

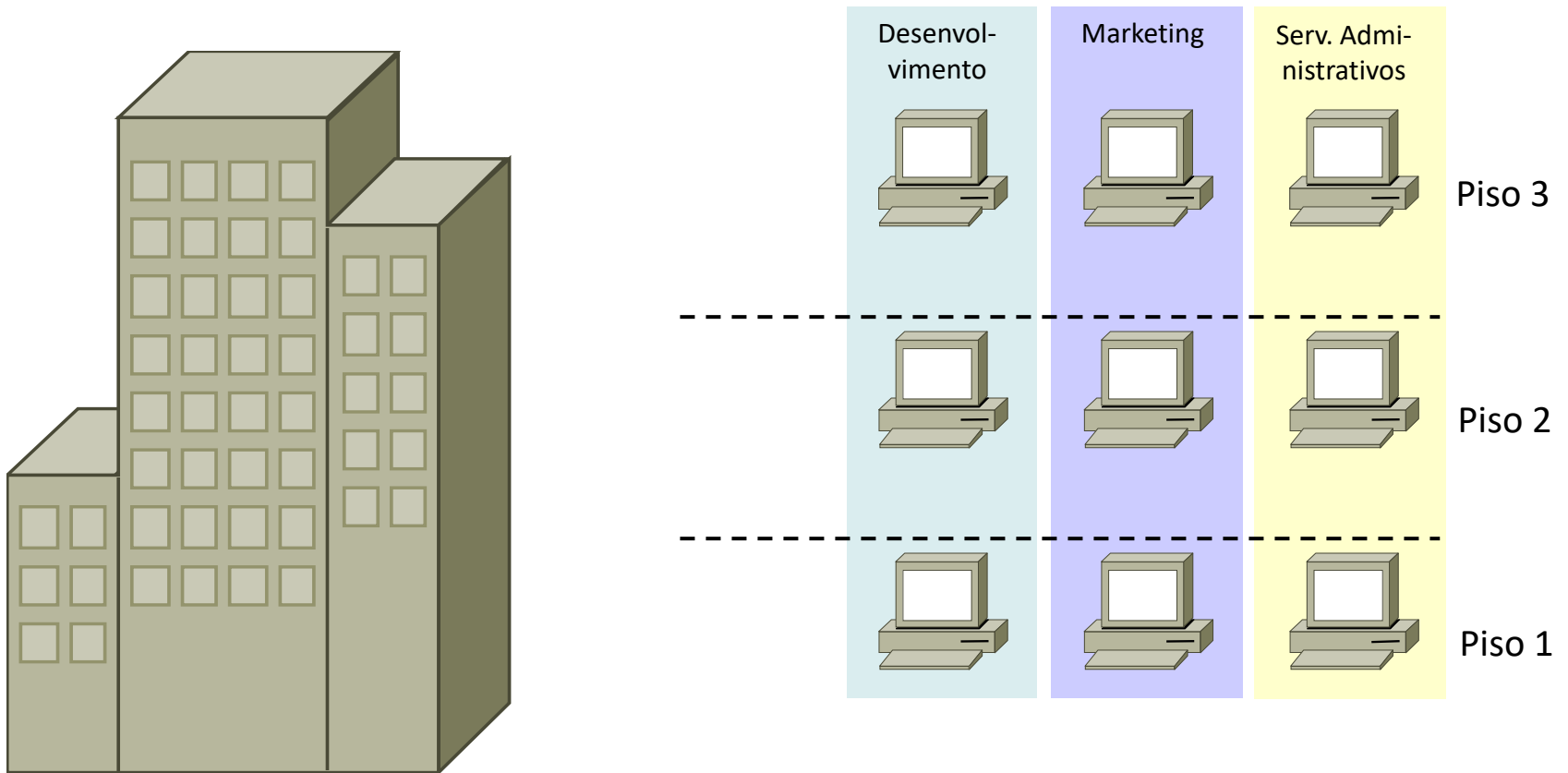
# Administração de Redes 2023/24

Virtual Local Area Networks (VLAN)

# Introdução

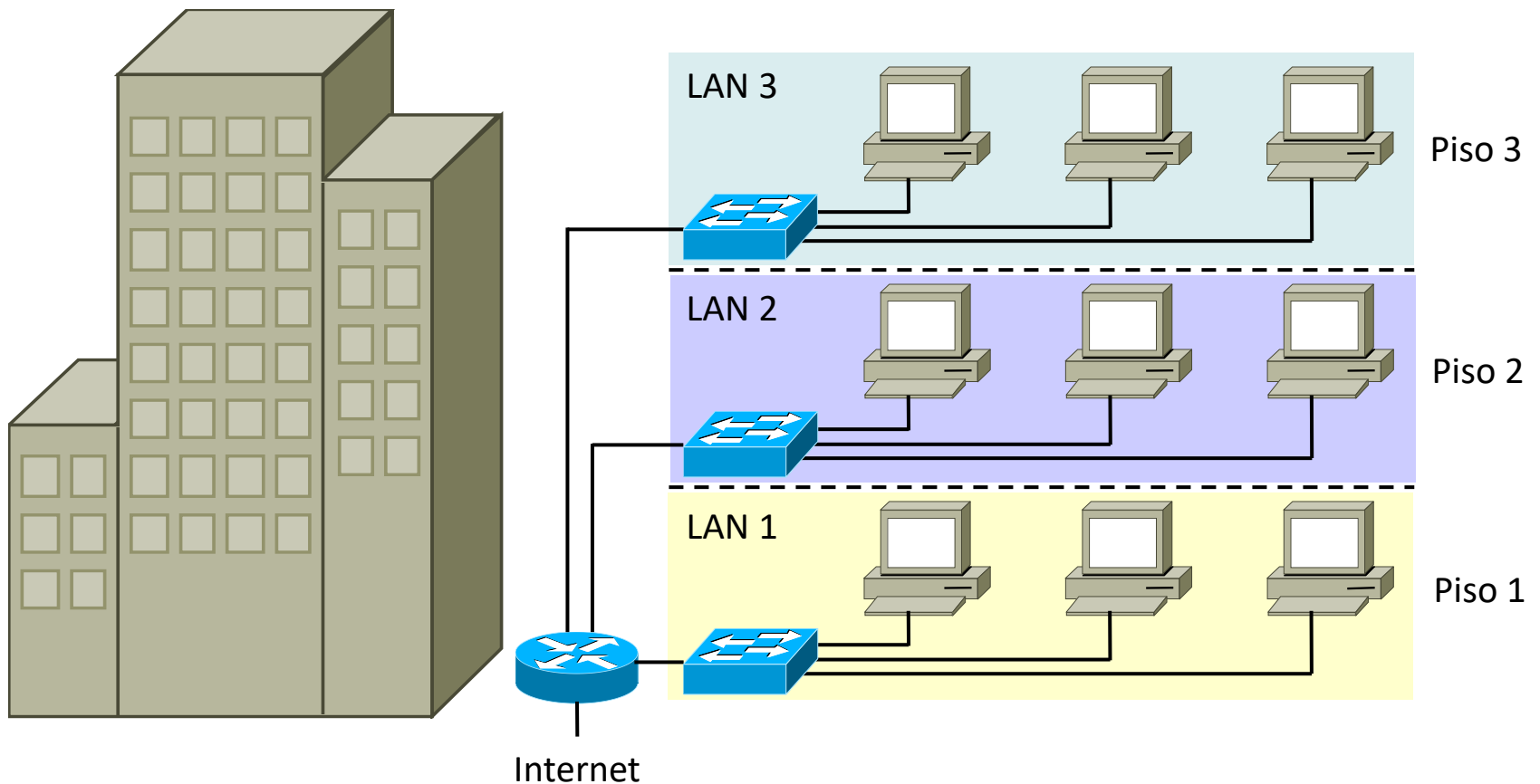
- Frequentemente é necessário dividir uma rede em "ilhas" sem ligação directa entre si (domínios de difusão separados)
  - Organização da rede, desempenho, segurança, privacidade, etc.
- Tradicionalmente, a divisão lógica correspondia à divisão física
  - E.g., com *ethernet* cada domínio de difusão corresponde a um ou mais computadores ligados entre si → LAN independente
  - Comunicação entre as diferentes LAN ("ilhas") através de *routers*
- Problema: muitas vezes a divisão lógica que se pretende não se mapeia bem na organização física do espaço

# Organização lógica desejada



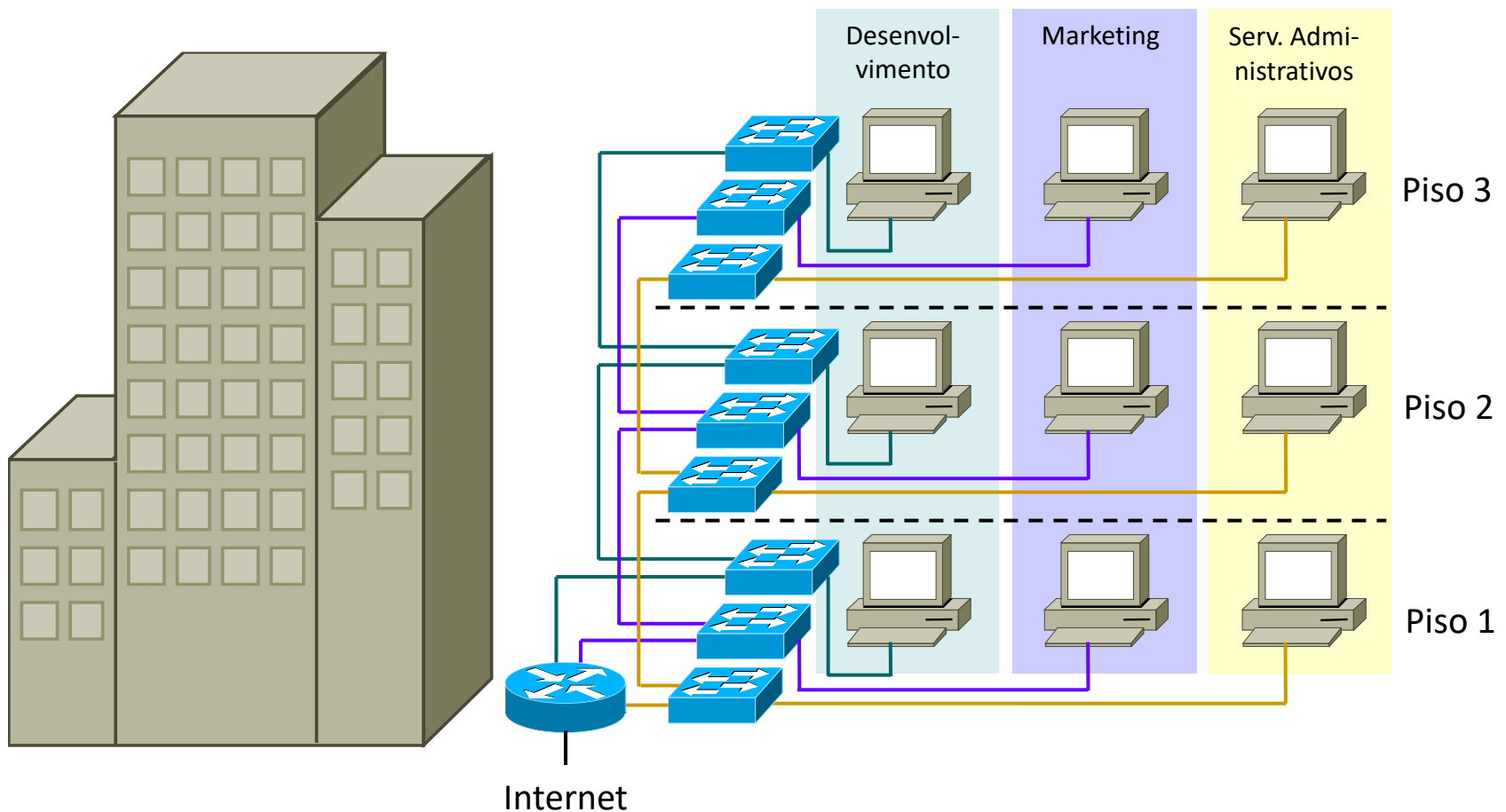
# Organização física

- Não se mapeia na organização lógica desejada



# Solução indesejável

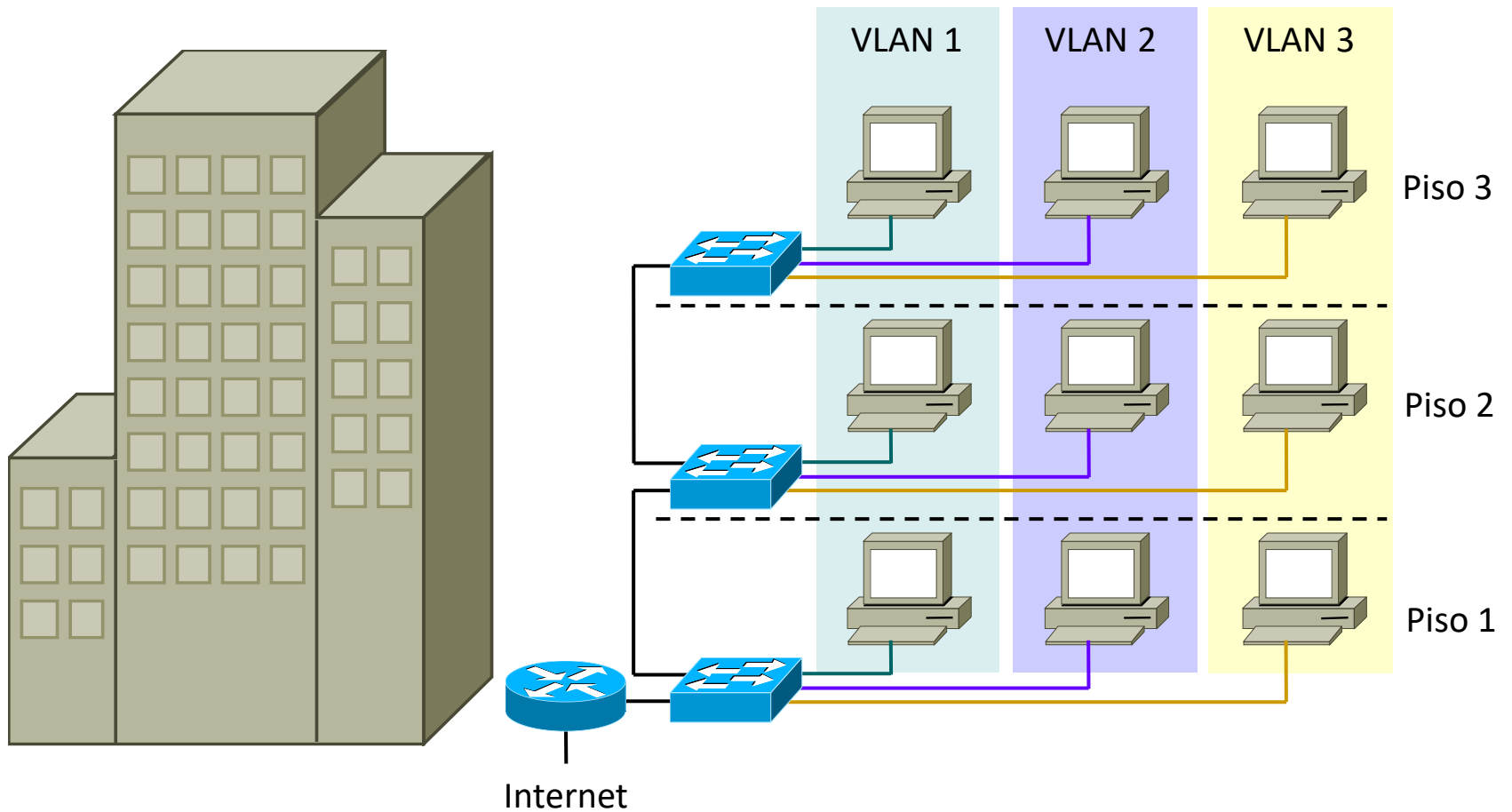
- Multiplicação do *hardware* necessário (comutadores, cablagem)
- A falta de uma porta no comutador de uma LAN obriga à compra de outro, mesmo que sobrem portas nos comutadores das outras LAN



# LAN Virtuais (VLAN)

- Muitos comutadores permitem configurar conjuntos de portas como se fossem LAN fisicamente independentes
  - LAN virtuais — VLAN
- Cada VLAN é um domínio de difusão
  - Tramas *broadcast* propagadas apenas às portas pertencentes à VLAN
- Não há comunicação directa entre VLAN diferentes
  - Cada VLAN vai corresponder a uma sub-rede diferente
  - Tal como no caso de várias LAN fisicamente independentes, a comunicação entre diferentes VLAN faz-se através de *routers*
    - Ou dos chamados comutadores de camada 3, que são basicamente 2-em-1 de comutador e *router*
- O uso de VLAN permite tornar a organização lógica da rede independente da configuração física dos equipamentos

# Uso de VLAN



# Atribuição de VLAN a portas físicas

- A atribuição de VLAN pode ser feita de diferentes formas
  - Por configuração directa — VLAN estáticas
  - De forma automática, segundo determinado critério — VLAN dinâmicas
- Alguns critérios para atribuição de VLAN a portas físicas
  - Endereço MAC do terminal
  - Autenticação 802.1x
  - Endereço IP do terminal
    - Critério de camada 3 (camada de rede)
    - A comutação continua a ser feita na camada 2 (ligação de dados), o endereço IP é usado apenas inicialmente para atribuir a VLAN à porta física



# Atribuição de VLAN a portas físicas

- Alguns comutadores permitem várias VLAN na mesma porta física, para pacotes de protocolos diferentes
  - Uso de portas (TCP, UDP) ou até informação da camada de aplicação!
  - Permite isolar e priorizar determinados tipos de tráfego (e.g., VoIP)
  - Permite fazer distribuição de carga
  - Violação da separação por camadas... ☹

# Interligação de comutadores com VLAN

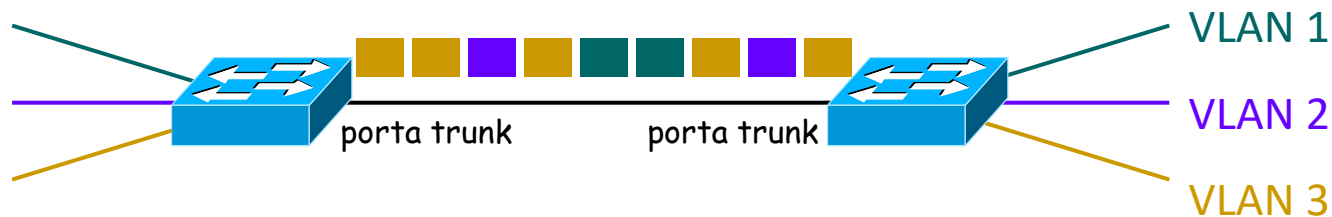
- Na interligação entre dois comutadores com várias VLAN têm que circular tramas de todas essas VLAN
- Não se podem misturar para não perder o isolamento entre VLAN diferentes
- Uma solução seria usar um cabo diferente para cada VLAN



- Esta solução é ineficiente
  - Impraticável com muitas VLAN

# Interligação de comutadores com VLAN

- Os comutadores que suportam VLAN têm dois tipos de configuração para cada porta
  - Modo acesso — pertence a uma única VLAN
  - Modo *trunk* — não pertence a uma VLAN específica, podendo transportar tramas de todas as VLAN
- A interligação entre comutadores faz-se usando portas *trunk*



- Para manter o isolamento entre VLAN, cada trama na ligação *trunk* tem que identificar a que VLAN pertence
  - Uso de uma etiqueta (VLAN tag)
- Tramas *ethernet* não têm campo para a etiqueta ☹
  - Portas *trunk* usam um encapsulamento diferente — 802.1Q

# Encapsulamento 802.1Q

- Trama enviada numa porta em modo acesso

Preamble 7	SFD 1	Dst Address 6	Src Address 6	Type 2	Data 46..1500	CRC 4
---------------	----------	------------------	------------------	-----------	------------------	----------

- Trama enviada numa porta em modo *trunk*

Preamble 7	SFD 1	Dst Address 6	Src Address 6	802.1Q Tag 4	Type 2	Data 42..1500	CRC 4
---------------	----------	------------------	------------------	-----------------	-----------	------------------	----------

Type (0x8100) 2 bytes	Prio 3 bits	DEI 1 bit	VLAN ID 12 bits
--------------------------	----------------	--------------	--------------------

- O tipo indica que é uma trama 802.1Q
- Prio e DEI controlam prioridade e possibilidade de descarte da trama
- VLAN ID de 12 bits permite 4096 VLAN diferentes

# VLAN Nativa

- Numa interface em modo *trunk*, a VLAN nativa é aquela
  - Cujas tramas são enviadas com encapsulamento *ethernet* normal
  - À qual são atribuídas tramas recebidas com encapsulamento *ethernet* normal
- Não confundir com VLAN-padrão (*default*), que é a VLAN atribuída a interfaces em modo acesso sem configuração explícita!
- Sem uma VLAN nativa, tramas recebidas com encapsulamento *ethernet* normal seriam descartadas
- Nos comutadores Cisco IOS, existe sempre uma VLAN nativa nas ligações *trunk* (embora possa ser filtrada)
- A VLAN nativa pode ser diferente em portas *trunk* diferentes
- Terminologia usada por outros fabricantes:
  - PVID (Port Vlan ID, aplicável apenas ao ingresso)
  - Untagged VLAN (aplicável apenas ao egresso)

# Configuração de VLAN em Cisco IOS

- Exemplo de criação de VLAN:

```
vtp mode transparent  
vlan 5  
  name Marketing
```

- A primeira linha indica que a configuração de VLAN é local
  - VTP é um protocolo para configuração centralizada de VLAN
  - O modo transparente é para não participar nesse protocolo
- A atribuição de nome à VLAN é opcional
  - Sem ela, o sistema atribuiria automaticamente o nome VLAN0005
- É possível criar várias VLAN de uma vez: `vlan 5,7-9,12`
  - Ficam com o nome automático
- A VLAN 1 (VLAN *default*) já vem preconfigurada
  - Usada por todas as portas a que não se atribua explicitamente outra

# Configuração de VLAN em Cisco IOS

- Configuração de f1/0 como porta de acesso na VLAN 5:  

```
interface FastEthernet 1/0  
  switchport mode access  
  switchport access vlan 5
```
- Configuração de f1/1 em modo *trunk* com encapsulamento 802.1Q:  

```
interface FastEthernet 1/1  
  switchport trunk encapsulation dot1q  
  switchport mode trunk
```
- Limitar as VLAN que circulam numa porta em modo *trunk*\* :  

```
switchport trunk allowed vlan 1,5,1002-1005
```

\* As VLAN 1 e 1002-1005 têm sempre que ser permitidas

# Configuração de VLAN em Cisco IOS

- Configuração da VLAN nativa numa porta em modo *trunk* :

```
interface FastEthernet 1/1  
  switchport trunk native vlan 5  
  switchport mode trunk
```



# Verificação das VLAN configuradas

```
SW1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa1/2, Fa1/3, Fa1/4, Fa1/5 Fa1/6, Fa1/7, Fa1/8, Fa1/9 Fa1/10, Fa1/11, Fa1/12, Fa1/13 Fa1/14, Fa1/15
5	Marketing	active	Fa1/0
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

# Verificação das interfaces trunk

```
SW1#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa1/1	on	802.1q	trunking	5

Port	Vlans allowed on trunk
Fa1/1	1-4094

Port	Vlans allowed and active in management domain
Fa1/1	1,5

Port	Vlans in spanning tree forwarding state and not pruned
Fa1/1	1,5

# Verificação do estado das interfaces

SW1#show interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa1/0		connected	5	a-full	a-100	10/100BaseTX
Fa1/1		connected	trunk	a-full	a-100	10/100BaseTX
Fa1/2		connected	1	a-full	a-100	10/100BaseTX
Fa1/3		connected	1	a-full	a-100	10/100BaseTX
Fa1/4		notconnect	1	auto	auto	10/100BaseTX
Fa1/5		notconnect	1	auto	auto	10/100BaseTX
Fa1/6		notconnect	1	auto	auto	10/100BaseTX
Fa1/7		notconnect	1	auto	auto	10/100BaseTX
Fa1/8		notconnect	1	auto	auto	10/100BaseTX
Fa1/9		notconnect	1	auto	auto	10/100BaseTX
Fa1/10		notconnect	1	auto	auto	10/100BaseTX
Fa1/11		notconnect	1	auto	auto	10/100BaseTX
Fa1/12		notconnect	1	auto	auto	10/100BaseTX
Fa1/13		notconnect	1	auto	auto	10/100BaseTX
Fa1/14		notconnect	1	auto	auto	10/100BaseTX
Fa1/15		notconnect	1	auto	auto	10/100BaseTX

# Configuração de VLAN em Cisco IOS

- Configuração do endereço IP do *router* numa dada VLAN
  - Semelhante à de qualquer outra interface

```
interface vlan 5  
  ip address 192.168.1.1 255.255.255.0  
  no shutdown
```

# Configuração de VLAN em Linux

Para funcionar como terminal ou router (sem comutação)

- Interfaces em modo acesso configuram-se normalmente
- Interfaces em modo *trunk* :
  1. Adicionar a(s) VLAN desejada(s)<sup>1</sup>

```
# vconfig add eth0 5
```

    - Ao criar a VLAN aparece uma nova interface (eth0.5, neste caso)
  2. Configurar a(s) interface(s) lógica(s)

```
ifconfig eth0.5 192.168.5.2 netmask 255.255.255.0 up
```
  3. O endereço na VLAN nativa configura-se na interface-mãe

```
ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
```

<sup>1</sup> Em vez do comando `vconfig` também pode usar-se o comando `ip`:  
`ip link add link eth0 name eth0.5 type vlan id 5`

# Configuração de VLAN em Linux

- Pode configurar de forma permanente interfaces VLAN
  - E.g., /etc/sysconfig/network-scripts/ifcfg-eth0.5
  - Ficheiro deve conter a linha  
VLAN=yes
- Verificar as VLAN configuradas:

```
# cat /proc/net/vlan/config
VLAN Dev name      | VLAN ID
Name-Type: VLAN_NAME_TYPE_RAW_PLUS_VID_NO_PAD
eth0.5             | 5   | eth0
```