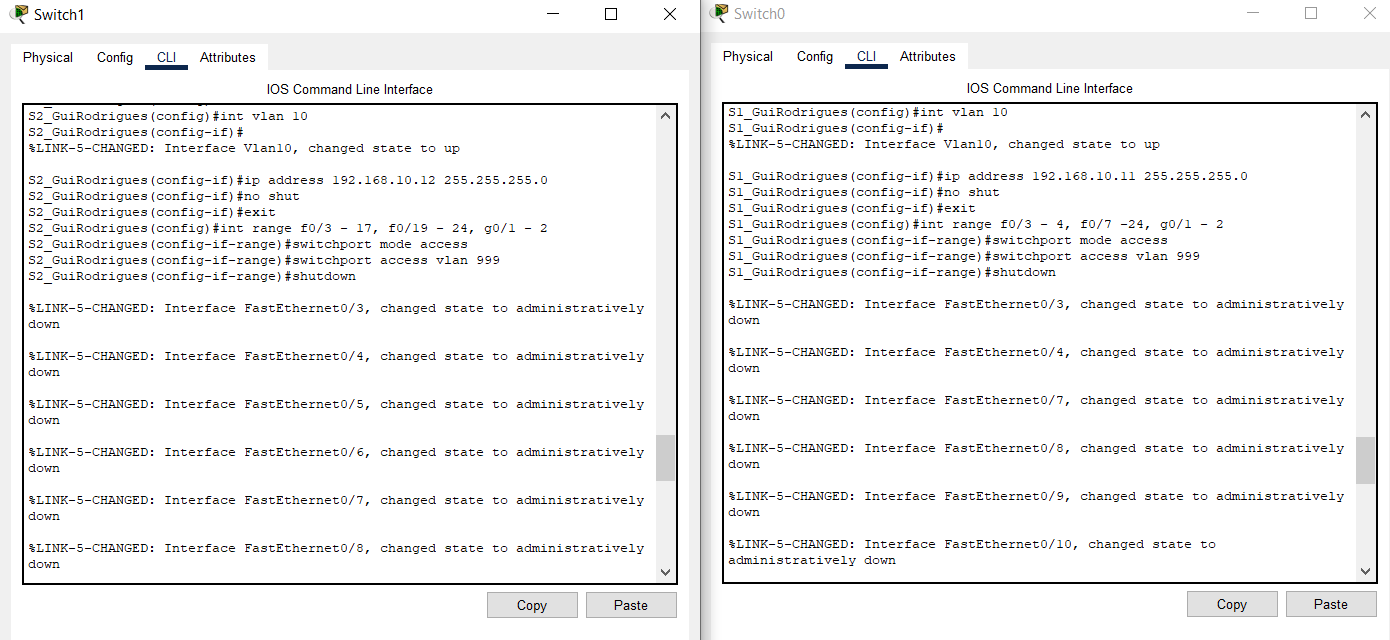


Ilustração : Configurações da Vlan 10 no swich 1

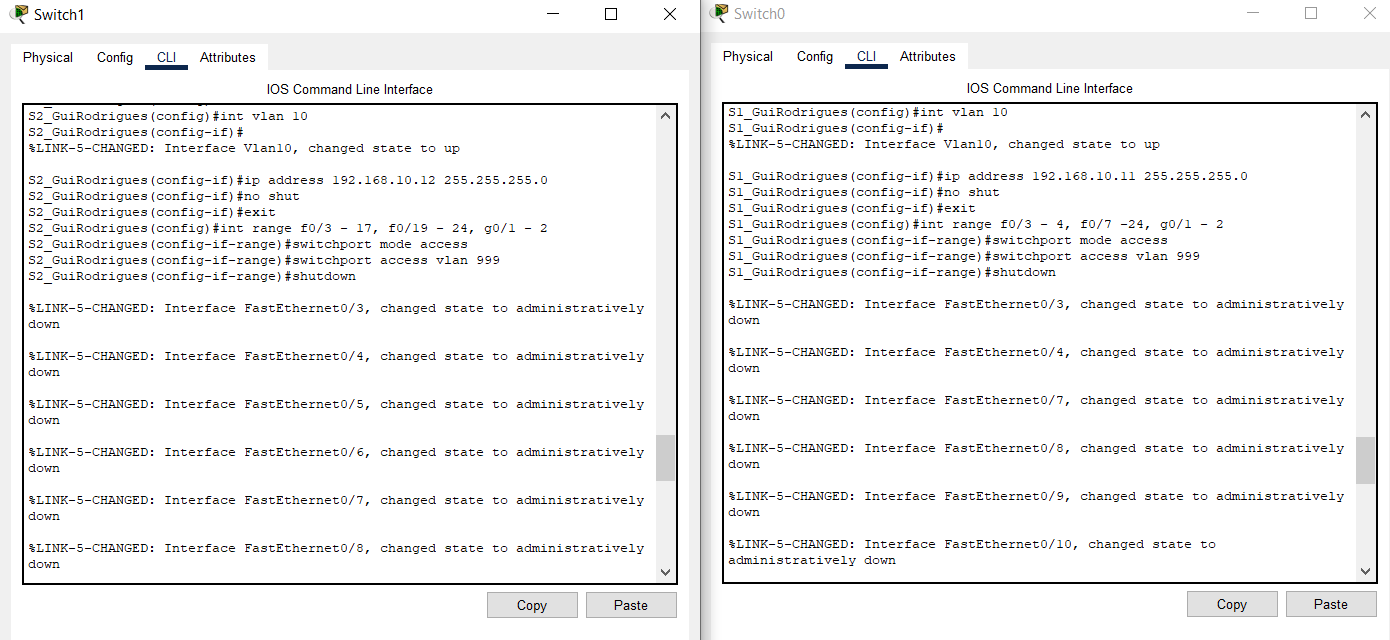


Ilustração : Configurações da Vlan 10 no swich 2

No passo seguinte portas usadas à VLAN apropriada foram atribuídas e configuradas para modo de acesso estático.

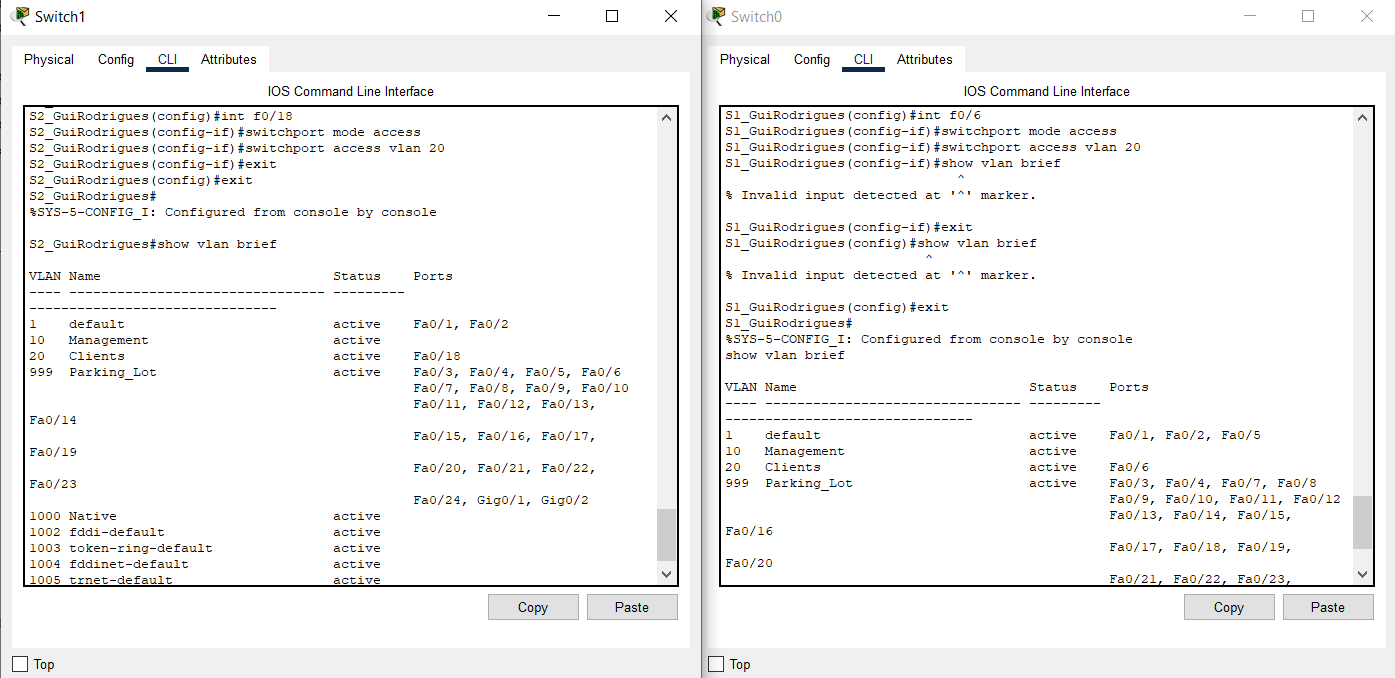


Ilustração : Associoação a vlan 20 switch 2

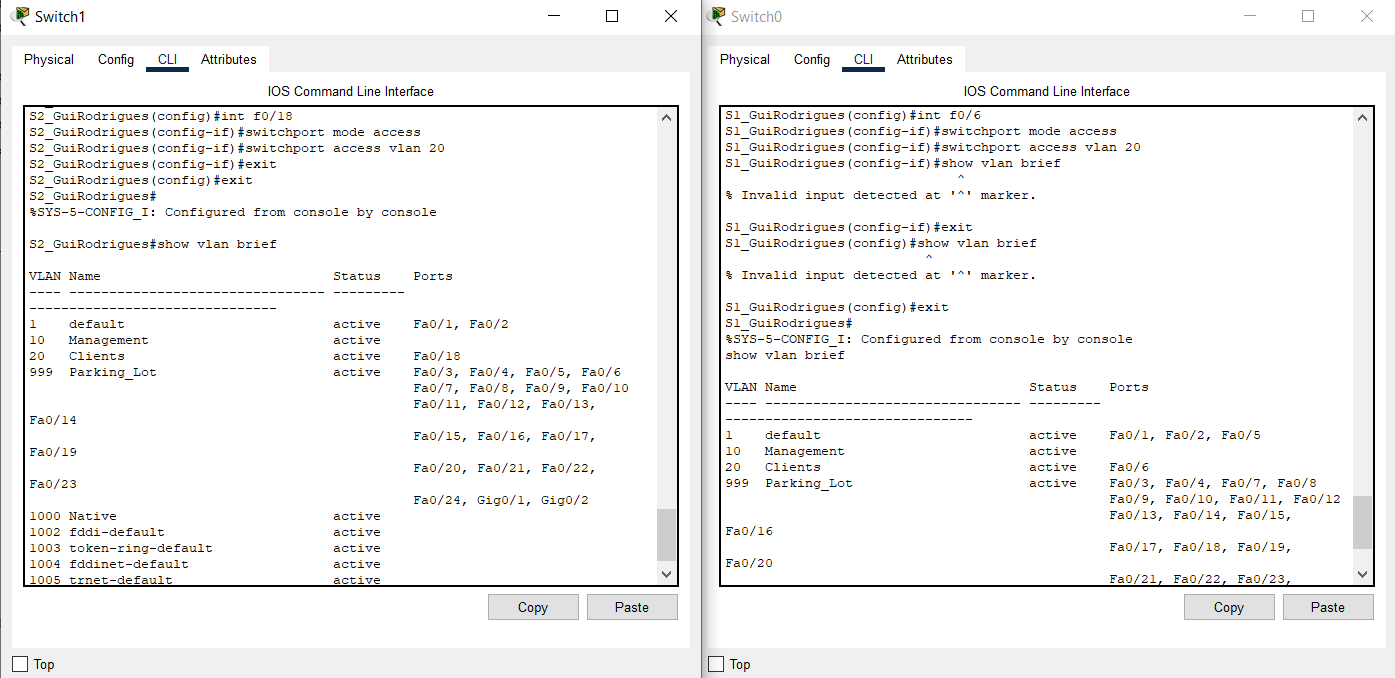


Ilustração : Associoação a vlan 20 switch 2

**Parte 3**

Na Parte 3, configuraremos manualmente as interfaces F0/1 e F0/2 como “**trunk”** 802.1Q.

Primeiro alteramos o modo **switchport** nas interfaces para forçar o entroncamento.

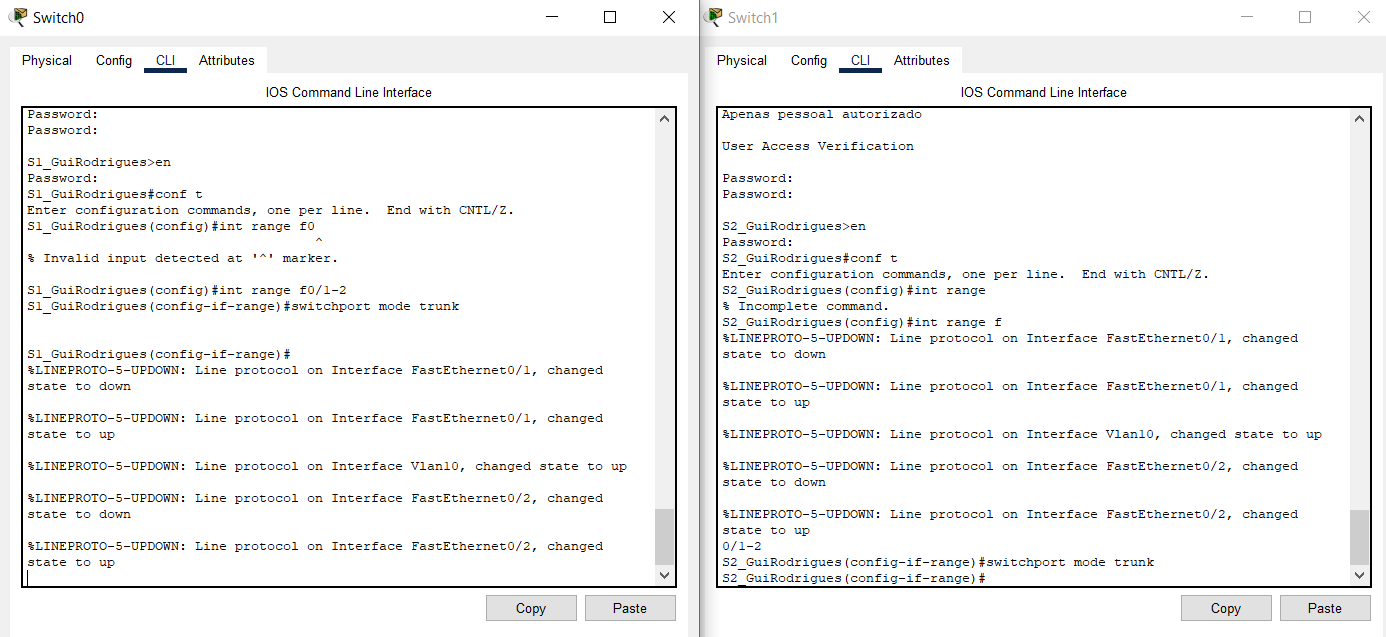


Ilustração : Modo forçamento trunk no switch 1

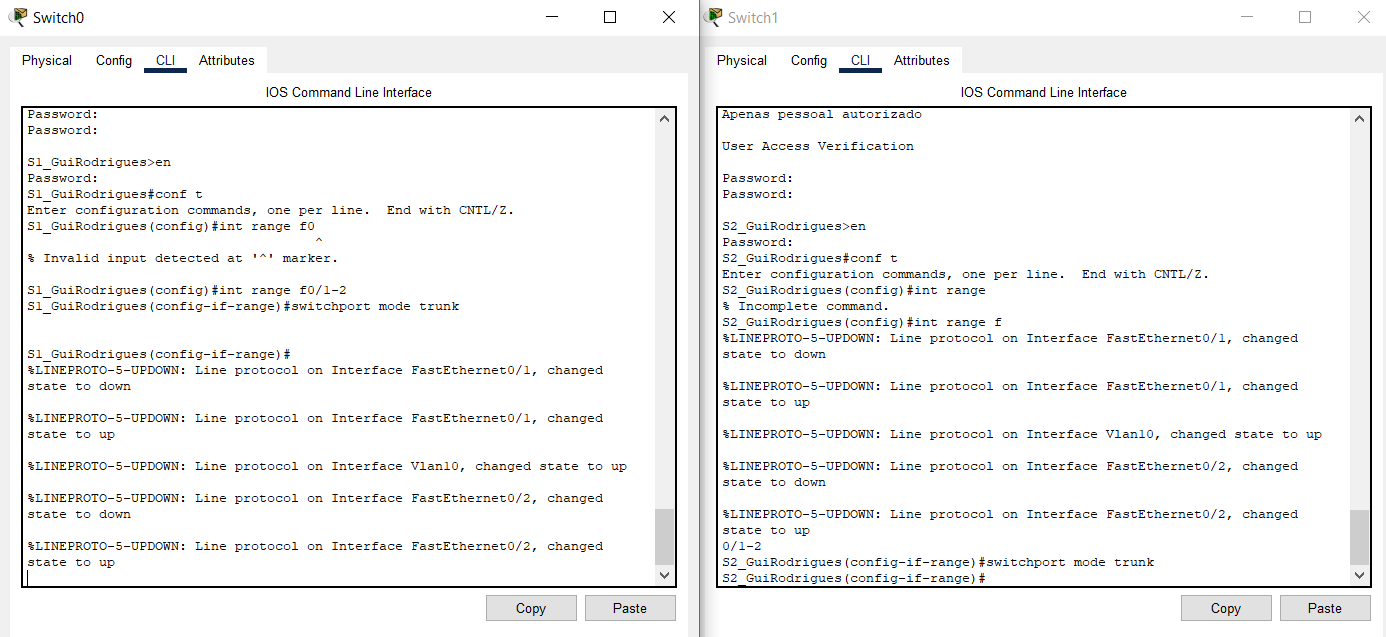


Ilustração : Modo forçamento trunk no switch 2

Em seguida iremos definir a **VLAN** 1000 como “**Native**” em ambos o **switches** e definir as **VLAN’s** permitidas.

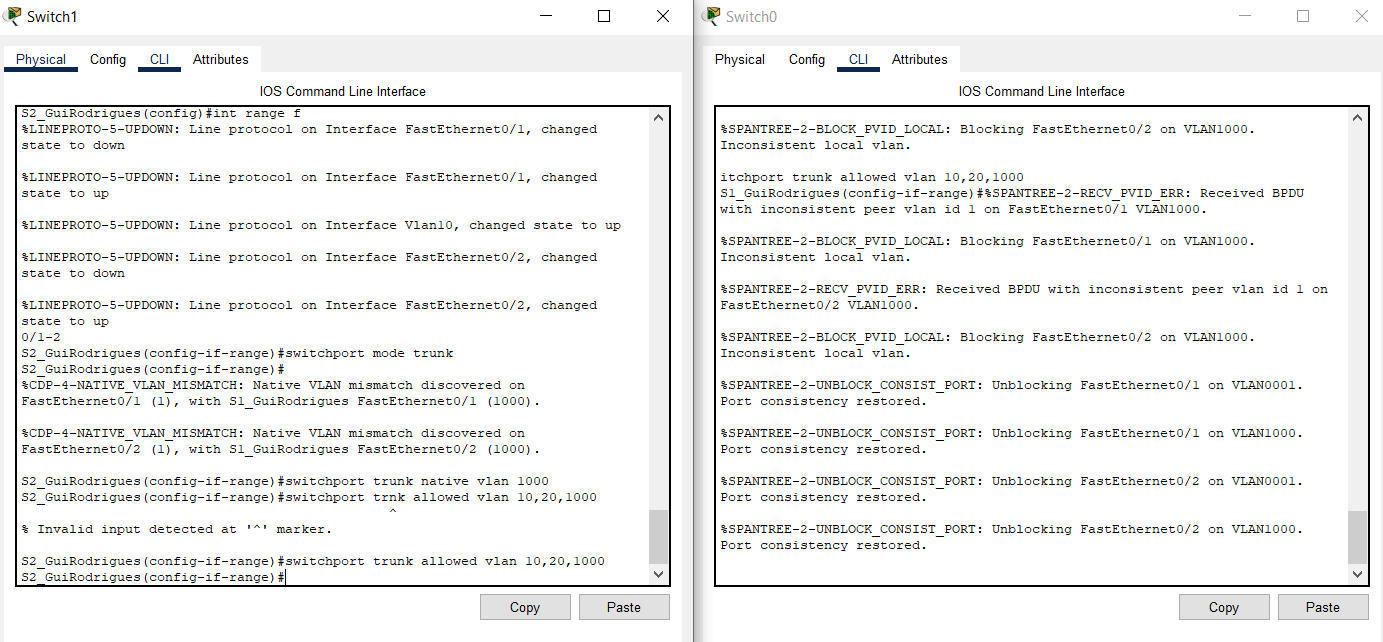


Ilustração : Definição da trunk nativa e das vlan permitidas S2

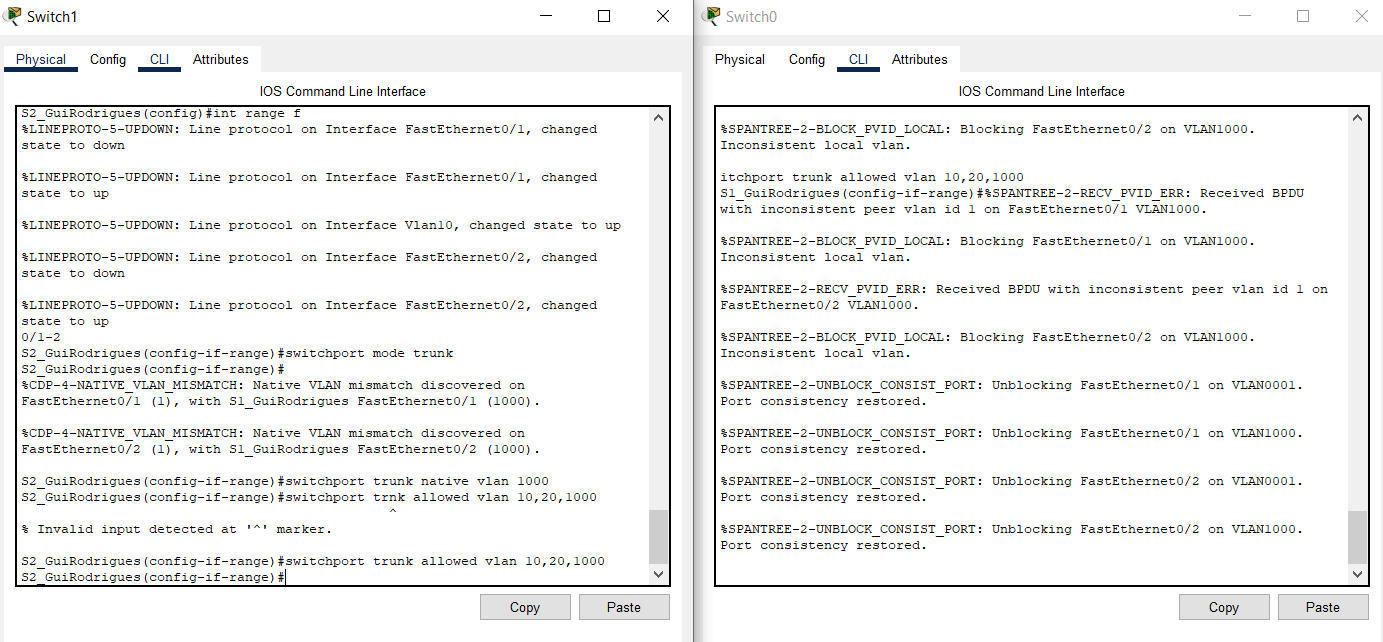


Ilustração :Definição da trunk nativa e das vlan permitidas S1

Depois fazemos a verificação da configuração.

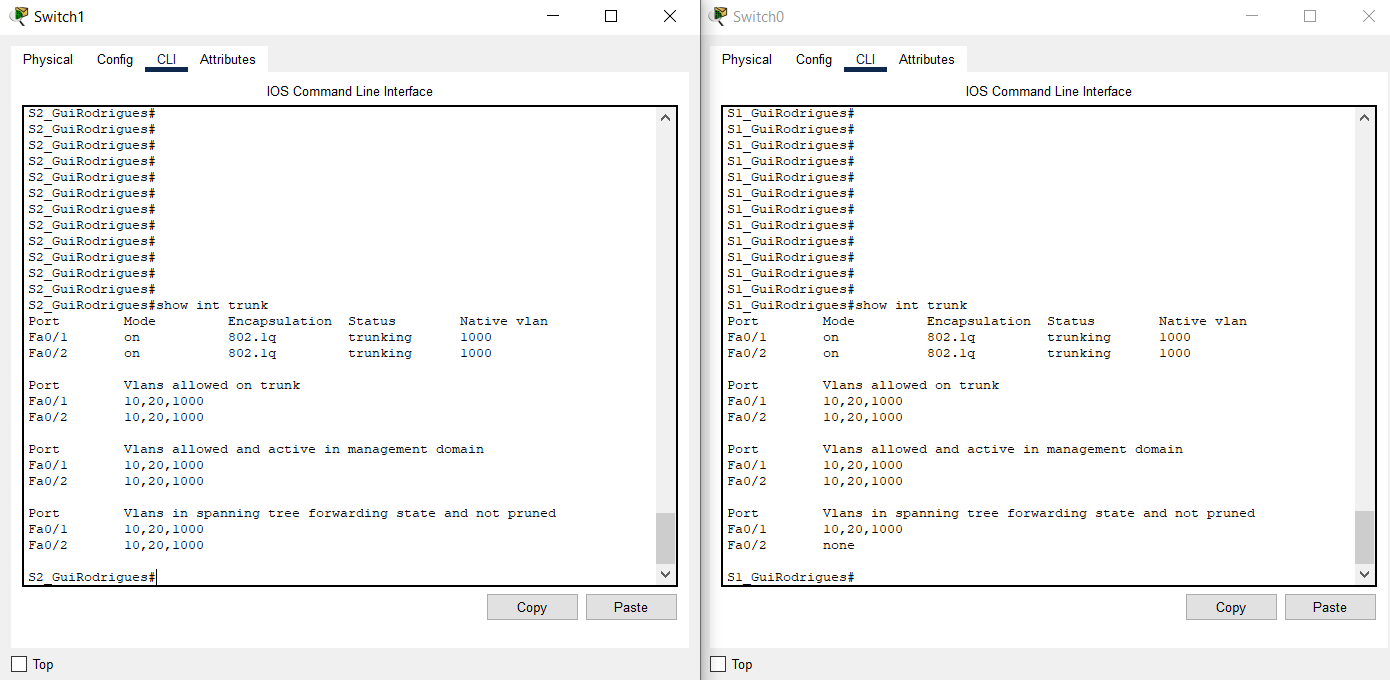


Ilustração : Confrimação da configuração

**Parte 4**

Na última parte vamos criar um **EtherChannel** baseado em **LACP** usando **F0/1** e **F0/2** usando o grupo número 1, com ambos os switches negociando ativamente o protocolo **EtherChannel**.

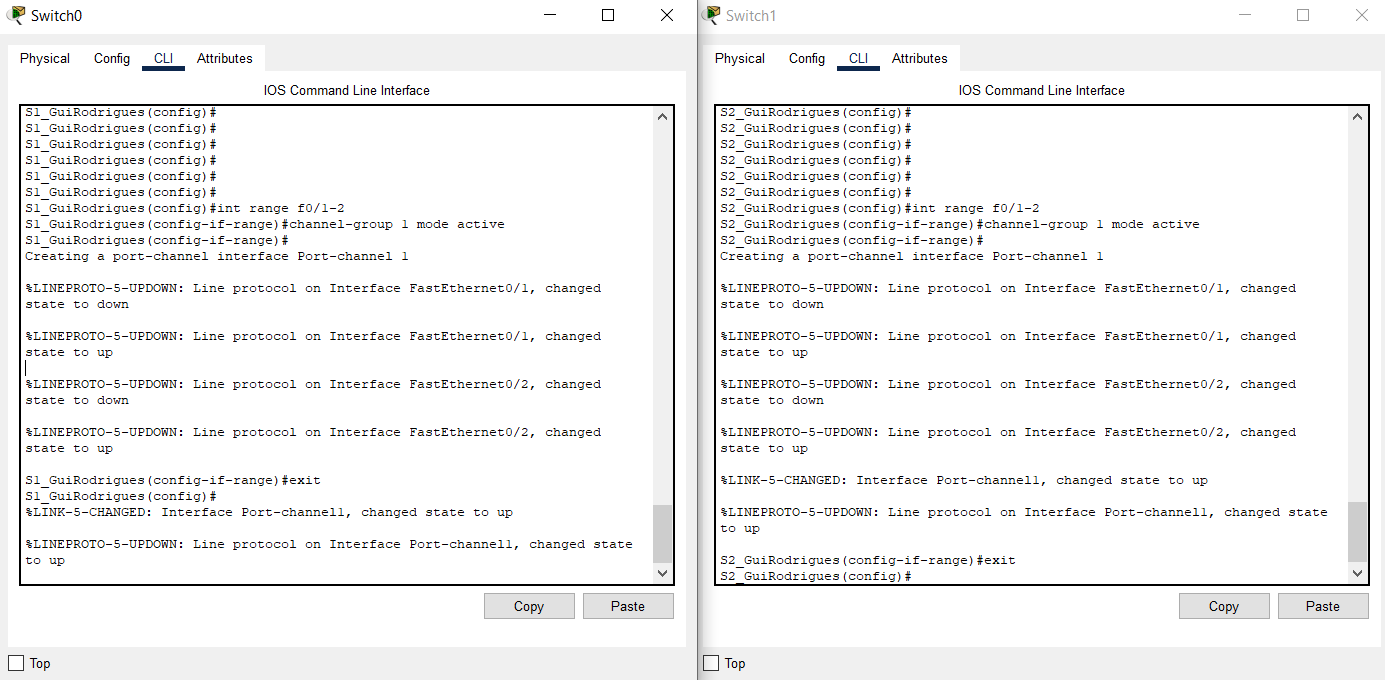


Ilustração : Criação do EtherChannel S1

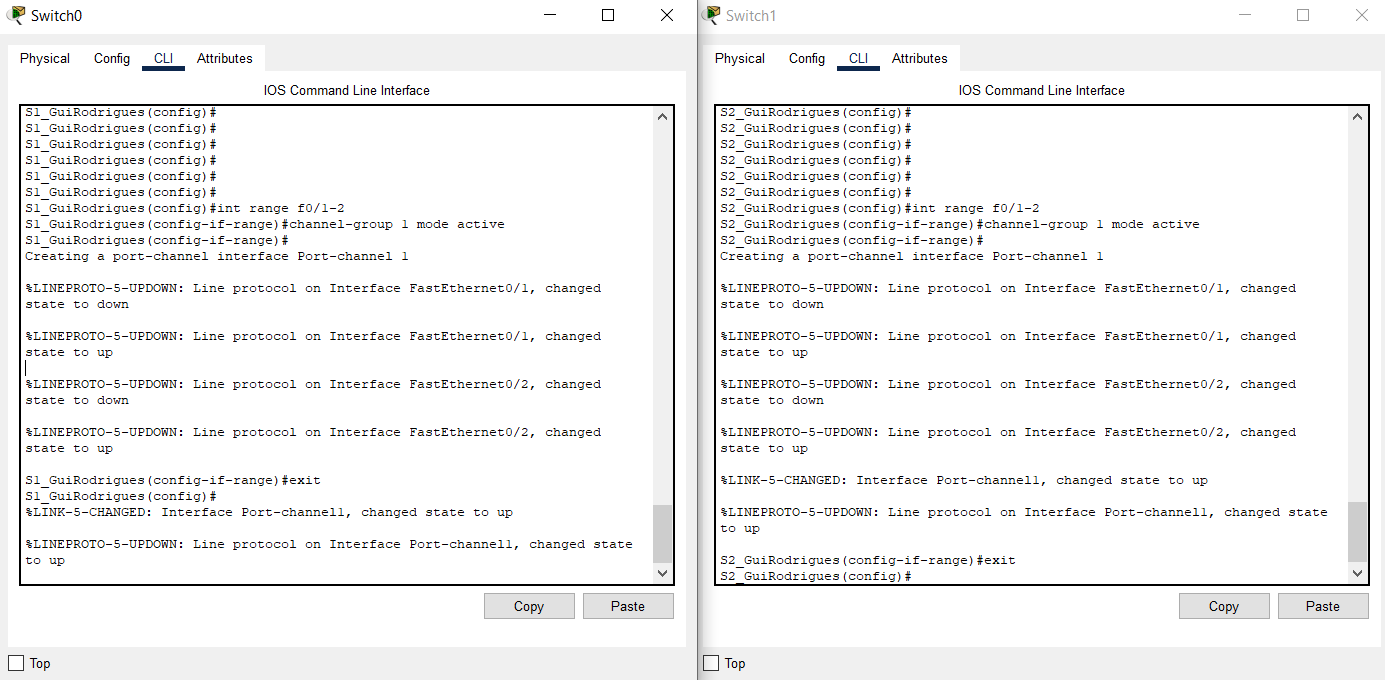


Ilustração : Criação do EtherChannel S2

Podemos em seguida verificar a configuração realizada.

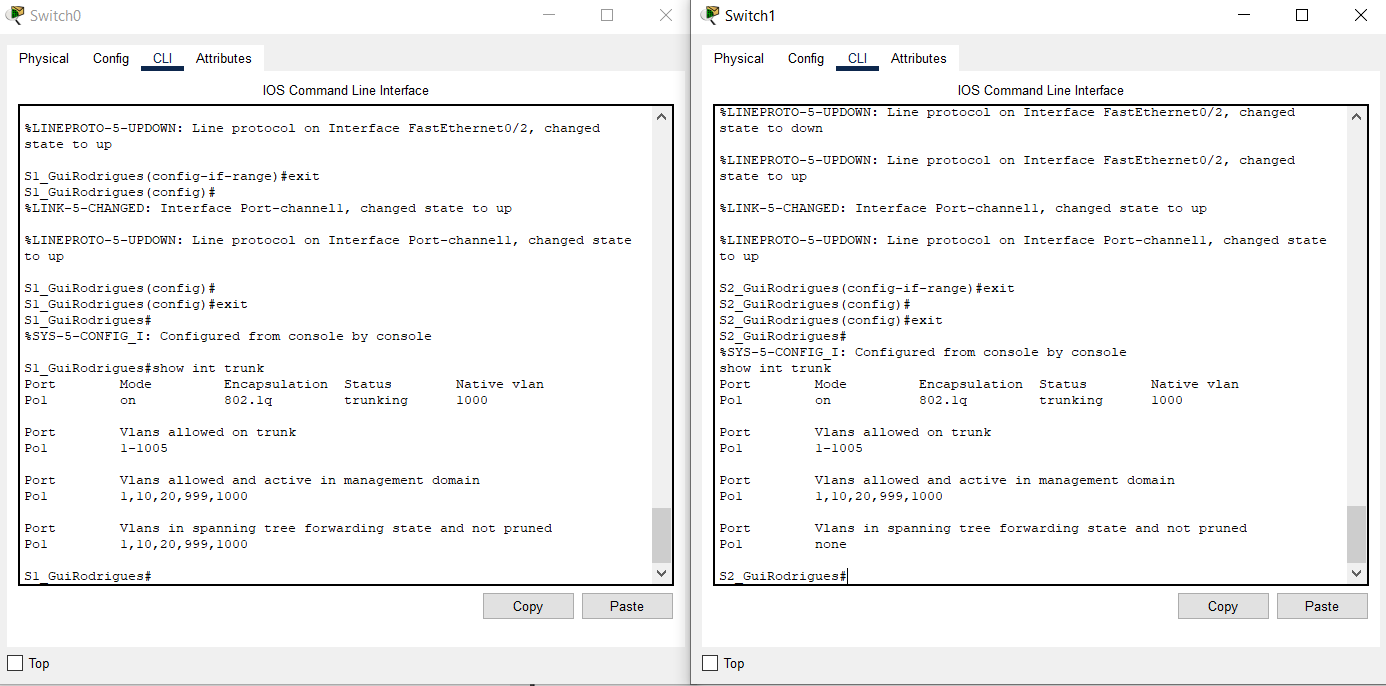


Ilustração : Verificação da criação do etherchannel

Para mostra o sumario do **EtherChannel** para verificar a configuração fazemos o seguinte:

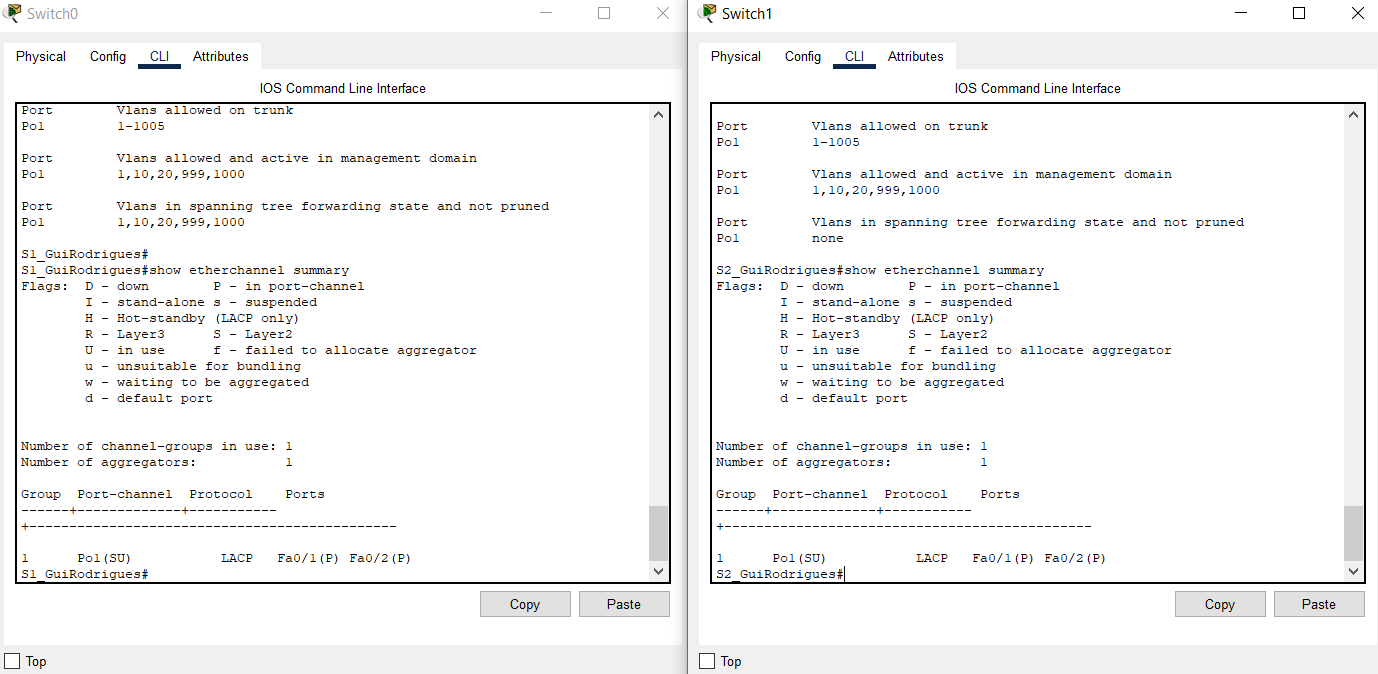


Ilustração : Sumario do EtherChannel

## 08.5.1 Lab - Configure DHCPv6

**Requisitos**

* 2 Routers (Cisco 4221 com a imagem universal Cisco IOS XE Release 16.9.4);
* 2 Switches (Cisco 2960 com a imagem lanbasek9 do Cisco IOS Release 15.2);
* 2 PCs (Windows com um programa de emulação de terminal);
* Cabos de consola para configurar os dispositivos Cisco IOS através das portas de console;
* Cabos Ethernet.

## Fichas futuras

## Fichas futuras

# Conclusão

Neste relatório, foram apresentados os passos necessários para configurar um switch Cisco. Esses passos são essenciais para garantir a segurança e a funcionalidade do switch.