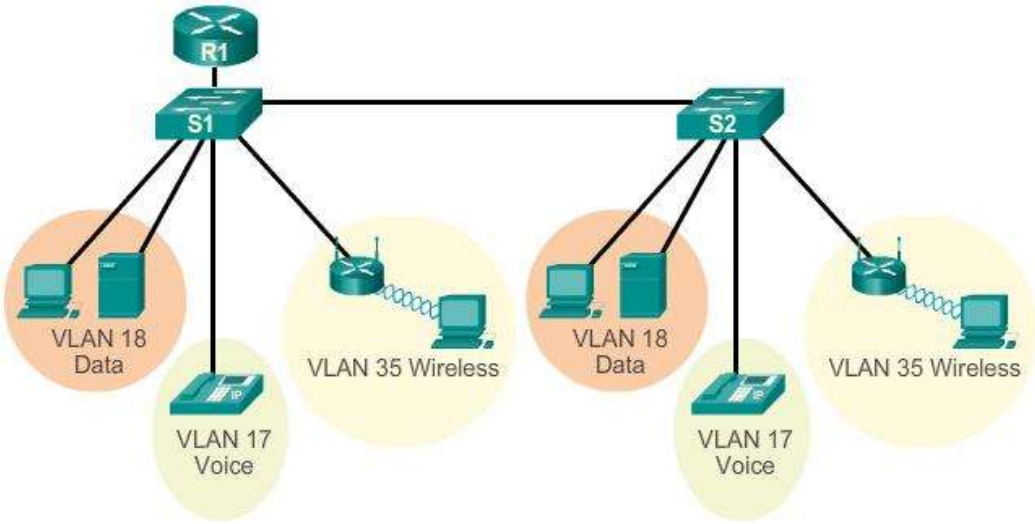
IPS Instituto Politécnico de Setúbal

Escola Superior de Tecnologia de Setúbal

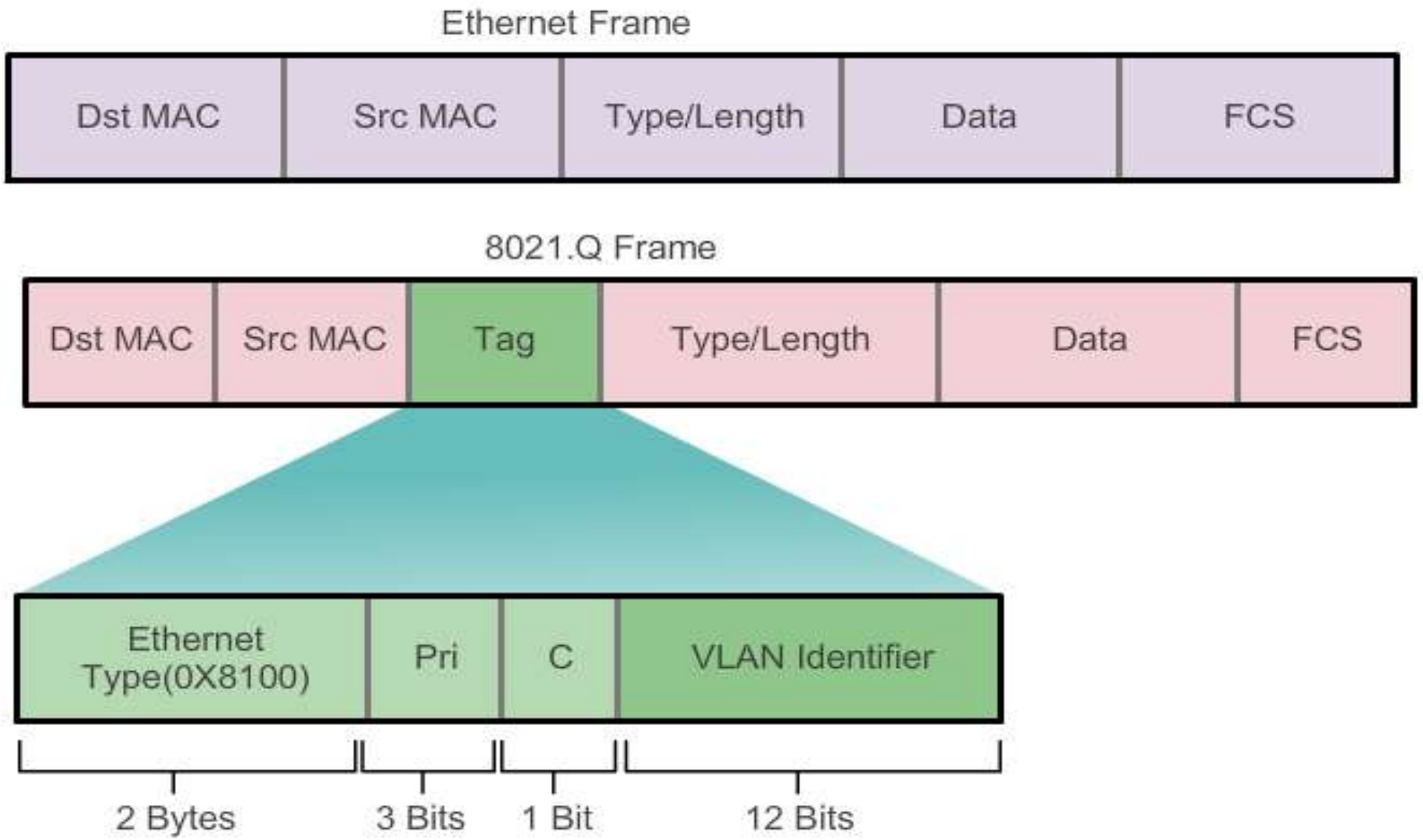


Virtual Local Area Networks (VLAN's)

Slides do CCNA Routing & Switching revistos e atualizados por
Luísa Caeiro, Jorge Martins e Teles Rodrigues

ESTSetúbal (v1)

Marcação das *Frames* para Identificação de VLANs



VLANs Nativas e *Tagging* 802.1q

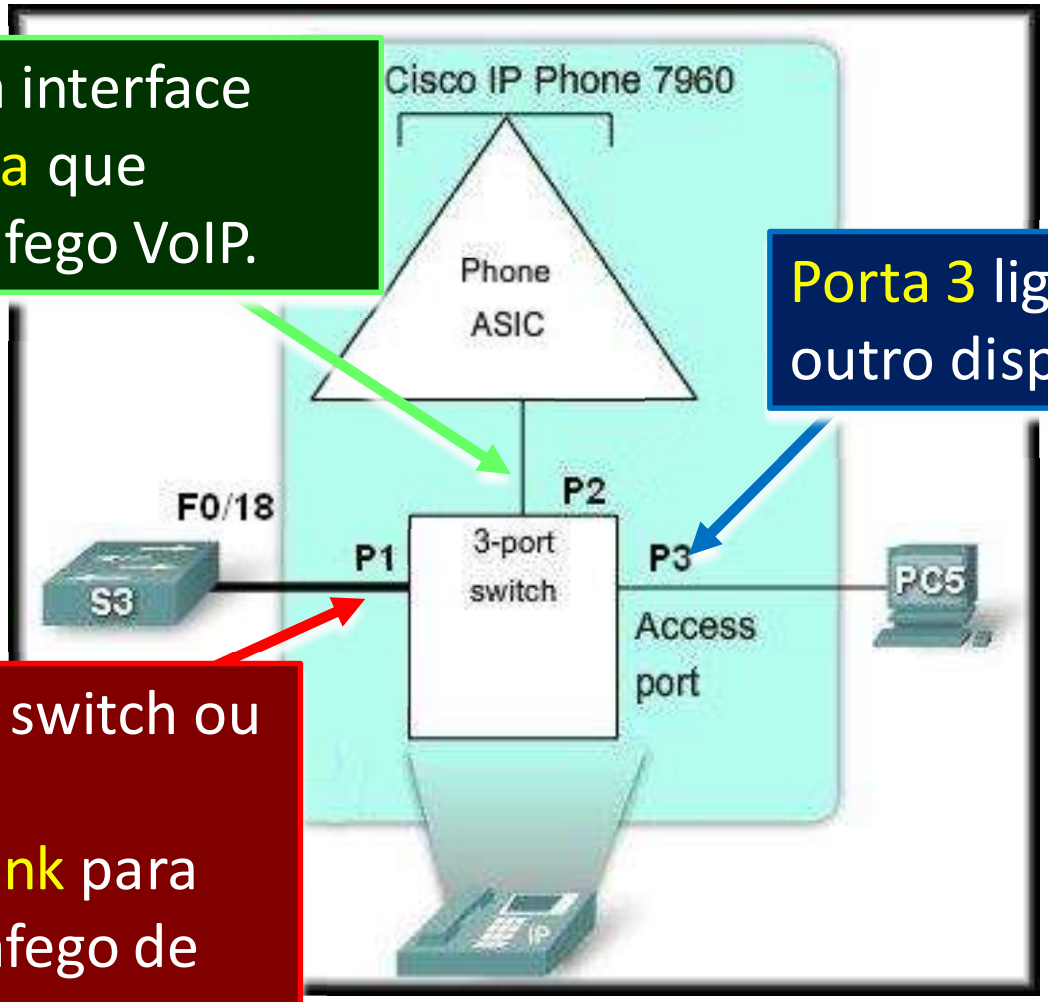
- As *frames* que pertencem à VLAN nativa não são marcadas.
- Se as *frames* recebidas não estiverem marcadas (*untagged)*, mantêm-se *untagged* e são encaminhadas na VLAN nativa.
- Se não existirem portas associadas à VLAN nativa e não existirem outras ligações de trunk, as *frames untagged* são descartadas.
- Nos switches Cisco, a VLAN nativa por omissão é a VLAN 1.

Marcação na VLAN de Voz

- O tráfego VoIP é *time-sensitive* e tem os seguintes requisitos:
  - Largura de banda garantida para assegurar qualidade de voz.
  - Prioridade na transmissãoem relação a outro tipo de tráfego de rede.
  - Capacidade para se encaminhado por fora de áreas congestionadas da rede.
  - Atraso inferior a 150 ms na rede.
- A VLAN de voz permite que as portas de acesso transportem tráfego de voz sobre IP a partir de um telefone IP.
- O switch pode-se ligar a um telefone IP Cisco 7960 e transportar tráfego de voz sobre IP. O switch suporta qualidade de serviço (QoS)
- A qualidade do som de uma chamada de voz sobre IP pode deteriorar-se se os pacotes não forem enviados regularmente.

Marcação na VLAN de Voz

Porta 2 é uma interface 10/100 interna que transporta tráfego VoIP.



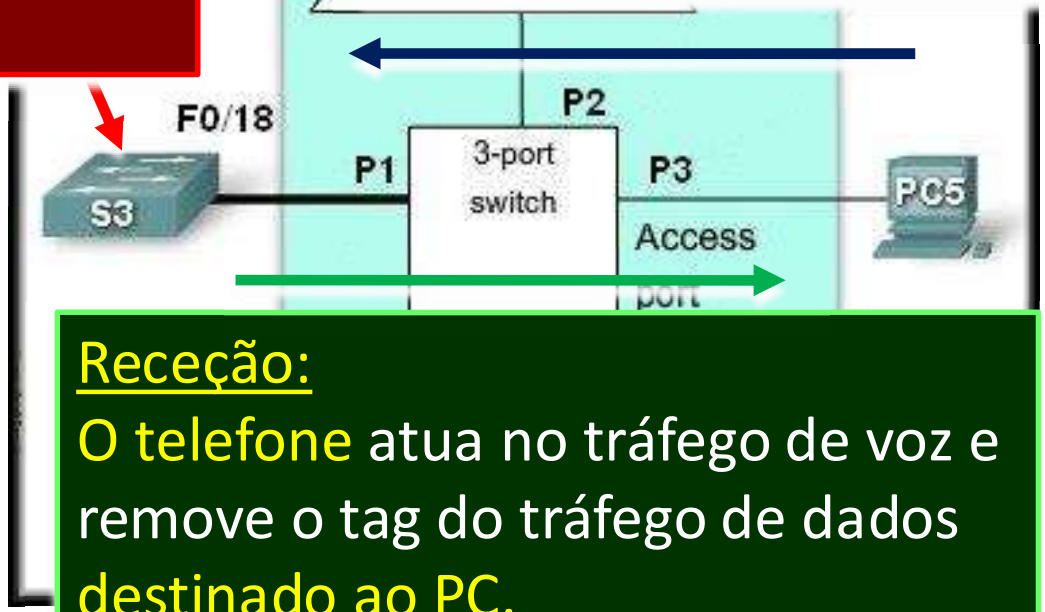
Porta 3 liga um PC ou outro dispositivo.

Porta 1 liga a um switch ou dispositivo VoIP.
Atua com um trunk para transporte de tráfego de voz e dados.

Marcação na VLAN de Voz

O switch S3 está configurado para transportar tráfego de voz na VLAN 150 e tráfego de dados na VLAN 20.

<u>Envio:</u>
O telefone marca o tráfego de voz na VLAN 150 e envia o tráfego de dados *untagged*. O switch marca o tráfego de dados na VLAN 20.



<u>Receção:</u>
O telefone atua no tráfego de voz e remove o tag do tráfego de dados destinado ao PC.

VLAN IDs nos Switches Catalyst

- Os switches Cisco da série Catalyst 2960 and 3560 suportam até 4000 VLANs.
- As VLANs estão divididas em duas categorias:
  - **VLANs na gama normal (VLAN 1 a 1005)**
    - Configurações guardadas em flash:vlan.dat
    - VLAN Trunking Protocol (VTP) só aprende e guarda VLANs da gama normal
  - **VLANs na gama estendida (VLAN 1006 a 4096)**
    - Configurações guardadas no ficheiro *running configuration*
    - VTP não aprende VLANs da gama estendida

Criação de uma VLAN

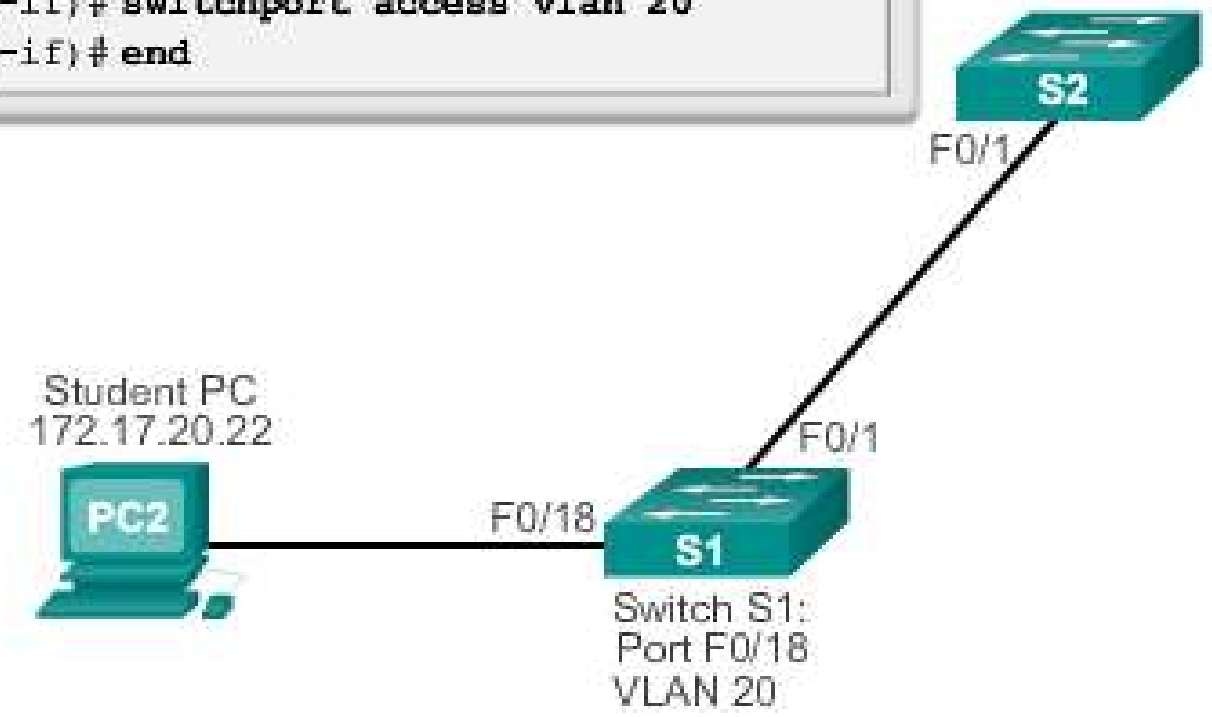
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan_id`
Specify a unique name to identify the VLAN.	`S1(config)# name vlan_name`
Return to the privileged EXEC mode.	`S1(config)# end`

Atibuição de Portas às VLANs

Cisco Switch IOS Commands	
Enter global configuration mode.	S1 # **configure terminal**
Enter interface configuration mode for the SVI.	S1(config) # **interface** *interface_id*
Configure the management interface IP address.	S1(config) # **ip address 172.17.99.11**
Set the port to access mode.	S1(config-if) # **switchport mode access**
Assign the port to a VLAN.	S1(config-if) # **switchport access vlan** *vlan_id*
Return to the privileged EXEC mode.	S1(config-if) # **end**

Atibuição de Portas às VLANs

```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



Alteração da atribuição da Porta a uma VLAN

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

Alteração da atribuição da Porta a uma VLAN

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
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, Fa0/12, Fa0/1
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/
                                     Gi0/2
20   student              active     Fa0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Apagar VLANs

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh 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, Fa0/12, 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
S1#
```

Verificação da Informação de VLAN

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

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

S1#
```

Verificação da Informação de VLAN

```
S1# show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Configuração de *Trunk* IEEE 802.1q

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Force the link to be a trunk link.	`S1(config-if)# switchport mode trunk`
Specify a native VLAN for untagged 802.1Q trunks.	`S1(config-if)# switchport trunk native vlan vlan id`
Specify the list of VLANs to be allowed on the trunk link.	`S1(config-if)# switchport trunk allowed vlan vlan-list`
Return to the privileged EXEC mode.	`S1(config-if)# end`

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

Reinicialização do *Trunk* para Estado por Omissão

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Reinicialização do *Trunk* para Estado por Omissão

Return Port to Access Mode

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

Verificação da Configuração de *Trunk*

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Introdução ao *Dynamic Trunking Protocol*

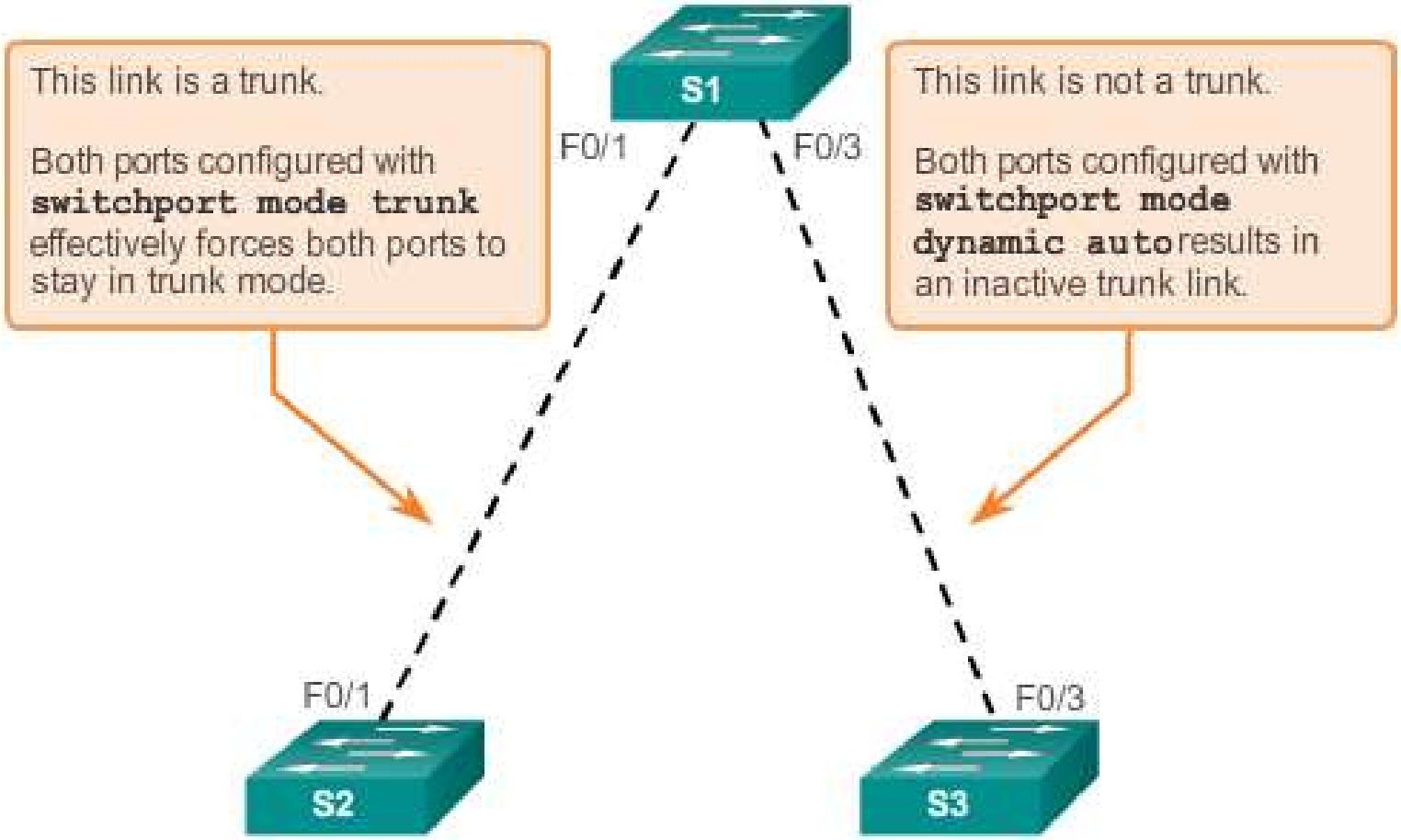
- Uma porta de *trunk* pode ser configurada para negociar e estabelecer um *trunk* com outra a que esteja ligada.
- O protocolo *Dynamic Trunking Protocol (DTP)* gere a negociação do *trunk* se a porta no switch vizinho estiver também configurada num modo *trunk* que suporte DTP.
- DTP é um protocolo proprietário da Cisco e está ativo por omissão nos switches Cisco Catalyst 2960 and 3560:

Modos de Interface Negociados

- O modo DTP por omissão é o *dynamic auto*.
- Os outros modos DTP suportados são: *dynamic desirable trunk* e *nonegotiate.*

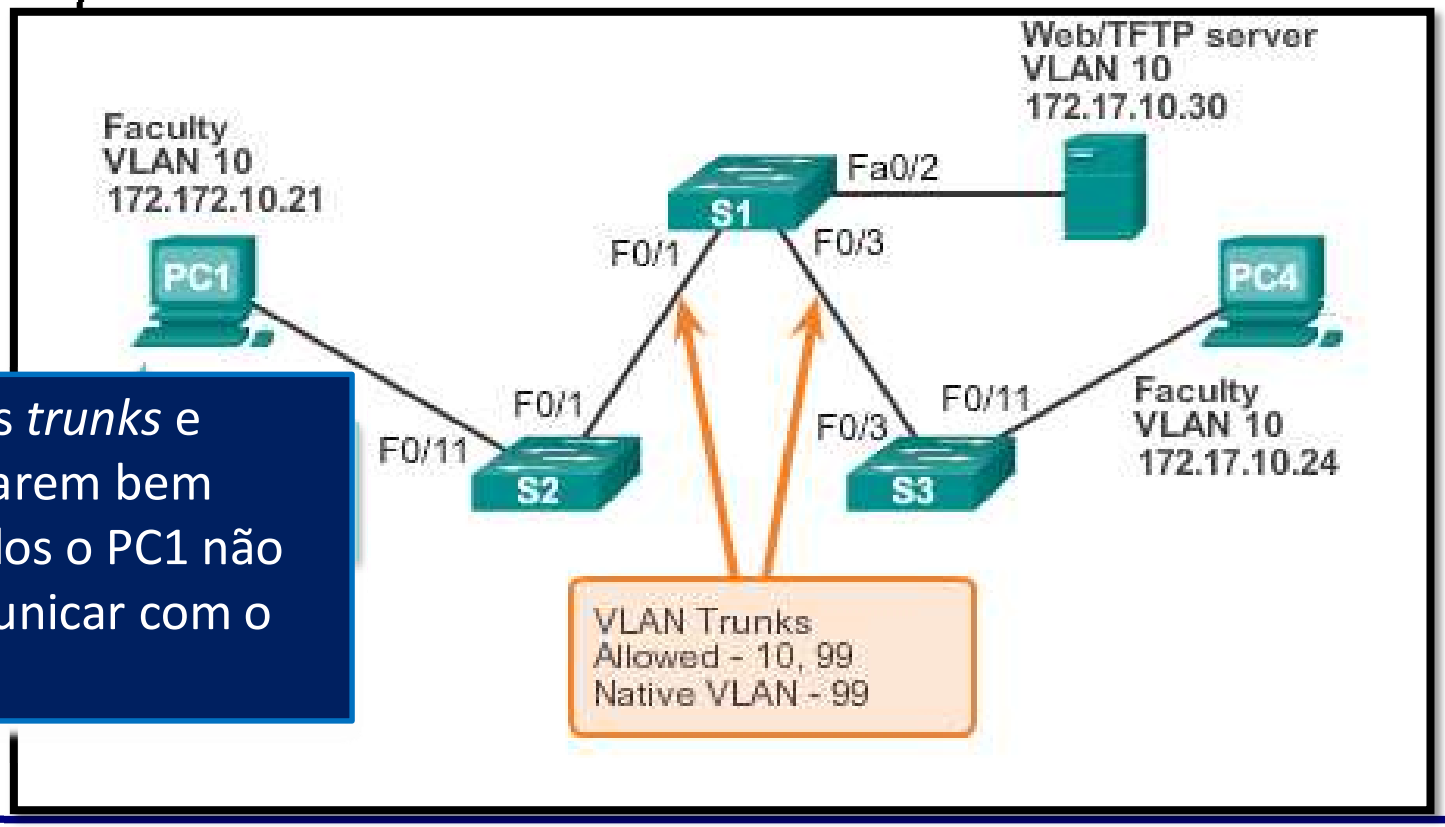
	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

Modos de Interface Negociados



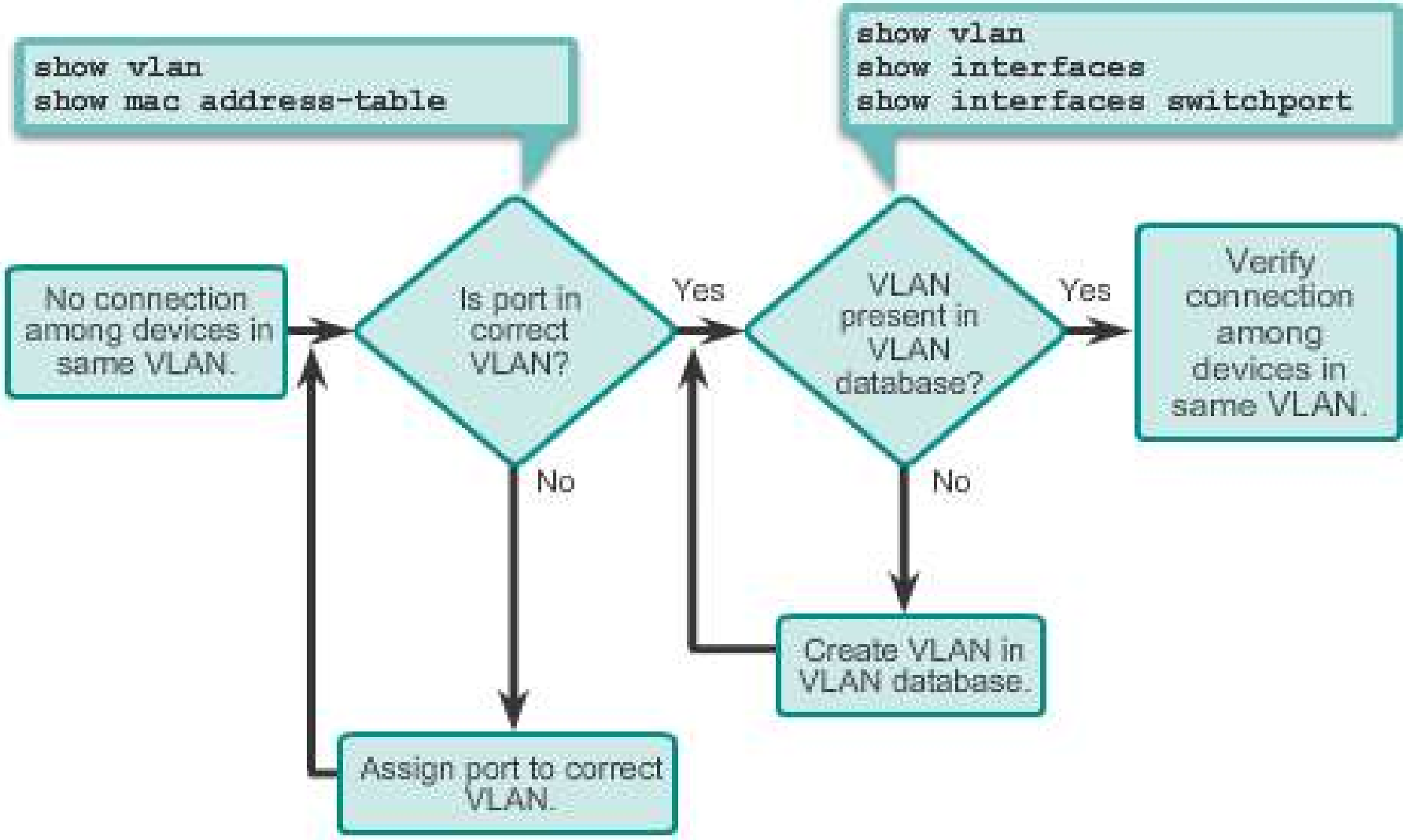
Endereçamento IP nas VLANs

- É prática comum associar uma VLAN com uma rede IP.
- Todos os dispositivos numa VLAN devem estar na mesma rede IP para comunicar entre si.

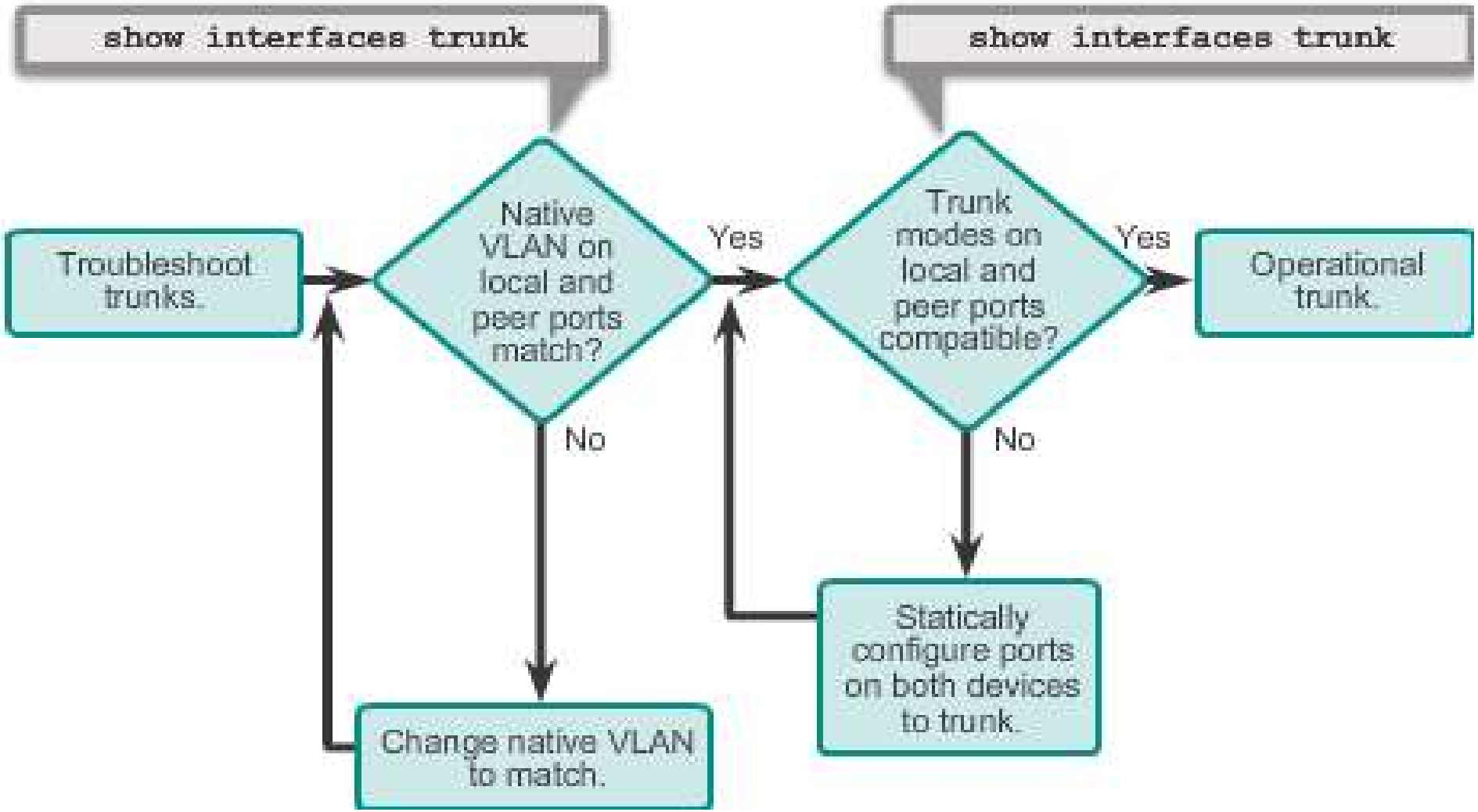


Apesar dos *trunks* e VLANs estarem bem configurados o PC1 não pode comunicar com o Servidor.

Resolução de Problemas com VLANs



Resolução de Problemas com *Trunks*



Problemas Comuns com *Trunks*

- Problemas *com trunks* estão normalmente associados a configurações incorretas.
- Os problemas mais comuns são:
  - VLAN nativa não corresponde nas duas extremidades.
  - Modo de *Trunk* não corresponde nas duas extremidades.
  - VLANs não permitidas no *Trunk*.

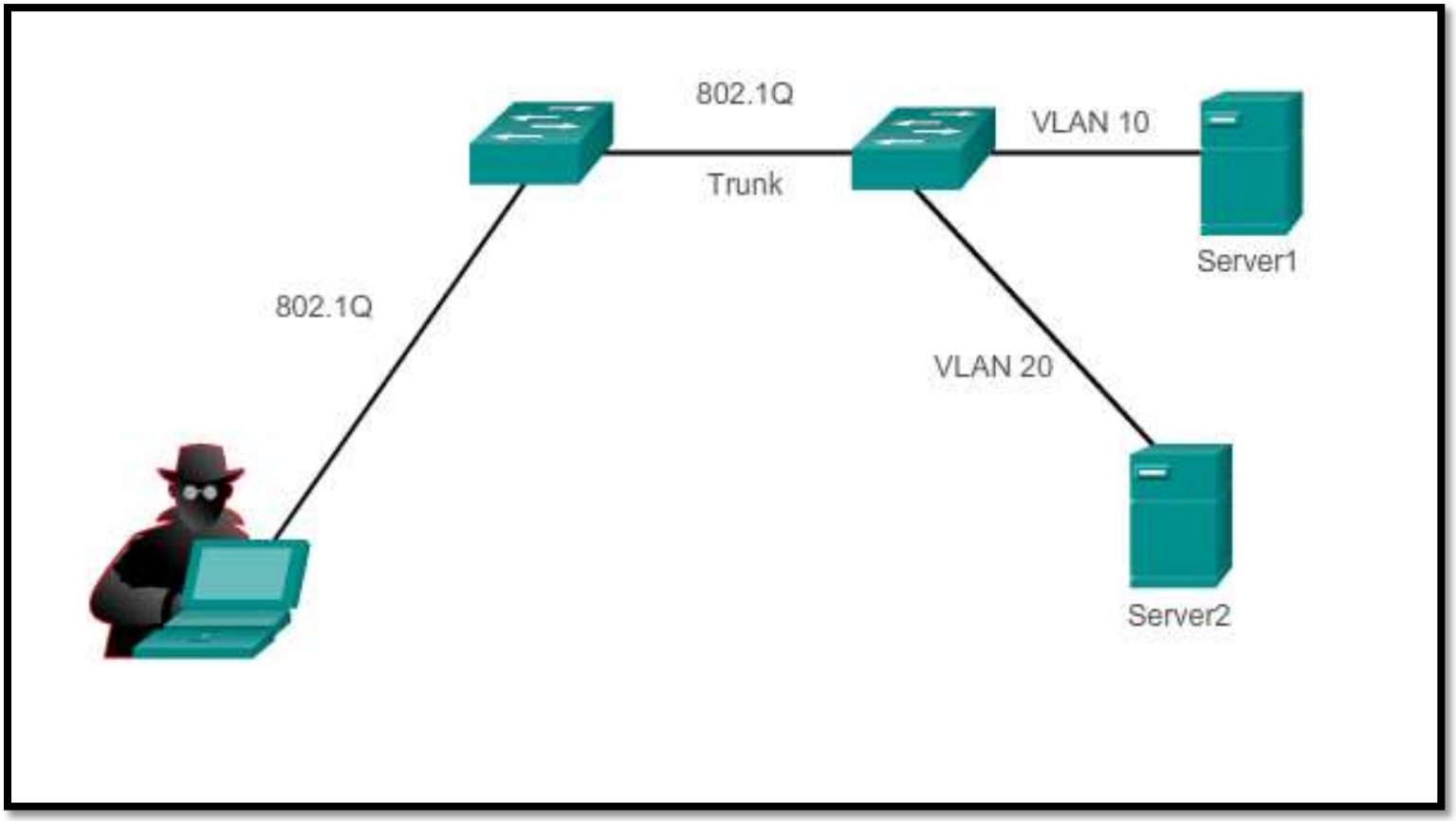
Modo de *Trunk* Incompatível

- Se uma porta numa ligação de trunk está configurda com um modo de *trunk* incompativel com a porta de *trunk* no switch vizinho, a formação do trunk entre os dois vizinhos falha.
- Use o comando *show interfaces trunk* para verificar o estado das portas de *trunk* nos switches.
- Para corrigir o problema, configure as interfaces com os modos de *trunk* adequados.

Lista de VLANs Incorreta

- As VLANs devem estar permitidas no *trunk* antes das suas *frames* poderem ser transmitidas.
- Use o comando *show interfaces trunk* para assegurar que as VLANs certas estão a ser permitidas no trunk.
- Use o comando *switchport trunk allowed vlan* para especificar que VLANs são permitidas na ligação de *trunk*.

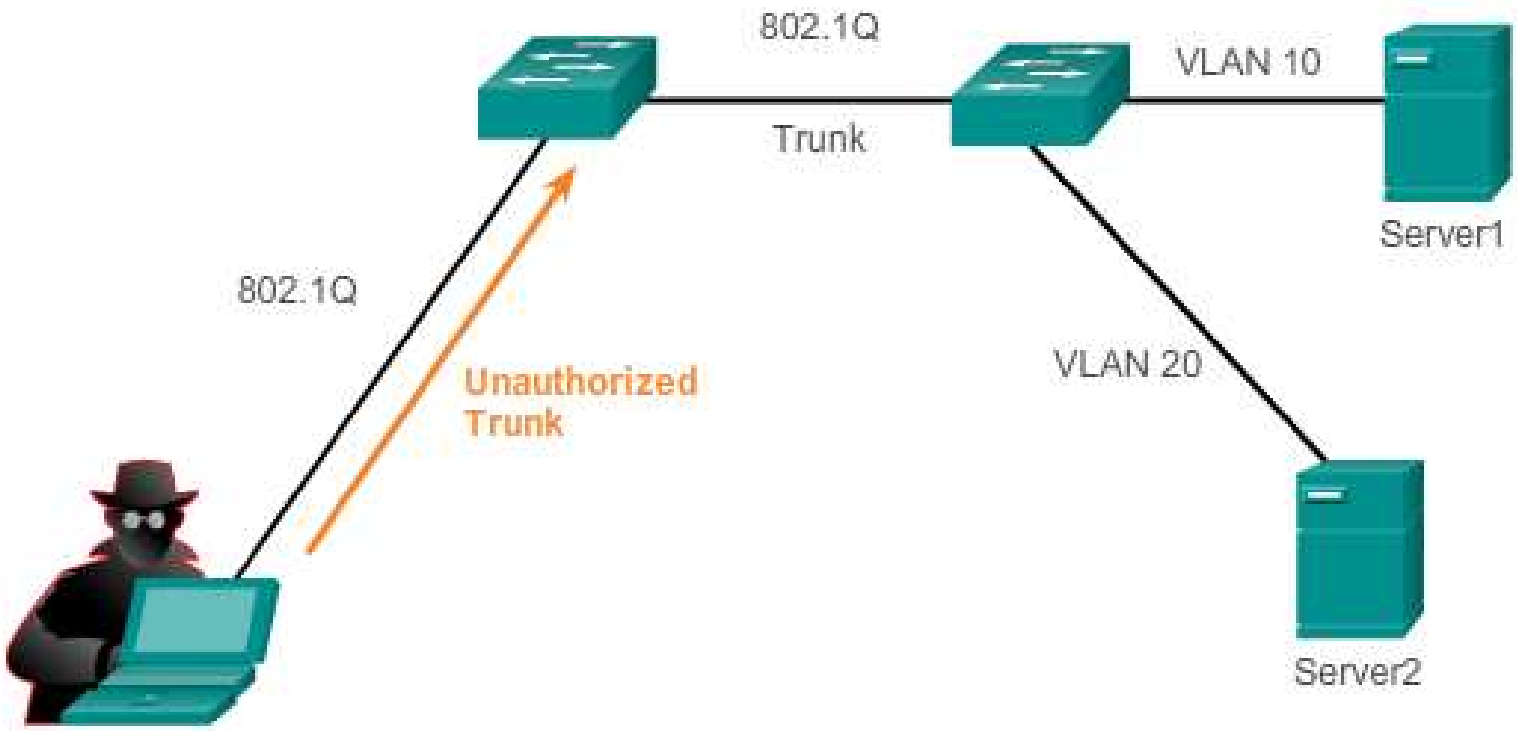
Segurança nas VLANs



Ataques nas VLANs – *Switch Spoofing*

- Switch *Spoofing* é um tipo de *VLAN hopping attack uma vez que* o *attacker* passa a ter acesso a outras VLANs.
- É explorado fato da configuração por omissão das portas do switch ser *dynamic auto:*
  - Se o *attacker* configurar um *host* para atuar como switch em modo *trunk,* pode ganhar acesso a qualquer VLAN.
- Para impedir um ataque deste tipo, em que se cria a ilusão (*spoofing*) de um switch, devem desativar-se o trunking em todas as portas excepto as que são especificamente *trunks*.

Ataques nas VLANs – *Switch Spoofing Attack*

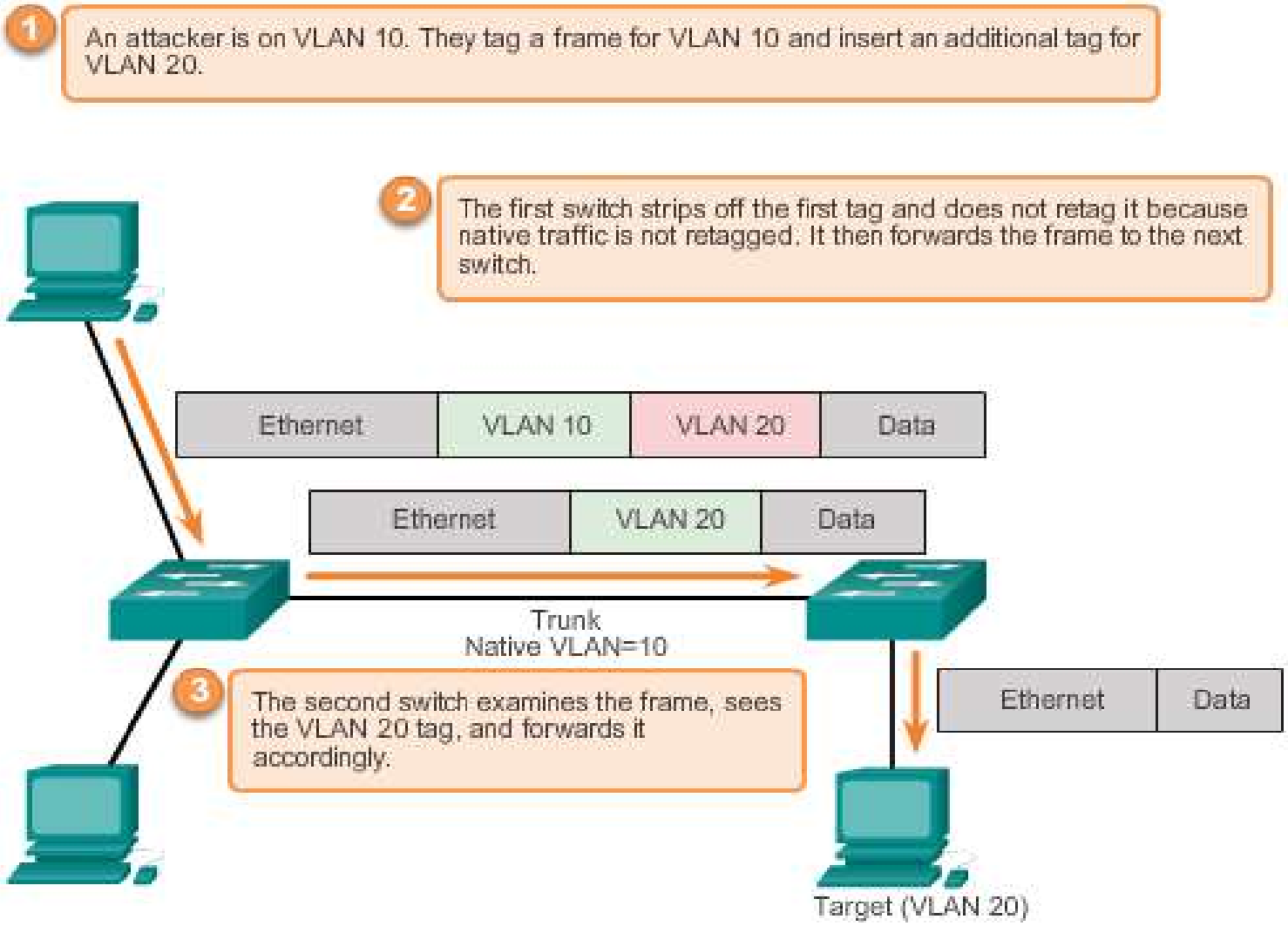


Attacker gains access to the server VLAN.

Ataques nas VLANs - *Double-Tagging*

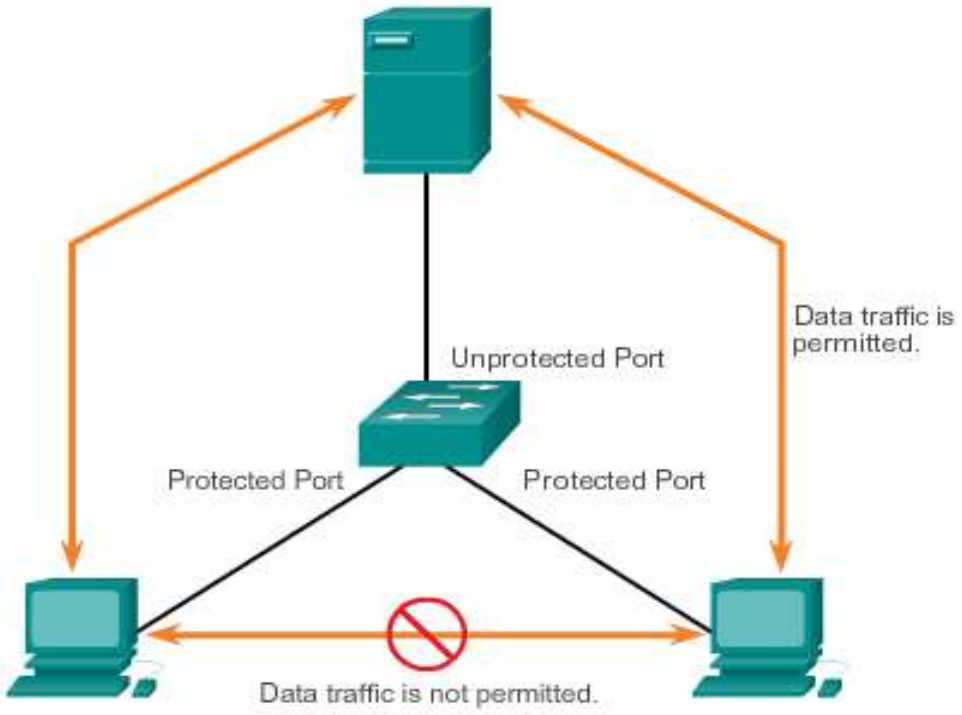
- O *Double-tagging attack* explora a forma como o *hardware* desencapsula as *tags* 802.1q na maioria dos switches, aplicando apenas um nível de desencapsulamento:
  - A transferência da *frame* pode ser forçada para outra VLAN através da introdução de um 2º VLAN ID não autorizado.
- Se a *frame* for enviada na VLAN nativa e marcada com o seu VLAN ID, o switch remove o cabeçalho da VLAN nativa e não volta a marcar a *frame*, sendo o 2º *tag* o considerado.
- A melhor abordagem para mitigar este ataque é garantir que a VLAN nativa nas portas de *trunk* é diferente da VLAN de qualquer porta usada.

Attacks on VLANs - *Double-Tagging Attack*



PVLAN Edge

- A funcionalidade *Private VLAN (PVLAN) Edge*, também conhecida como proteção de portas, assegura que não há trocas de tráfego *unicast*, *broadcast*, ou *multicast* entre portas protegidas no switch.
  - Uma porta protegida só troca tráfego com portas não protegidas.
  - Evita ataques diretos entre PCs.
  - Só tem relevância local.



Orientações para Desenho de VLANs

- Retirar todas as portas da VLAN 1 e atribuí-las a uma VLAN que não esteja em uso.
- Desativar todas as portas não usadas.
- Separar o tráfego de gestão do tráfego de dados de utilizador.
- Alterar a VLAN de gestão para outra que não a VLAN 1.
- Alterar a VLAN de nativa para outra que não a VLAN 1
- Assegurar que só os dispositivos na VLAN de gestão podem-se ligar aos switches.

Orientações para Desenho de VLANs

- Permitir apenas ligações remotas ao switch por SSH.
- Desativar auto negociação nas portas de *trunk*.
- Não usar os modos de porta *auto* ou *desirable*.
- Utilizar VLANs separadas para tráfego de VoIP e de dados.