



# **Monitoramento e Gerenciamento de Redes**

**- Switching VLANs -**

**Mauro Cesar Bernardes**

**São Paulo, 2023**

# Plano de Aula

- **Objetivo**

- Revisar conceitos importantes sobre de redes de comunicação;
- Preparar para o primeiro projeto avançado de redes.

- **Conteúdo**

- Endereços de camada de enlace
- Endereços de camada de rede
- Switch

- **Metodologia**

- Aula expositiva sobre os conceitos de Switch, com desenvolvimento de atividade prática e configuração em simulador (*Packet Tracer*).

# Agenda do Primeiro semestre - 2023

Janeiro 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
52							1
1	2	3	4	5	6	7	8
2	9	10	11	12	13	14	15
3	16	17	18	19	20	21	22
4	23	24	25	26	27	28	29
5	30	31					

Fevereiro 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
5			1	2	3	4	5
6	6	7	8	9	10	11	12
7	13	14	15	16	17	18	19
8	20	21	22	23	24	25	26
9	27	28					

Março 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
9			1	2	3	4	5
10	6	7	8	9	10	11	12
11	13	14	15	16	17	18	19
12	20	21	22	23	24	25	26
13	27	28	29	30	31		

Aula02 Switch+VLAN

Abril 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
13						1	2
14	3	4	5	6	7	8	9
15	10	11	12	13	14	15	16
16	17	18	19	20	21	22	23
17	24	25	26	27	28	29	30

Maio 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
18	1	2	3	4	5	6	7
19	8	9	10	11	12	13	14
20	15	16	17	18	19	20	21
21	22	23	24	25	26	27	28
22	29	30	31				

Junho 2023							
Nº	Se	Te	Qu	Qu	Se	Sá	Do
22				1	2	3	4
23	5	6	7	8	9	10	11
24	12	13	14	15	16	17	18
25	19	20	21	22	23	24	25
26	26	27	28	29	30		

○ Início das aulas

○ 1º Checkpoint da disciplina

○ 2º Checkpoint da disciplina

○ 3º Checkpoint da disciplina

# 1º Ponto importante:

**Fique atento ao horário de início das aulas**  
**Atrasos refletem descaso!**

# 2º Ponto importante:

## Plágio no meio acadêmico pode ser qualificado como crime

- No meio acadêmico o plágio configura-se pelo ato de assinar ou apresentar como seu o resultado produzido por outra pessoa ou grupo, ou seja, copiar o trabalho alheio.
- Além de uma conduta imoral e antiética, plágio pode ser qualificado como crime de violação de direito autoral no Brasil, com repercussões negativas em sua carreira acadêmica e profissional.
- Entre as atitudes consideradas como plágio no meio acadêmico estão:
  1. entregar um trabalho acadêmico que contenha cópia parcial ou total de trabalho entregue por outra pessoa ou equipe;
  2. usar as ideias de outra pessoa sem indicar a autoria;
  3. utilizar o texto de outra pessoa, alterando algumas das palavras, ou a ordem das palavras, sem a devida citação da fonte;
  4. usar as ideias de outra pessoa, sem referência ao autor;
  5. recortar e colar da Internet conteúdo sem a devida citação da fonte.
- Atividades classificadas como plágio receberão, a critério do professor, nota zero, independente da autoria.
- Portanto, tenha isso em mente antes de compartilhar sua atividade ou realizar cópia, mesmo que parcial, de atividade desenvolvida por algum colega.

# Cadastro NetAcademy

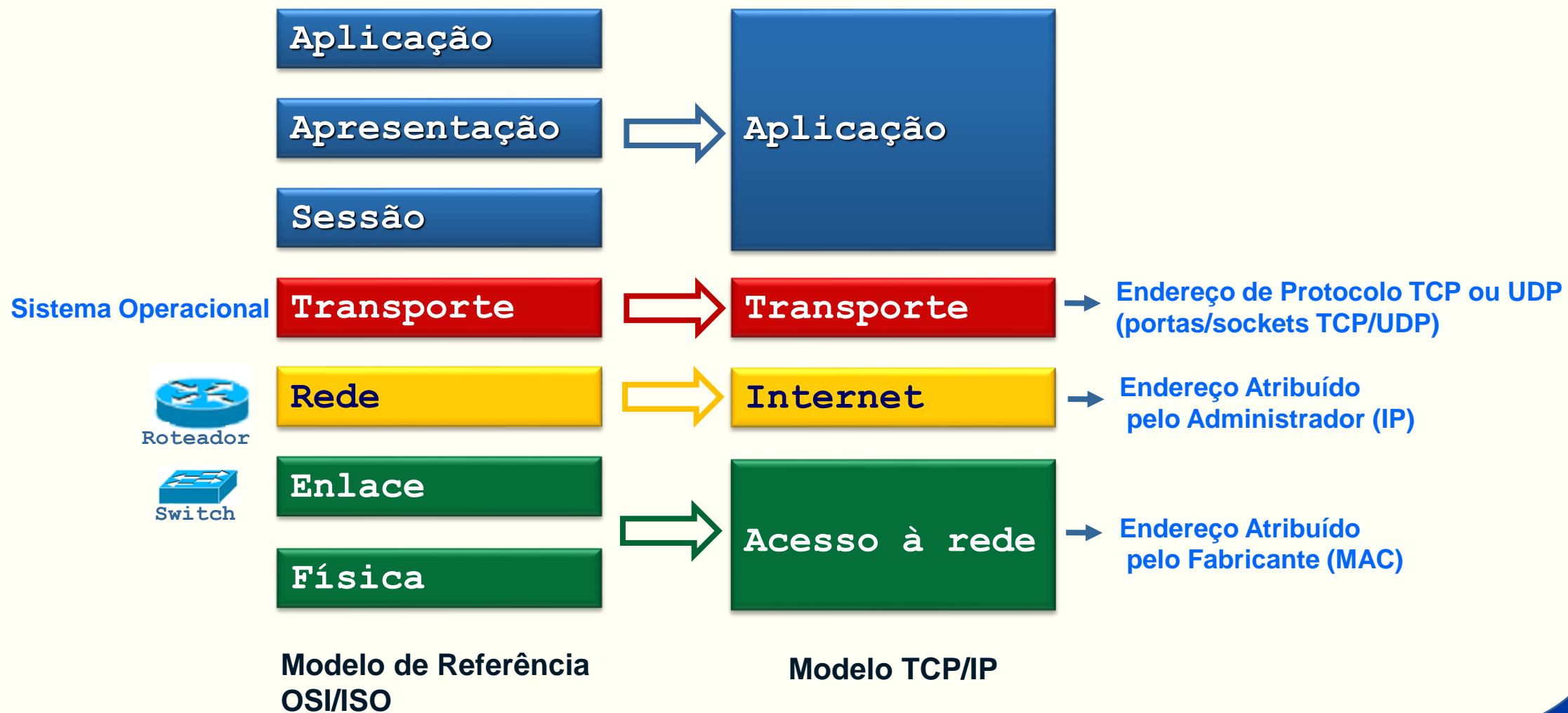


<https://forms.gle/rfmqAQkrC6CDoCLw8>

# Breve Revisão:

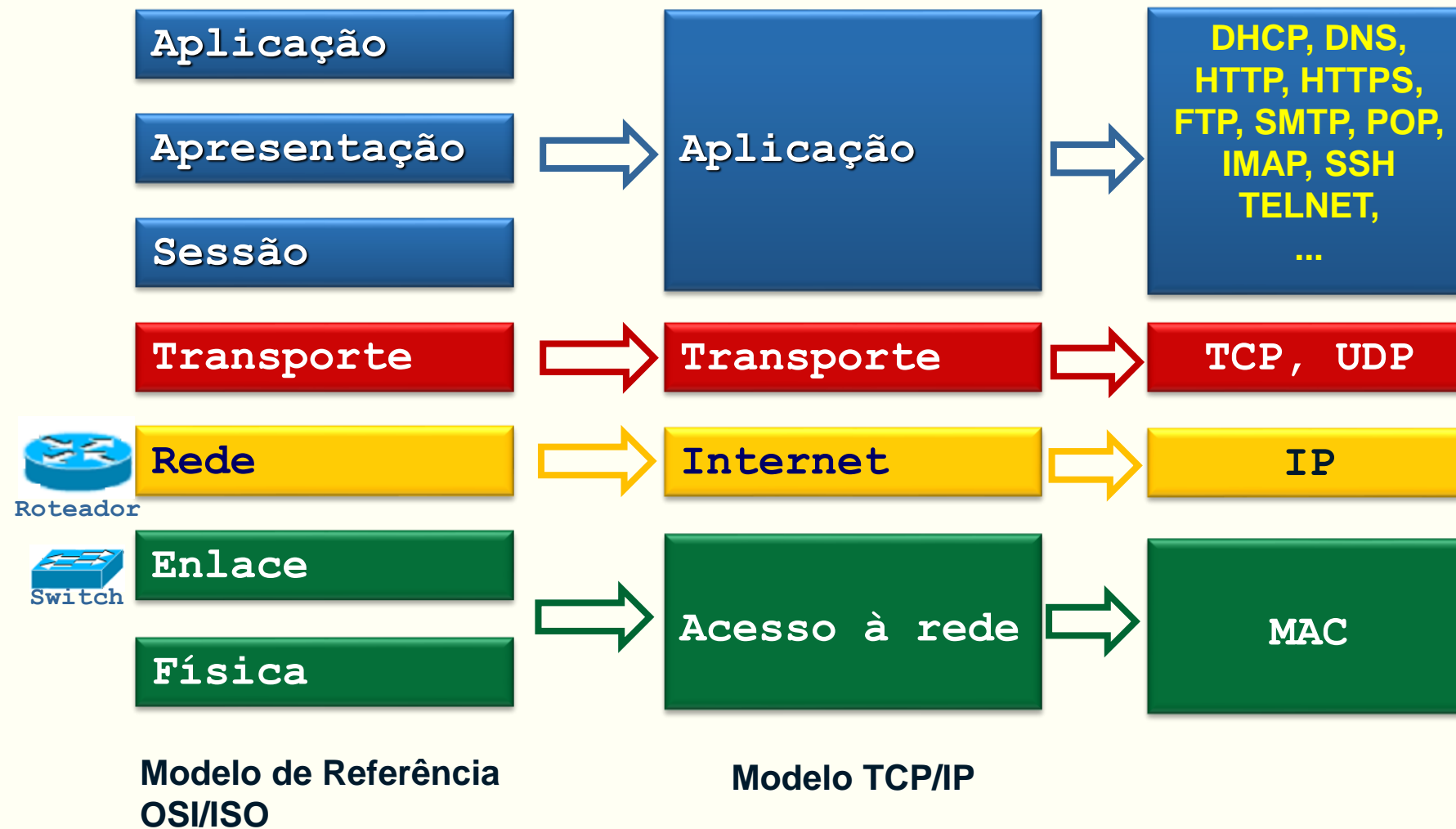
- **Modelo OSI x TCP/IP**
- **Endereços de Camada 2**
- **Switches**

# Revisão: OSI x TCP/IP

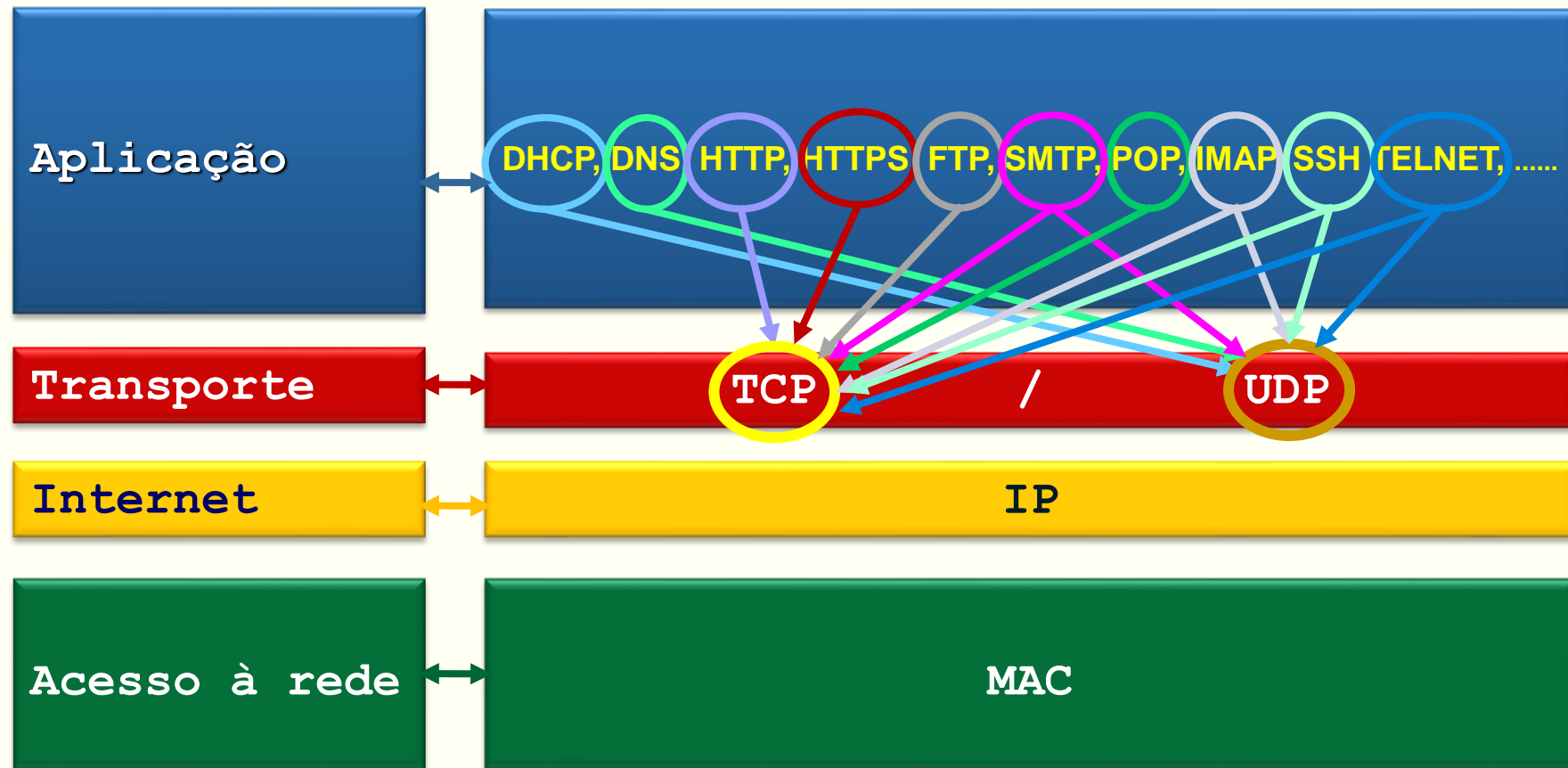




# Revisão: OSI x TCP/IP



# Revisão: TCP/IP



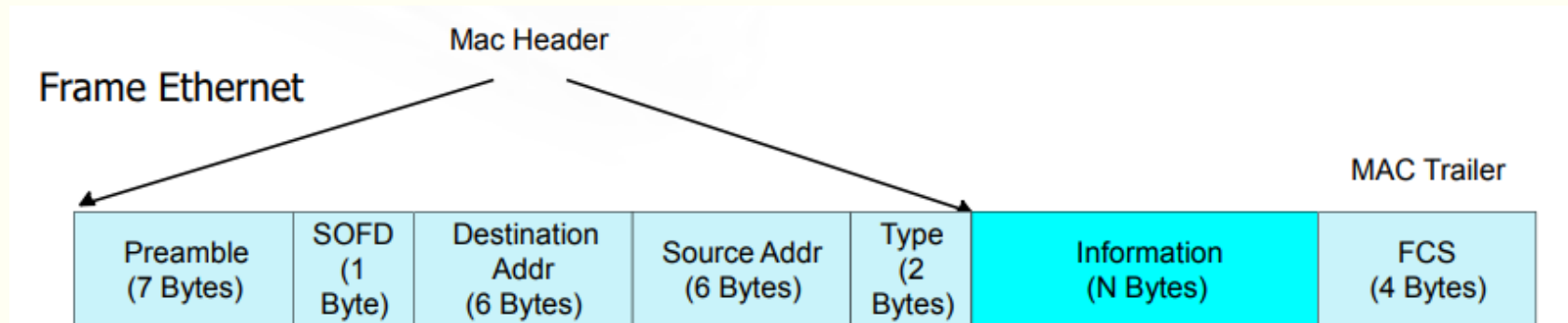
Modelo TCP/IP

# **Endereço MAC**

**(A camada 2)**

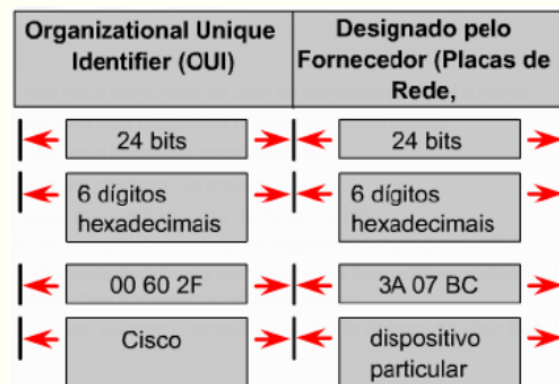
# Endereço MAC

- Tecnologias como Ethernet possuem esquemas próprios de endereçamento no nível de enlace/acesso à rede
- Normalmente, os protocolos do nível MAC (*Media Access Control*) usam endereços físicos na formatação das suas primitivas
- Logo, no nível MAC, para que um *frame* possa enviado de um host a outro em um enlace de dados, o endereço físico do *host* destino deve ser conhecido
- Endereço MAC = Endereço Ethernet = Endereço físico



# Endereço Físico: Representação

- O tamanho (número de bits) do endereço físico varia conforme a tecnologia de rede.
- No caso da tecnologia *Ethernet* para redes locais, esse endereço Físico é conhecido como endereço MAC (*Media Access Control*) e é estruturado da seguinte forma:
  - os endereços têm 48 bits (6 bytes), representados por seis números hexadecimais, separados por “:”
  - os 3 primeiros bytes definem o identificador do fabricante
  - os 3 últimos bytes são definidos pelo fabricante, de forma única
  - Exemplos: **02:60:8C:03:1D:91**; **08:00:5A:07:4B:95**; **00:60:2F:FA:78:C6**



# Endereço Físico: Camada 2

- Cada interface de rede (NIC – *Network Interface Card*) vem com um identificador único e exclusivo de fábrica.
- Este identificador é conhecido como: endereço físico, endereço de *hardware da interface* ou *endereço MAC*.
- Para garantir que não haverá conflitos de endereços, fabricantes de interfaces de rede (ex. *Ethernet*) devem ser registrados junto a uma autoridade central.
- O código identificador do fabricante é chamado de OUI - *Organizationally Unique Identifier*.



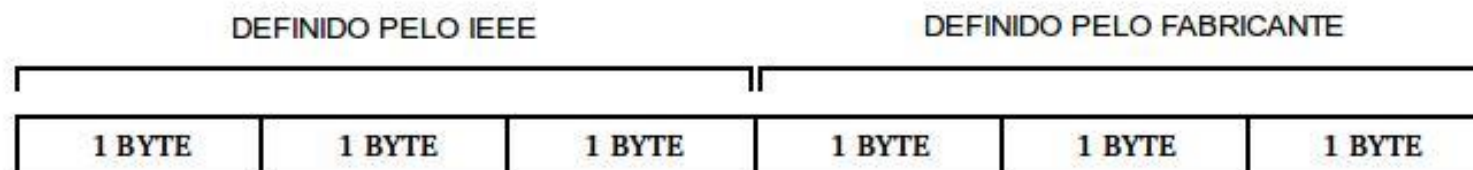
# Endereço MAC: Camada 2

- O **Endereço MAC** (*Media Access Control*) é um endereço físico associado à interface de comunicação, que conecta um dispositivo à rede.
- O MAC é **um endereço “único”**, não havendo duas interfaces com a mesma numeração.
- Esse endereço é utilizado para controle de acesso em redes de computadores (acesso à Rede Local (LAN)).
- Sua identificação é **gravada em hardware**, isto é, na memória ROM da placa de rede de equipamentos como *desktops*, *notebooks*, roteadores, *smartphones*, *tablets*, impressoras de rede.



# Endereço MAC: Representação

- O endereço MAC é formado por um conjunto de 6 bytes separados por dois pontos (":") ou hífen ("-"), sendo cada byte representado por dois algarismos na forma hexadecimal, como por exemplo: "**00:19:B9:FB:E2:58**".
- Cada algarismo em hexadecimal corresponde a uma palavra binária de **4 bits**, desta forma, os **12 algarismos** que formam o endereço totalizam **48 bits (6 bytes)**.
- Há uma padronização dos endereços MAC administrada pela IEEE (*Institute of Electrical and Electronics Engineers*) que define que os três primeiros bytes, chamados OUI (*Organizationally Unique Identifier*), são destinados a identificação do fabricante - eles são fornecidos pela própria IEEE.
- Os três últimos bytes são definidos pelo fabricante, sendo este responsável pelo controle da numeração de cada placa que produz.
- Apesar de ser único e gravado em hardware, o endereço MAC pode ser alterado através de técnicas específicas.





# Endereço Físico: Visualização

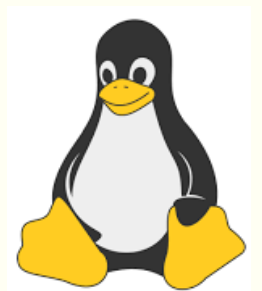
- O endereço da camada de enlace, também chamado de endereço físico ou endereço MAC pode ser facilmente visualizado nos sistemas operacionais:
  - Microsoft Windows, utilizando-se o comando **ipconfig /all**
  - Em sistemas Unix, o comando **ifconfig** exibe as interfaces e seus respectivos endereços de enlace
- A seguir são exibidas as saídas resumidas dos comandos **ipconfig/all** e **ifconfig**, respectivamente.



```
c: \>ipconfig/all
```

```
Adaptador Ethernet Conexão local:
```

```
Endereço físico . . . . . : 00-88-14-4D-4C-FB
```



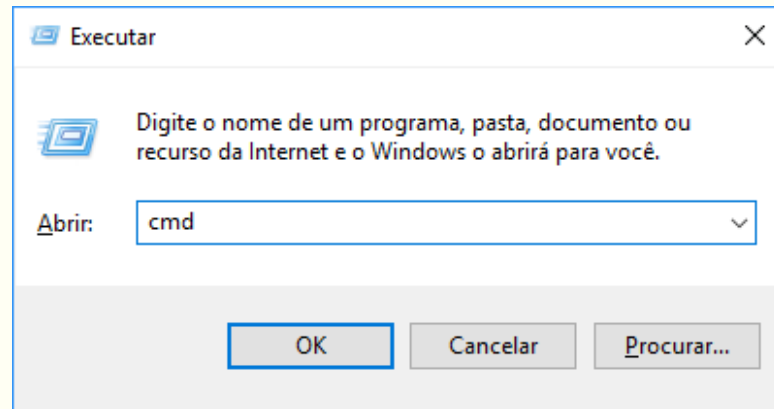
```
~$ ifconfig
```

```
eth0 Link encap:Ethernet__Endereço de HW__00:1D:7D:B2:34:F9
```

```
inet end.:
```

```
192.168.88.50__Bcast:192.168.88.255__Mask:255.255.255.0
```

# Endereço Físico: Visualização



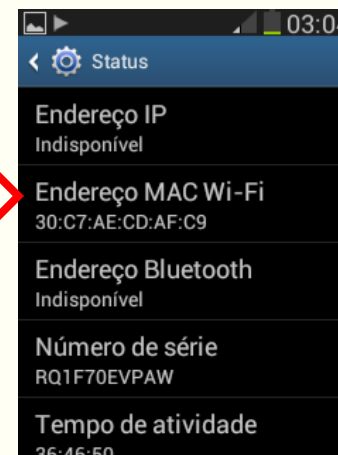
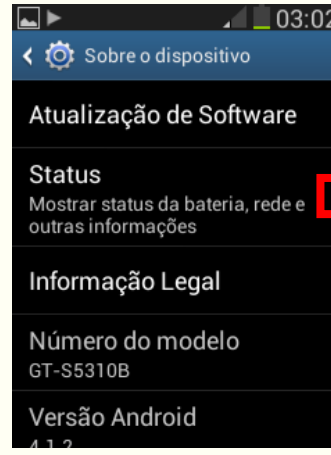
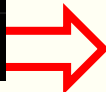
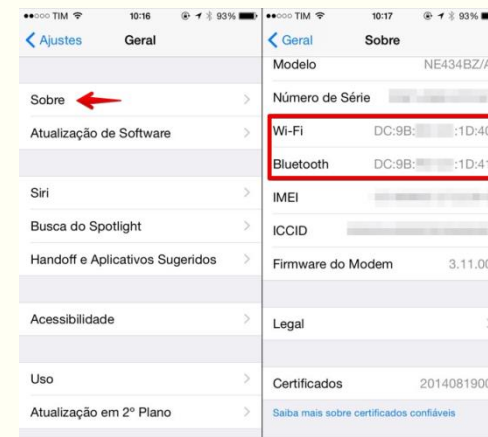
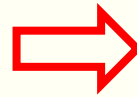
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [versão 10.0.15063]
(c) 2017 Microsoft Corporation. Todos os direitos reservados.
C:\Users>ipconfig/all
```

```
C:\WINDOWS\system32\cmd.exe
Adaptador de Rede sem Fio Conexão de Rede sem Fio:

Sufixo DNS específico de conexão. . . . . :
Descrição . . . . . : Dell Wireless 1702 802.11b/g/n
Endereço Físico . . . . . : E0-06-E0-FD-EC-06
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::3cde:fe80:160:a07e%12(Preferencial)
```

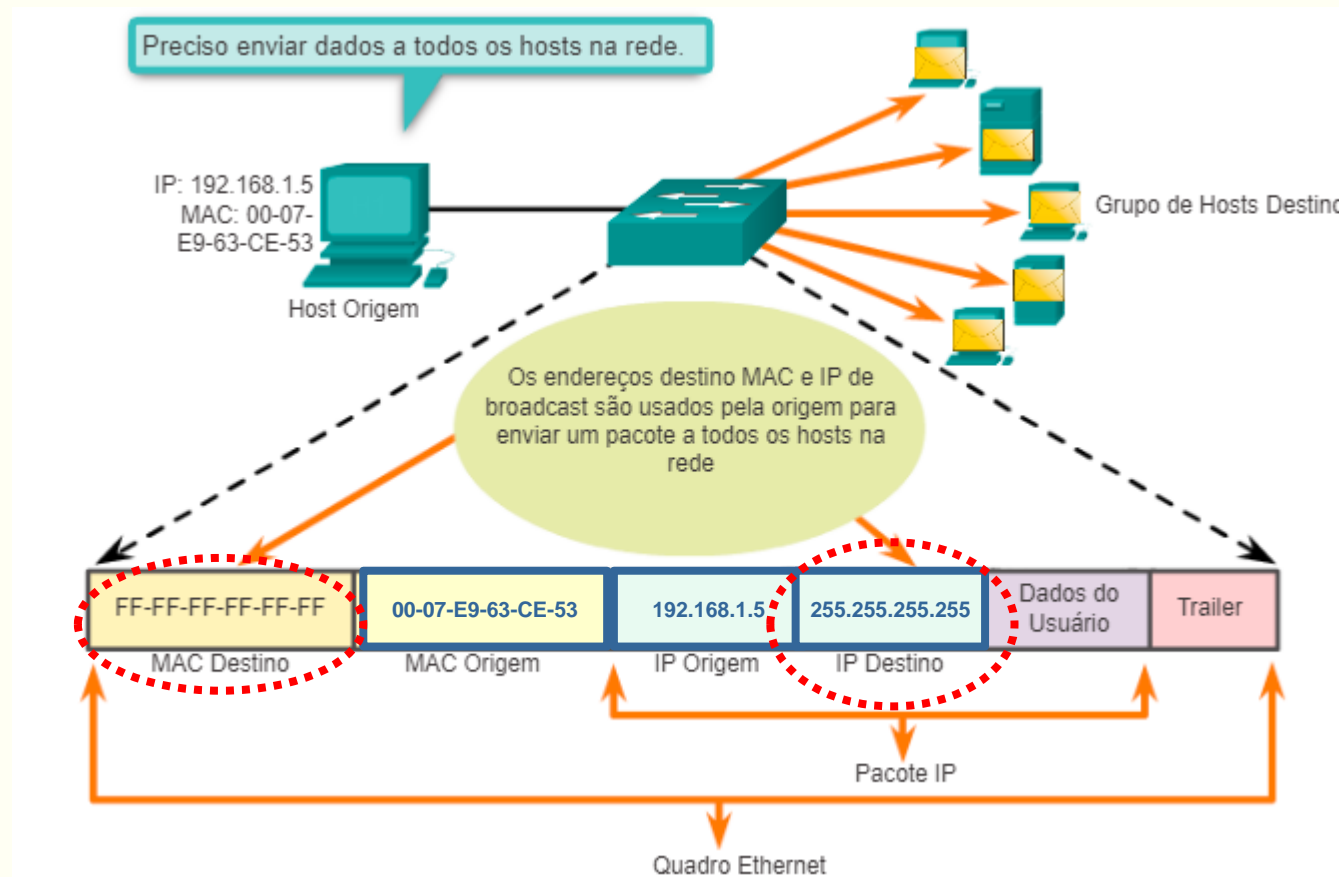


# Endereço Físico: Visualização



# Endereço de Broadcast: Camada 2

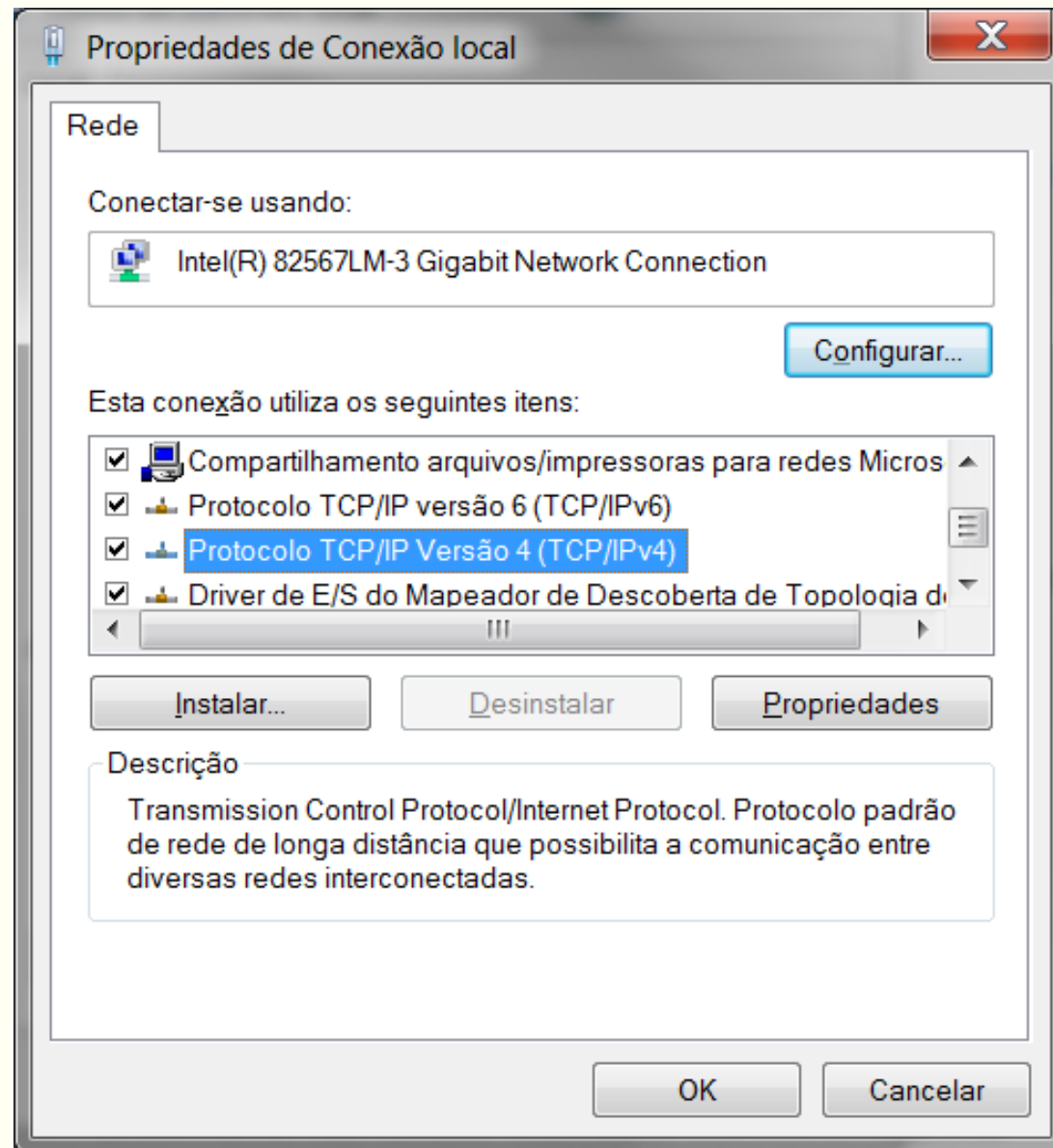
Em redes locais seguindo o padrão Ethernet, o endereço MAC de broadcast é em hexadecimal é **FF-FF-FF-FF-FF-FF**.



# **Endereço Internet Protocol (IP)**

## **(A camada de Rede)**

# Atribuição do endereço IP



# Atribuição do endereço IPv4

**Propriedades de Protocolo TCP/IP** [?] [X]

**Geral**

As configurações IP podem ser atribuídas automaticamente se a rede oferecer suporte a esse recurso. Caso contrário, você precisa solicitar ao administrador de rede as configurações IP adequadas.

☐ Obter um endereço IP automaticamente

☒ Usar o seguinte endereço IP:

Endereço IP: 192 . 168 . 1 . 2

Máscara de sub-rede: 255 . 255 . 255 . 0

Gateway padrão: 192 . 168 . 1 . 1

☐ Obter o endereço dos servidores DNS

☒ Usar os seguintes endereços de servidor DNS:

Servidor DNS preferencial: 208 . 67 . 222 . 222

Servidor DNS alternativo: 208 . 67 . 220 . 220

Avançado...

OK Cancelar

# Formato do Endereçamento IPv4

131 . 108 . 122 . 204

**Representado em formato decimal, separados por ponto, contendo número de 0 a 255**

10000011 01101100 01111010 11001100

## Endereço de 32 bits

10000011.01101100.01111010.11001100

7 6 5 4 3 2 1 0  
2 2 2 2 2 2 2 2

## Endereço agrupado em bytes

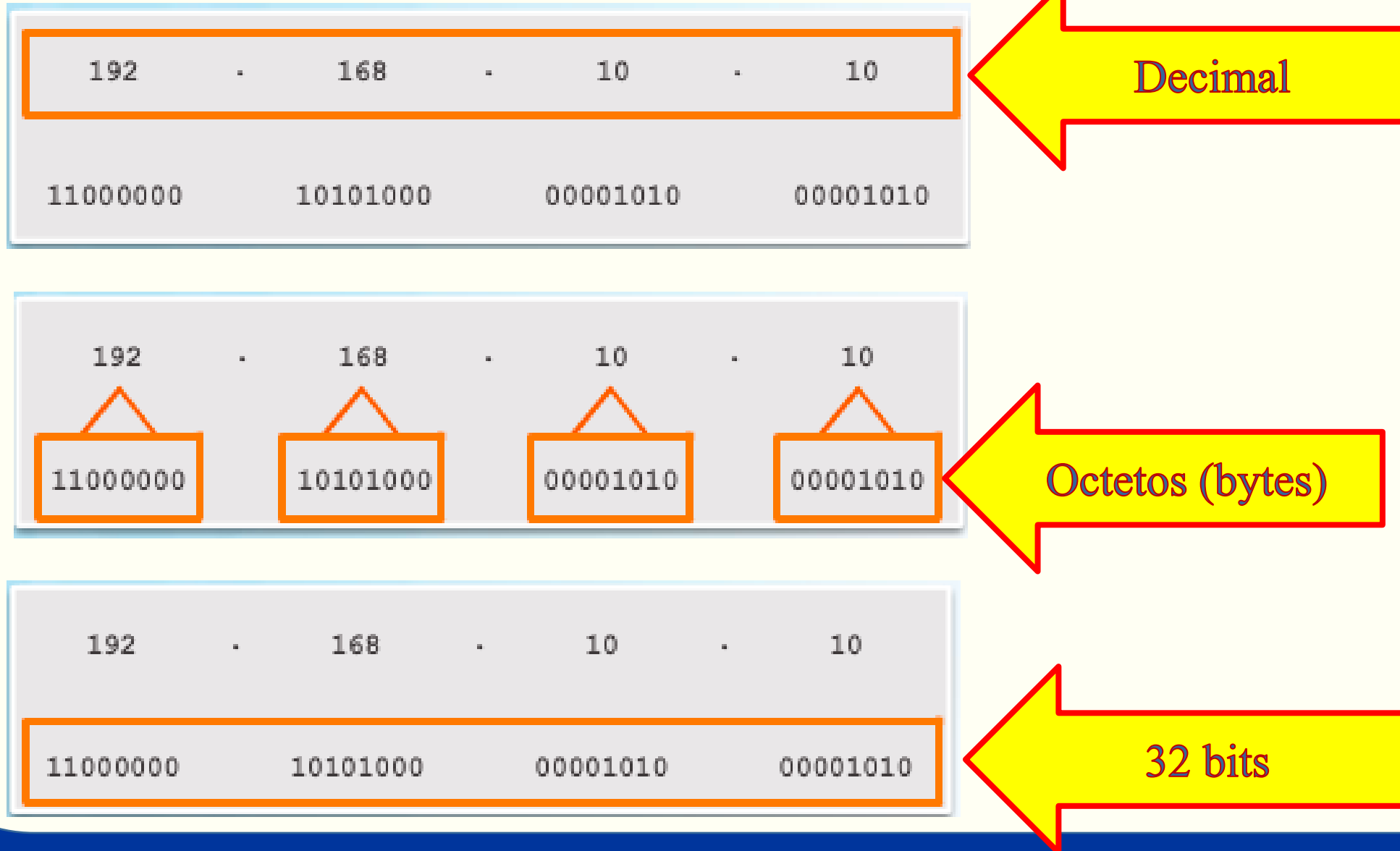
131.108.122.204

Parte da Rede    Parte do Host

Binário	Decimal
00000000	0
11111111	255

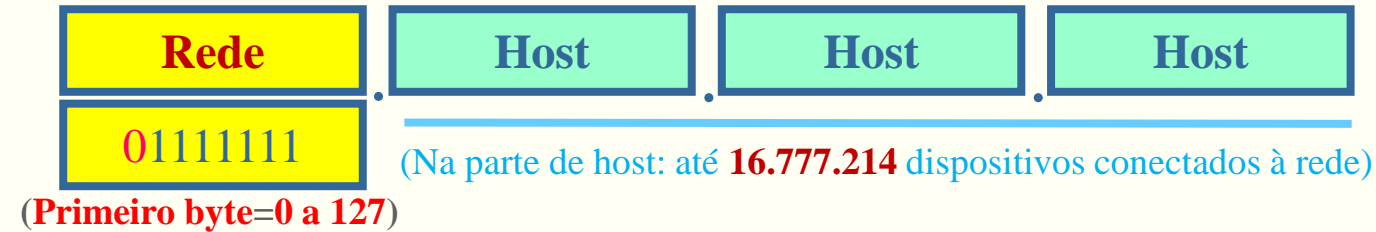


# Formato do Endereçamento IPv4

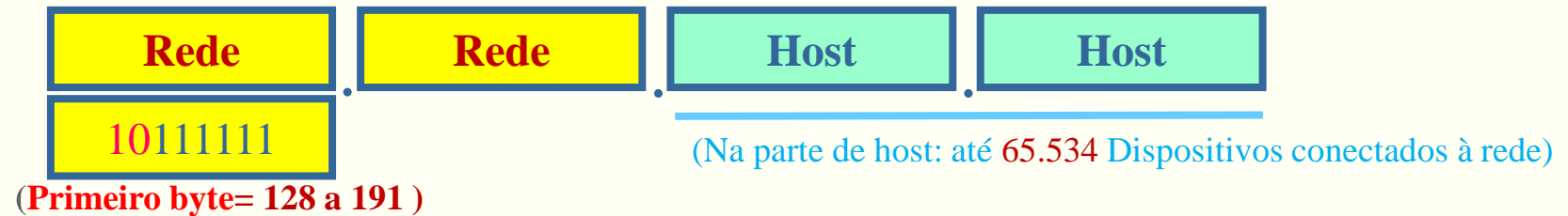


# Classes de Endereços IPv4

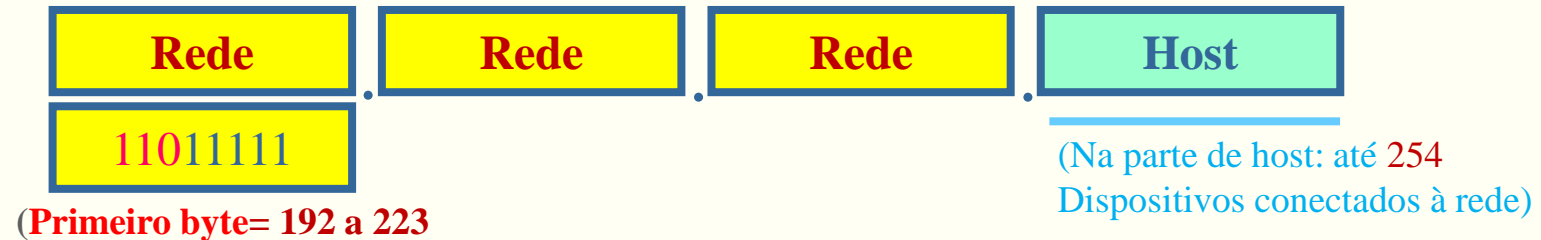
## Classe A



## Classe B



## Classe C



## Classe D

Primeiro byte: 224 a 239

## Classe E

Primeiro byte: 240 a 255

# Revisando

## Classe A

112	240	13	20
Rede	Host	Host	Host
01111111	(0 a 127) (16.777.214 dispositivos conectados à rede)		

## Máscara Padrão

Em binário	11111111	00000000	00000000	00000000
Em decimal	255	0	0	0

## Endereço de Rede

Em decimal	112	0	0	0
Em binário	01110000	00000000	00000000	00000000

## Endereço de Broadcast

Em decimal	112	255	255	255
Em binário	01110000	11111111	11111111	11111111

# Revisando

## Classe B

191	168	13	20
Rede	Rede	Host	Host
10111111	(128 a 191) (65.534 dispositivos conectados à rede)		

## Máscara Padrão

Em binário	11111111	11111111	00000000	00000000
Em decimal	255	255	0	0

## Endereço de Rede

Em decimal	191	168	0	0
Em decimal	10111111	10101000	00000000	00000000

## Endereço de Broadcast

Em decimal	191	168	255	255
Em binário	10111111	10101000	11111111	11111111

# Revisando

## Classe C

200	200	200	20
Rede	Rede	Rede	Host
11011111	(192a 223) (254 dispositivos conectados à rede)		

## Máscara Padrão

Em binário	11111111	11111111	11111111	00000000
Em decimal	255	255	255	0

## Endereço de Rede

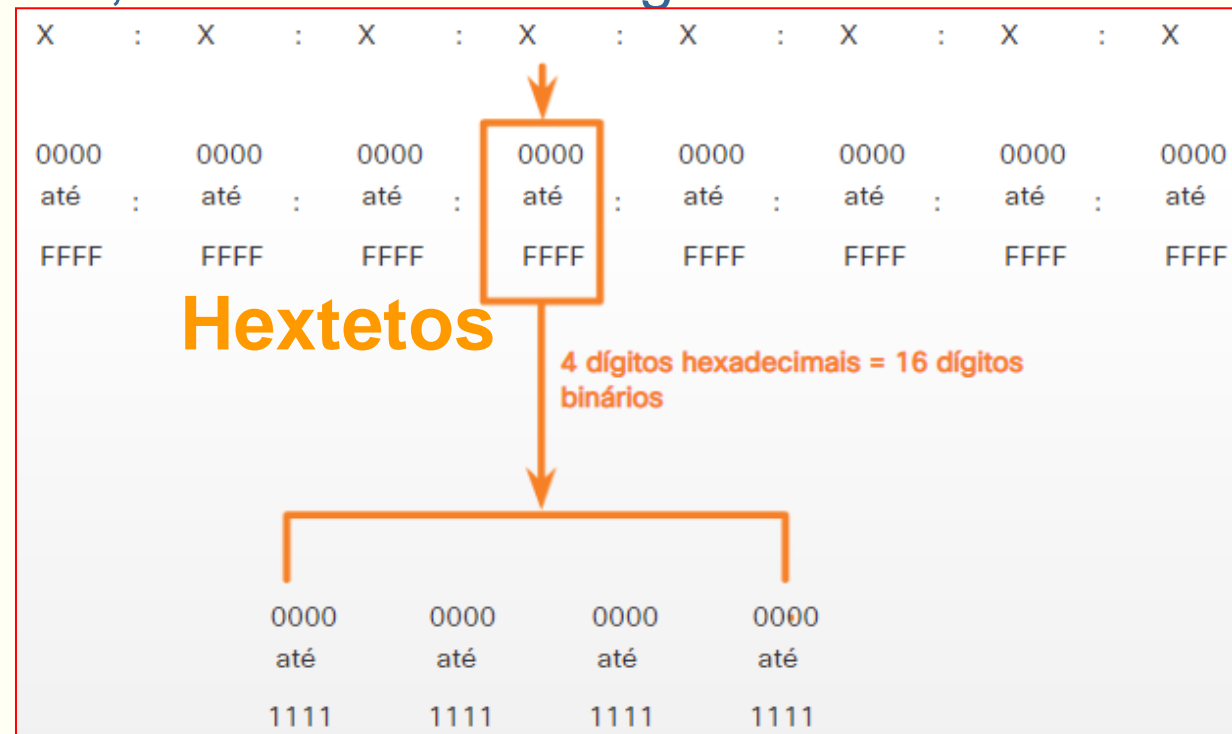
Em decimal	200	200	200	0
Em decimal	11001000	11001000	11001000	00000000

## Endereço de Broadcast

Em decimal	200	200	200	255
Em binário	11001000	11001000	11001000	11111111

# Representação do endereço IPv6

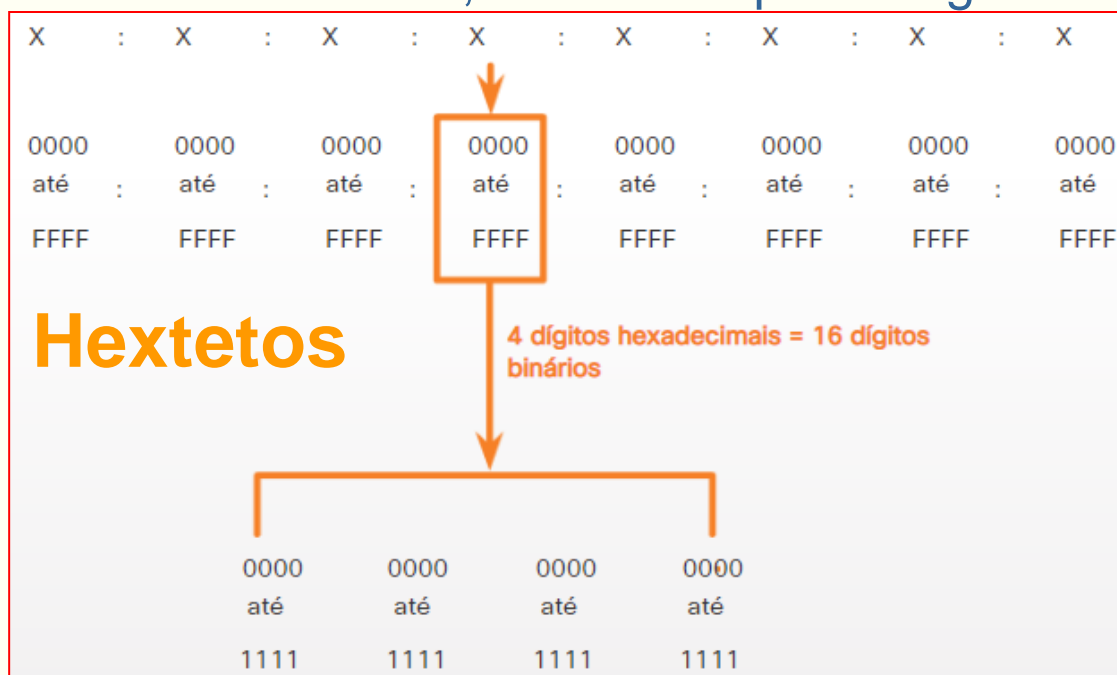
- Os **endereços IPv6 têm 128 bits** e são escritos como uma sequência de valores hexadecimais, muitas vezes chamados de **hextetos**.
- Cada 4 bits são representados por um único dígito hexadecimal, **totalizando 32 dígitos hexadecimais**, como mostra a Figura.



- Os endereços IPv6 não diferenciam maiúsculas e minúsculas e podem ser escritos tanto em minúsculas como em maiúsculas

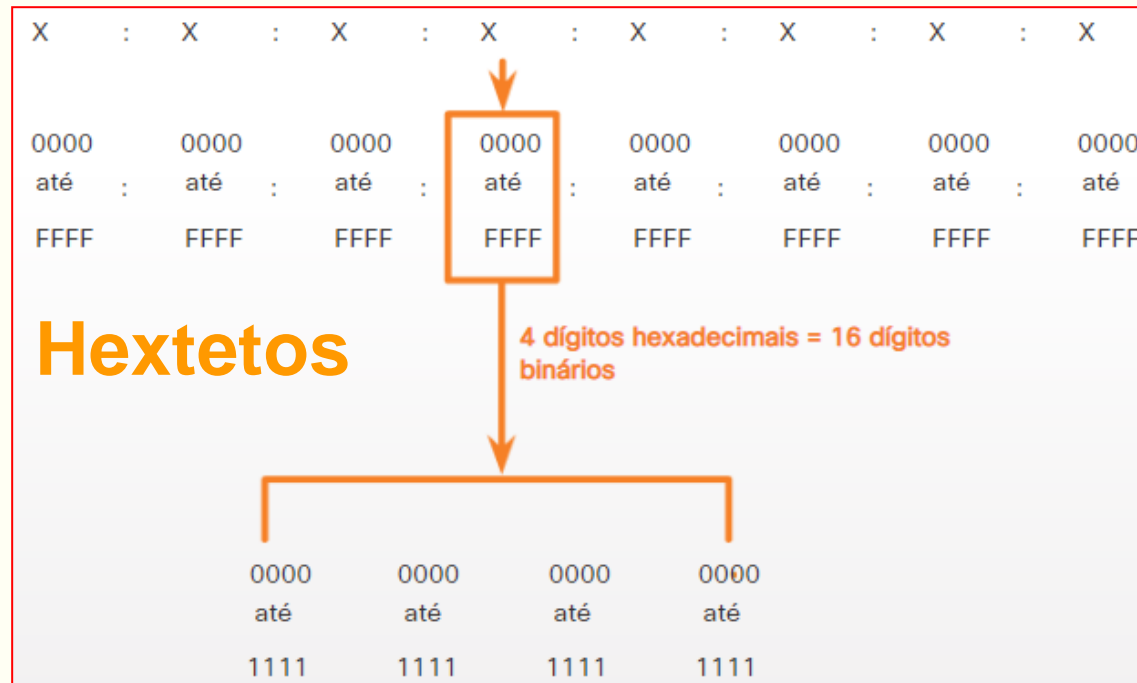
# Representação do endereço IPv6: **Formato preferencial**

- Como mostrado na Figura, o **formato preferencial** para escrever um endereço IPv6 é: **x: x: x: x: x: x: x: x**, com cada “x” consistindo de quatro valores hexadecimais.
- Quando falamos de 8 bits de um endereço IPv4, usamos o termo **octeto** (um endereço IPv4 é representado 4 octetos).
- No IPv6, um **hexteto** é o termo não oficial usado para se referir a um segmento de 16 bits ou quatro valores hexadecimais (um endereço IPv6 é representado por 8 hextetos).
- Cada “x” equivale a um único **hexteto**, 16 bits ou quatro dígitos hexadecimais.



# Representação do endereço IPv6: **Formato preferencial**

- **Formato preferencial** significa que o endereço IPv6 é gravado usando todos os 32 dígitos hexadecimais.
- Isso não significa necessariamente que é o método ideal para representar o endereço IPv6.
- Veremos duas regras para ajudar a reduzir o número de dígitos necessários para representar um endereço IPv6.





# Representação do endereço IPv6: **Formato preferencial**

A Figura apresenta exemplos de endereços IPv6 no formato preferencial.

32 dígitos

2001	:	0DB8	:	0000	:	1111	:	0000	:	0000	:	0000	:	0200
2001	:	0DB8	:	0000	:	00A3	:	ABCD	:	0000	:	0000	:	1234
2001	:	0DB8	:	000A	:	0001	:	0000	:	0000	:	0000	:	0100
2001	:	0DB8	:	AAAA	:	0001	:	0000	:	0000	:	0000	:	0200
FE80	:	0000	:	0000	:	0000	:	0123	:	4567	:	89AB	:	CDEF
FE80	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
FF02	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
FF02	:	0000	:	0000	:	0000	:	0000	:	0001	:	FF00	:	0200
0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0001
0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000	:	0000

# Representação do endereço IPv6: **Regra 1**

- **Omitir 0 à esquerda:**
  - A primeira regra para ajudar a reduzir a notação de endereços IPv6 é omitir os 0s (zeros) à esquerda de qualquer seção de 16 bits ou hexteto. Por exemplo:
    - **01AB** pode ser representado como **1AB**
    - **09F0** pode ser representado como **9F0**
    - **0A00** pode ser representado como **A00**
    - **00AB** pode ser representado como **AB**
  - Essa regra se aplica somente aos **0** à esquerda, e **NÃO** aos **0** à direita.
  - Caso contrário, o endereço ficaria ambíguo.
  - Por exemplo, o hexteto “**ABC**” poderia ser “**0ABC**” ou “**ABC0**”, mas essas duas representações não se referem ao mesmo valor

# Representação do endereço IPv6: **Regra 1**

- As Figuras mostram vários exemplos de como a omissão dos 0 à esquerda pode ser usada para reduzir o tamanho de um endereço IPv6.
- O formato preferencial é exibido para cada exemplo.
- Observe como a omissão dos 0 à esquerda em cada exemplo resulta em uma representação menor do endereço

Preferencial	0000:0000:0000:0000:0000:0000:0000:0000
Nenhum 0 à esquerda	0: 0: 0: 0: 0: 0: 0: 0

Preferencial	2001:0DB8:000A:1000:0000:0000:0000:0100
Nenhum 0 à esquerda	2001: DB8: A:1000: 0: 0: 0: 100

Preferencial	FF02:0000:0000:0000:0000:0000:0000:0001
Nenhum 0 à esquerda	FF02: 0: 0: 0: 0: 0: 0: 1

Preferencial	0000:0000:0000:0000:0000:0000:0000:0001
Nenhum 0 à esquerda	0: 0: 0: 0: 0: 0: 0: 1

Preferencial	2001:0DB8:0000:A300:ABCD:0000:0000:1234
Nenhum 0 à esquerda	2001: DB8: 0:A300:ABCD: 0: 0:1234

Preferencial	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Nenhum 0 à esquerda	FE80: 0: 0: 0: 123:4567:89AB:CDEF

Preferencial	FF02:0000:0000:0000:0000:0001:FF00:0200
Nenhum 0 à esquerda	FF02: 0: 0: 0: 0: 1:FF00: 200

Preferencial	0000:0000:0000:0000:0000:0000:0000:0000
Nenhum 0 à esquerda	0: 0: 0: 0: 0: 0: 0: 0

# Representação do endereço IPv6: **Regra 2**

## Omitir todos os segmentos 0

- A segunda regra para ajudar a reduzir a notação de endereços IPv6 é que o uso de dois-pontos duplo (::) pode substituir uma única sequência contígua de um ou mais segmentos de 16 bits (hextetos) compostos exclusivamente por 0.
- Os dois-pontos em dobro (::) só podem ser usados uma vez em um endereço; caso contrário, haveria mais de um endereço resultante possível.
- Quando associada à técnica de omissão dos 0 à esquerda, a notação de endereço IPv6 pode ser bastante reduzida.
- É o chamado formato compactado.
- Possíveis expansões do endereço ambíguo compactado:
  - 2001:0DB8::ABCD:0000:0000:1234
  - 2001:0DB8::ABCD:0000:0000:0000:1234
  - 2001:0DB8:0000:ABCD::1234
  - 2001:0DB8:0000:0000:ABCD::1234
- Endereço incorreto:
  - 2001:0DB8::ABCD::1234

# Representação do endereço IPv6: Regra 2

- As Figuras mostram vários exemplos de como o uso de dois-pontos duplo (::) e a omissão de 0 à esquerda podem reduzir o tamanho de um endereço IPv6.

Preferencial	2001:0DB8:0000:1111:0000:0000:0000:0200
Nenhum 0 à esquerda	2001: DB8: 0:1111: 0: 0: 0: 200
Compactado	2001:DB8:0:1111::200

Preferencial	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Nenhum 0 à esquerda	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Compactado	FE80::123:4567:89AB:CDEF

Preferencial	FF02:0000:0000:0000:0000:0001:FF00:0200
Nenhum 0 à esquerda	FF02: 0: 0: 0: 0: 1:FF00: 200
Compactado	FF02::1:FF00:200

Preferencial	0000:0000:0000:0000:0000:0000:0000:0000
Nenhum 0 à esquerda	0: 0: 0: 0: 0: 0: 0: 0
Compactado	::

Preferencial	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Nenhum 0 à esquerda	2001: DB8: 0: 0:ABCD: 0: 0: 100
Compactado	2001:DB8::ABCD:0:0:100
ou	
Compactado	2001:DB8:0:0:ABCD::100

Preferencial	FF02:0000:0000:0000:0000:0000:0000:0001
Nenhum 0 à esquerda	FF02: 0: 0: 0: 0: 0: 0: 1
Compactado	FF02::1

Preferencial	0000:0000:0000:0000:0000:0000:0000:0001
Nenhum 0 à esquerda	0: 0: 0: 0: 0: 0: 0: 1
Compactado	::1

# Exercício 1

Formato preferencial	2001	0000	0DB8	1111	0000	0000	0000	0200
Zeros à esquerda omitidos								
Formato compactado								

Formato preferencial	2001	0000	0DB8	1111	0000	0000	0000	0200
Zeros à esquerda omitidos	2001	0	DB8	1111	0	0	0	200
	✓	✓	✓	✓	✓	✓	✓	✓
Formato compactado	2001:0:DB8:1111::200							
	✓							

# Switches

# Switch

O **Switch** é o equipamento utilizado em redes de computadores para reencaminhar dados (*frames*) entre os diversos *hosts* de acordo com o **endereço MAC** (de origem e de destino), sendo destinado a para segmentação de redes locais.



Figura 1: Foto de um Switch D-Link de 24 portas



Figura 2: Representação de um switch



Figura 3: conexões de cabos em switches em um rack



# Switch

O comutador (em inglês, **Switch**) é um dispositivo utilizado em redes locais de computadores (LAN) para reencaminhar quadros (*frames*) entre os diversos hosts utilizando para isso o **endereço MAC** (endereço de camada 2).



Um **Switch** opera na camada 2 (Enlace) do modelo OSI, encaminhando os quadros de acordo com o endereço MAC de destino.

Porém, atualmente existem **switchs** que operam em conjunto na camada 3 (rede), herdando algumas propriedades dos roteadores (*routers*).

# Switch



Switch 48P Cisco 10/100/1000Mbps Rj45 2X Gigabit

**R\$ 2.823,20** [Processtec](#) **85% positivos** (218) [Comparar preços de 5+ lojas](#)

DESCRIÇÃO Fabricante: **Cisco** Systems - Inc Modelo do produto: SG250-50-K9-BR  
Nome de marca: **Cisco** Nome do produto: SG250-50 ...



Switch Cisco | Catalyst 3850 | Capacidade 88 Gbps | 24x Portas | MPN: WS-C3850-24U-L

**R\$ 49.299,15** [FourServ](#)

★★★★★ 1 comentário sobre o produto

A **Cisco** Catalyst 3850 Series é a próxima geração de classe empresarial **switches** de acesso da camada empilháveis ? que ...



Switch 48P Cisco 10/100/1000Mbps Poe+ 2P Sfp Gerenciável

**R\$ 6.668,64** [Processtec](#) **85% positivos** (218) [Comparar preços de 5+ lojas](#)

A **Cisco** 220 Series, parte do portfólio de negócios de pequenas e médias empresas do **Cisco**, é uma série de **switches** ...



Switch Cisco | Catalyst 3650 | 48 Portas Poe | Gigabit | 4 SFP | MPN: WS-C3650-48PS-L

**R\$ 55.249,15** [FourServ](#)

Cisco Catalyst 3650 48 Port PoE 4x1G Uplink IP Base



Switch Cisco SG220 | 24 Portas | 10/100/1000 | Gigabit | 02 SFP | Layer2 | MPN: SG220-26-K9-BR

**R\$ 1.359,15** [FourServ](#) [Comparar preços de 5+ lojas](#)

A **Cisco** Série 220 parte da linha de soluções **Cisco** Small Business Network. É uma série de **switches** inteligentes e acessíveis ...



Switch Cisco | Catalyst 2960X | 48 Portas Gigabit | PoE 740W | 2 SFP+ | Layer3 | Gerenciável | MPN: WS-C2960X-48FPD-LB

**R\$ 17.594,15** [FourServ](#) [Comparar preços de 2 lojas](#)

★★★★★ 2 comentários sobre o produto

PoE - 48x 10/100/1000



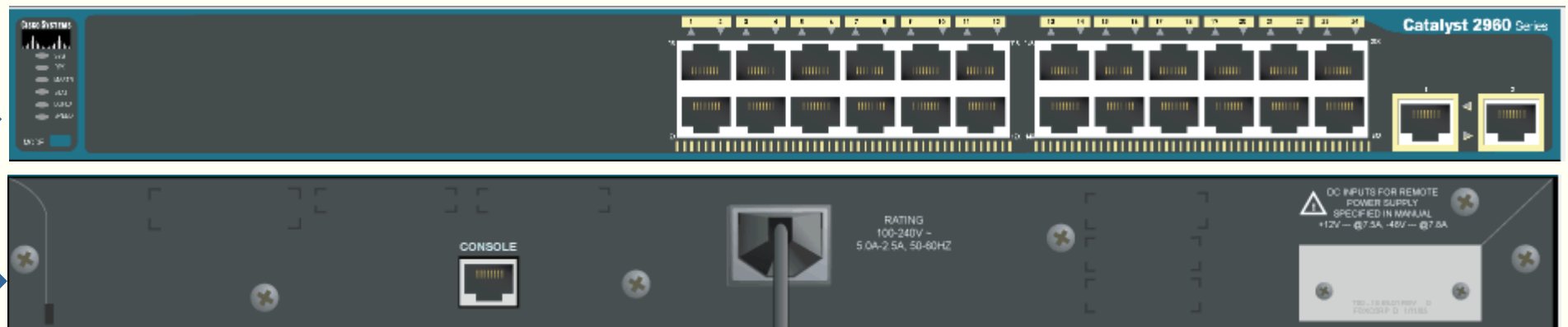
Switch Rede RJ45 08 Portas KP-E08

**R\$ 44,45** [Acessório Facil](#)

O **Switch** 8 Portas 10/100Mbps KP-E08 fornece uma maneira fácil de expandir a sua rede cabeada. Todas as 8 portas suportam auto ...

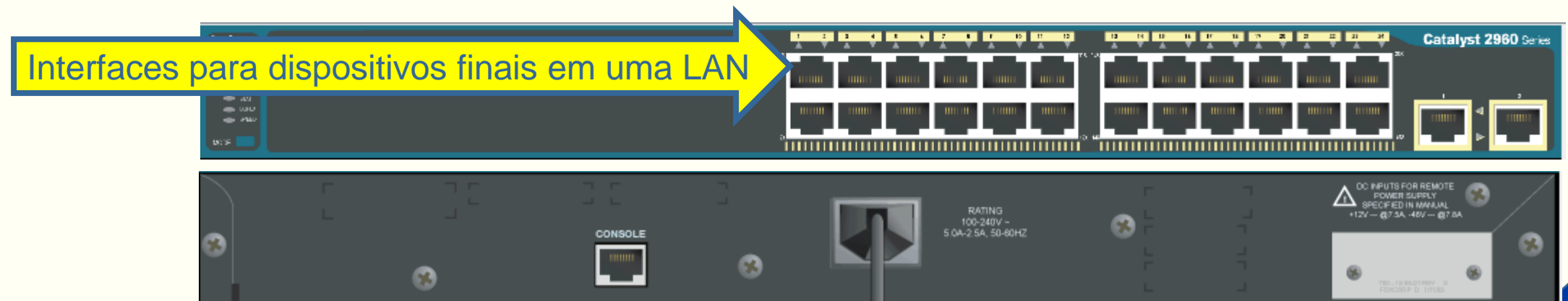
# Switch

- Um **Switch** é um equipamento de rede que permite interconectar dispositivos em uma rede de computadores, usando **comutação de pacotes** para receber dados de um dispositivo de origem, processar e encaminhar dados a um dispositivo de destino;
- A decisão de encaminhamento é feita com base no **endereço MAC (o endereço Físico gravado na interface de rede)** de origem e de destino
- Um switch que pode operar em mais de uma camada é chamado de Switch Multilayer



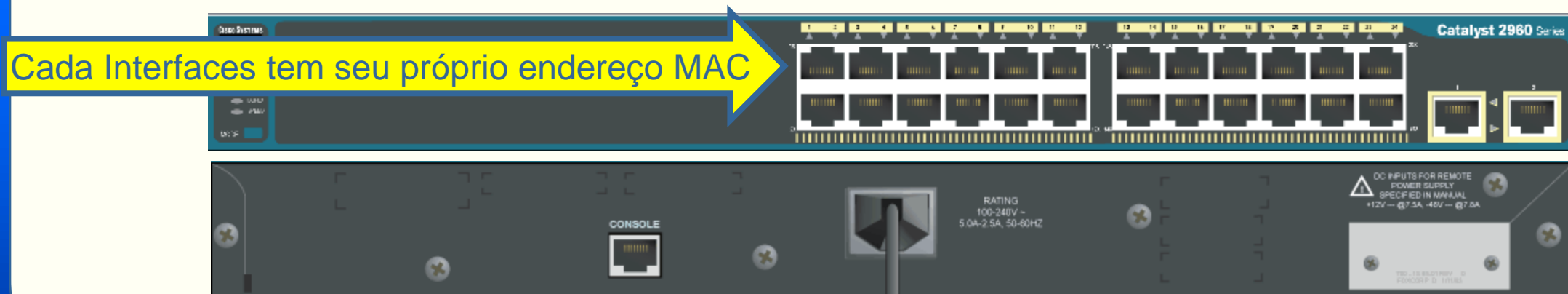
# Switch

- O switch permite a conexão de dispositivos em uma rede local por meio de suas interfaces (portas).
- É possível encontrar switches com a partir de 4 portas até 48 (ou mais em alguns modelos especiais), operando em velocidades que podem variar entre Fast Ethernet (100 Mbps) e 10 Gbps (ou mesmo maior, em modelos muito especializados).
- O cenário mais comum é de Switches com interfaces operando a *GigaEthernet* (1 Gbps).
- É possível também associar alguns modelos de switches para permitir a conexão de mais dispositivos a um mesmo segmento de rede, com maior número de portas.



# A tabela de endereços MAC do switch

- Um switch usará o endereço MAC de destino para determinar a interface de saída.
- Antes que um switch possa tomar essa decisão, ele deve saber qual interface o destino está localizado.
- Um switch cria uma tabela de endereços MAC, também conhecida como uma tabela CAM (*Content Addressable Memory*), gravando o endereço MAC de origem na tabela juntamente com a porta recebida.



# A tabela de endereços MAC do switch

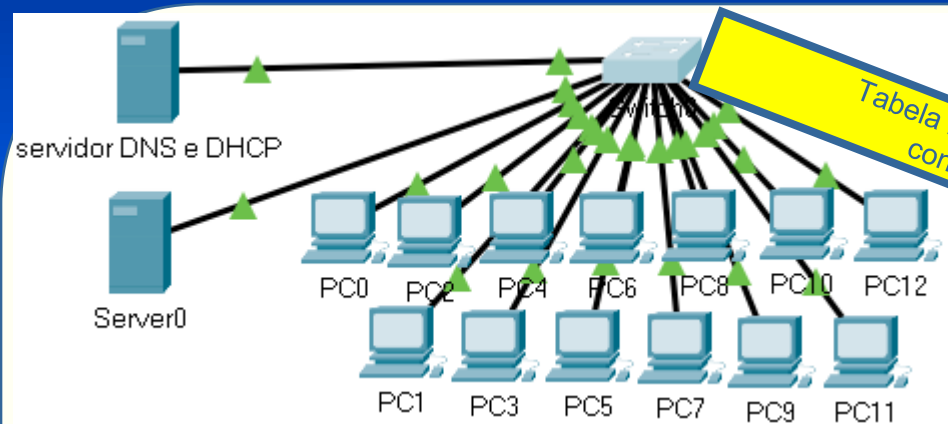


Tabela MAC dos Equipamentos conectados ao Switch

- Os switches utilizam os endereços de hardware (**MAC Address**) dos dispositivos conectados a ele para processar e encaminhar dados na camada de enlace (nível 2 no modelo OSI).
- Alguns modelos de switch também conseguem processar dados no nível 3 (camada de rede), incorporando assim algumas funcionalidades de roteamento.

Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch# show mac-address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
-----
1       0000.0c28.2552    DYNAMIC   Fa0/6
1       0000.0c6a.7759    DYNAMIC   Fa0/10
1       0001.6371.b816    DYNAMIC   Fa0/5
1       0001.97db.2594    DYNAMIC   Fa0/4
1       0001.c7dd.9669    DYNAMIC   Fa0/8
1       0002.4a95.e211    DYNAMIC   Fa0/9
1       0005.5e7a.4b17    DYNAMIC   Fa0/11
1       000c.cf0a.e56b    DYNAMIC   Fa0/13
1       000c.cfce.b844    DYNAMIC   Fa0/2
1       0050.0f70.bc71    DYNAMIC   Fa0/7
1       0060.3ecb.c313    DYNAMIC   Fa0/14
1       0090.2b1e.49aa    DYNAMIC   Fa0/3
1       00d0.970b.d8dc    DYNAMIC   Fa0/12
1       00d0.97ed.10d8    DYNAMIC   Fa0/15
1       00d0.d319.4409    DYNAMIC   Fa0/1

Switch#
Switch#
Switch#
Switch#
```

Ctrl+F6 to exit CLI focus

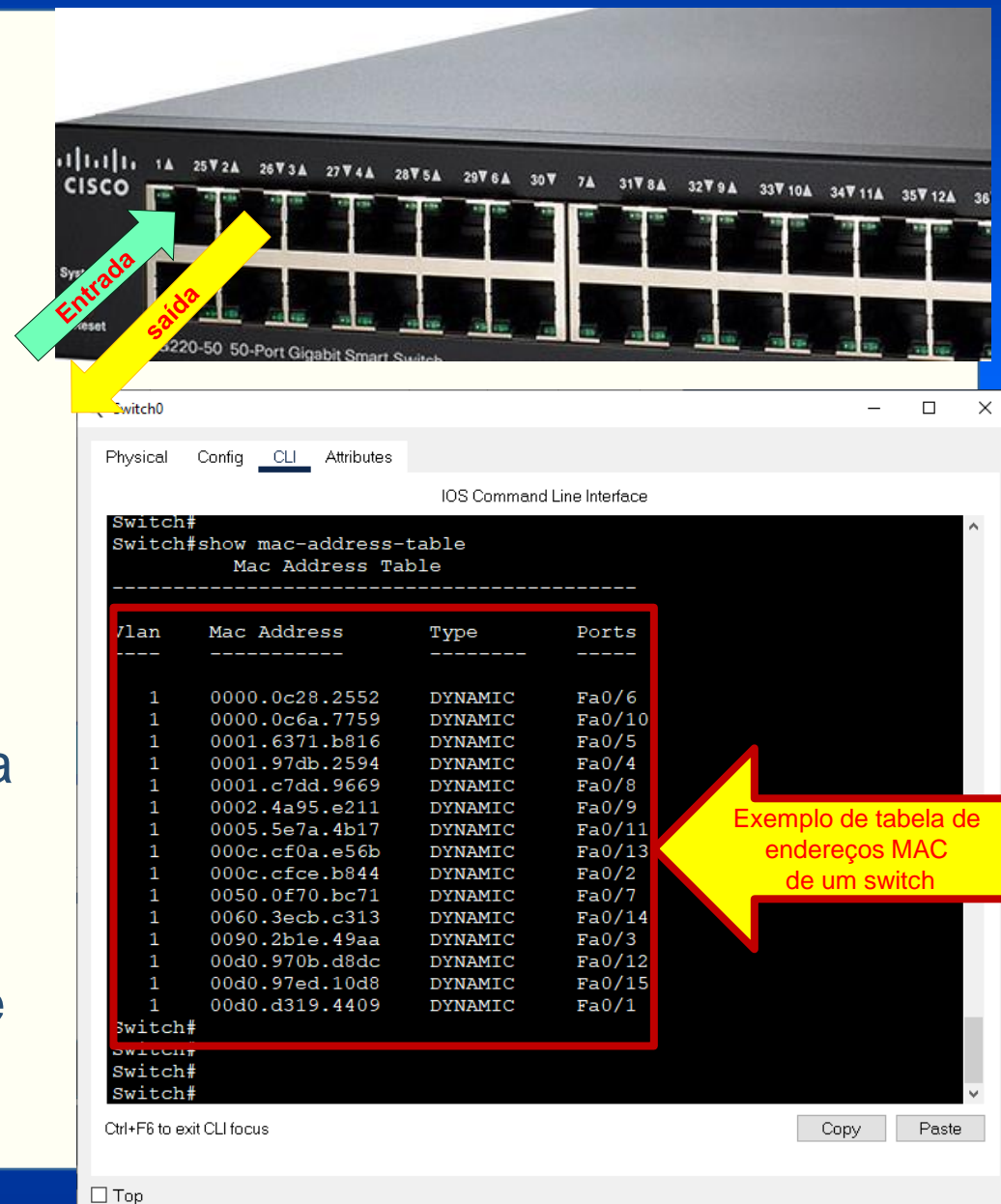
Copy Paste

Top



# Switching de encaminhamento de quadros na rede

- Dois termos são associados a quadros que entram ou saem de uma interface:
  - **entrada**: entrar pela interface no switch
  - **Saída**: sair pela interface no switch
- Um switch encaminha quadros Ethernet com base na interface de entrada e no endereço MAC de destino.
- Um switch usa sua **Tabela de endereços MAC** para tomar decisões de encaminhamento.
- **Observação**: um switch nunca permitirá que o tráfego seja encaminhado para fora da interface que recebeu o tráfego.



# O método de aprendizado e encaminhamento do switch

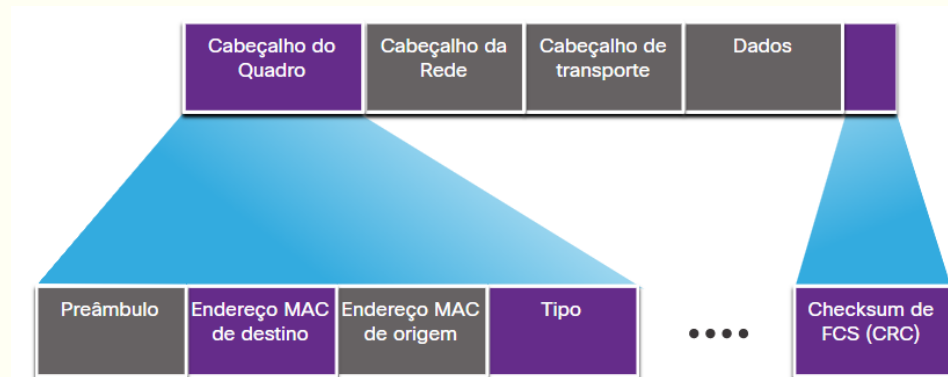
O switch usa um processo de duas etapas:

## Etapa 1. Aprender

- Examina o endereço de origem;
- Adiciona o MAC de origem se não estiver na tabela;
- Redefine a definição de tempo de intervalo para 5 minutos se a origem estiver na tabela

## Etapa 2. Encaminhar

- Examina o endereço de destino;
- Se o MAC de destino estiver na tabela de endereços MAC, ele será encaminhado para a porta especificada;
- Se um MAC de destino não estiver na tabela, ele será encaminhado a todas as interfaces, exceto a que foi recebida.





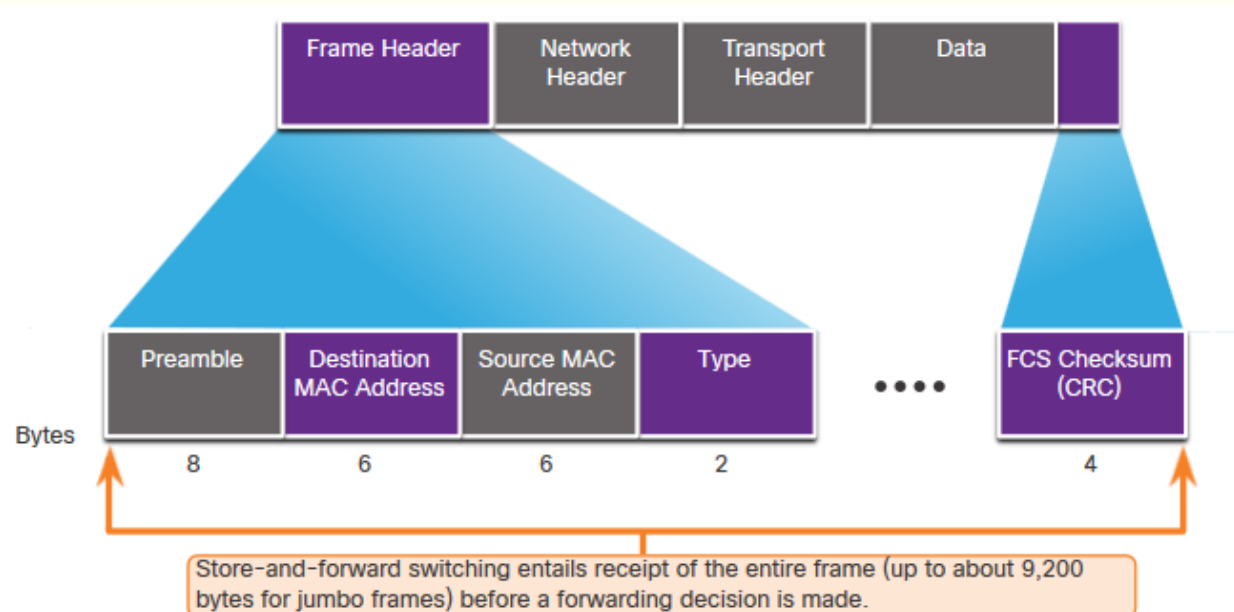
# Switch de encaminhamento de quadros

- Os switches usam software em circuitos integrados específicos de aplicativos (ASICs) para tomar decisões muito rápidas.
- Um switch usará um dos dois métodos para tomar decisões de encaminhamento depois de receber um quadro:
  - **Switching Store and Forward** - Recebe todo o quadro e garante que o quadro é válido. A comutação de armazenamento e encaminhamento é o método de comutação preferido da Cisco.
  - **Switching cut-through** — Encaminha o quadro imediatamente após determinar o endereço MAC de destino de um quadro de entrada e a porta de saída.

# Store-and-Forward Switching

**Store and Forward** tem duas características principais:

- **Verificação de erros** — O switch verificará a Sequência de Verificação de Quadro (FCS) para erros de CRC. Quadros ruins serão descartados.
- **Buffering** — A interface de entrada armazenará o porta-retratos enquanto verifica o FCS. Isso também permite que o switch se ajuste a uma diferença de potencial nas velocidades entre as portas de entrada e saída.

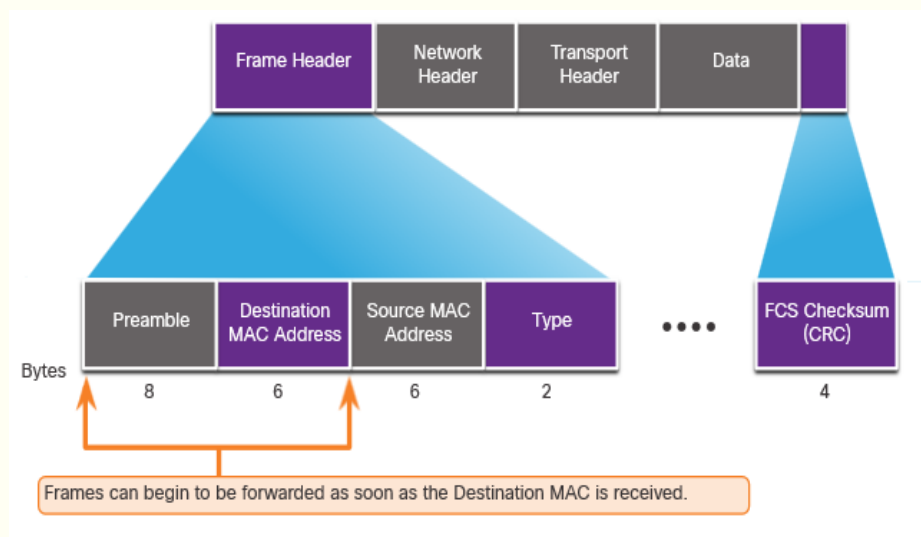


# Cut-Through Switching

O **Cut-Through** encaminha o quadro imediatamente após determinar o MAC de destino.

■ Conceitos de comutação **Cut-Through**:

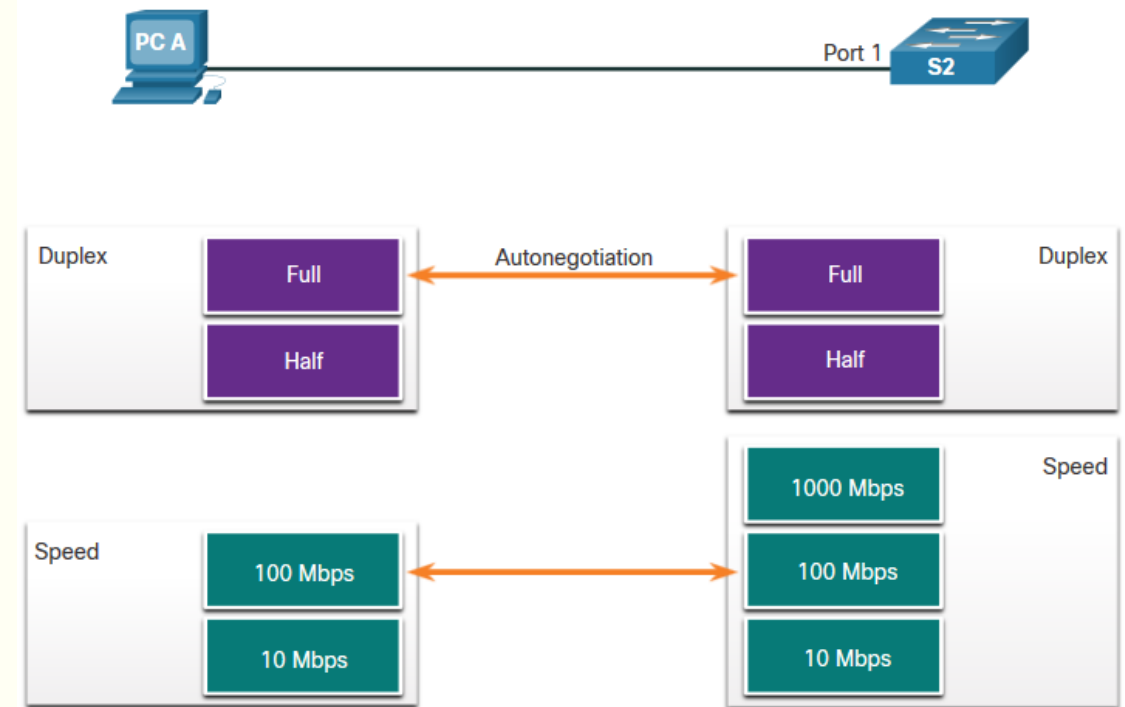
- É apropriado para switches que precisam de latência abaixo de 10 microssegundos
- Não verifica o FCS, para que ele possa propagar erros
- Pode levar a problemas de largura de banda se o switch propagar muitos erros
- Não é possível suportar portas com velocidades diferentes que vão da entrada à saída



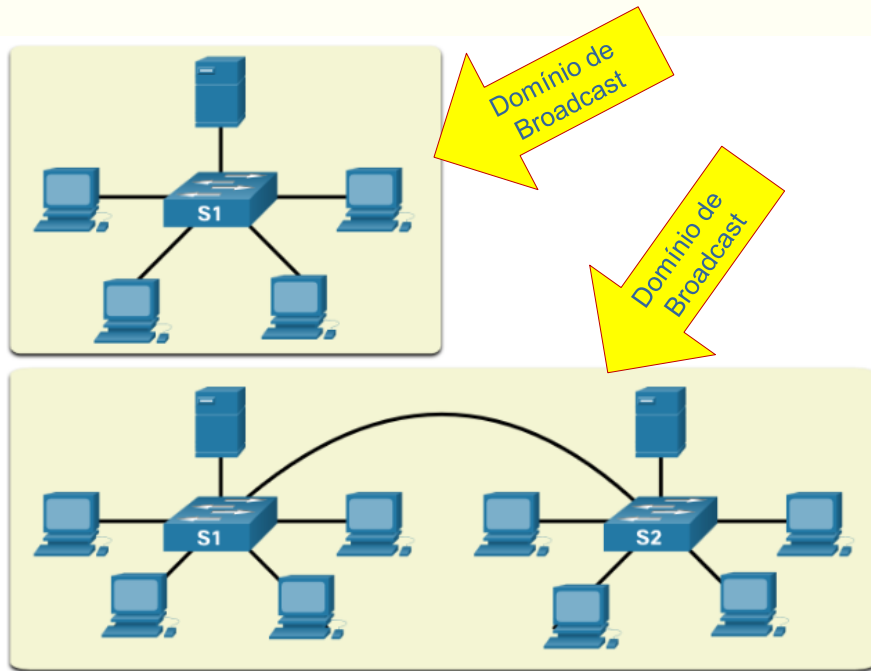
# Domínios de switching Domínios de colisão

Os switches eliminam domínios de colisão e reduzem o congestionamento

- Quando há *full duplex* no link, os domínios de colisão são eliminados.
- Quando houver um ou mais dispositivos em *half-duplex*, agora haverá um domínio de colisão.
  - Haverá agora disputa pela largura de banda.
  - Colisões agora são possíveis.
- A maioria dos dispositivos usam a negociação automática como configuração padrão para duplex e velocidade.



# Domínios de *Switching*: Domínios de broadcast



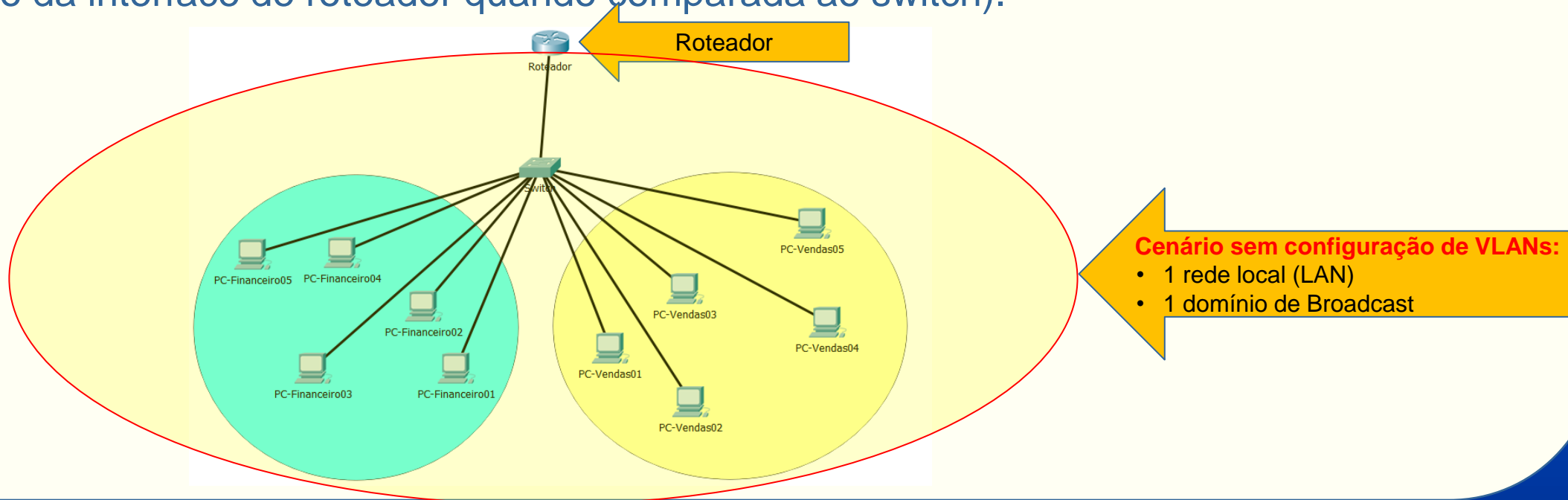
- Um domínio de *Broadcast* se estende por todos os dispositivos da Camada 1 ou da Camada 2 em uma LAN.
  - Somente um dispositivo de camada 3 (roteador) quebrará o domínio de broadcast, também chamado de domínio de difusão MAC.
  - O domínio de broadcast consiste em todos os dispositivos na LAN que recebem o tráfego de transmissão broadcast.
- Quando o switch de camada 2 receber a transmissão, ele encaminhará a todas as interfaces, exceto a interface de entrada.
- Muitas transmissões em broadcast podem causar congestionamento e desempenho de rede ruim.
- Aumentar os dispositivos na Camada 1 ou na Camada 2 fará com que o domínio de broadcast se expanda.

# VLAN

*(Virtual Local Area Network - Vlan)*

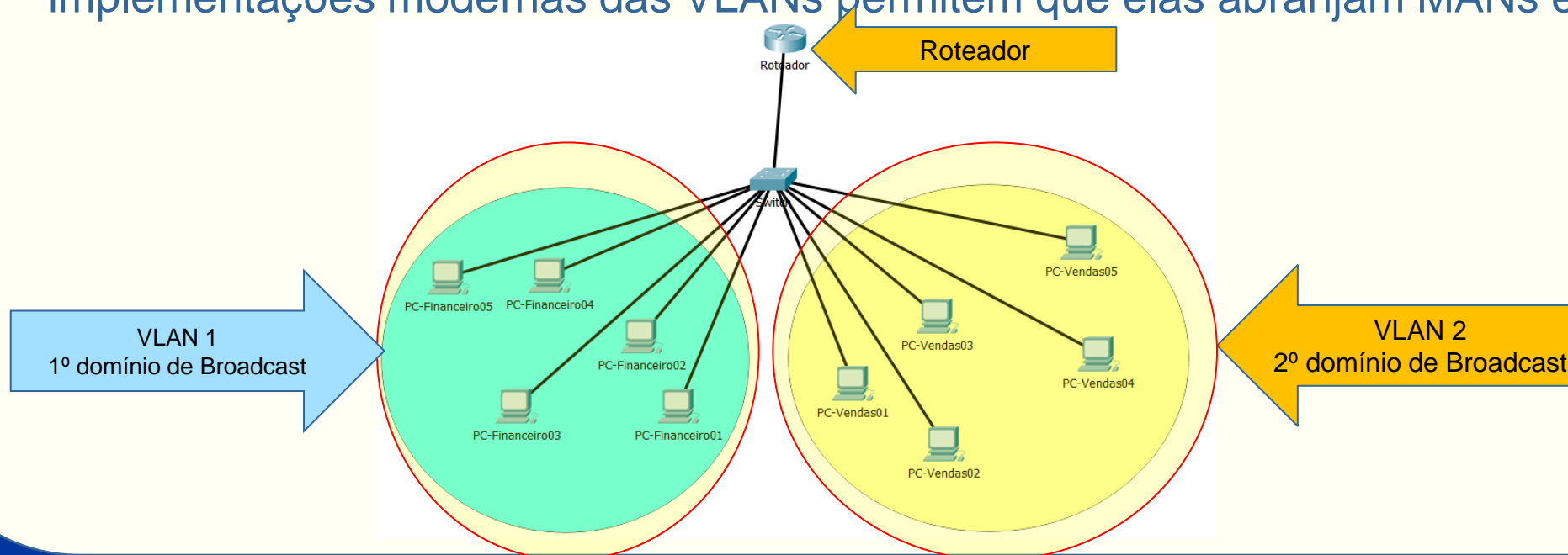
# Virtual Local Area Network - VLAN

- Uma das tecnologias usadas para **melhorar o desempenho** da rede é a **separação de grandes domínios de broadcast em domínios menores**.
- Apesar de **roteadores** bloquearem o tráfego de broadcast em uma interface, eles têm um **número limitado de interfaces de LAN**.
- A função principal de um **roteador** é **transferir informações entre redes**, e **não fornecer acesso à rede para dispositivos finais** (o que elevaria os custos de uma rede local em função do custo elevado da interface de roteador quando comparada ao switch).



# Virtual Local Area Network - VLAN

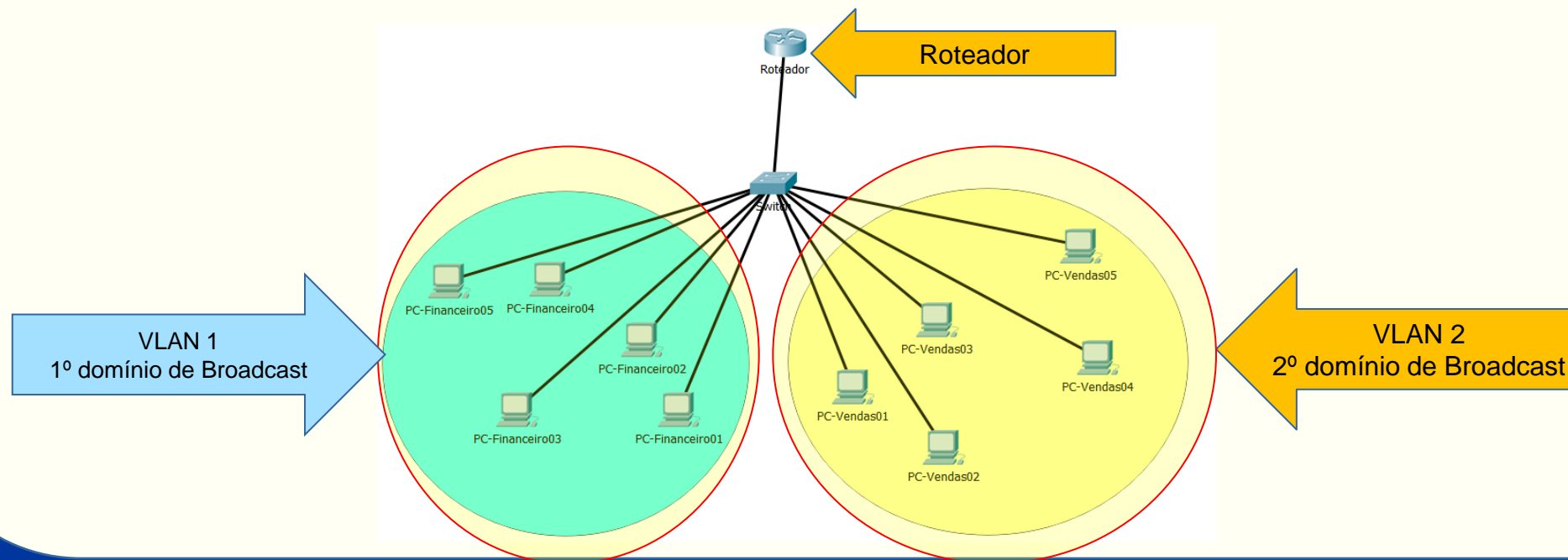
- Uma rede local virtual (VLAN, do inglês *Virtual Local Area Network*) pode ser criada em um switch de camada 2 para reduzir o tamanho dos domínios de broadcast, semelhante a um dispositivo da camada 3.
- As VLANs são incorporadas geralmente no projeto da rede. Com isso, é mais fácil a rede auxiliar os objetivos de uma empresa.
- Embora as VLANs sejam usadas principalmente nas redes locais comutadas, as implementações modernas das VLANs permitem que elas abranjam MANs e WANs.





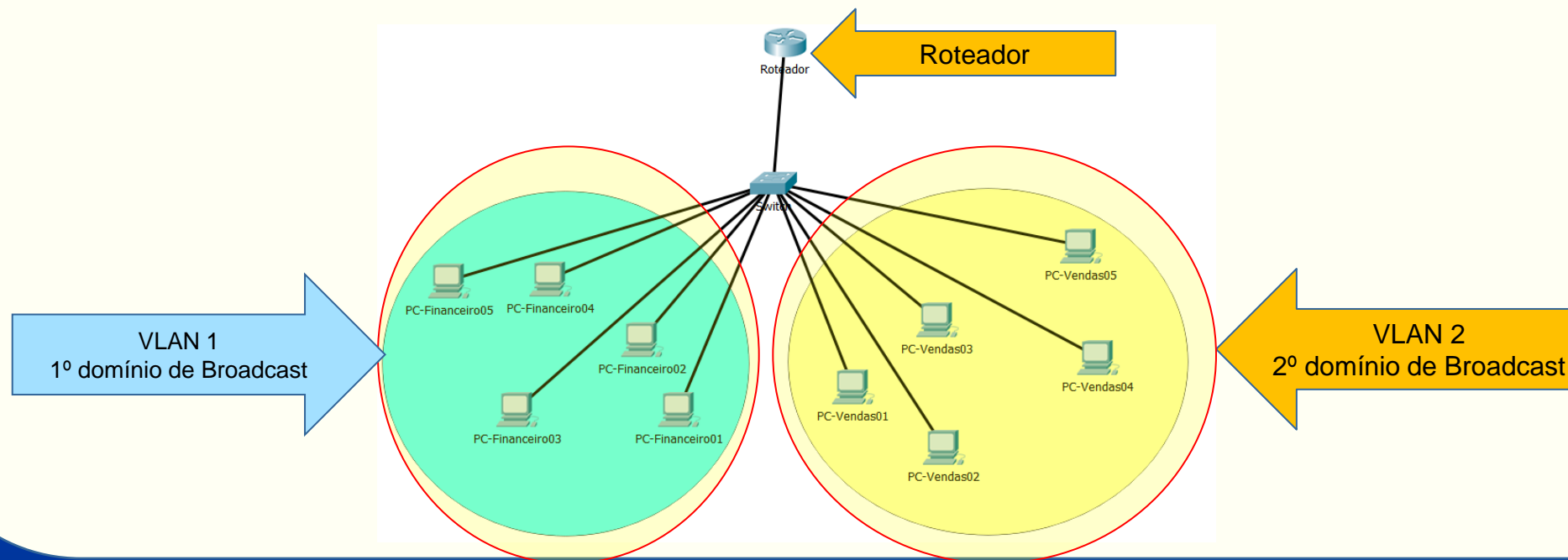
# Virtual Local Area Network - VLAN

- Como as VLANs segmentam a rede, um processo de Camada 3 é necessário para permitir que o tráfego mude de um segmento de rede para outro.
- Esse processo de roteamento na Camada 3 pode ser implementado usando um roteador ou uma interface de um switch Camada 3. A utilização de um dispositivo de Camada 3 fornece um método para controlar o fluxo de tráfego entre segmentos da rede, incluindo os segmentos de rede criados por VLANs.



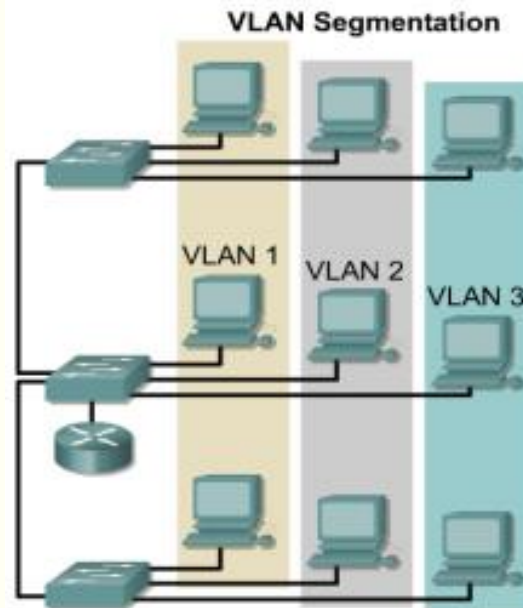
# Virtual Local Area Network - VLAN

- Na aula de hoje abordaremos como configurar, gerenciar e solucionar problemas de VLANs e troncos de VLAN.
- Na próxima aula estudaremos a implementação de roteamento entre VLANs com um roteador.



# *Virtual Local Area Network - VLAN*

- Uma **rede local virtual**, comumente chamada de **VLAN (*Virtual Local Area Network*)**, é uma rede logicamente independente.
- Várias VLANs podem coexistir em um mesmo **switch** de forma a dividir uma rede local (física) em mais de uma rede (virtual), criando diferentes **domínios de broadcast**.
- Uma VLAN também torna possível colocar em um mesmo domínio de broadcast, hosts com localizações físicas distintas e ligados a switches diferentes, como na figura a seguir.



# VLAN

- Um outro propósito de uma rede virtual é restringir acesso a recursos de rede sem considerar a topologia da rede, (porém este método é questionável e improvável).
- Redes virtuais operam na camada 2 do modelo OSI.
- No entanto, uma VLAN geralmente é configurada para mapear diretamente uma rede ou sub-rede IP, o que dá a impressão que a camada 3 está envolvida.
- As Ligações **switch-a-switch** e **switch-a-roteador** são chamadas de ligações **trancos**.
- Um roteador ou switch de camada 3 serve como o backbone entre o tráfego que passa através de VLANs diferentes

# VLAN

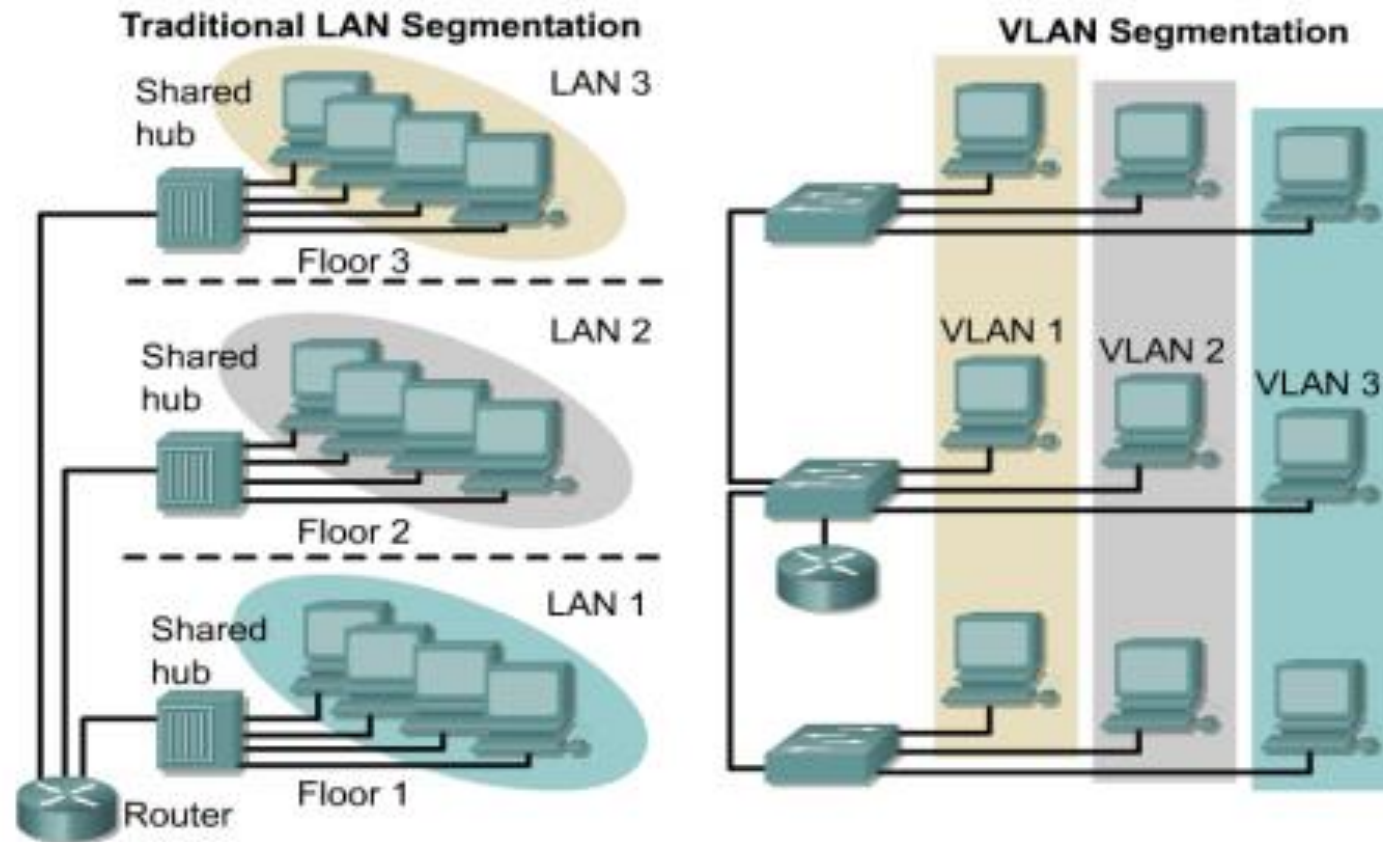
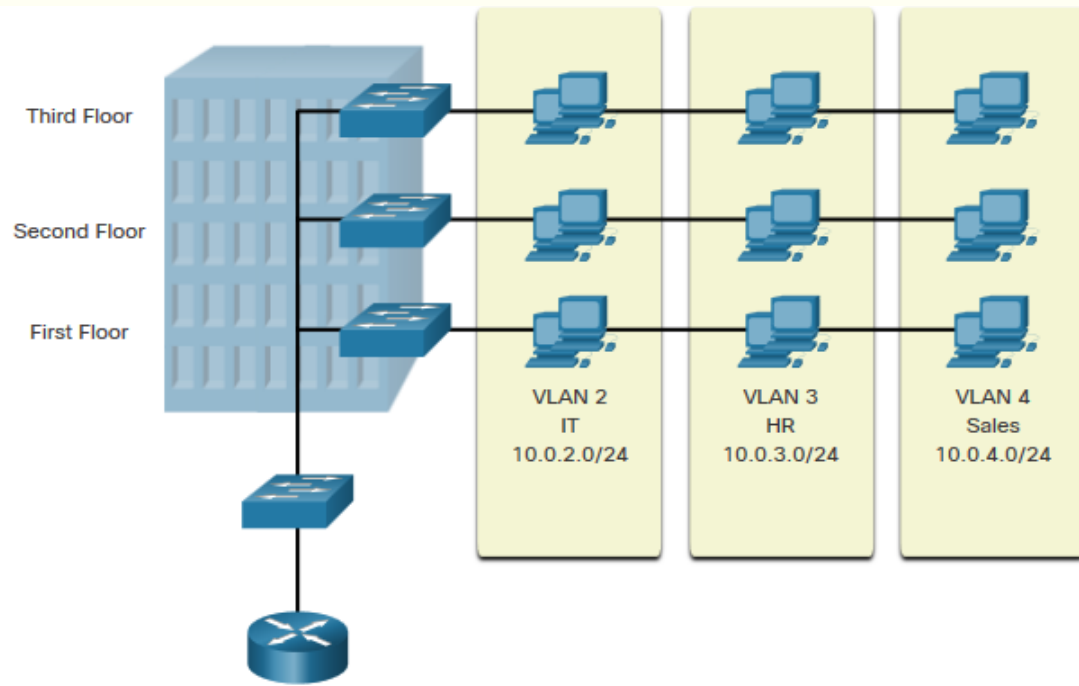


Figura 1 — Segmentação da rede com base na localização física (tradicional) ou em critérios lógicos (VLAN)

# VLAN



- VLANs são conexões lógicas com outros dispositivos semelhantes.
- A colocação de dispositivos em várias VLANs tem as seguintes características:
  - Fornece segmentação dos vários grupos de dispositivos nos mesmos switches
  - Fornecer uma organização mais gerenciável
    - Transmissões, multicasts e unicasts são isolados na VLAN individual
    - Cada VLAN terá seu próprio endereço de rede (sua própria faixa exclusiva de endereçamento IP)
    - Domínios de broadcast menores

# VLAN e Broadcast

- Todos os dispositivos de uma VLAN (*Virtual Local Area Network*) são membros do **mesmo domínio de *broadcast***, se um *host* transmitir um *broadcast* todos os dispositivos membros da VLAN receberão o *broadcast*.
- Uma VLAN é uma “subrede” ou segmento lógico formado por determinados membros.
- Dispositivos podem estar em qualquer ponto do bloco de switch, para isso é necessário um roteador para fazer a comunicação entre as VLANs.

# VLAN e Broadcast

- Os switches usando VLANs criam a mesma divisão da rede em domínios de broadcast separados;
- Com isso, um objetivo de implementação de uso de VLANs é, portanto, a diminuição do número de *broadcast* em uma rede local.
- Assim com o uso de switches torna-se uma solução de baixo custo para este propósito.



# Métodos de Configuração VLAN

- Redes virtuais podem ser configuradas de várias formas:
  - Nível do protocolo, IP, IPX, LAT, etc.
  - Baseada no endereço MAC.
  - Baseada na sub-rede IP.
  - Baseada na porta do *switch*, e portanto, baseada no mundo real, como em departamento de marketing versus finanças.

# Métodos de Configuração VLAN

## VLAN padrão (VLAN Default)

A VLAN 1 é uma default em switches e NÃO poderá ser excluída ou renomeada

```
Switch# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, 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 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

# Tipos de VLANs

## Data VLAN

- Dedicado ao tráfego gerado pelo usuário (e-mail e tráfego da web).
- A VLAN 1 é a VLAN de dados padrão porque todas as interfaces são atribuídas a essa VLAN.

## VLAN nativa

- Isso é usado somente para links de tronco.
- Todos os quadros são marcados em um link de tronco 802.1Q, exceto aqueles na VLAN nativa.

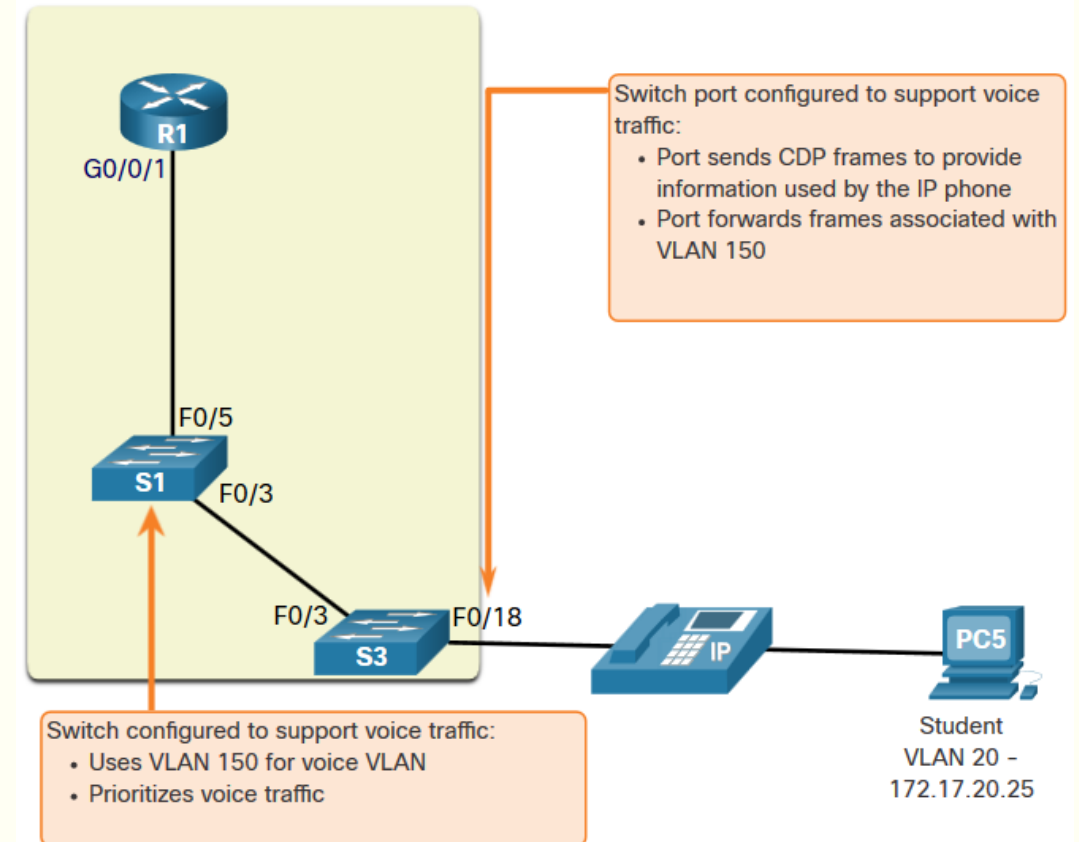
## VLAN de gerência

- Isso é usado para tráfego SSH/Telnet VTY e não deve ser transportado com tráfego de usuário final.
- Normalmente, a VLAN que é o SVI para o switch da Camada 2.

# Tipos de VLANs (cont.)

## VLAN de Voz

- Uma VLAN separada é necessária porque o tráfego de voz requer:
  - Garantia de largura de banda
  - High QoS priority
  - Capacidade de evitar congestionamentos
  - Atrasar menos que 150 ms da origem para o destino
- Toda a rede deve ser projetada para suportar voz.



# Configuração VLAN baseada em portas

- O mecanismo mais básico das VLAN consiste na atribuição de cada uma das portas do *switch* a uma dada VLAN, de modo a que haja comunicação direta apenas entre portas pertencentes à mesma VLAN.
- Pacotes recebidos pelo host em uma porta pertencente a uma VLAN, mesmo que sejam de *broadcast*, nunca são retransmitidos para portas pertencentes a VLANs diferentes (ou seja, cada VLAN é um domínio de *broadcast independente*).

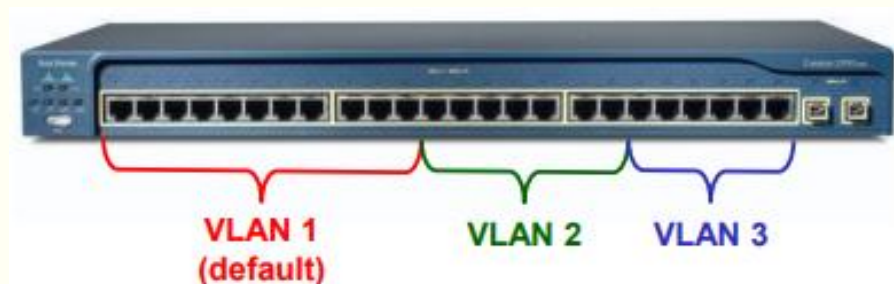


Figura 2 — Atribuição de portas físicas a diferentes VLAN

# Configuração VLAN baseada em portas

- A atribuição de uma porta (física) do comutador a uma dada VLAN pode ser feita através de configuração (VLAN estáticas), ou então de forma automática (VLAN dinâmicas).
- No segundo caso, a atribuição de uma porta a uma VLAN pode fazer-se com base em critérios como o endereço MAC da máquina ligada nessa porta (critério de camada 2), do seu endereço IP (critério de camada 3), ou ainda por autenticação através do protocolo 802.1x.

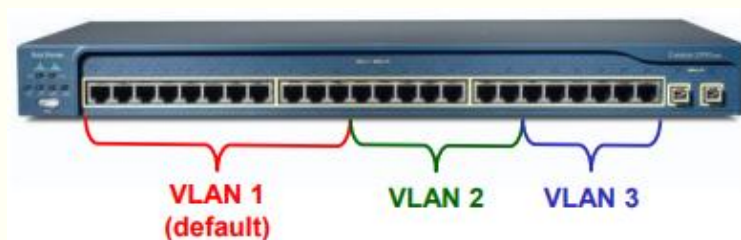
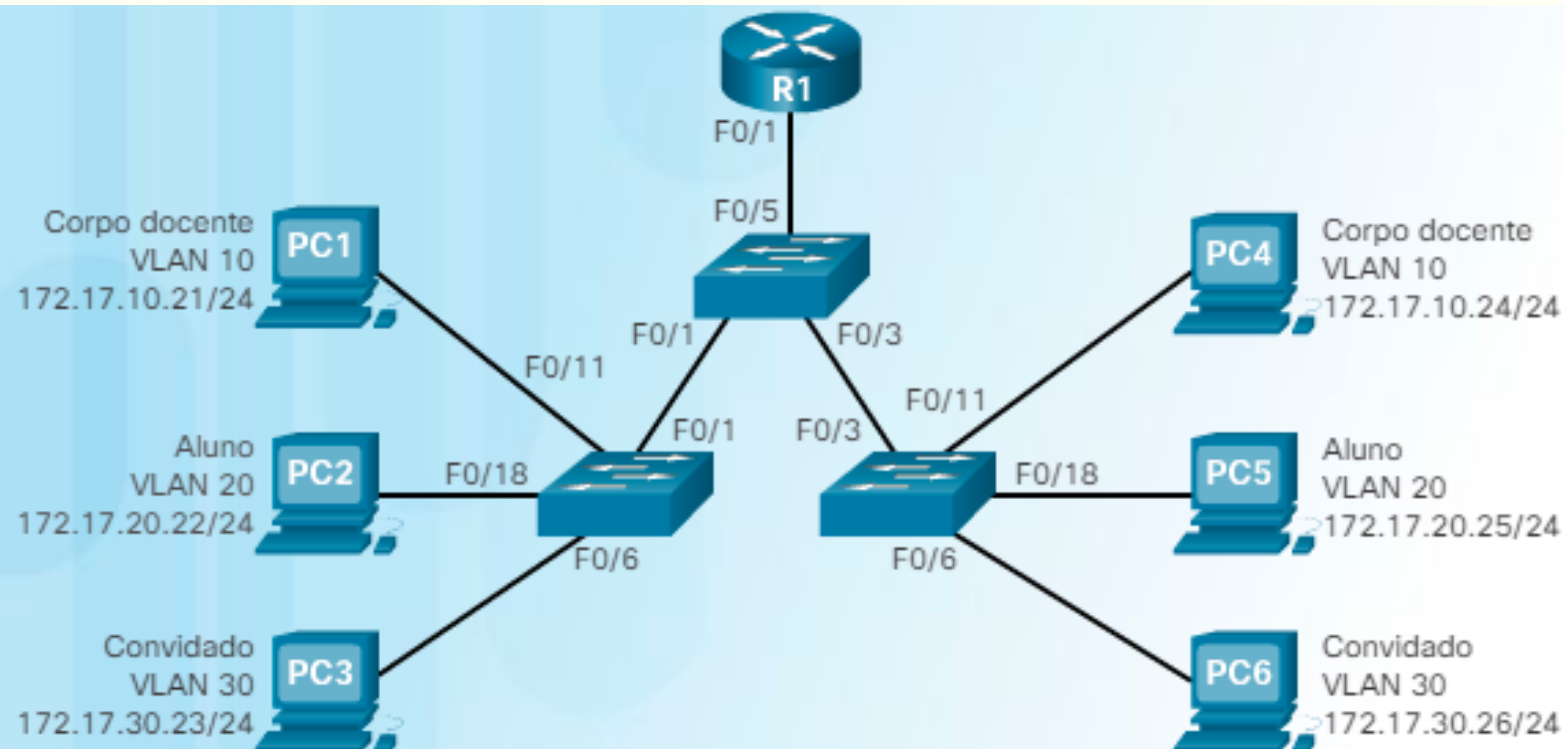


Figura 2 — Atribuição de portas físicas a diferentes VLAN

# VLAN: Resumo

- Criado em software, nos switches, na camada 2;
- Divide uma rede LAN em segmentos (VLAN), em agrupamentos definidos pelo administrador;
- Cada VLAN será uma nova rede LAN, exigindo um endereço de rede específico
- Cada VLAN será um domínio de broadcast (broadcasts ficam confinados no segmento)
- Usuários na mesma VLAN estão contidos no mesmo domínio de broadcast;
- Como cada VLAN é uma rede distinta, o tráfego entre VLANs deve passar necessariamente por um roteador, camada 3.

# Benefícios de VLAN



- Maior segurança
- Custo reduzido
- Melhor desempenho
- Domínios de transmissão menores
- Eficiência de TI
- Eficiência de gerenciamento
- Projeto e gerenciamento de aplicativos mais simples

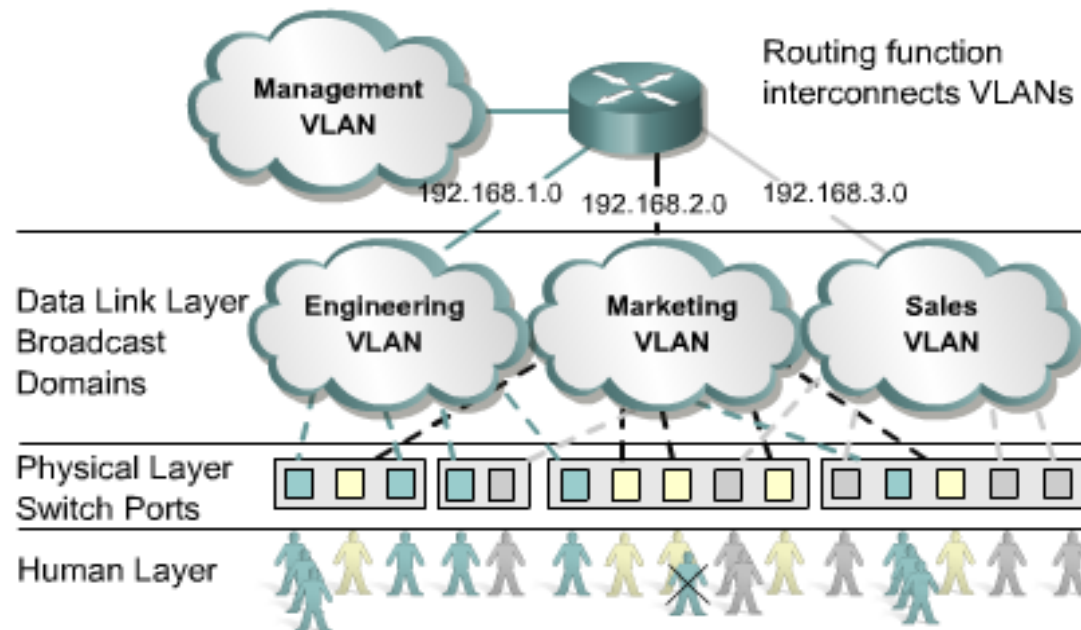


# Benefícios de VLAN

Vantagens	Descrição
Diminui o tamanho do domínio de Broadcast	Dividir a LAN reduz o tamanho de domínios de broadcast (quantos menores os domínios de broadcast, maior o desempenho)
Melhora de segurança	Somente usuários na mesma VLAN podem se comunicar juntos
Melhora da Eficiência	As VLANs podem agrupar dispositivos com requisitos semelhantes, por exemplo, em uma universidade: corpo docente, administrativo e alunos
Custo reduzido	Um switch pode suportar vários grupos ou VLANs
Melhor desempenho	Pequenos domínios de difusão reduzem o tráfego, melhorando a largura de banda
Simplificar o gerenciamento da rede	Grupos semelhantes precisarão de aplicativos semelhantes e outros recursos de rede

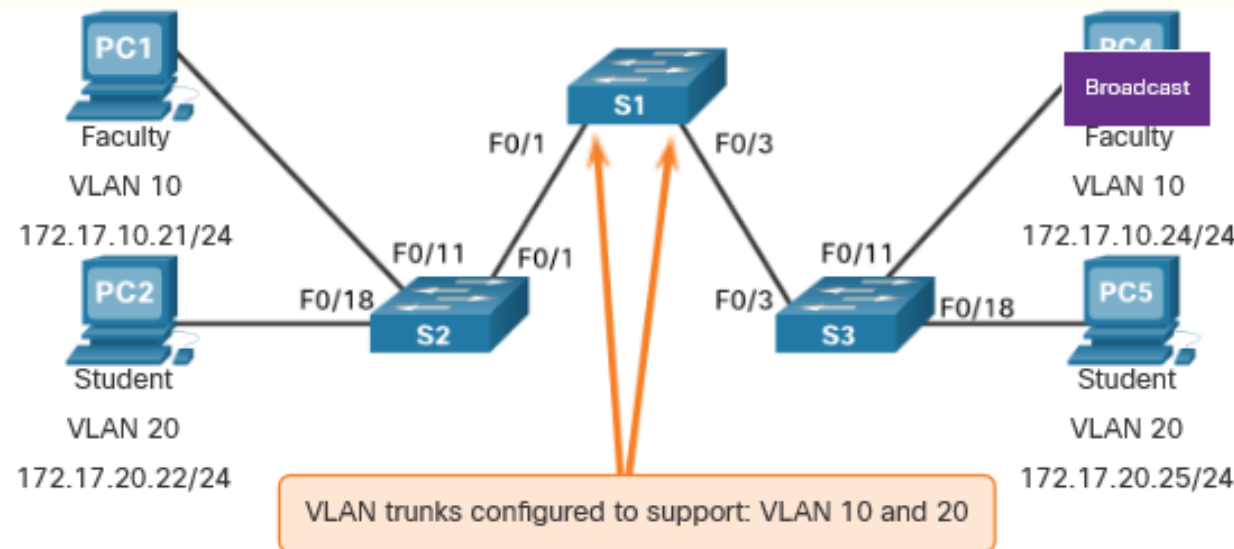
# Mais Benefícios de VLAN

- **Benefícios em relação a implementação de VLANs:**
  - Redução do tamanho e o aumento do número de broadcast;
  - Agrupamento lógico de usuários e de recursos conectados em portas administrativamente definidas no switch;
  - Aumento das opções de segurança;
  - Flexibilidade e escalabilidade no controle de tráfego da rede.



# Redes grandes com VLANs

- Com VLANs, o tráfego unicast, multicast e broadcast é confinado a uma VLAN. S
- em um dispositivo de camada 3 para conectar as VLANs, os dispositivos em VLANs diferentes não podem se comunicar.



**VLAN**

**Portas *Trunk* (tronco)**

# Portas *Trunk*

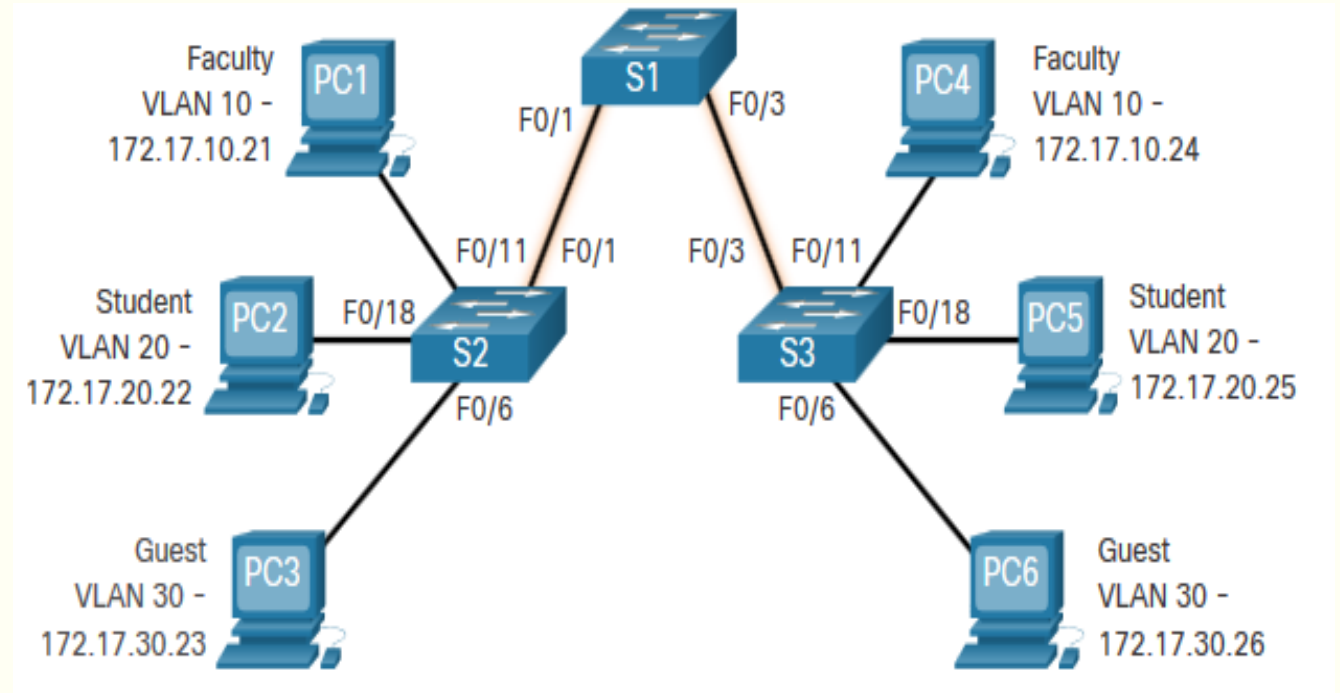
- **Porta *Trunk*:**
  - Porta que carrega o tráfego de múltiplas VLANs e pertence por default a todas as VLANs da database (tabela com as VLANs e informações referentes a elas) do switch.
- **Portas *Trunk* 802.1Q**
  - Portas *trunk* 802.1Q (padrão do IEEE) aceitam tráfego com e sem tag.
    - Caso um frame receba um tag, será encaminhado para a VLAN referida.
    - Se um pacote chegar sem *tag* à porta *trunk* ele será encaminhado para a VLAN default (por padrão é a VLAN 1, mas pode ser definida pelo usuário).

# VLANs in a Multi-Switched Environment: VLAN Trunks

Um tronco é um link ponto a ponto entre dois dispositivos de rede.

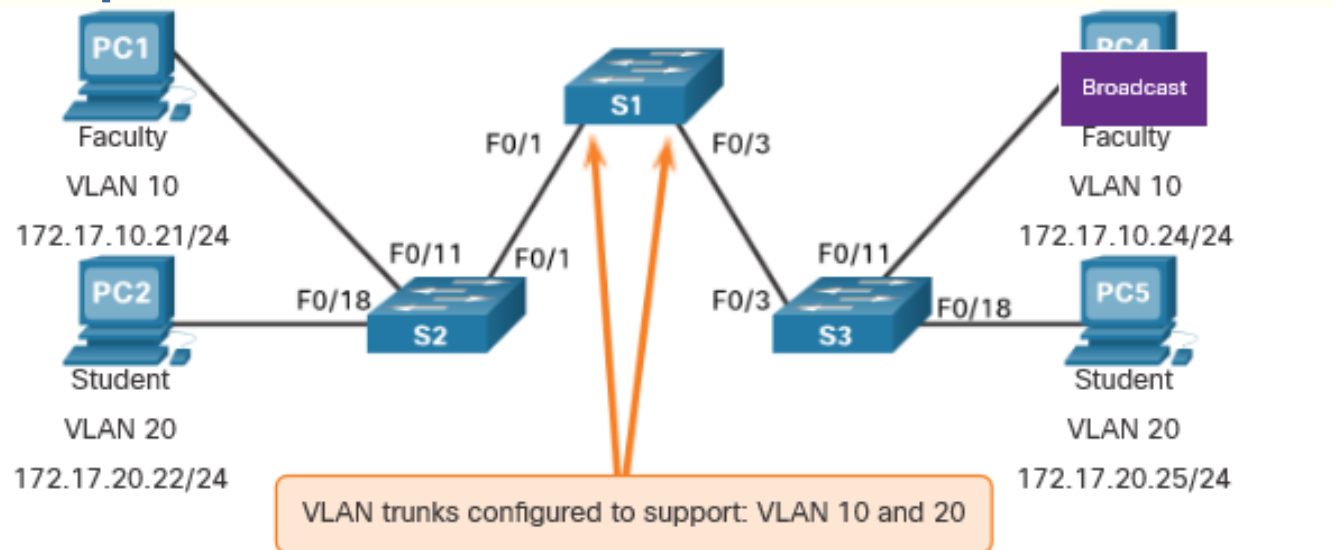
Funções de tronco Cisco:

- Permitir mais de uma VLAN
- Estenda a VLAN em toda a rede
- Por padrão, suporta todas as VLANs
- Suporta entroncamento 802.1Q



# VLANs in a Multi-Switched Environment: VLAN Trunks

- Com VLANs, o tráfego unicast, multicast e broadcast é confinado a uma VLAN.
- Sem um dispositivo de camada 3 para conectar as VLANs, os dispositivos em VLANs diferentes não podem se comunicar.



PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

# Exemplo de configuração de portas Trunk em Vlan

As sub-redes associadas a cada VLAN são:

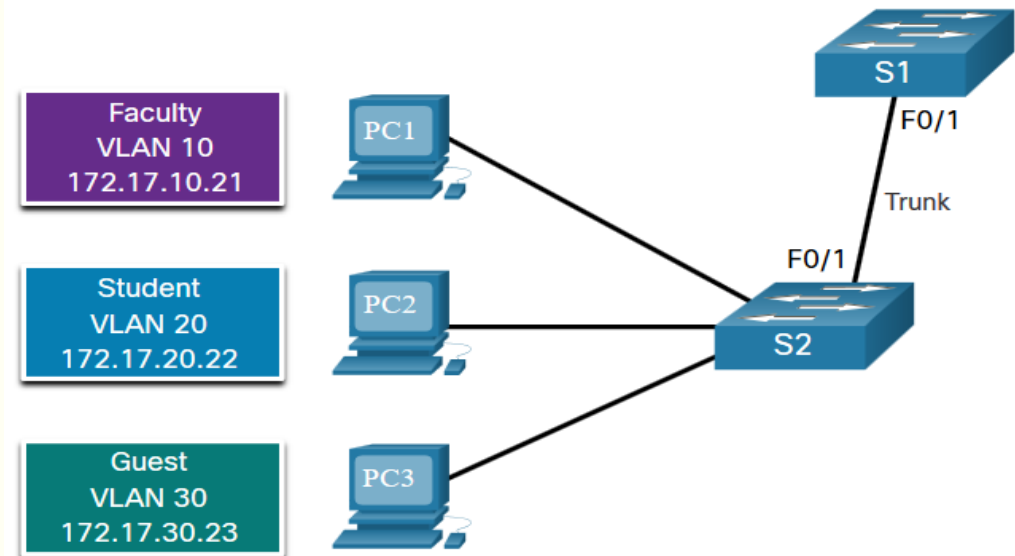
⇒ VLAN 10 - Faculty/Staff - 172.17.10.0/24

⇒ VLAN 20 - Estudantes - 172.17.20.0/24

⇒ VLAN 30 - Convidado - 172.17.30.0/24

⇒ VLAN 99 - Nativo - 172.17.99.0/24

- A porta F0/1 em S1 está configurada como uma porta de tronco.
- **Observação:** Isso pressupõe que o Switch S1 usa a marcação 802.1q.
- Os switches de camada 3 exigem que o encapsulamento seja configurado antes do modo de tronco.



Prompt	Comando
S1 (config) #	Interface fa0/1
S1 (config-if) #	Switchport mode trunk
S1 (config-if) #	Switchport trunk native vlan 99
S1 (config-if) #	Switchport trunk allowed vlan 10,20,30,99
S1 (config-if) #	end



# Configurando VLANs

*(Virtual Local Area Network - Vlan)*

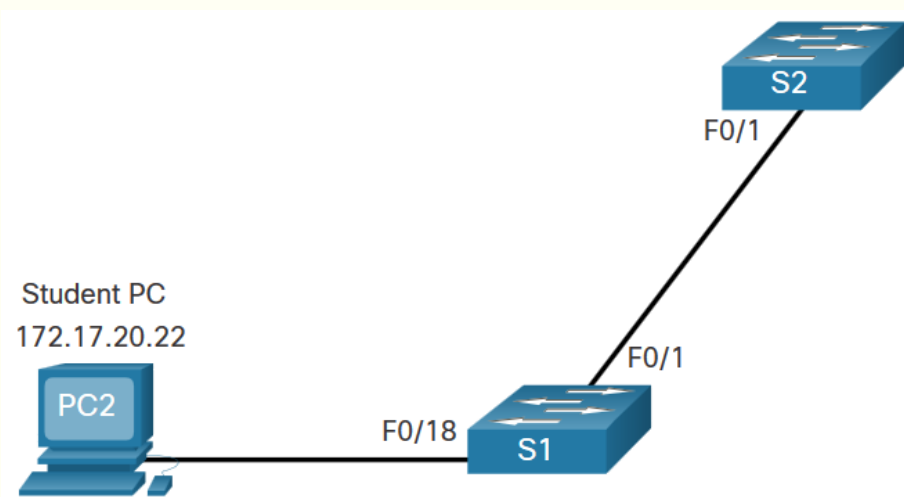
# Comandos de criação de VLAN

VLANs são configuradas no modo de configuração global  
(**configure terminal**)

Tarefa	Comando IOS
Entre no modo de configuração global.	Switch# <code>configure terminal</code>
Crie uma VLAN com um ID válido.	Switch(config)# <code>vlan vlan-id</code>
Especifique um nome exclusivo para identificar a VLAN.	Switch(config-vlan)# <code>name vlan-name</code>
Volte para o modo EXEC privilegiado.	Switch (config-vlan) # <code>end</code>
Entre no modo de configuração global.	Switch# <code>configure terminal</code>

# Exemplo de criação de VLAN

- Para mover o PC *Student* para uma VLAN 20, cria-se a VLAN primeiro e, em seguida, define-se um nome para ela.
- Se não for criado um nome, o IOS fornecerá um nome padrão de vlan com um número de quatro dígitos da VLAN. Por exemplo, vlan0020 para VLAN 20.



Prompt no switch	Comando
S1#	configure terminal
S1 (config) #	vlan 20
S1 (config-vlan) #	name student
S1 (config-vlan) #	end

# Comandos de atribuição de porta VLAN

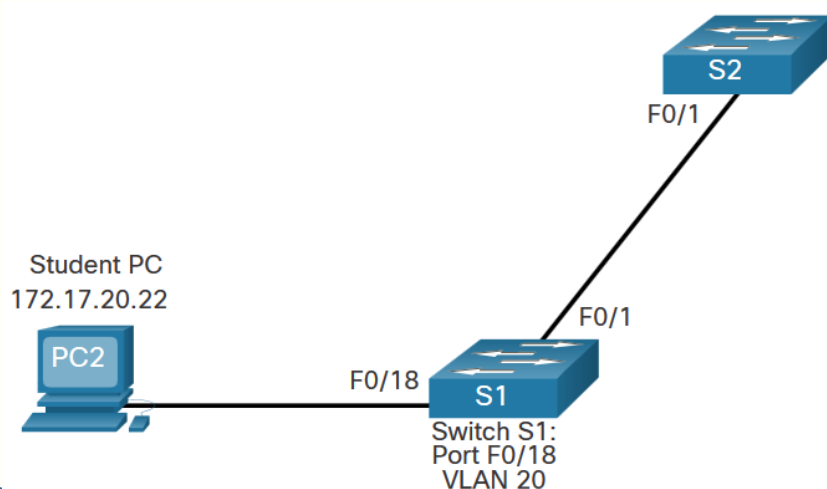
Uma vez que a VLAN é criada, podemos então atribuí-la às interfaces corretas.

Tarefa	Comando
Entre no modo de configuração global.	<code>Switch# configure terminal</code>
Entre no modo de configuração da interface.	<code>Switch(config)# interface <i>interface-id</i></code>
Configure a porta para o modo de acesso.	<code>Switch(config-if)# switchport mode access</code>
Atribua a porta a uma VLAN.	<code>Switch(config-if)# switchport access vlan <i>vlan-id</i></code>
Volte para o modo EXEC privilegiado.	<code>Switch(config-if)# end</code>

# Exemplo de associação de Portas a uma VLAN

Devemos associar uma interface do Switch a uma VLAN criada

- Assim que o dispositivo receber a VLAN, o dispositivo final precisará das informações de endereço IP para essa VLAN
- Aqui, Student PC recebe 172.17.20.22



Prompt	Comando
S1#	<code>configure terminal</code>
S1 (config) #	<code>Interface fa0/18</code>
S1 (config-if) #	<code>Switchport mode access</code>
S1 (config-if) #	<code>Switchport access vlan 20</code>
S1 (config-if) #	<code>end</code>

# Verificação das informações de configuração de uma VLAN

Use o comando `show vlan`. A sintaxe completa é:

`show vlan [brief | id vlan-id | name vlan-name | summary]`

```
S1# show interface vlan 20
Vlan20 is up, line protocol is up
  Hardware is EtherSVI, address is 001f.6ddb.3ec1 (bia 001f.6ddb.3ec1)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set

(Output omitted)
```

```
S1# show vlan summary
Number of existing VLANs           : 7
Number of existing VTP VLANs       : 7
Number of existing extended VLANs  : 0
```

Tarefa	Command Option
Display VLAN name, status, and its ports one VLAN per line.	<code>brief</code>
Display information about the identified VLAN ID number.	<code>id vlan-id</code>
Display information about the identified VLAN name. The <i>vlan-name</i> is an ASCII string from 1 to 32 characters.	<code>name vlan-name</code>
Exiba informações de resumo da VLAN.	<code>resumo</code>

# Associação da porta VLAN de alteração da configuração da VLAN

Há várias maneiras de alterar a associação à VLAN:

- Utilizar o comando **switchport access vlan vlan-id**
- usar a vlan sem switchport access para colocar a interface de volta na VLAN 1

Usar os comandos show vlan brief ou show interface fa0/18 switchport para verificar a associação de VLAN correta.

```
S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, 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 Gi0/1, Gi0/2
20	student	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

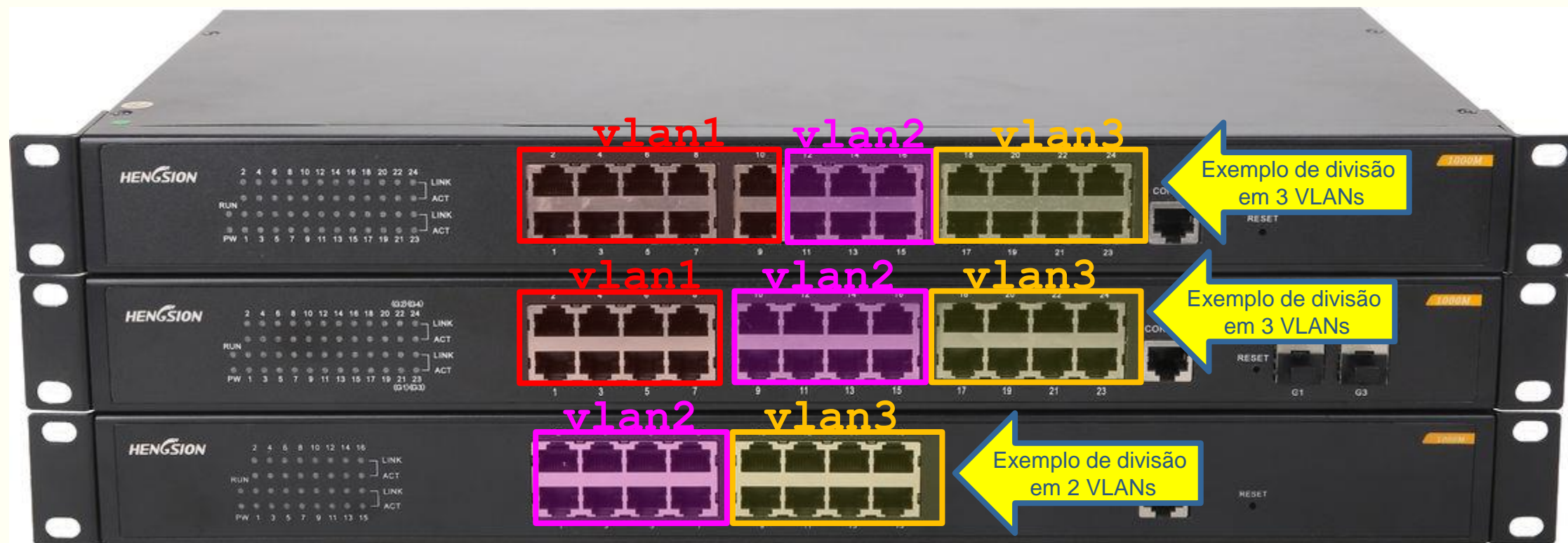
```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

# Configuração de VLAN: Excluir VLANs

- Exclua VLANs com o comando: `no vlan vlan-id`
- Exclua todas as VLANs com os comandos `delete flash:vlan.dat` ou `delete vlan.dat`.
- Reinicie o switch (ou recarregue a configuração) ao excluir todas as VLANs.



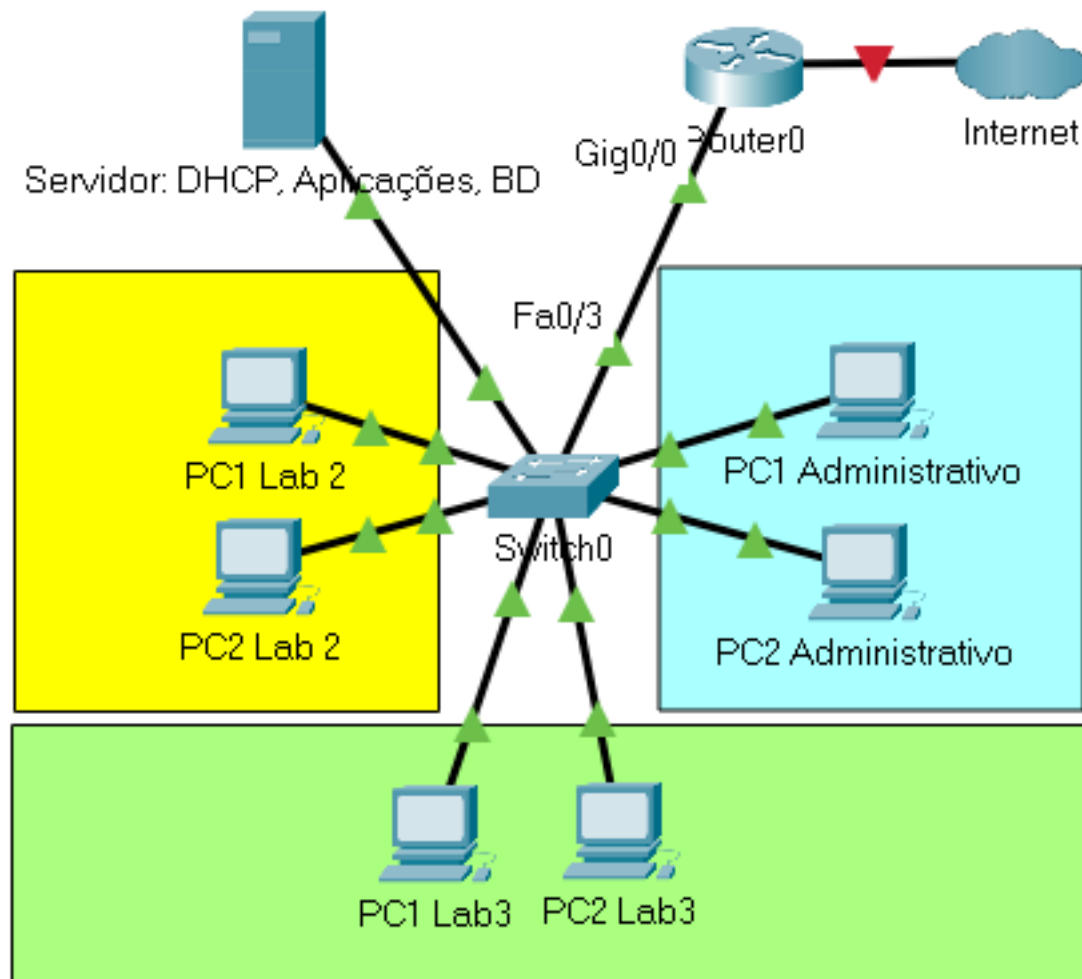
# Configuração VLAN



**Preparação para Atividade Prática:**

**Analise os cenários**

# Analise a topologia: **Passo 1**



Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch>
Switch>
Switch>
Switch>
Switch>
Switch>show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, 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 Gig0/1, Gig0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Switch>  
Switch>  
Switch>  
Switch>  
Switch>

Ctrl+F6 to exit CLI focus

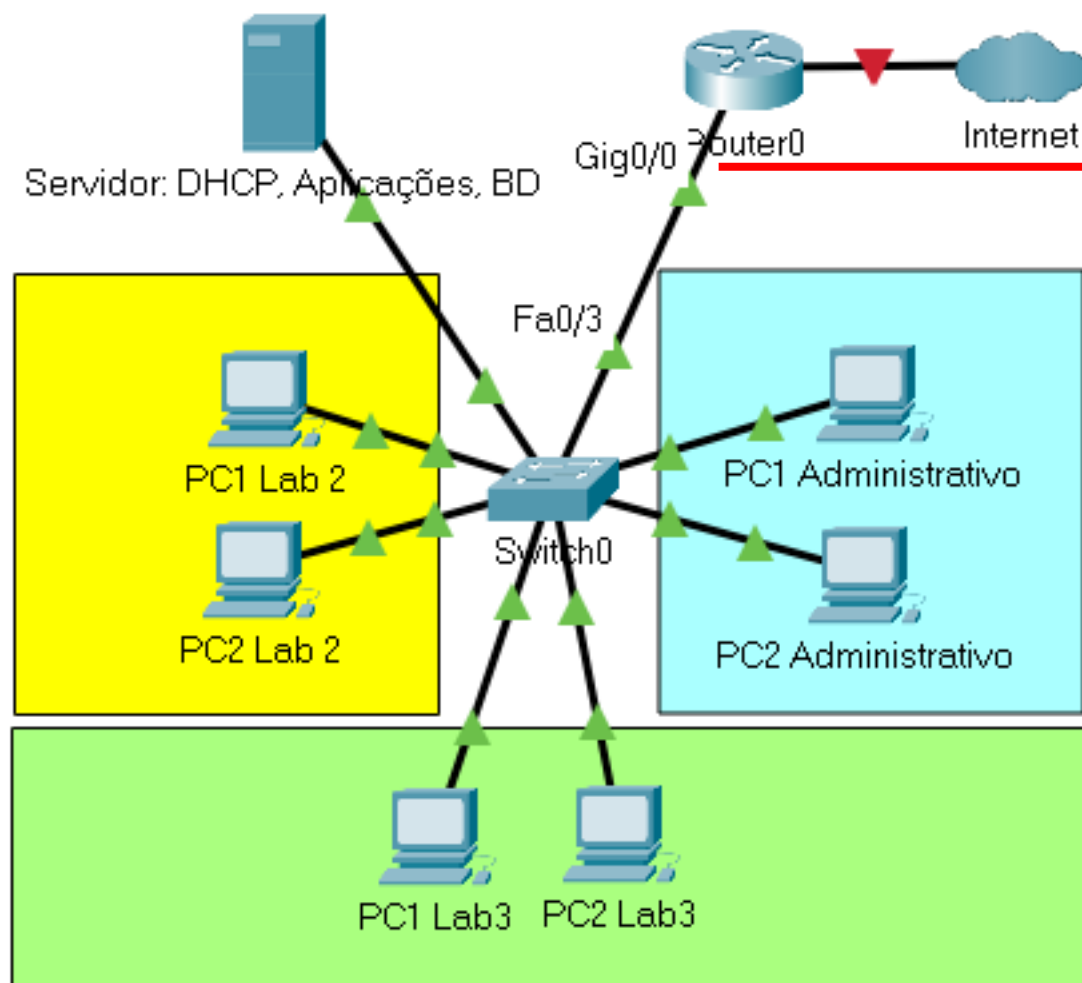
Copy Paste

☐ Top

**Default:** Todas as interfaces do Switch0 em uma única VLAN: Vlan1

Arquivo: Aula 02 2023 VLAN.pkt

# Analise a topologia: **Passo 2**



## **IMPORTANTE:**

Até o momento todos os equipamentos estão em um único domínio de broadcast, com todos os equipamentos no mesmo endereço de rede, compartilhando o mesmo gateway:

**Rede:** 192.168.1.0

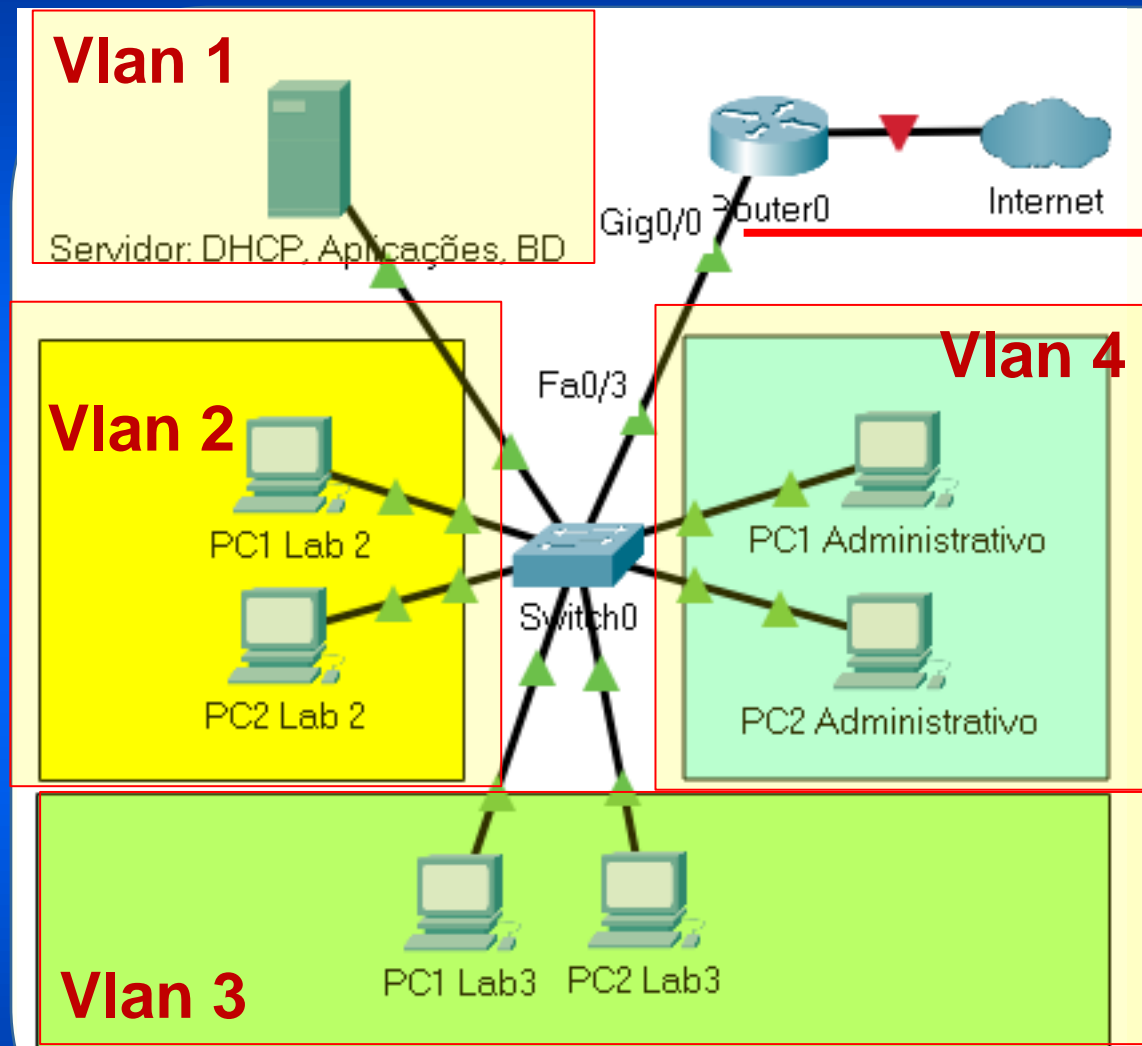
**Máscara:** 255.255.255.0

**Broadcast:** 192.168.1.255

**Gateway:** 192.168.1.1

**Até aqui temos um  
ÚNICO DOMÍNIO DE BROADCAST**

## Analise a topologia: **Passo 3**



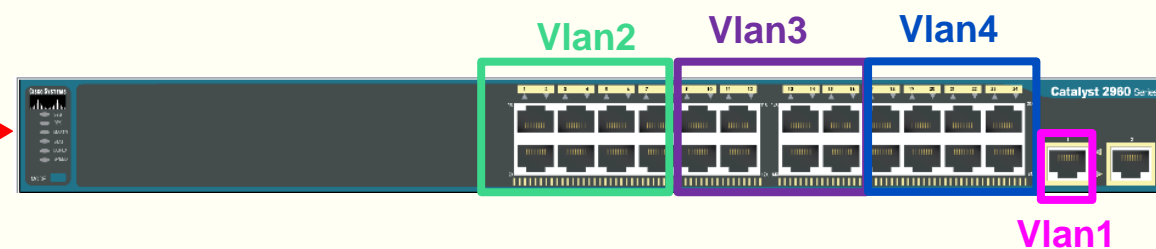
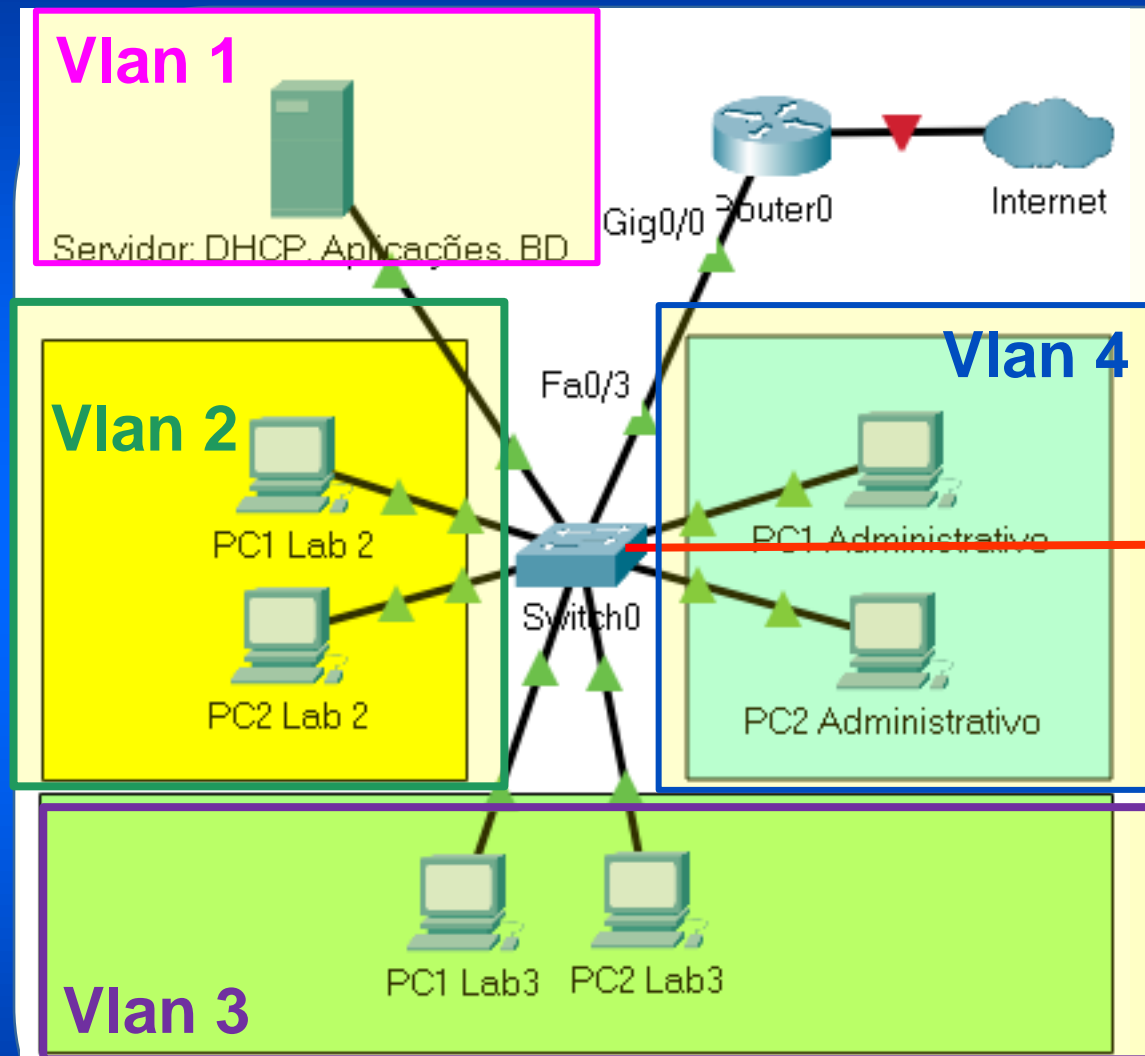
## Melhoras na configuração:

- Iremos dividir a rede em 4 redes diferentes, compartilhando a mesma interface do roteador.
- Para isso iremos configurar 4 redes virtuais (4 VLANs)

**Dessa forma teremos**  
**Quatro DOMÍNIOS DE BROADCAST:**  
**Vlan1, Vlan2, Vlan3 e Vlan4**

**Arquivo:** Aula 02 2023 VLAN.pkt

# Analise a topologia: **Passo 4**

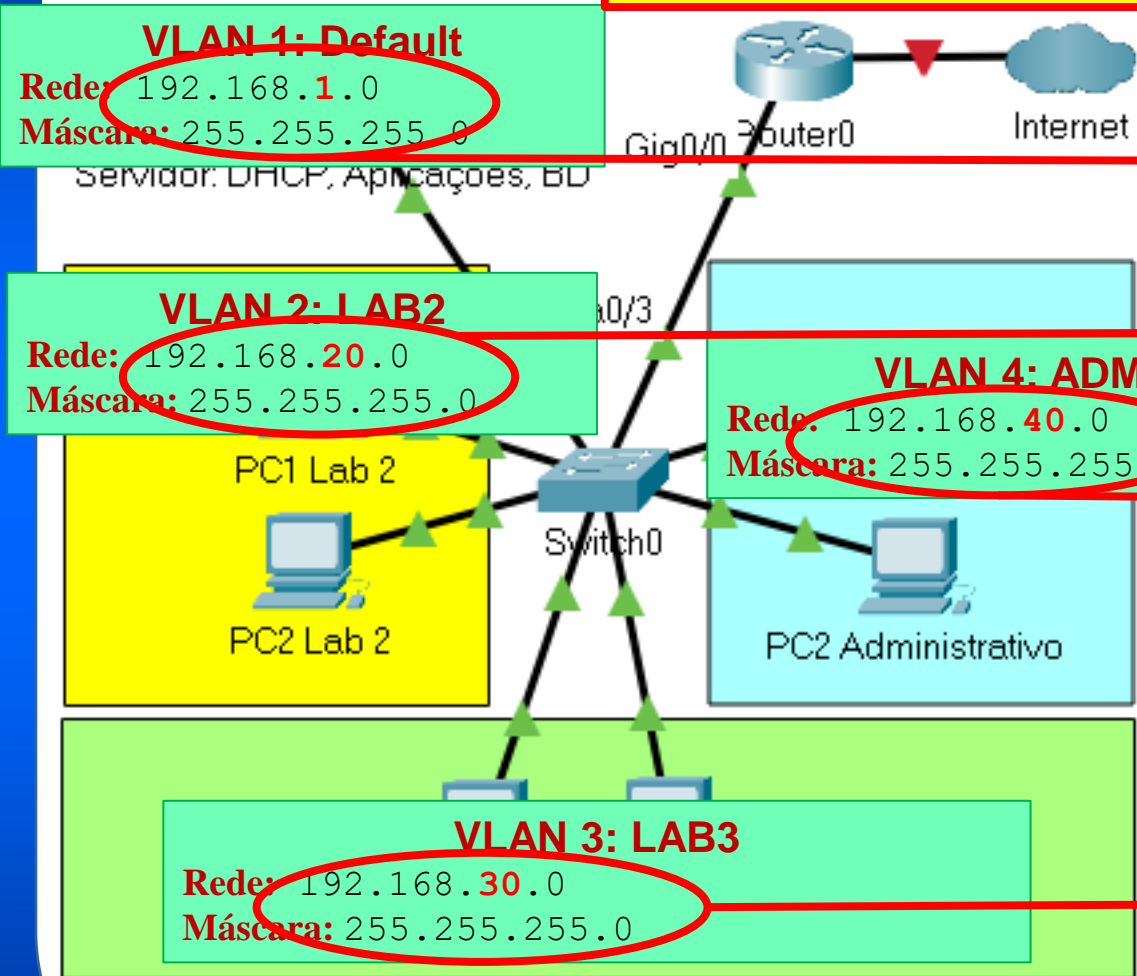


**Dessa forma teremos  
Quatro DOMÍNIOS DE BROADCAST:  
Vlan1, Vlan2, Vlan3 e Vlan4**

Arquivo: Aula 02 2023 VLAN.pkt

## Analise a topologia: Passo 5

Com a divisão em VLANs precisaremos alocar endereços de rede exclusivos para cada VLAN



4 endereços de rede:

**Vlan1 default:**  
**192.168.1.0 /24**

## Vlan2 LAB2:

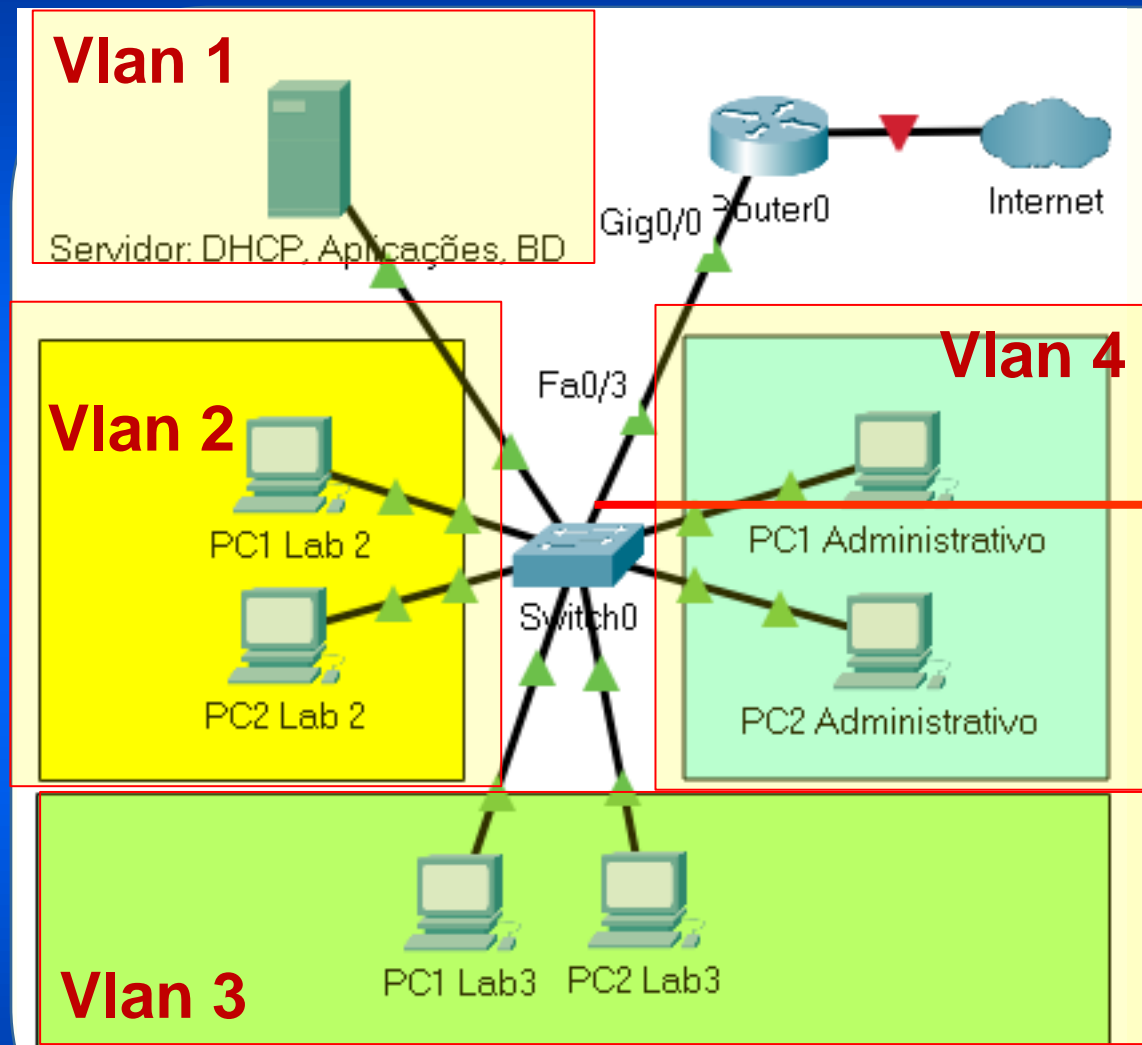
192.168.20.0 /24

**Vlan3 LAB3:**  
**192.168.30.0 /24**

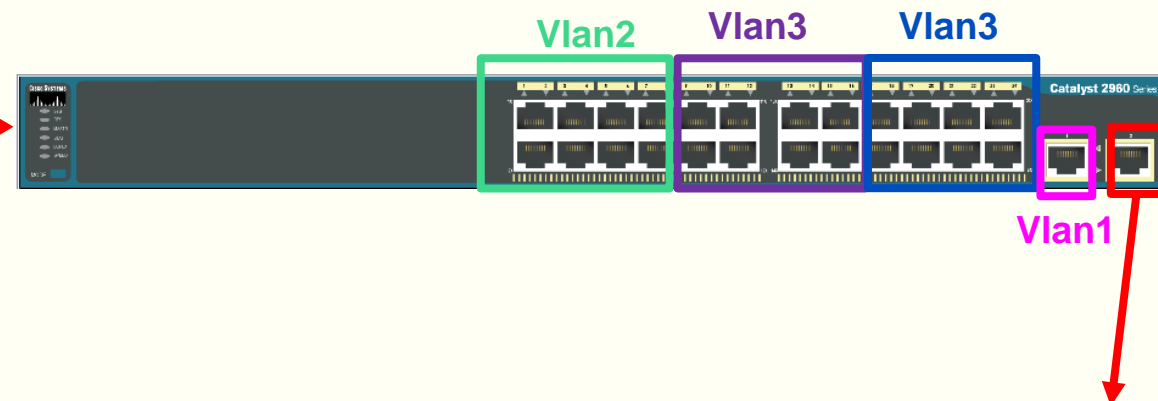
**Vlan4 ADM:**  
**192.168.40.0 /24**

**Arquivo:** Aula 02 2023 VLAN.pkt

# Analise a topologia: **Passo 6**



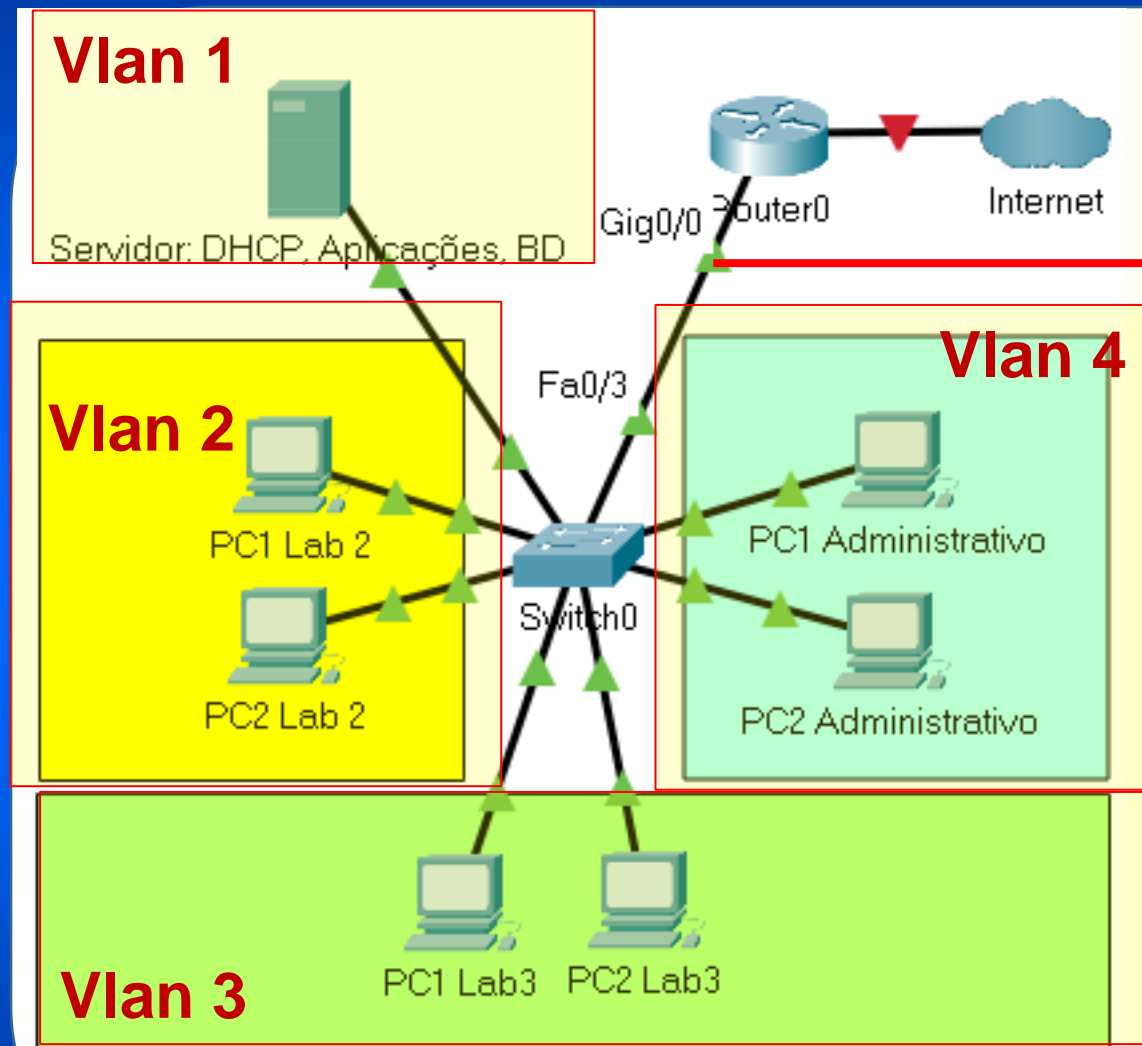
Arquivo: Aula 02 2023 VLAN.pkt



Pelo cabo (link) entre o Switch e o Roteador passarão os dados de todas as VLANs. A interface Gig0/2 do Switch0 onde conecta esse link deverá ser transformada em uma interface **TRONCO (TRUNK)** e **associada a TODAS AS VLANS**



# Analise a topologia: **Passo 7**

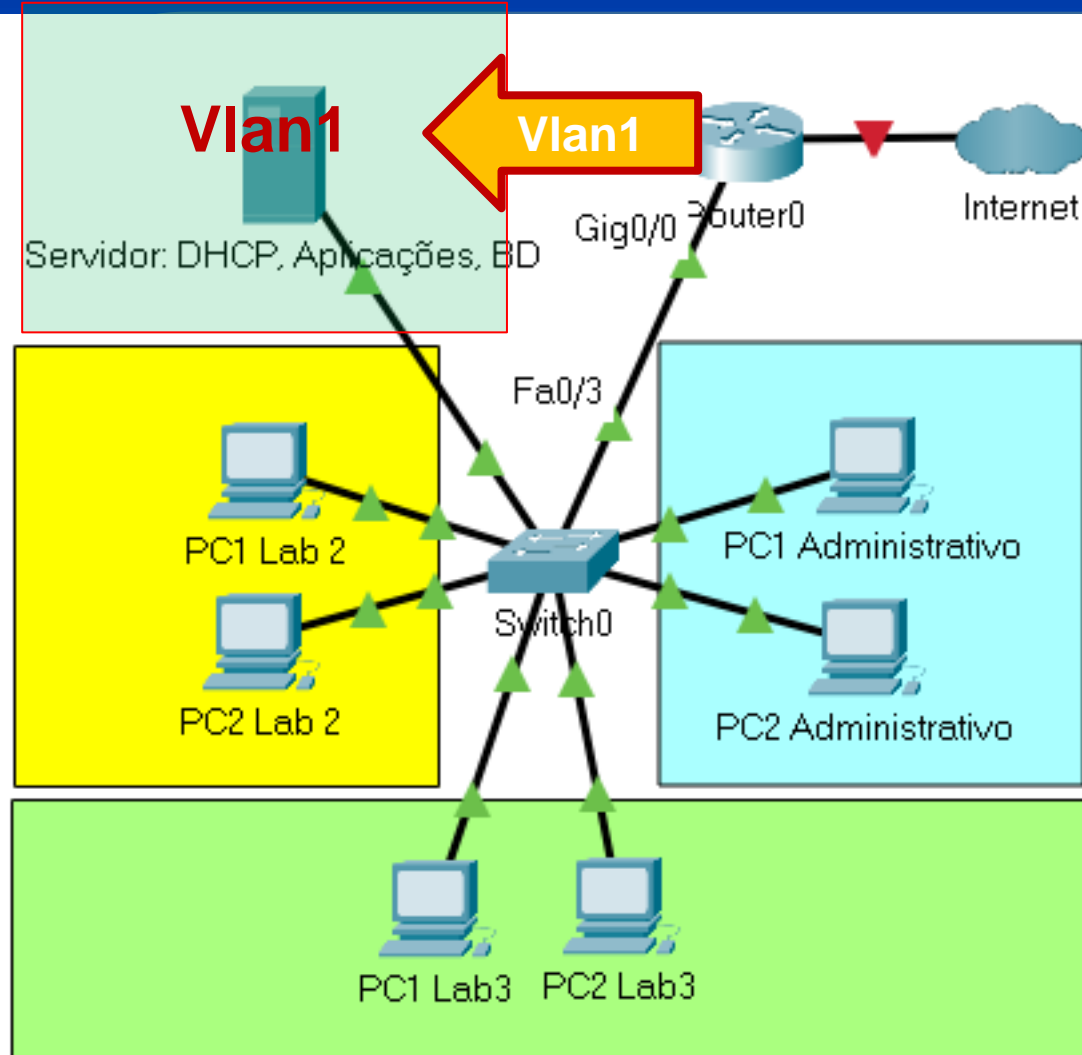


**A interface do Roteador (interface Gig0/0) que era gateway de toda a rede precisará ser dividida em 4 sub-interfaces (interfaces lógicas), sendo que cada sub-interface será o gateway de uma VLAN.**

# **Atividade Prática:**

## **Configuração dos cenários**

# Configurando uma VLAN (VLAN 1)



Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch>
Switch>
Switch>
Switch>
Switch>
Switch>show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, 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 Gig0/1, Gig0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Switch>
Switch>
Switch>
Switch>
Switch>

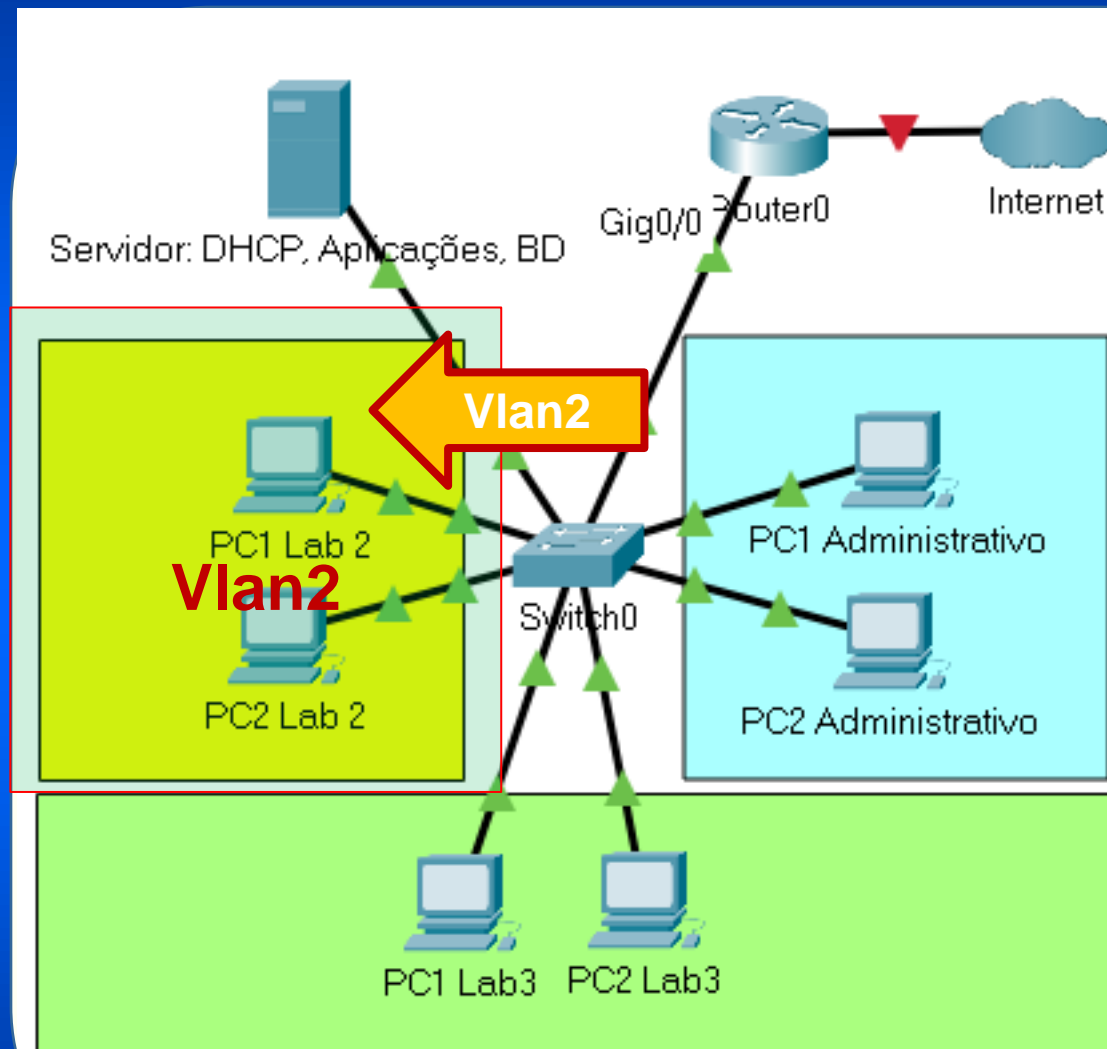
Ctrl+F6 to exit CLI focus

Copy Paste

Top

**Default:** Todas as interfaces do switch estão em uma única VLAN: Vlan1  
Iremos configurar as demais VLANs nos próximos slides

# Configurando uma VLAN (VLAN 2)



Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch#  
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

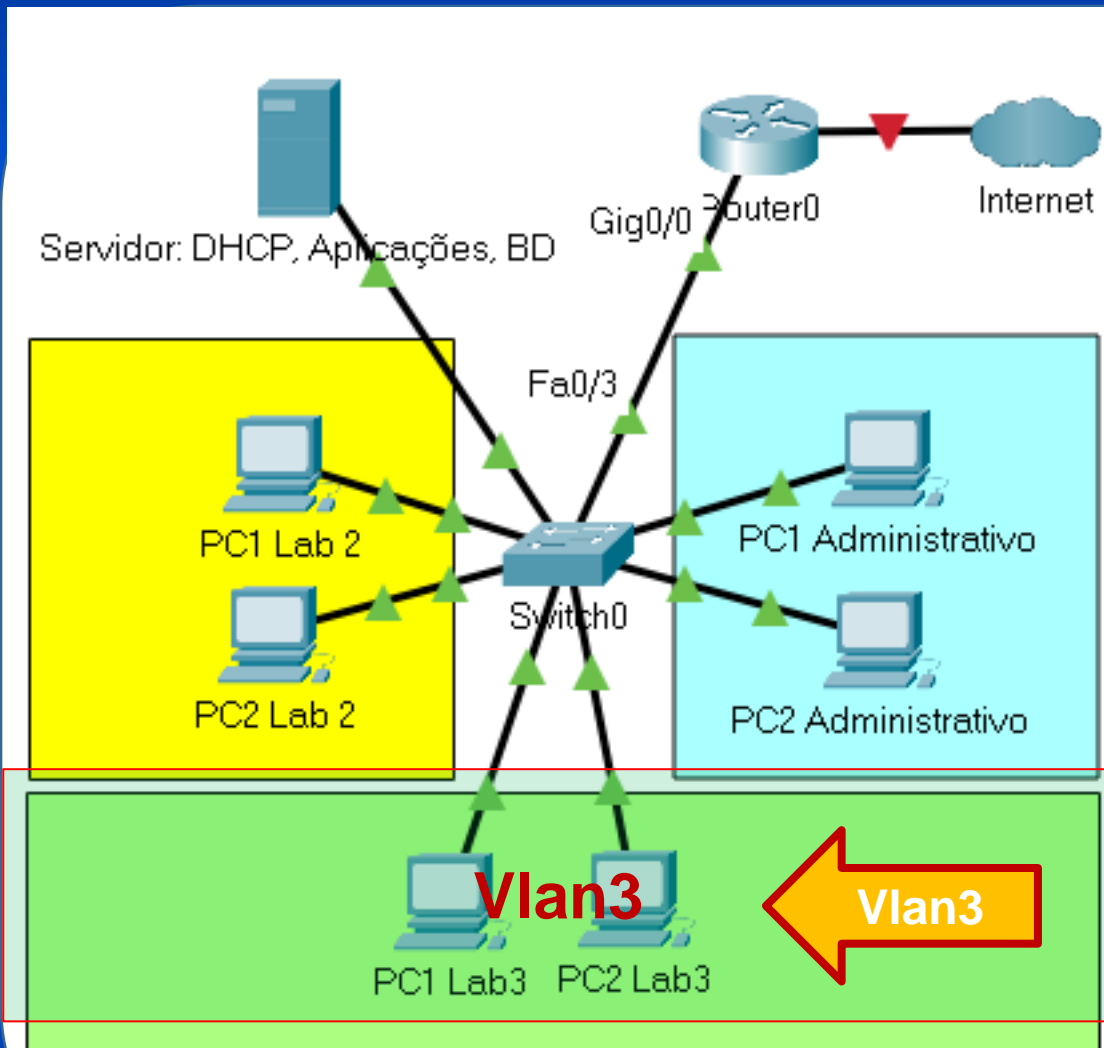
```
Switch#  
Switch#  
Switch#configure terminal  
Switch(config)#vlan 2  
Switch(config-vlan)#name LAB2  
Switch(config-vlan)#
```

Copy Paste

Top

Arquivo: Aula 09a 2021 VLAN.pkt

# Configurando uma VLAN (VLAN 3)



```
Switch0
Switch#
Switch#show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/3, 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

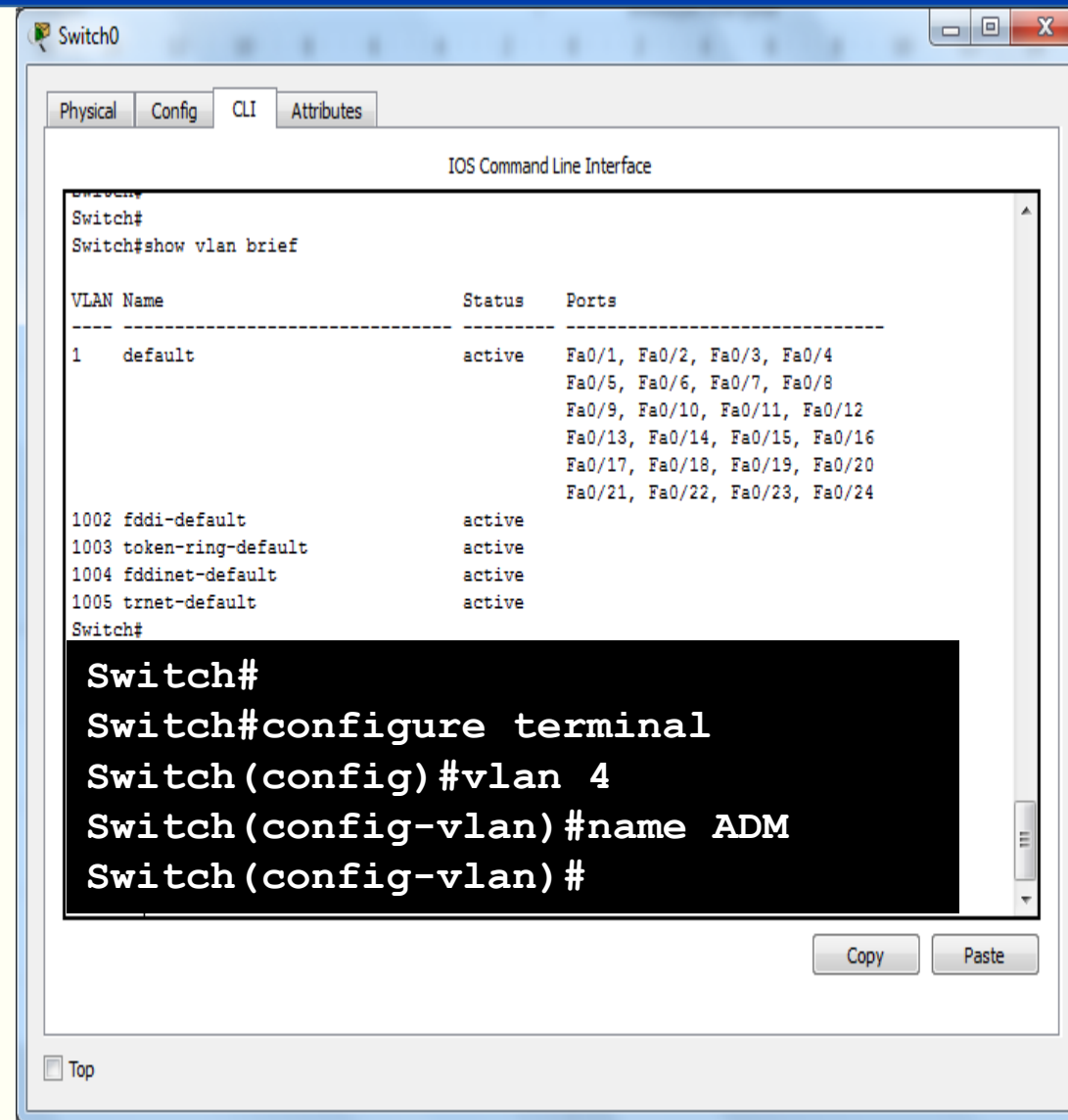
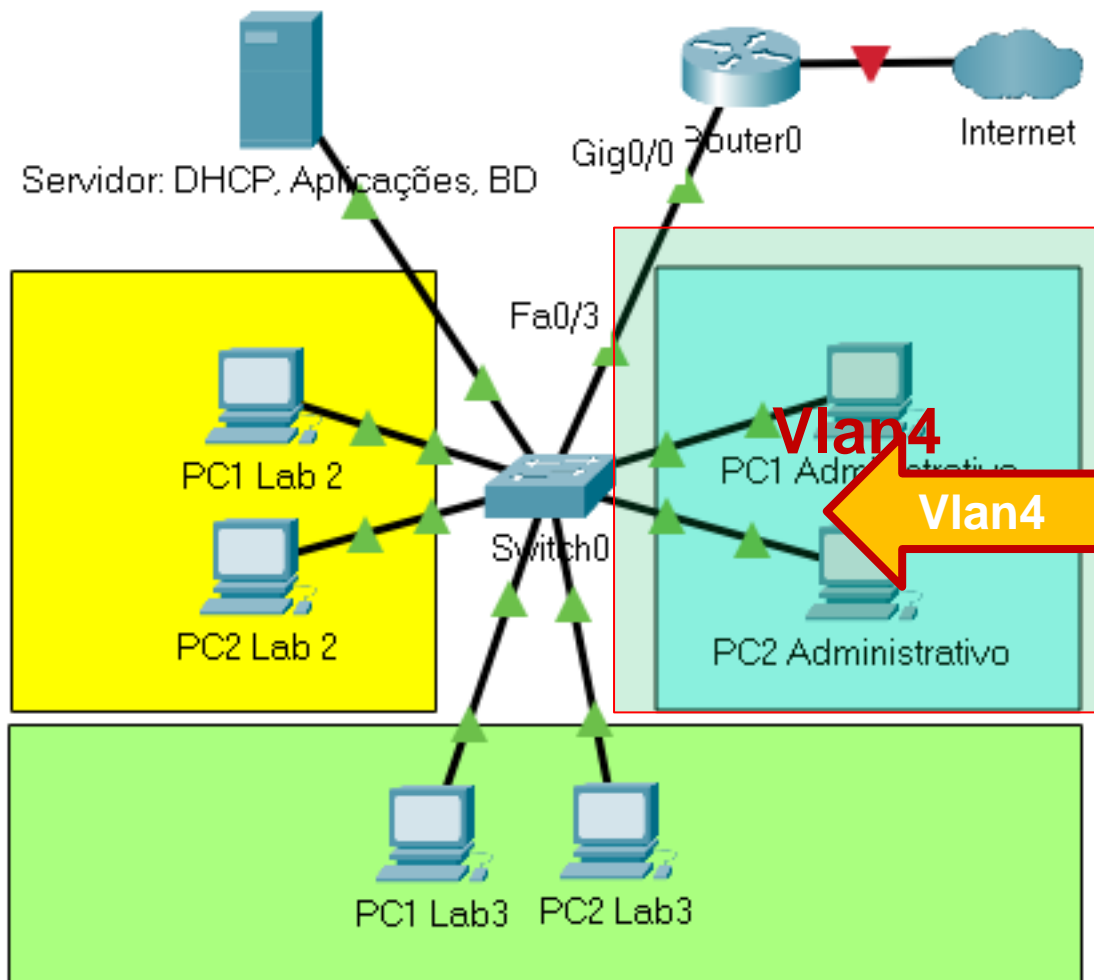
1002 fddi-default        active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

Switch#
Switch#
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch#
Switch#configure terminal
Switch(config)#vlan 3
Switch(config-vlan)#name LAB3
Switch(config-vlan)#
```

Arquivo: Aula 09a 2021 VLAN.pkt

# Configurando uma VLAN (VLAN 4)



Arquivo: Aula 09a 2021 VLAN.pkt

# Associando as portas do Switch à VLAN 2

Switch0

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Switch(config)#
Switch(config)#
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
Switch#
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, 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 Gig0/1, Gig0/2
2	LAB2	active	
3	LAB3	active	
4	ADM	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Switch#

Ctrl+F6 to exit CLI focus

Top

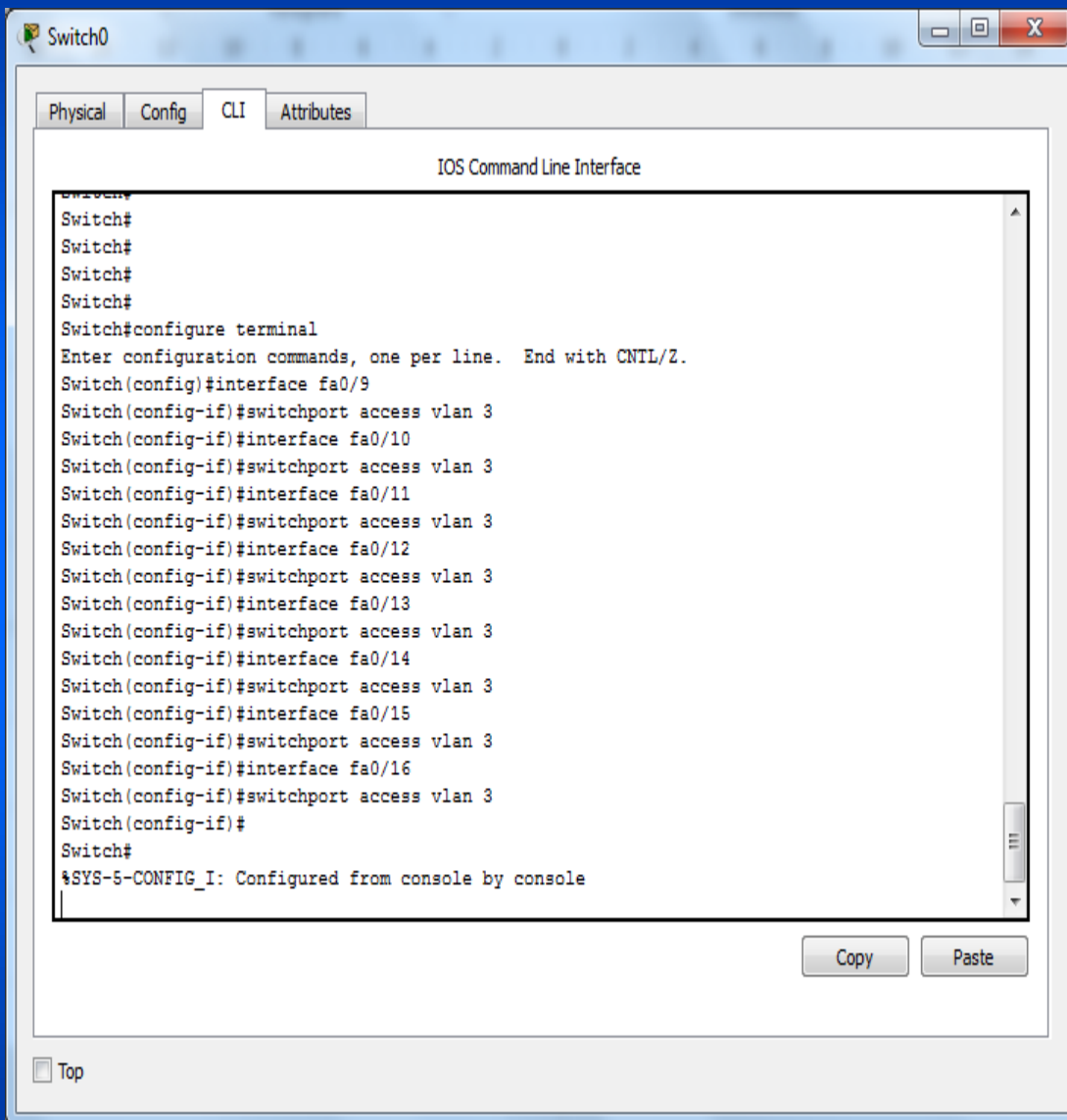
```
Switch#
Switch#configure terminal
Switch(config)#interface fa0/1
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/2
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/3
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/4
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/5
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/6
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/7
Switch(config-if)#switchport access vlan 2
Switch(config-if)#interface fa0/8
Switch(config-if)#switchport access vlan 2
Switch(config-if)#
```

Mover individualmente  
cada interface para a **Vlan2**

ou (utilizando **range**):

```
Switch#
Switch#configure terminal
Switch(config)#interface range fa0/1-8
Switch(config-if)#switchport access vlan 2
```

# Associando as portas do Switch à VLAN 3



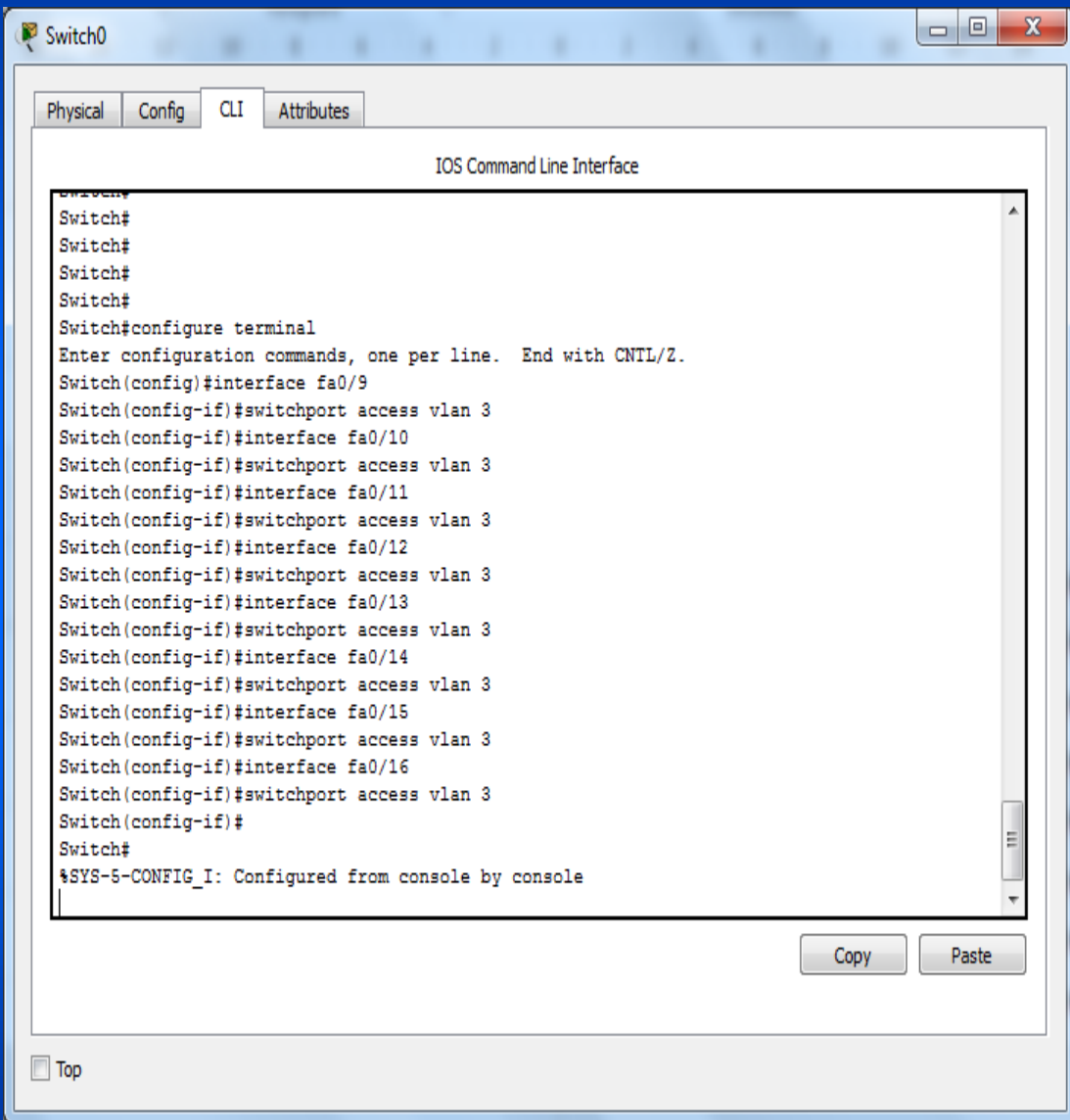
```
Switch#
Switch#configure terminal
Switch(config)#interface fa0/9
Switch(config-if)#switchport access vlan 3
Switch(config-if)#interface fa0/10
Switch(config-if)#switchport access vlan 3
Switch(config-if)#interface fa0/11
Switch(config-if)#switchport access vlan 3
Switch(config-if)#interface fa0/12
Switch(config-if)#switchport access vlan 3
Switch(config-if)#interface fa0/13
Switch(config-if)#switchport access vlan 3
Switch(config-if)#interface fa0/14
Switch(config-if)#switchport access vlan 3
Switch(config-if)#interface fa0/15
Switch(config-if)#switchport access vlan 3
Switch(config-if)#interface fa0/16
Switch(config-if)#switchport access vlan 3
```

ou (utilizando **range**):

```
Switch#
Switch#configure terminal
Switch(config)#interface range fa0/9-16
Switch(config-if)#switchport access vlan 3
```



# Associando as portas do Switch à VLAN 4



```
Switch#
Switch#configure terminal
Switch(config)#interface fa0/17
Switch(config-if)#switchport access vlan 4
Switch(config-if)#interface fa0/18
Switch(config-if)#switchport access vlan 4
Switch(config-if)#interface fa0/19
Switch(config-if)#switchport access vlan 4
Switch(config-if)#interface fa0/20
Switch(config-if)#switchport access vlan 4
Switch(config-if)#interface fa0/21
Switch(config-if)#switchport access vlan 4
Switch(config-if)#interface fa0/22
Switch(config-if)#switchport access vlan 4
Switch(config-if)#interface fa0/23
Switch(config-if)#switchport access vlan 4
Switch(config-if)#interface fa0/24
Switch(config-if)#switchport access vlan 4
```

ou (utilizando **range**):

```
Switch#
Switch#configure terminal
Switch(config)#interface range fa0/17-24
Switch(config-if)#switchport access vlan 4
```

# VLANs configuradas

Switch0

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Gig0/1, Gig0/2
2	LAB2	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8
3	LAB3	active	Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16
4	ADM	active	Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
```

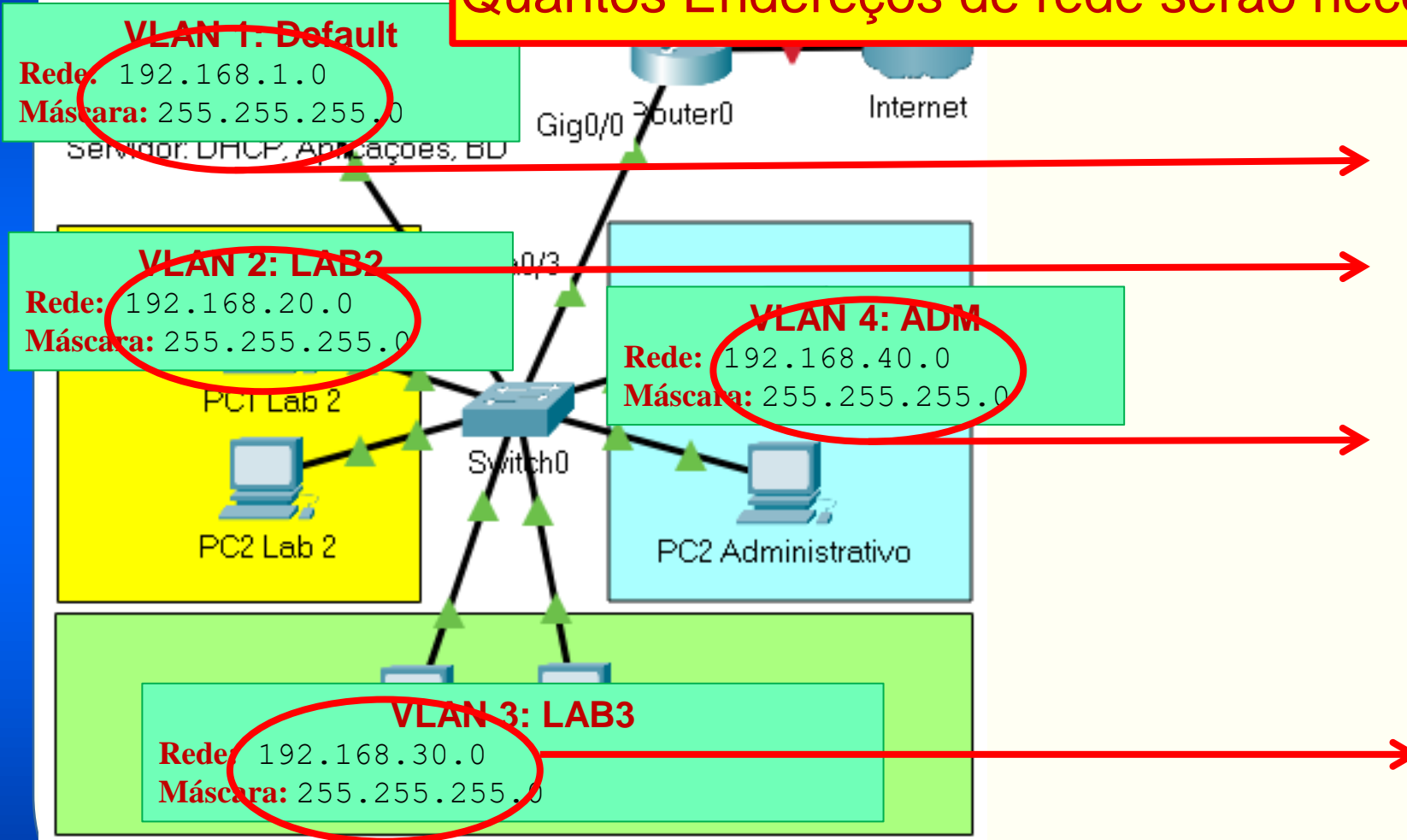
Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

# Endereços de Rede (sub-redes)

Quantos Endereços de rede serão necessários?



4 endereços de rede:

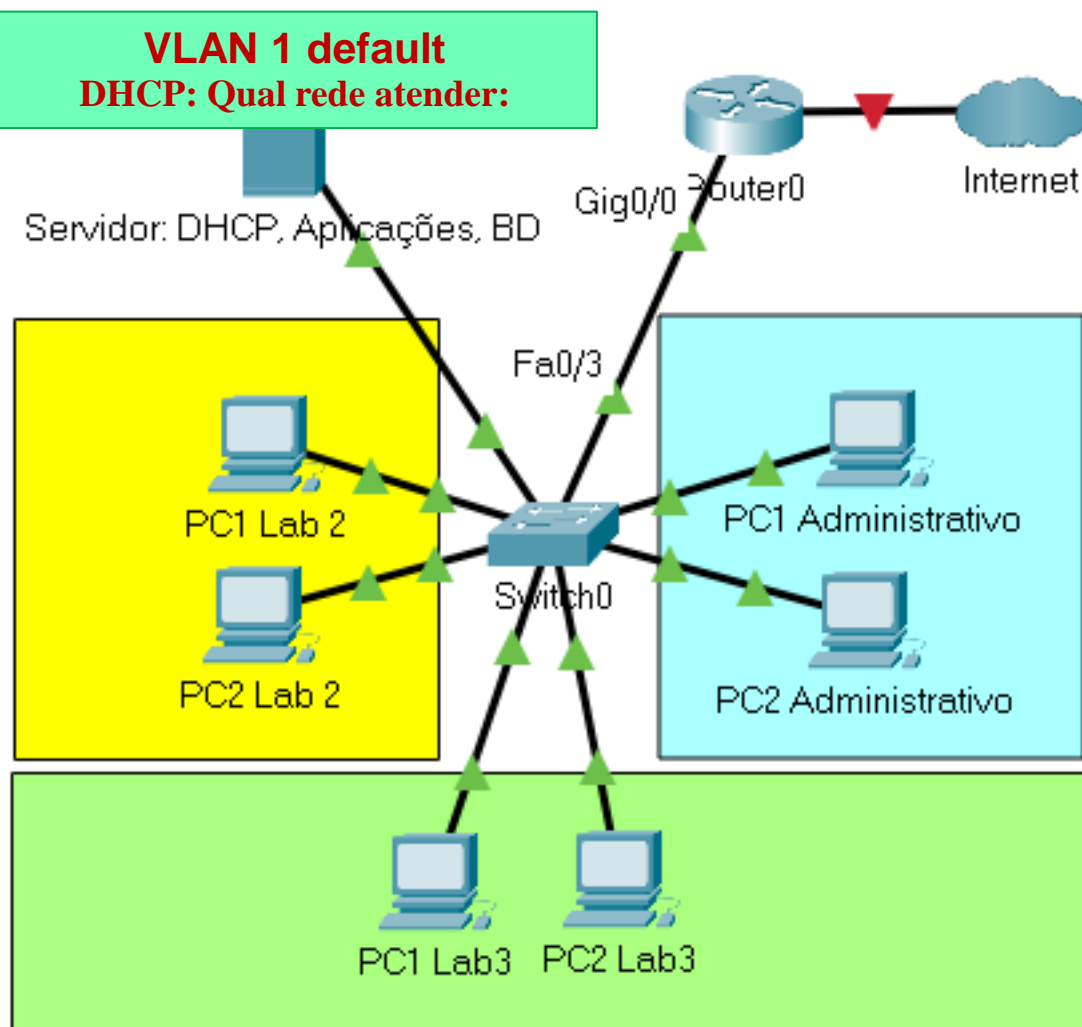
**Vlan default:**  
**192.168.1.0**

**Vlan LAB2:**  
**192.168.20.0**

**Vlan LAB3:**  
**192.168.30.0**

**Vlan ADM:**  
**192.168.40.0**

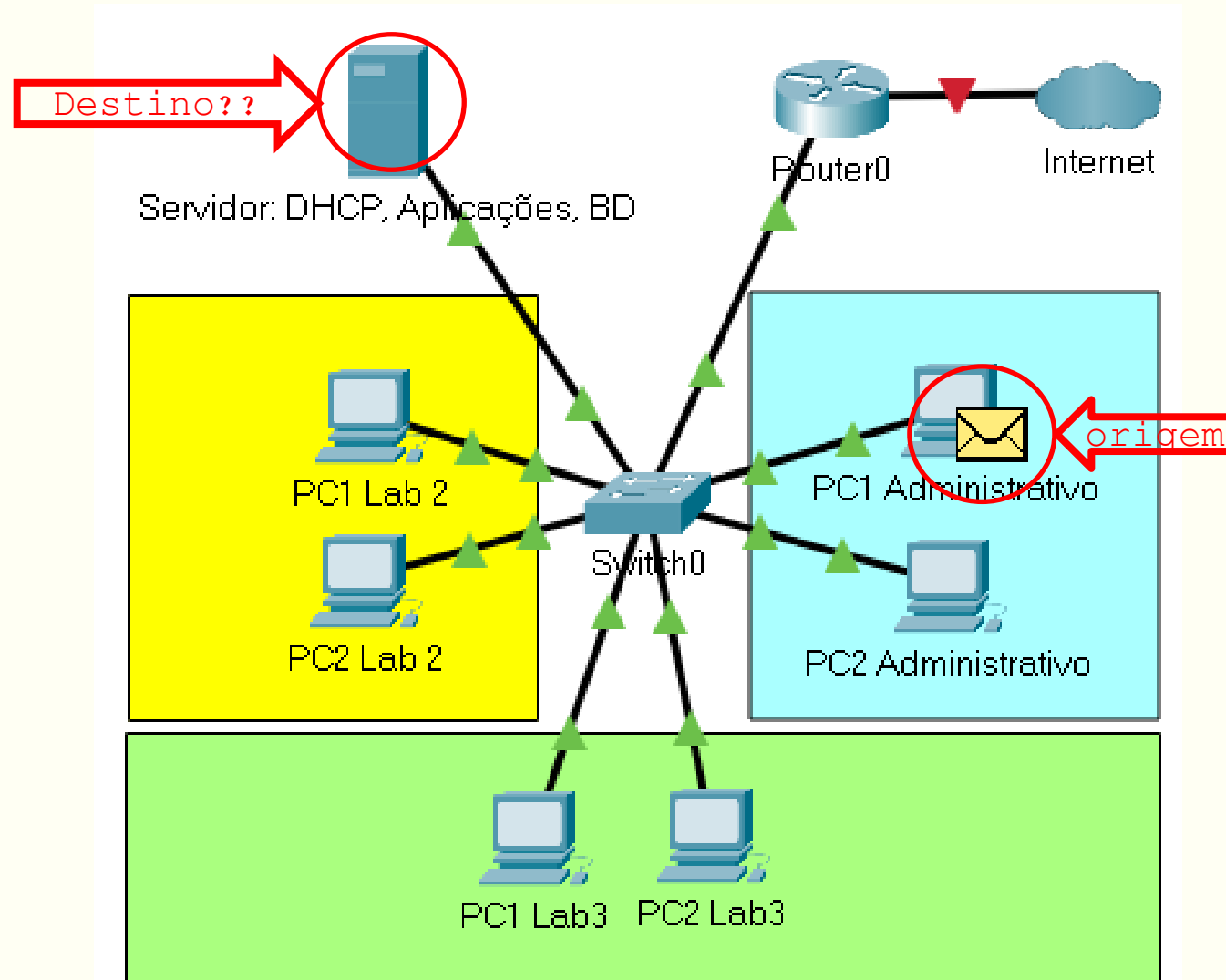
# Endereços de Rede (sub-redes)



## Problema:

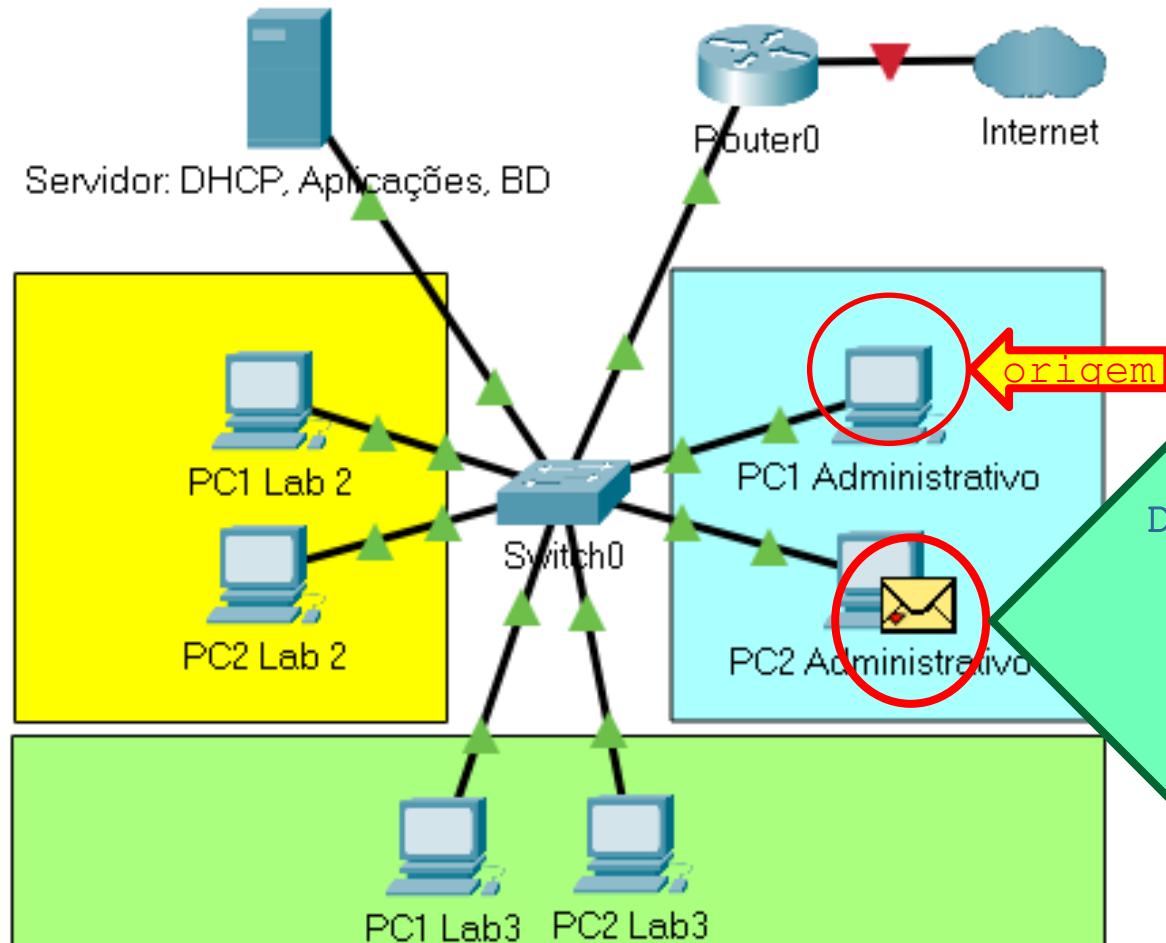
A quem o servidor DHCP irá atender em uma requisição de configuração de Protocolo IP

# Requisição de IP via DHCP



# Comunicação entre VLANs distintas

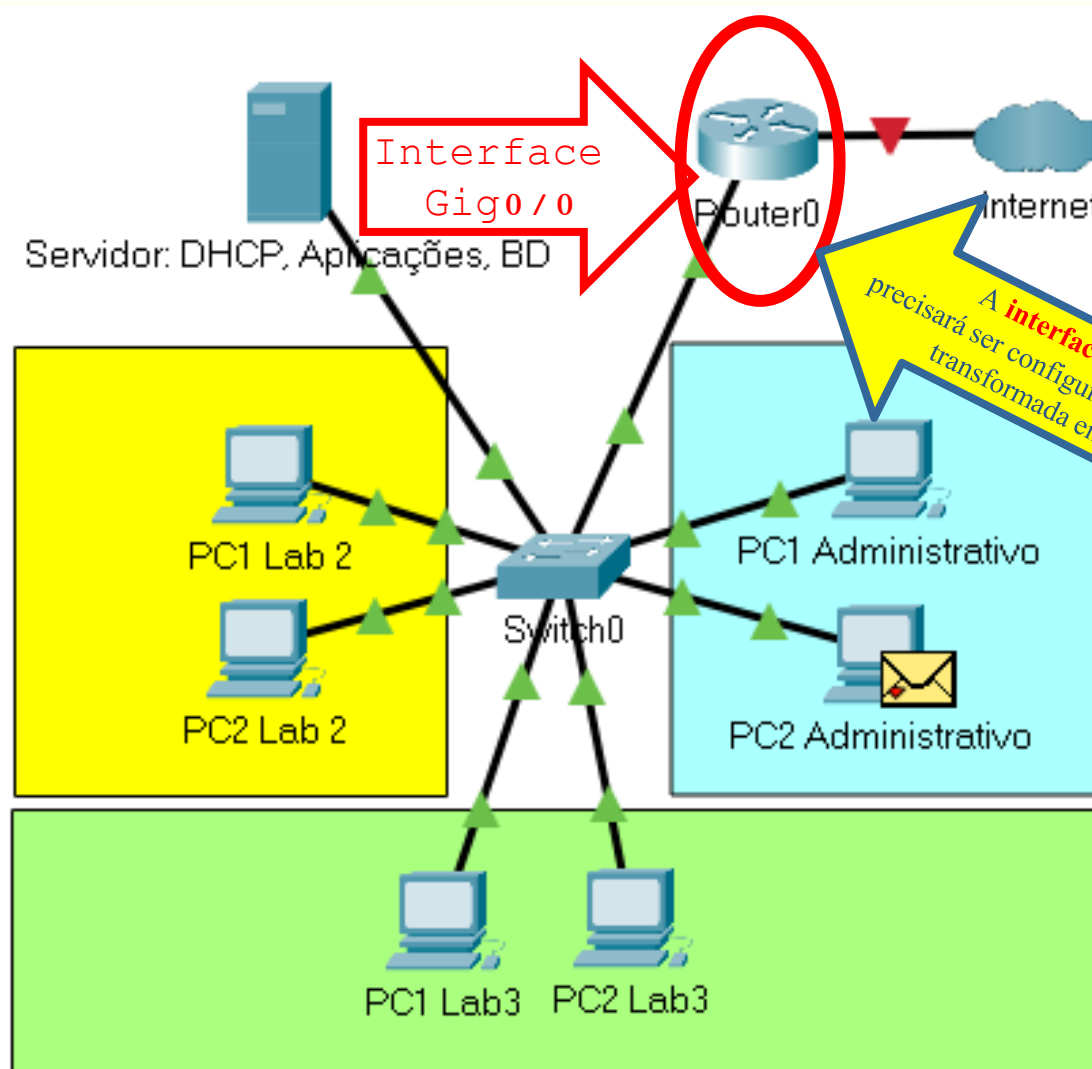
**Não há comunicação entre as VLANs sem roteamento!!!**



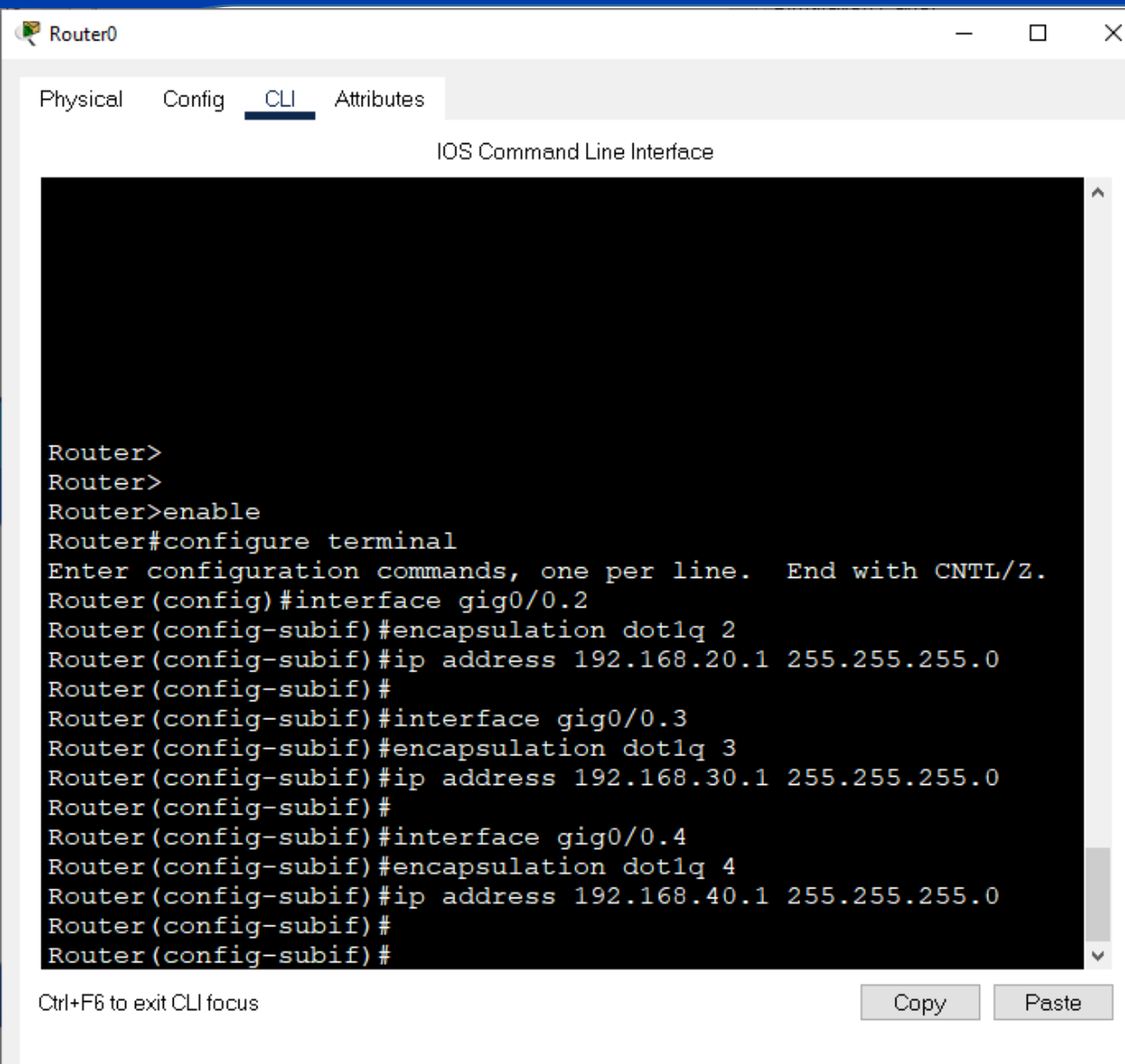
**FALHA:**

Servidor DHCP está em VLAN diferente (Default): outro domínio de broadcast!!!

# Roteador: Para comunicação entre VLANs



# Configurando Sub-interfaces 802.1q no roteador



```
Router>
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gig0/0.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#interface gig0/0.3
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#interface gig0/0.4
Router(config-subif)#encapsulation dot1q 4
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

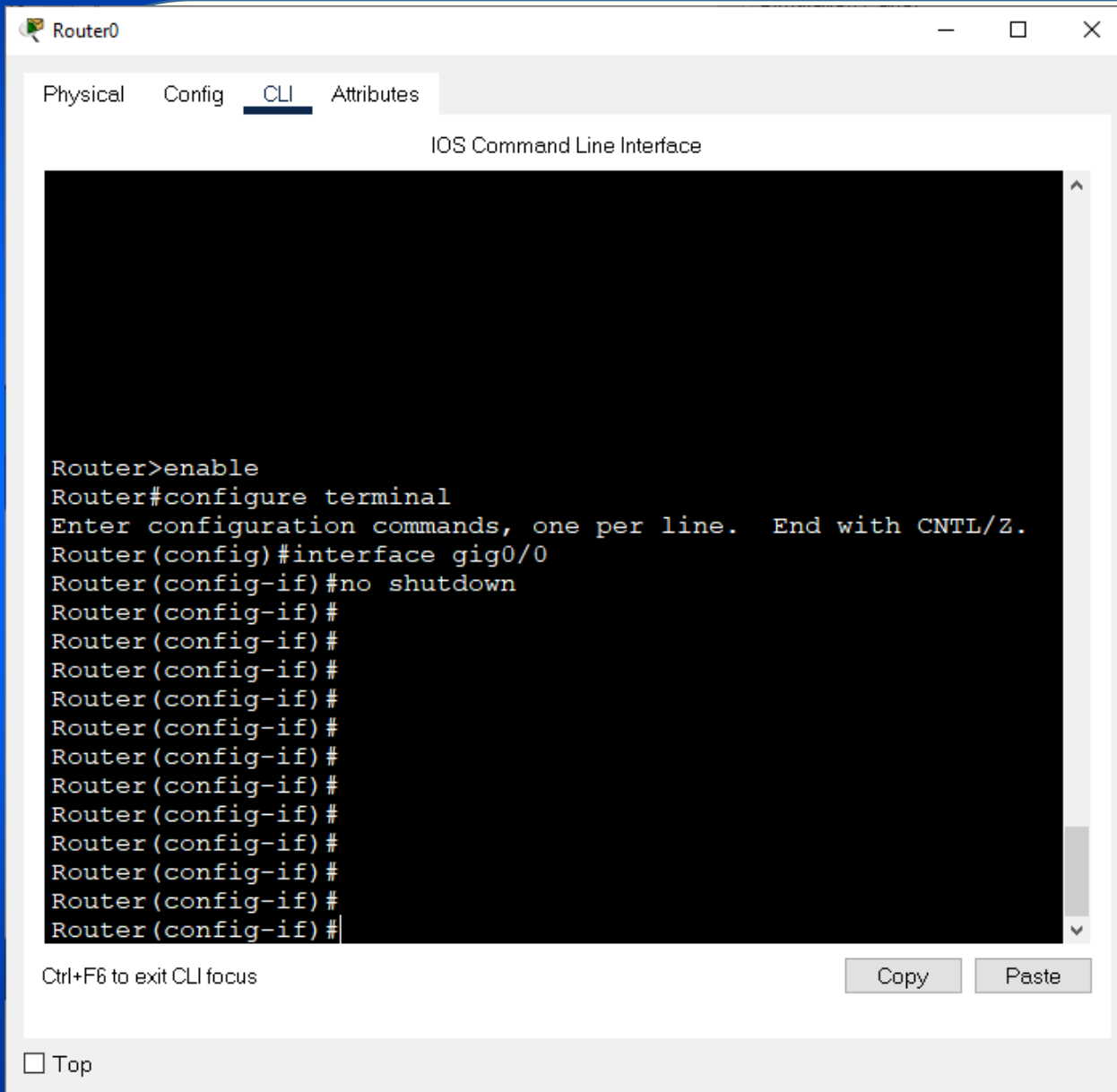
```
Router>enable
Router#configure terminal
Router(config)#interface gig0/0.1
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 192.168.1.1 255.255.255.0
Router(config-subif)#
Router(config)#interface gig0/0.2
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#interface gig0/0.3
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#
Router(config-subif)#interface gig0/0.4
Router(config-subif)#encapsulation dot1q 4
Router(config-subif)#ip address 192.168.40.1 255.255.255.0
Router(config-subif)#
```

As sub-interfaces se tornam os *gateways* das VLANs:

gig0/0.1 = 192.168.1.1 = gateway da VLAN default  
gig0/0.2 = 192.168.20.1 = gateway da VLAN LAB2  
gig0/0.3 = 192.168.30.1 = gateway da VLAN LAB3  
gig0/0.4 = 192.168.40.1 = gateway da VLAN ADM



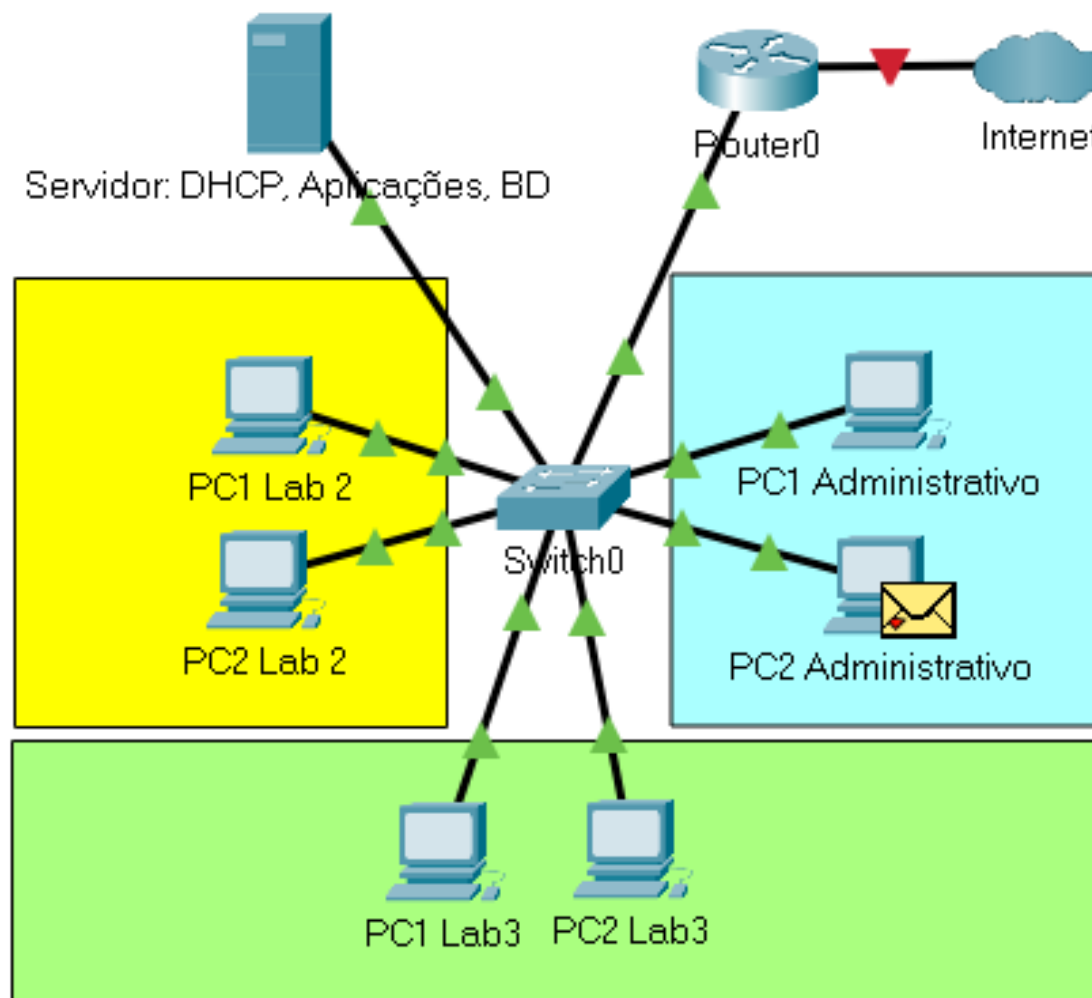
# ‘Ligando’ a interface gig0/0



```
Router>enable
Router#
Router#configure terminal
Router(config)#interface fa0/0
Router(config-if)#no shutdown
```

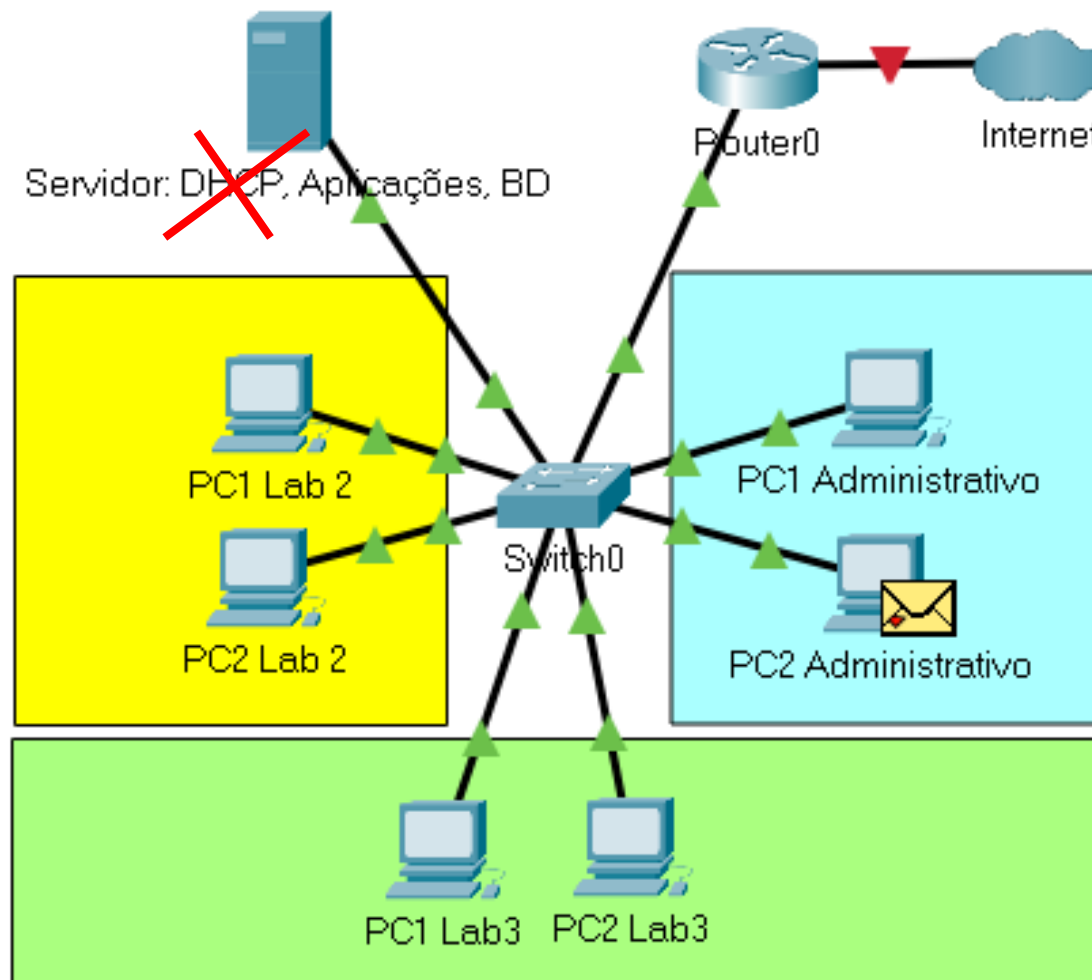
Todas as sub-interfaces serão ligadas!!!

# Em qual VLAN ficará o DHCP?



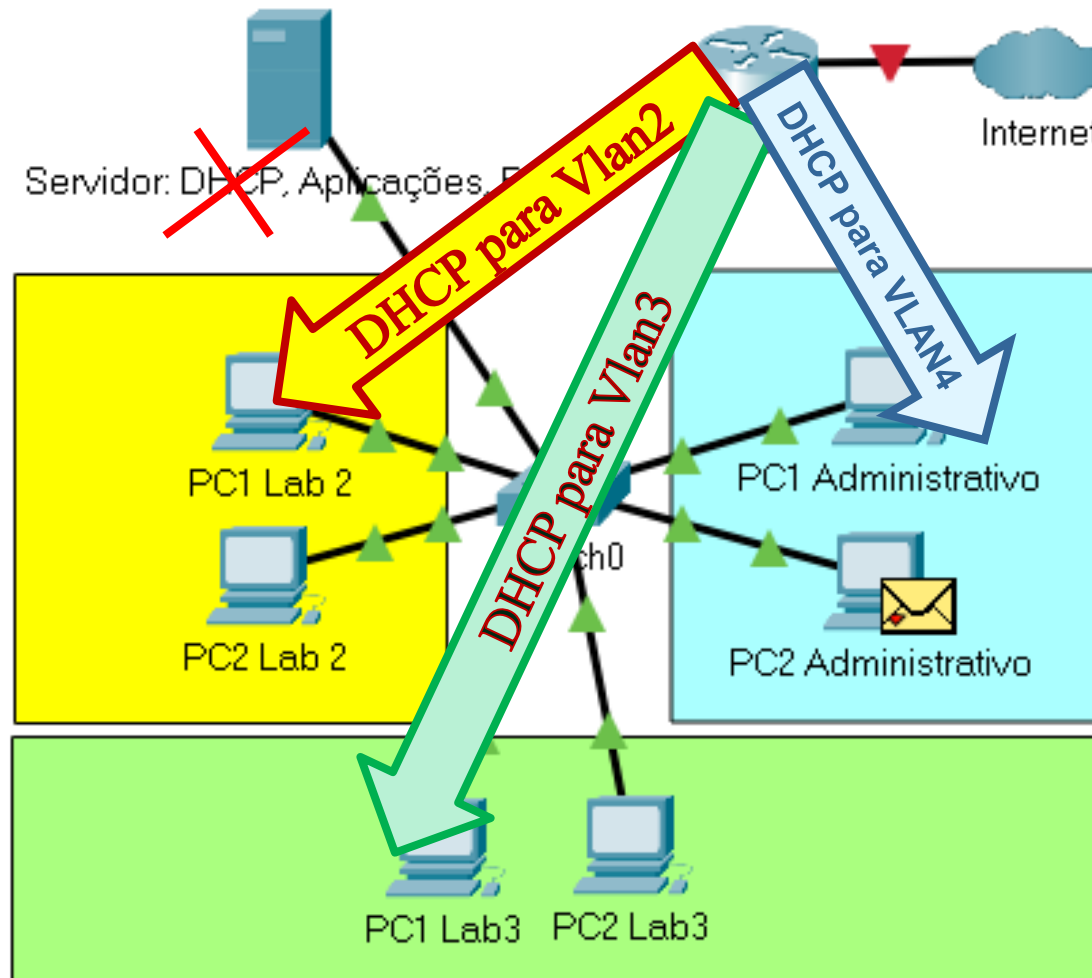
**Precisaremos de um servidor para cada VLAN?**

# Configuração do Roteador como DHCP



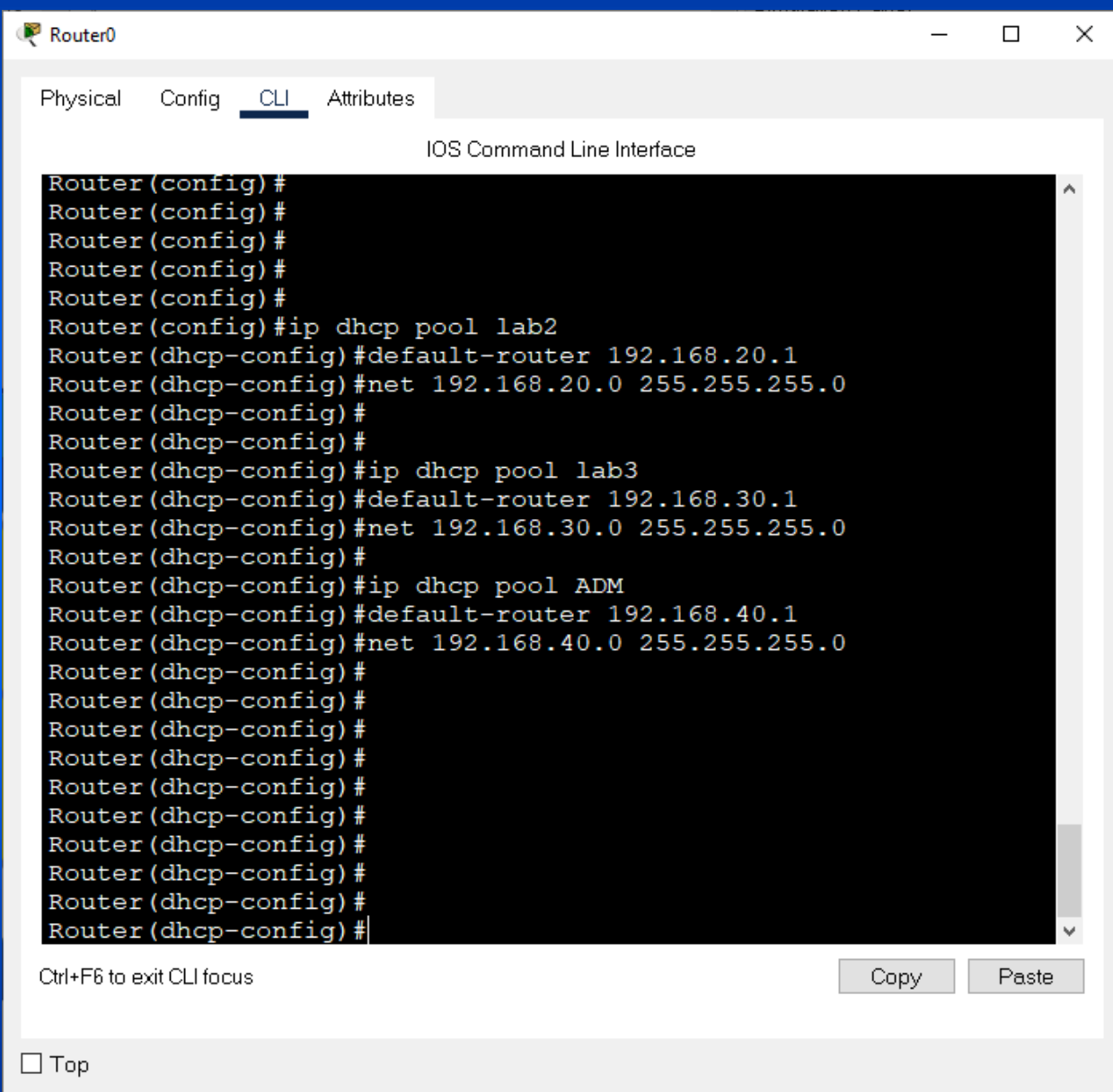
**Pode-se escolher o roteador para o papel do servidor DHCP**

# Configuração do Roteador como DHCP



**Porém precisaremos de 3 serviços DHCP: 1 DHCP para cada VLAN**

# Configuração do Roteador como DHCP



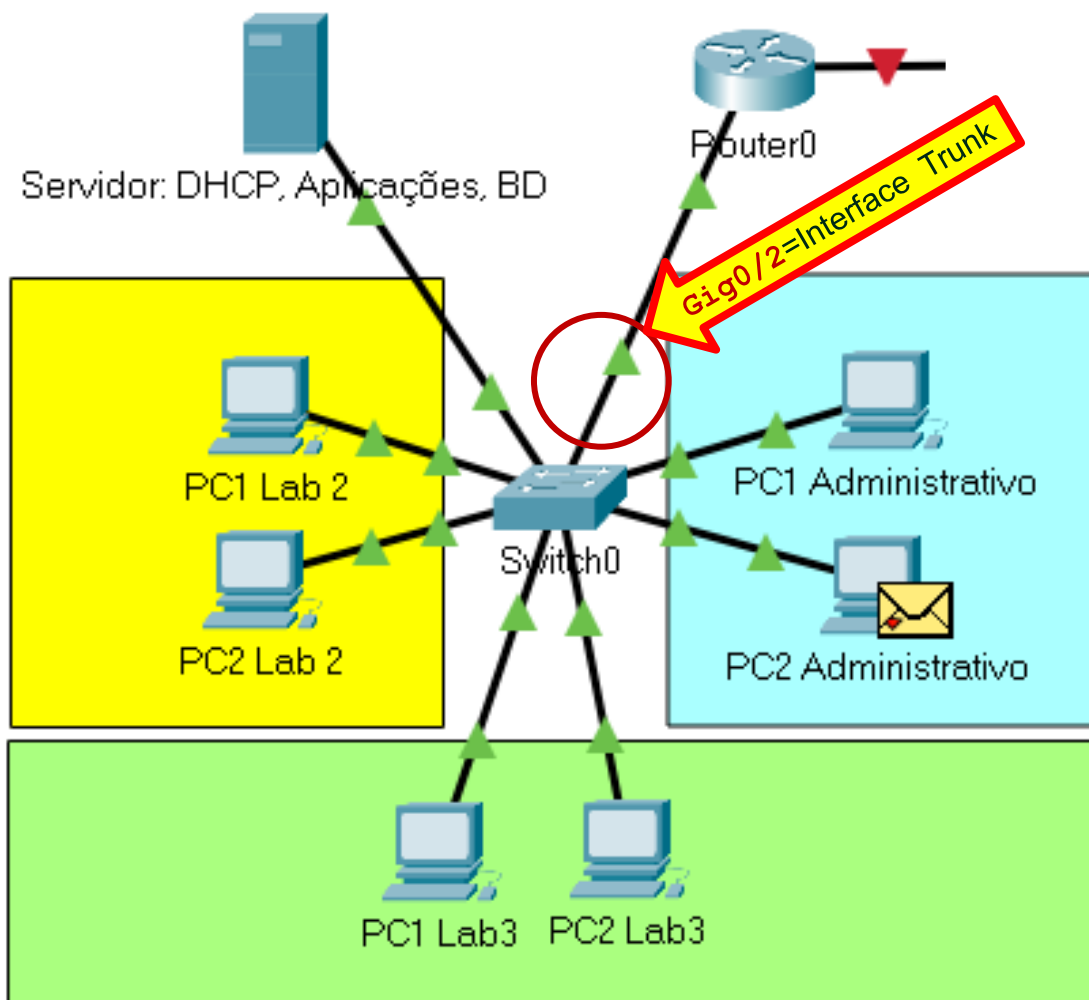
## Um Pool DHCP para cada VLAN:

```
Router#
Router#configure terminal
Router(config)#ip dhcp pool lab2
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#net 192.168.20.0 255.255.255.0
Router(dhcp-config)#end
Router#
Router#
Router#configure terminal
Router(config)#ip dhcp pool lab3
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#net 192.168.30.0 255.255.255.0
Router(dhcp-config)#^Z
Router#
Router#configure terminal
Router(config)#ip dhcp pool ADM
Router(dhcp-config)#default-router 192.168.40.1
Router(dhcp-config)#net 192.168.40.0 255.255.255.0
Router(dhcp-config)#^Z
Router#
```

**VLAN**

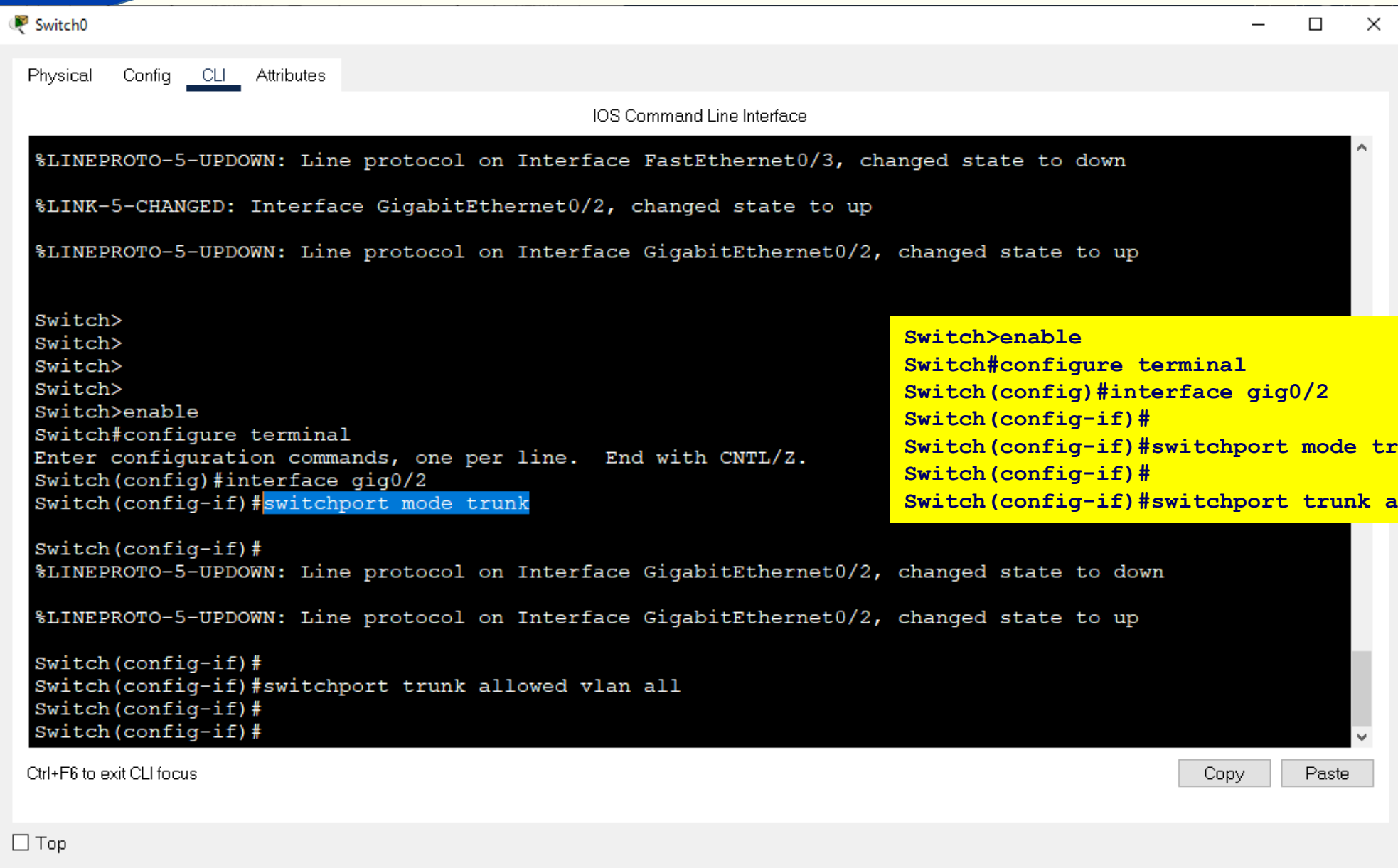
**Configurando Modo Trunk**

# Configuração da Porta *Trunk* no Switch



- Pela interface **Gig0/2**, que faz a ligação com o roteador, passará o tráfego de todas as VLANs.
- A interface **Gig0/2** precisará 'pertencer' a todas as VLANs, **e não** apenas a uma única VLAN.
- A interface **Gig0/2** precisará, então, ser configurada como interface TRUNK (tronco)
- Uma interface Trunk permitirá o tráfego de mais de uma vlan associadas a ela

# Configuração do Switch (porta *Trunk*)



The screenshot shows a network switch configuration window titled "Switch0". It has tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The interface shows a series of status messages and configuration commands. A yellow callout box highlights the commands to enable terminal configuration and set the port to trunk mode.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

Switch>
Switch>
Switch>
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface gig0/2
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up

Switch(config-if)#
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#
Switch(config-if)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top



# **VLAN, DHCP e Trunk**

## **Resumo de configuração**

# Resumo da Configuração de VLAN: exemplo de comandos

## Criar VLAN, exemplo:

```
Switch(vlan)#vlan 2  
Switch(vlan)#name marketing  
Switch(vlan)#exit
```

## Definir a VLAN de uma porta em modo acesso, exemplo:

```
Switch(config)#interface fastethernet f0/9  
Switch(config-if)#switchport mode access  
Switch(config-if)#switchport access vlan 2
```

## Definir a VLAN de uma porta em modo tronco (*trunk*), exemplo:

```
Switch(config-if)#interface ethernet f0/7  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#switchport trunk allowed vlan all
```

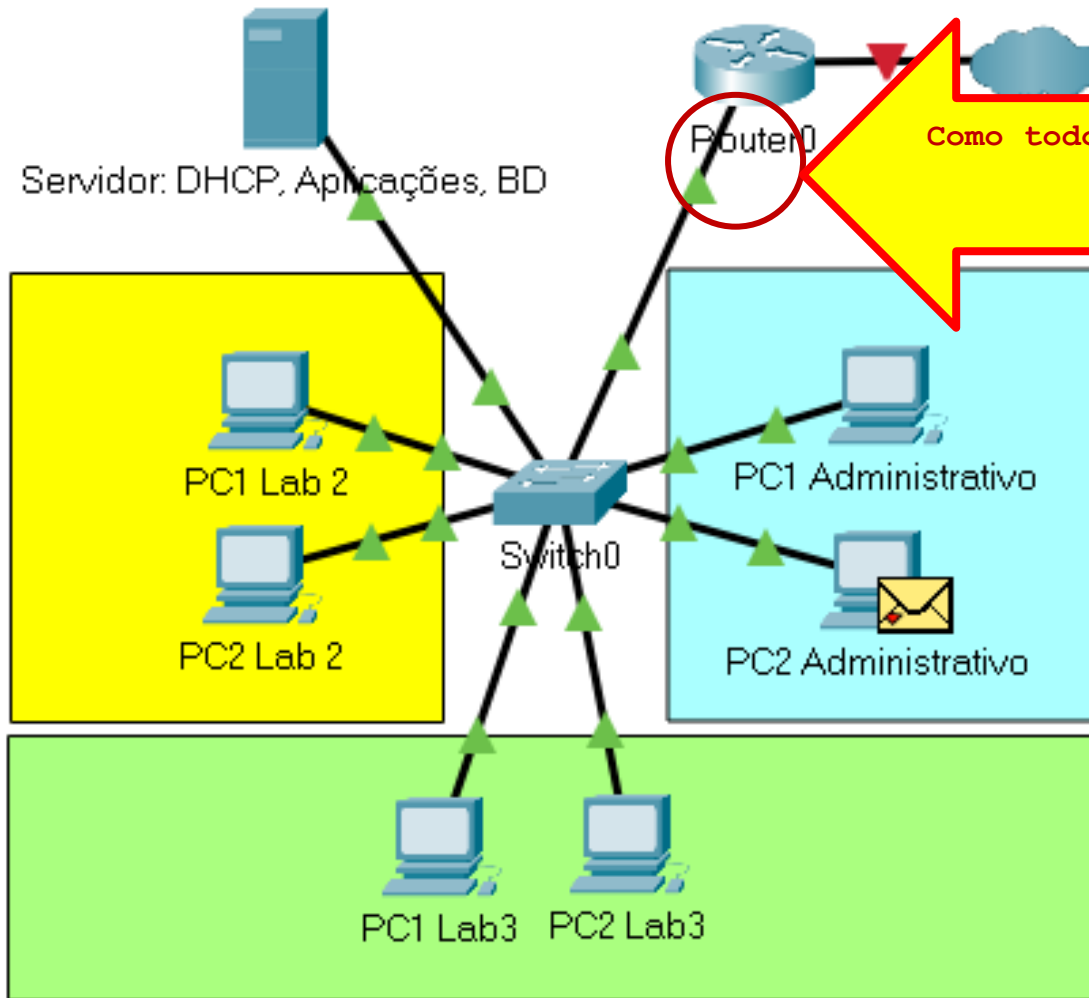
## Definir a DHCP no roteador, exemplo:

```
Router#configure terminal  
Router(config)#ip dhcp pool lab2  
Router(dhcp-config)#default-router 192.168.20.1  
Router(dhcp-config)#net 192.168.20.0 255.255.255.0
```

**ACL**

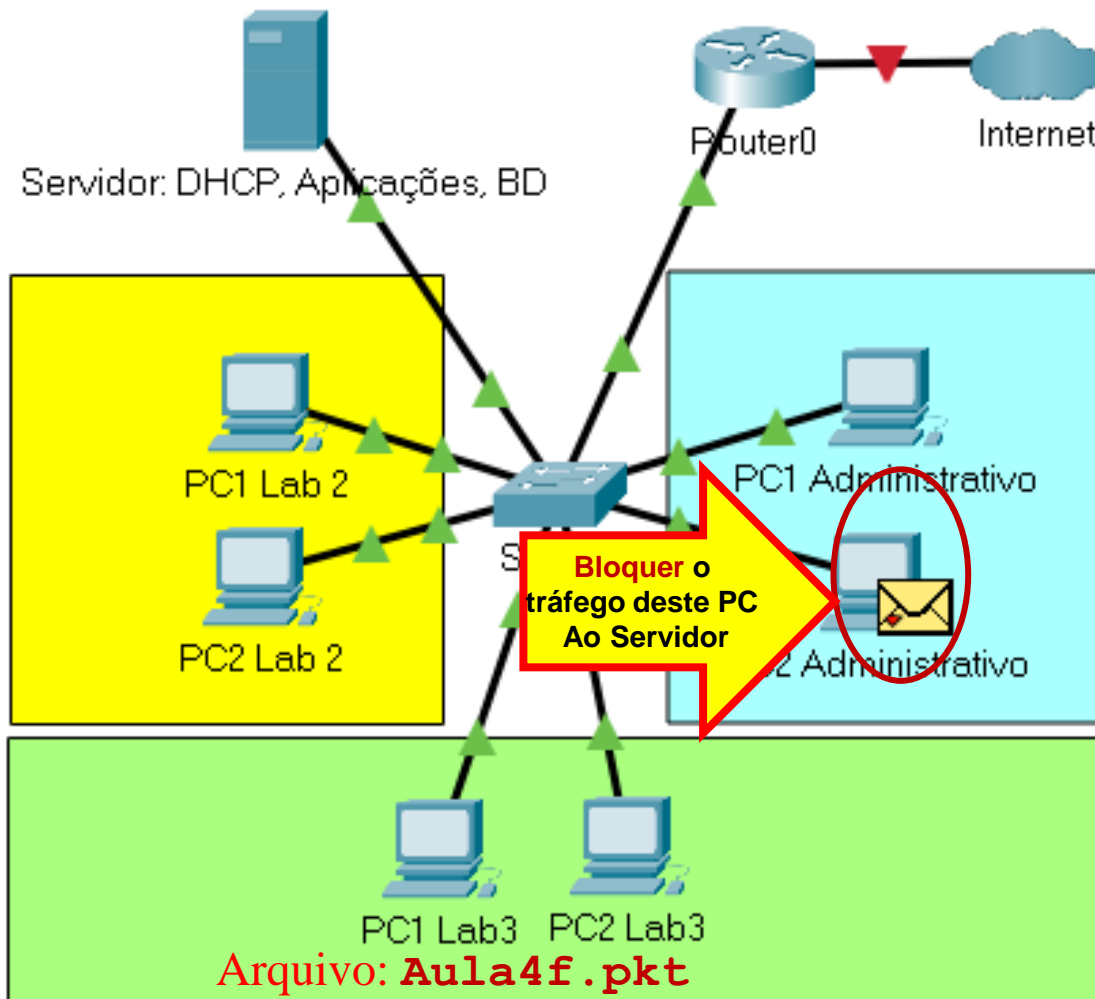
**- Access Control List -**

# Segurança: configuração de ACL

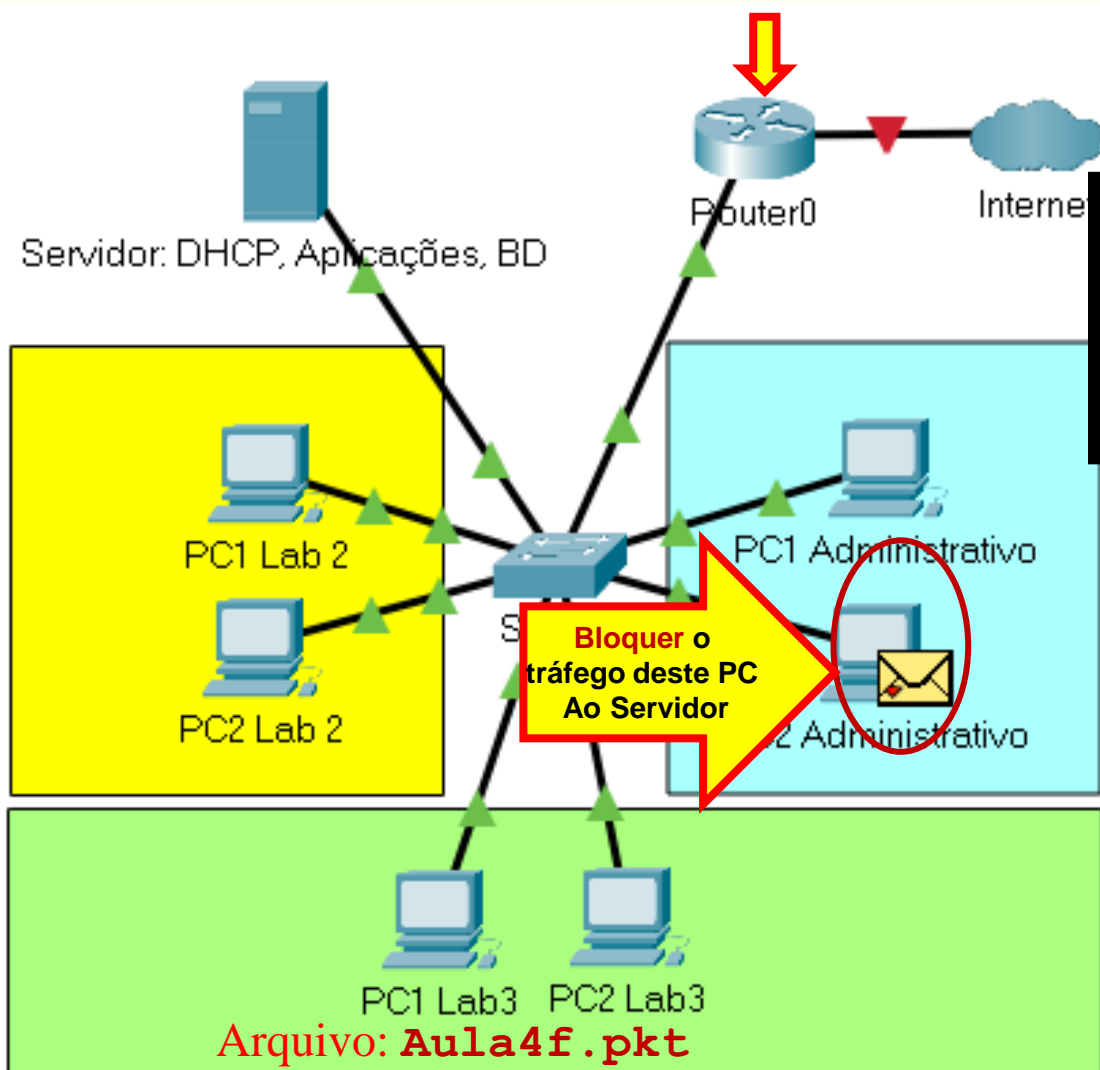


Como todo tráfego ENTRE vlans passará pelo roteador, poderemos implementar um 'Firewall' nesse equipamento

# Segurança: configuração de ACL



# Segurança: configuração de ACL



```
router>enable
router#configure terminal
router(config)#access-list 1 deny host 192.168.40.3
router(config)#access-list 1 permit any
router(config)#interface fa0/0.1
Router(config)#ip access-group 1 out
```

**VLAN**

**Resumo de configuração**

# Resumo da Configuração de VLAN

## Criar VLAN

```
Switch(vlan)#vlan 2  
Switch(vlan)#name marketing  
Switch(vlan)#exit
```

## Definir a VLAN de uma porta em modo acesso

```
Switch(config)#interface fastethernet f0/9  
Switch(config-if)#switchport mode access  
Switch(config-if)#switchport access vlan 2
```

## Definir a VLAN de uma porta em modo tronco (*trunk*)

```
Switch(config-if)#interface ethernet f0/7  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#switchport trunk allowed vlan all
```



# Para estudo:

## Conceitos Essenciais de Roteamento e Switching

**Capítulo 5**  
Configuração de switches

**Capítulo 6**  
VLANs

**Capítulo 7**  
Listas de Controle de Acesso

**Capítulo 8**  
DHCP

**Capítulo 9**  
NAT para IPv4

**Capítulo 10**  
Descoberta, gerenciamento e manutenção  
de dispositivos

**Seção 6.0**  
Ferramentas

**Seção 6.1**  
Segmentação de VLAN

**Seção 6.2**  
Implementações de VLAN

**Seção 6.3**  
Roteamento entre VLANs com o  
uso de roteadores

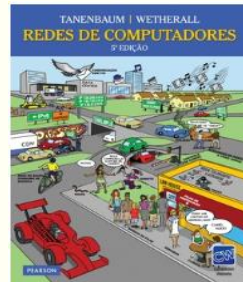
**Seção 6.4**  
Resumo

<https://www.netacad.com/>

# Referências Bibliográficas



Kurose, James F. Redes de computadores e a Internet: uma abordagem top-down/James F. Kurose e Keith W. Ross; 6ª edição, São Paulo: Addison Wesley, 2013. ISBN 978-85-8143-677-7.



Tanenbaum, Andrew S; Wetherall, David. Redes de Computadores. São Paulo: Pearson Prentice Hall, 2011. 5ª edição americana. ISBN 978-85-7605-924-0.



BIRKNER, Mathew H. Projeto de Interconexão de Redes. São Paulo: Pearson Education do Brasil, 2003. ISBN 85.346.1499-7.

## Referências Bibliográficas

- Tanenbaum, A.; Wetherall, D. Redes de Computadores. 5ª ed. Pearson, 2011.
- Wikipedia. IEEE 802.1Q. Disponível em [http://en.wikipedia.org/wiki/IEEE\\_802.1Q](http://en.wikipedia.org/wiki/IEEE_802.1Q)
- IEEE. 802.1Q-2011 - IEEE Standard for Local and metropolitan area networks-- Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks. Disponível em <http://standards.ieee.org/findstds/standard/802.1Q-2011.html>
- ODOM, W. CCNA ICND2 – Guia Oficial de Certificação do Exame. 2ª ed. Alta Books, 2008.