Capítulo 3: Implementar a segurança através de VLANs

Roteamento e Switching

Cisco | Networking Academy®
Mind Wide Open™

Capítulo 3

3.1 Segmentação de VLAN

3.2 Implementação de VLAN

3.3 Segurança e design da VLAN

3.4 Resumo

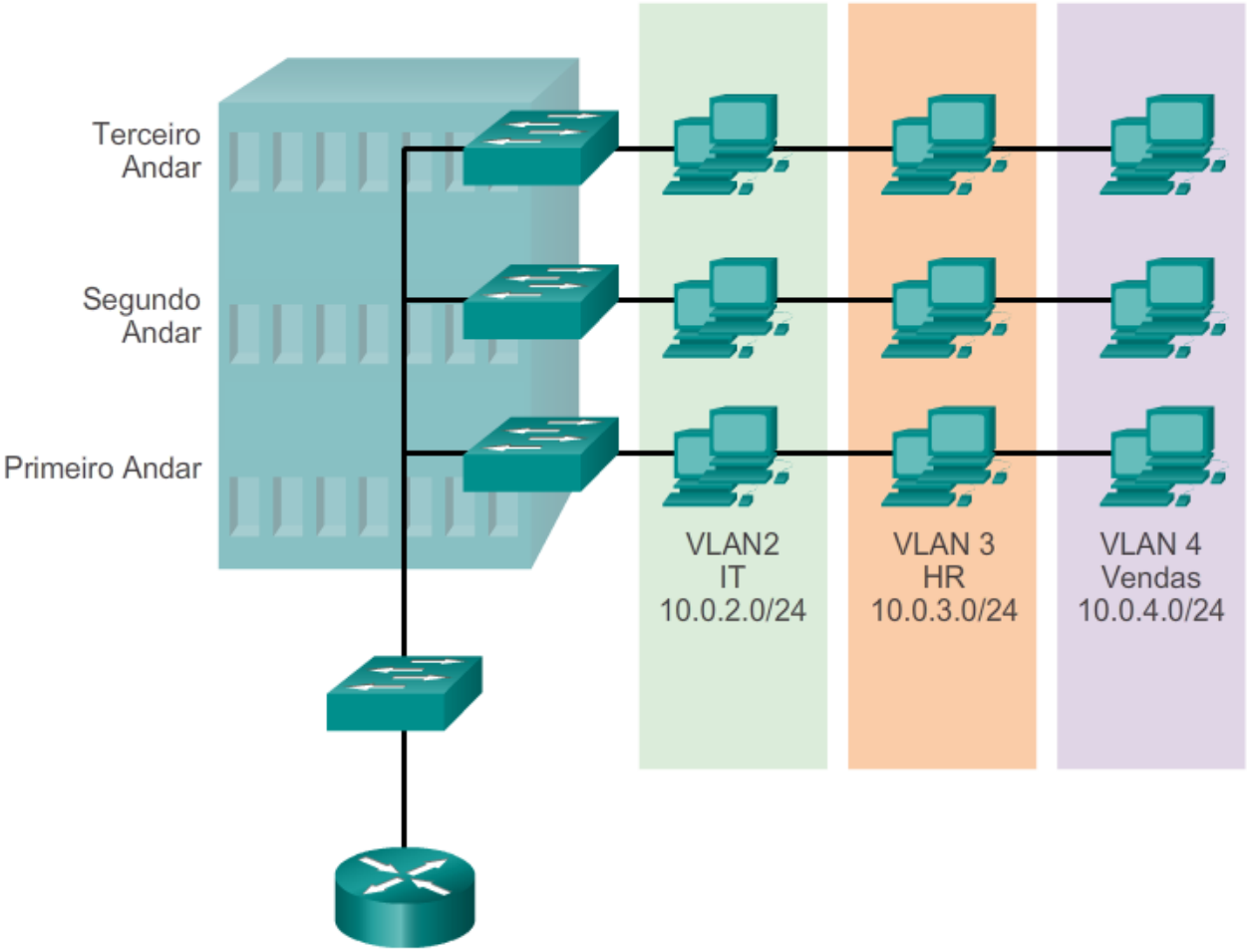
Capítulo 3: Objetivos

- Explicar a finalidade da VLAN em uma rede comutada
- Analisar como um switch encaminha a configuração de VLAN baseada em quadros em um ambiente multicomutado
- Configurar uma porta de switch a ser atribuída a uma VLAN com base nos requisitos
- Configurar uma porta de tronco em um switch de LAN
- Configurar o Dynamic Trunk Protocol (DTP)
- Identificar e Solucionar Problemas de Configuração de VLAN e Tronco em uma Rede Comutada
- Configurar recursos de segurança para atenuar ataques em um ambiente segmentado por VLAN
- Explicar as práticas recomendadas de segurança para um ambiente segmentado por VLAN

Definições de VLAN

- A VLAN (LAN virtual) é uma partição lógica de uma rede da camada 2
- Várias partições podem ser criadas, permitindo a coexistência de várias VLANs
- Cada VLAN é um domínio de broadcast, geralmente com sua própria rede IP
- As VLANS são mutuamente isoladas e os pacotes só podem transmitir entre eles por meio de um Roteador
- O particionamento da rede da camada 2 é realizado dentro de um dispositivo da camada 2, geralmente um switch.
- Os hosts agrupados em uma VLAN não reconhecem as VLANs existentes

Definições de VLAN



Vantagens de VLANs

- Segurança
- Redução de custo
- Melhor desempenho
- Domínios de broadcast menores
- Maior eficiência da equipe de TI
- Projeto e gerenciamento de aplicativos mais simples

Tipos de VLANs

- VLAN de dados
- VLAN padrão
- VLAN nativa
- VLAN de gerência

Tipos de VLANs

VLAN 1

```
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
```

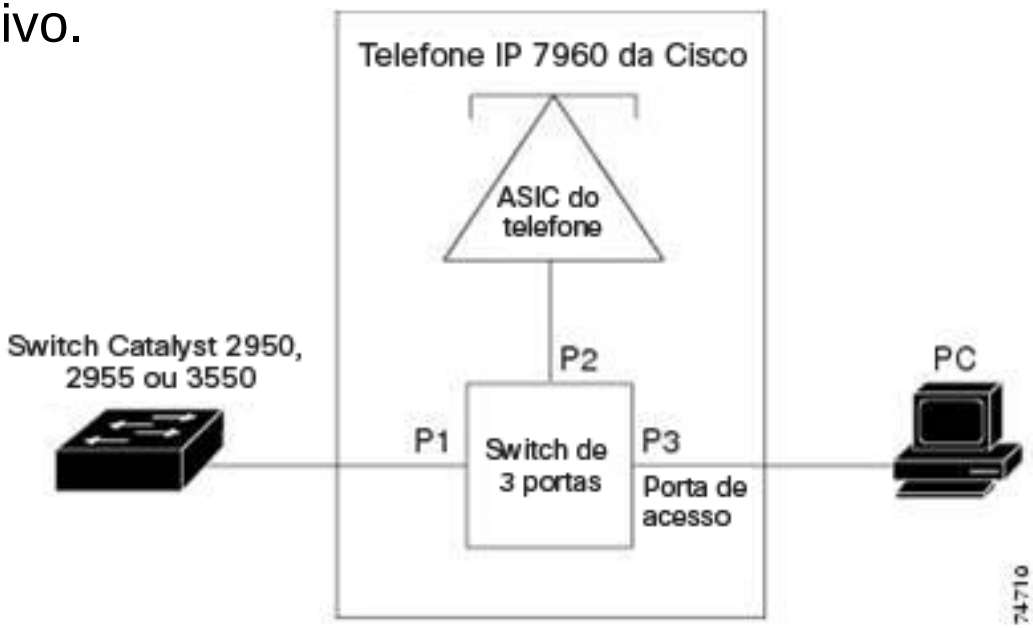
- Todas as portas estão atribuídas à VLAN 1 para encaminhar dados por padrão.
- A VLAN nativa é a VLAN 1 por padrão.
- A VLAN de gerenciamento é a VLAN 1 por padrão.
- A VLAN 1 não pode ser renomeada ou excluída.

VLANs de voz

- O tráfego de VoIP é urgente e requer:
  - Largura de banda garantida para assegurar a qualidade de voz
  - Prioridade de transmissão sobre outros tipos de tráfego de rede
  - Capacidade para roteamento em áreas congestionadas na rede
  - Atraso de menos de 150 ms na rede
- O recurso de VLAN de voz permite que as portas de acesso transportem o tráfego de voz IP de um telefone IP
- O switch pode se conectar a um Telefone IP Cisco 7960 e transportar o tráfego de voz IP
- Como a qualidade do som de uma chamada de telefone IP poderá se deteriorar se os dados forem enviados de modo irregular, o switch suporta qualidade de serviço (QoS)

VLANs de voz

- O Telefone IP Cisco 7960 contém um switch integrado de três portas 10/100:
  - A porta 1 conecta-se ao switch
  - A porta 2 é uma interface 10/100 interna que transporta o tráfego do telefone IP
  - A porta 3 (porta de acesso) se conecta a um PC ou a outro dispositivo.



VLANs em um ambiente multicomutado

Troncos de VLAN

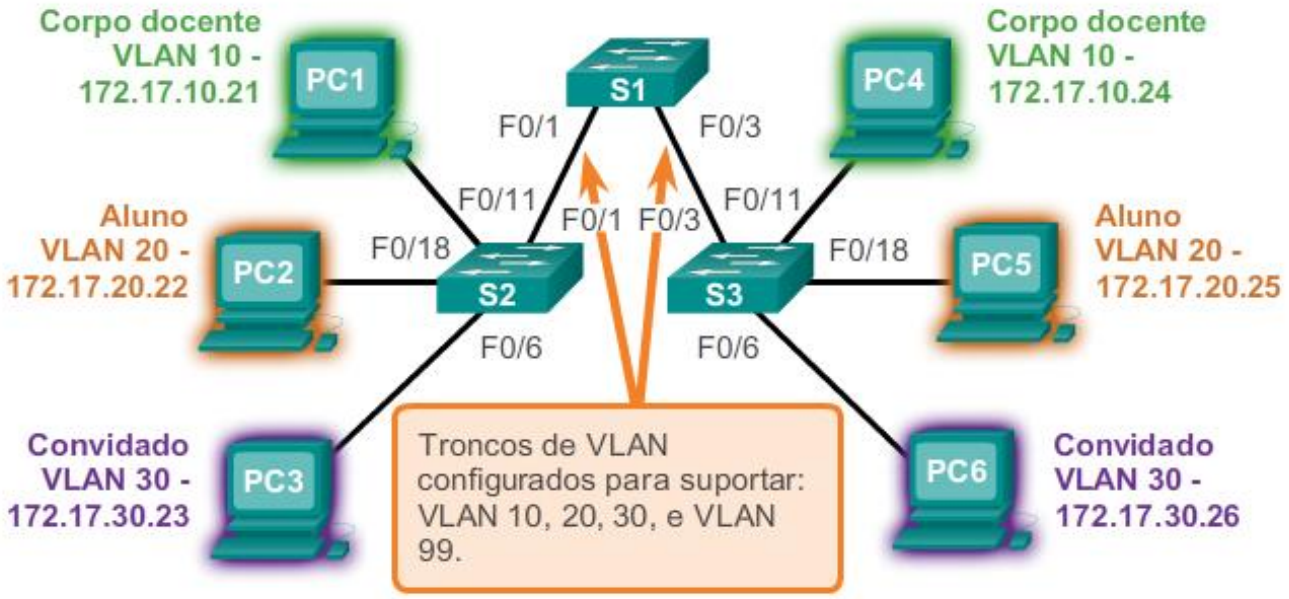
- Um tronco de VLAN contém mais de uma VLAN
- Geralmente estabelecido entre switches para que dispositivos na mesma VLAN possam se comunicar quando conectados fisicamente a switches diferentes
- Um tronco de VLAN não está associado a nenhuma VLAN. As portas de tronco utilizadas para estabelecer o link do tronco também não estão
- O IOS Cisco suporta IEEE802.1q, um protocolo popular de tronco de VLAN

VLANs em um ambiente multicomutado

Troncos de VLAN

VLAN 10 - Corpo Docente - 172.17.10.0/24
VLAN 20 - Aluno - 172.17.20.0/24
VLAN 30 - Convidado - 172.17.30.0/24
VLAN 99 - Gerenciamento e Nativa - 172.17.99.0/24

Fa0/1-5 são interfaces de tronco 802.1Q com a VLAN nativa 99.
Fa0/11-17 estão na VLAN 10
. Fa0/18-24 estão na VLAN 20.
Fa0/6-10 estão na VLAN 30.



VLANs em um ambiente multicomutado

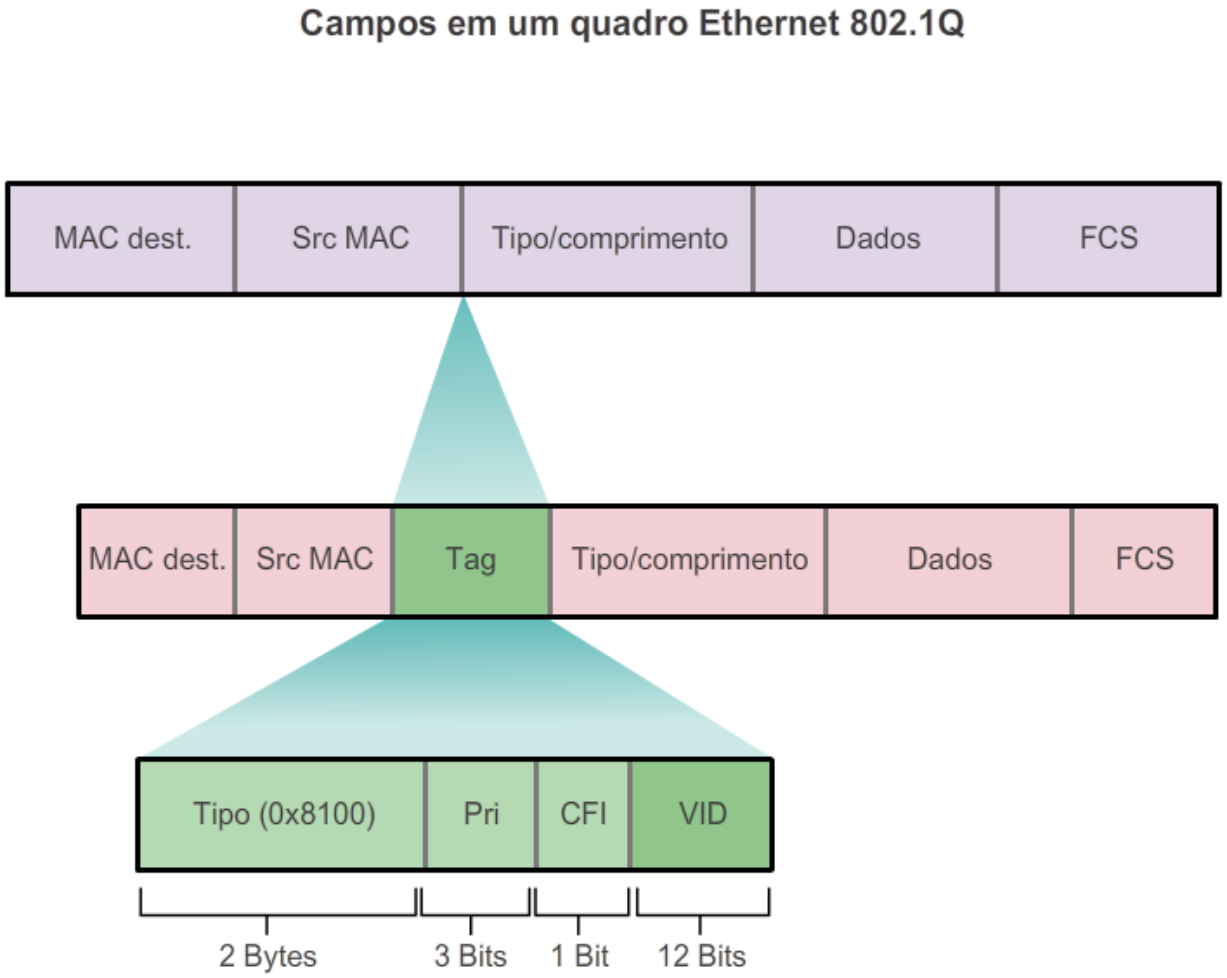
Controlando domínios de broadcast com VLANs

- As VLANs podem ser usadas para limitar o alcance de quadros de broadcast
- Uma VLAN é Um domínio de broadcast por si só
- Portanto, um quadro de broadcast enviado por um dispositivo em uma VLAN específica é encaminhado dentro dessa VLAN.
- Isso ajuda a controlar o alcance de quadros de broadcast e seu impacto na rede
- Quadros unicast e multicast são encaminhados na VLAN de origem também

Marcar quadros de Ethernet para identificação de VLAN

- A marcação de quadros é usada para transmitir corretamente vários quadros de VLANs por meio de um link de tronco
- Os switches marcarão os quadros para identificar a VLAN a que pertencem. Existem protocolos de marcação diferentes, mas o IEEE 802.1q é muito popular
- O protocolo define a estrutura do cabeçalho de marcação adicionado ao quadro
- Os switches adicionarão marcas de VLAN aos quadros antes de colocá-los em links de tronco e removerão as marcas antes de encaminhar os quadros por meio de portas não de tronco
- Depois que forem marcados corretamente, os quadros poderão atravessar alguns switches por meio de links de tronco e ainda serão encaminhados dentro da VLAN correta no destino

Marcar quadros de Ethernet para identificação de VLAN

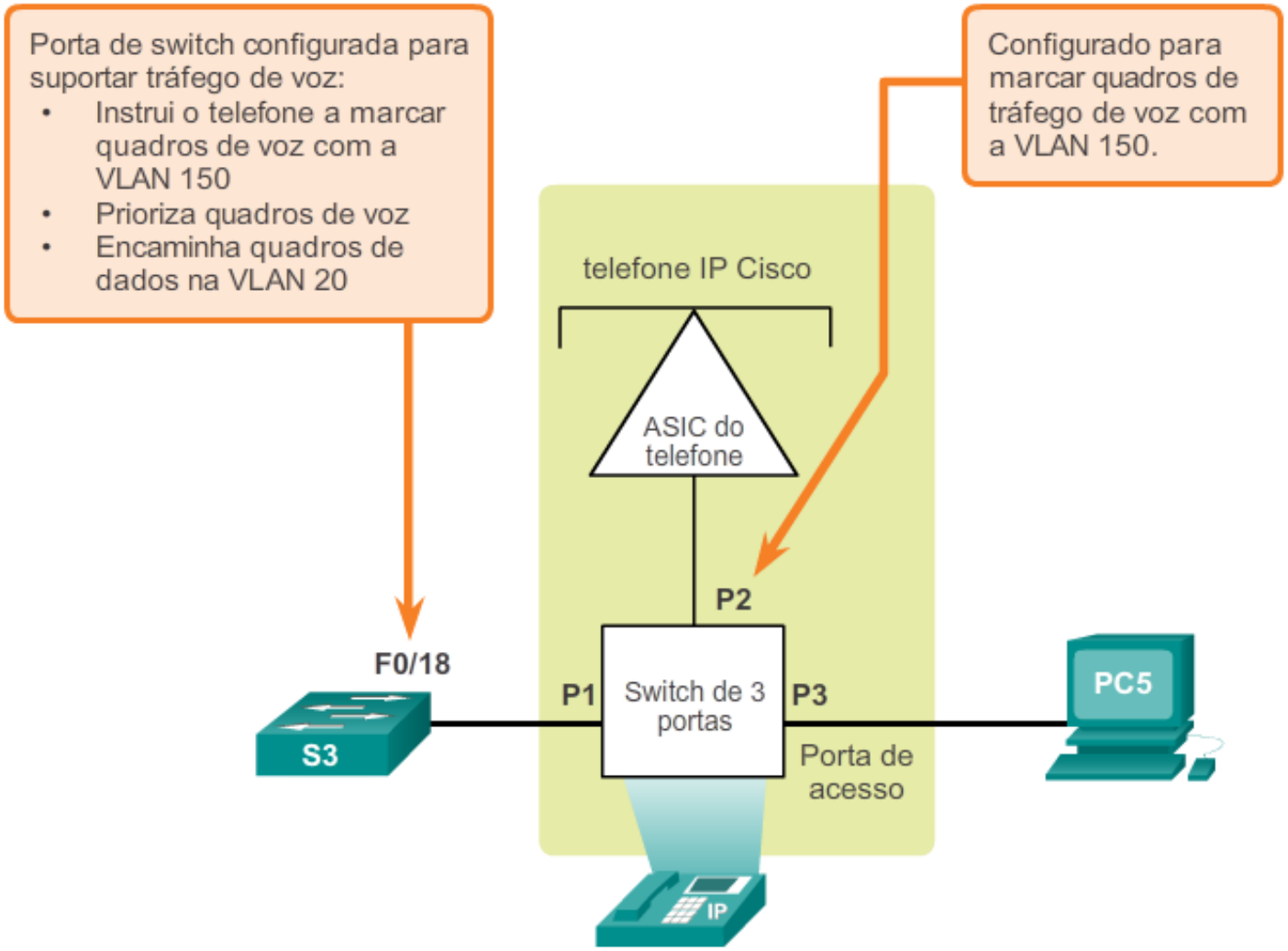


VLANs nativas e marcação 802.1q

- Um quadro que pertence à VLAN nativa não será marcado
- Um quadro que for recebido sem marcação permanecerá assim e será colocado na VLAN nativo quando encaminhado
- Se não houver portas associadas à VLAN nativa e a outros links de tronco, um quadro não marcado será descartado
- Nos switches da Cisco, a VLAN nativa é a VLAN 1 por padrão

VLANs em um ambiente multicomutado

Marcação de VLAN de voz



Intervalos de VLANs em Switches Catalyst

- Os switches Catalyst série 2960 e 3560 suportam mais de 4.000 VLANs
- Essas VLANs estão divididas em 2 categorias:
- VLANs do intervalo normal
  - VLANs números 1 até 1005
  - Configurações armazenadas em vlan.dat (em flash)
  - O VTP só pode aprender e armazenar VLANs do intervalo normal
- VLANs do intervalo estendido
  - VLANs números 1006 até 4096
  - Configurações armazenadas em running-config (na NVRAM)
  - O VTP não reconhece as VLANs do intervalo estendido

Criando uma VLAN

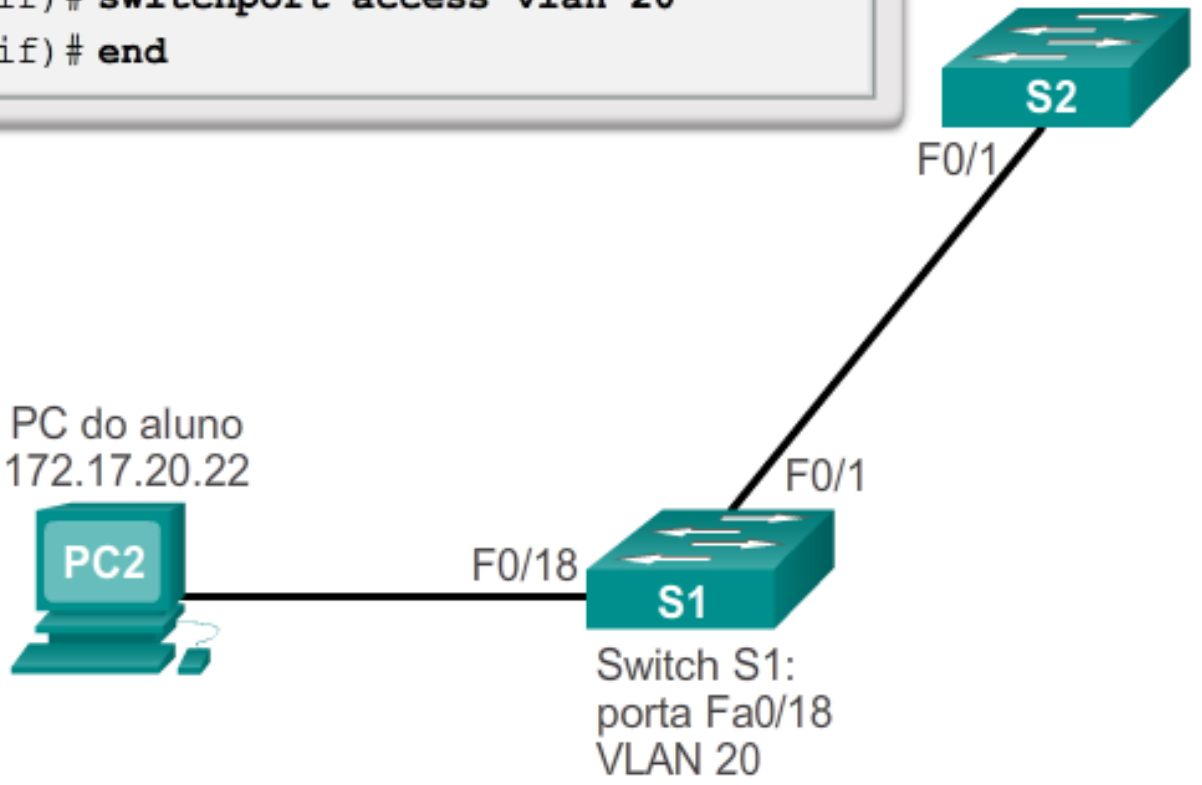
Comandos do switch Cisco IOS	
Entre no modo de configuração global.	`S1# configure terminal`
Crie uma VLAN com um número de identificação válido.	`S1(config)# vlan vlan-id`
Especifique um nome exclusivo para identificar a VLAN.	`S1(config-vlan)# name vlan-name`
Volte para o modo EXEC privilegiado.	`S1(config-vlan)# end`

Atribuição de portas a VLANs

Comandos do switch Cisco IOS	
Entre no modo de configuração global.	`S1# configure terminal`
Entre no modo de configuração da interface para SVI.	`S1(config)# interface` *interface_id*
Configure a porta para o modo de acesso.	`S1(config-if)# switchport mode access`
Atribua a porta a uma VLAN.	`S1(config-if)# switchport access vlan` *vlan_id*
Volte para o modo EXEC privilegiado.	`S1(config-if)# end`

Atribuição de portas a 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
```



Atribuição de VLAN

Alterar associação de porta de 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#
```

Atribuição de VLAN

Alterar associação de porta de 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#
```

Atribuição de VLAN

Excluindo 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#
```

Atribuição de VLAN

Verificar informações 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#
```

Verificar informações 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
```

Atribuição de VLAN

Configurando links de tronco IEEE 802.1q

Comandos do switch Cisco IOS	
Entre no modo de configuração global.	`S1# configure terminal`
Entre no modo de configuração da interface para SVI.	`S1(config)# interface` *interface_id*
Force o link a ser um link de tronco.	`S1(config-if)# switchport mode trunk`
Especifique uma VLAN nativa para os troncos 802.1Q não marcados.	`S1(config-if)# switchport trunk native vlan` *vlan_id*
Especifique a lista de VLANs a serem permitidas no link de tronco.	`S1(config-if)# switchport trunk allowed vlan` *vlan-list*
Volte para o modo EXEC privilegiado.	`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
```

Atribuição de VLAN

Redefinir o tronco para o estado padrão

Exemplo de redefinição de link de tronco

```
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
<saída omitida>
```

Redefinir o tronco para o estado padrão

Porta de retorno para o modo de acesso

```
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
<saída omitida>
```

Atribuição de VLAN

Verificando a configuração do tronco

Verificando a configuração do tronco

```
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
<saída omitida>
```

Introdução ao DTP

- As portas de switch podem ser configuradas manualmente para formar troncos
- As portas de switches também podem ser configuradas para negociar e estabelecer um link de tronco a um par conectado
- O Dynamic Trunking Protocol (DTP) é um protocolo para gerenciar a negociação do tronco
- O DTP é um protocolo proprietário da Cisco e é ativado por padrão nos switches Cisco Catalyst 2960 e 3560
- Se a porta do switch vizinho for configurada em um modo de tronco que suporte o DTP, ela gerenciará a negociação
- A configuração de DTP padrão para switches Cisco Catalyst séries 2960 e 3560 é dynamic auto

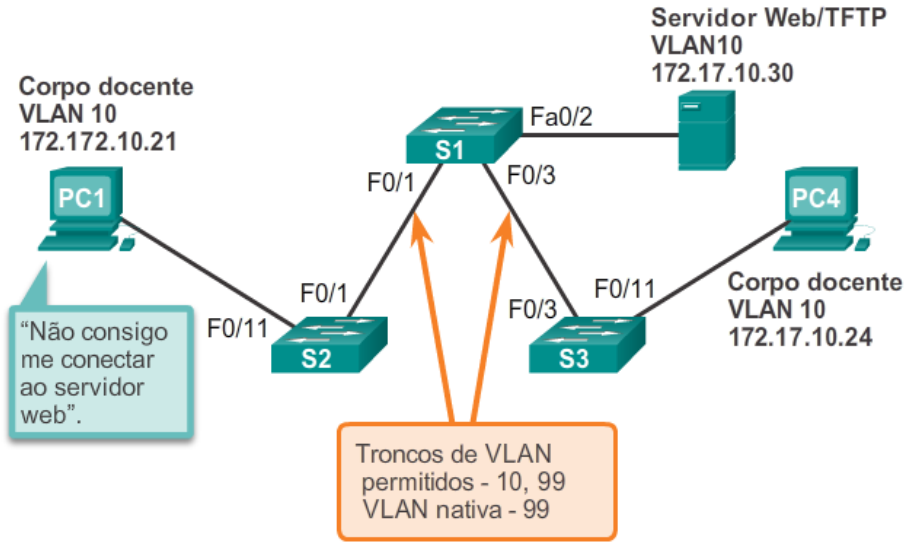
Modos de interface negociados

- O Cisco Catalyst 2960 e o 3560 suportam os seguintes modos de tronco:
  - switchport mode dynamic auto
  - switchport mode dynamic desirable
  - switchport mode trunk
  - switchport nonegotiate

	Dynamic Auto	Dynamic Desirable	Tronco	Acesso
Dynamic Auto	Acesso	Tronco	Tronco	Acesso
Dynamic Desirable	Tronco	Tronco	Tronco	Acesso
Tronco	Tronco	Tronco	Tronco	Conectividade limitada
Acesso	Acesso	Acesso	Conectividade limitada	Acesso

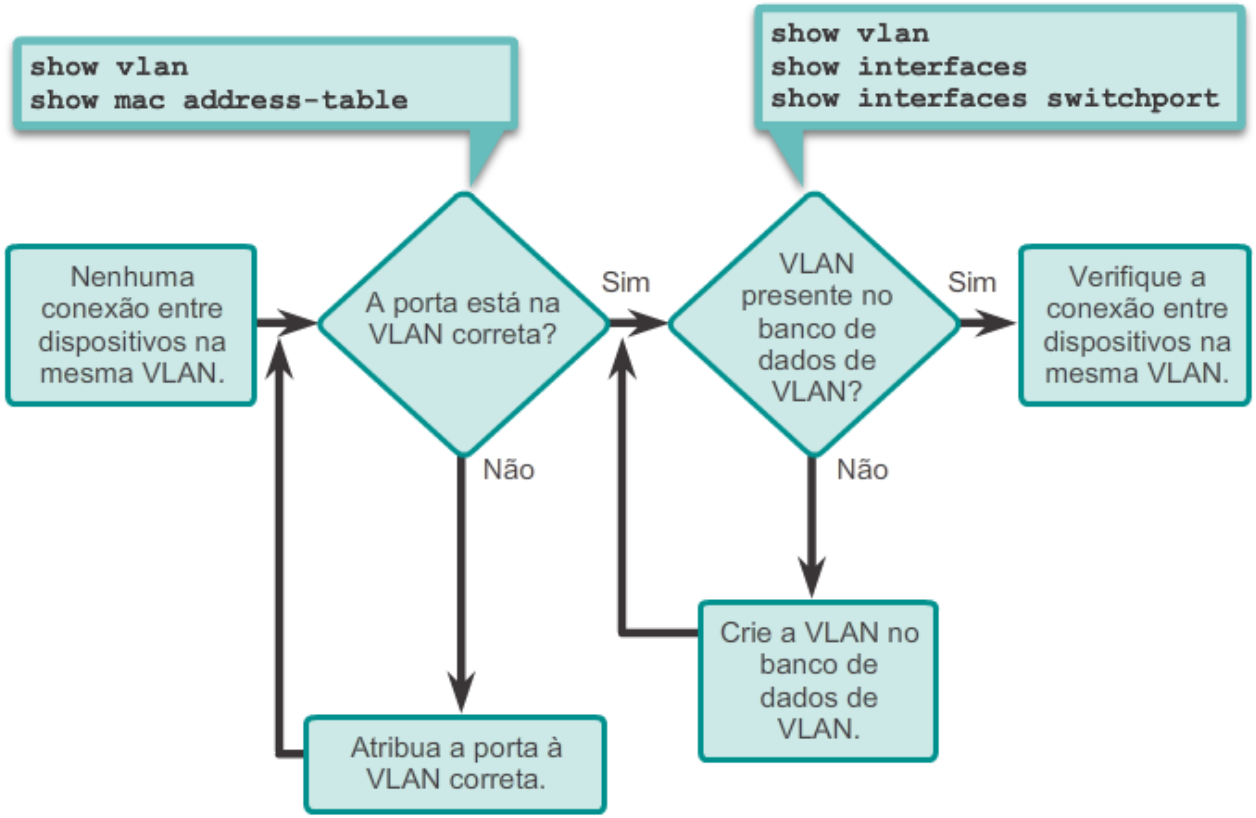
Problemas de endereçamento com VLAN

- É uma prática muito comum associar uma VLAN a uma rede IP
- Como as redes IP diferentes se comunicam apenas por meio de um roteador, todos os dispositivos dentro de uma VLAN devem ser parte da mesma rede IP para se comunicar
- Na imagem abaixo, PC1 não pode se comunicar com o servidor porque tem um endereço IP incorreto configurado

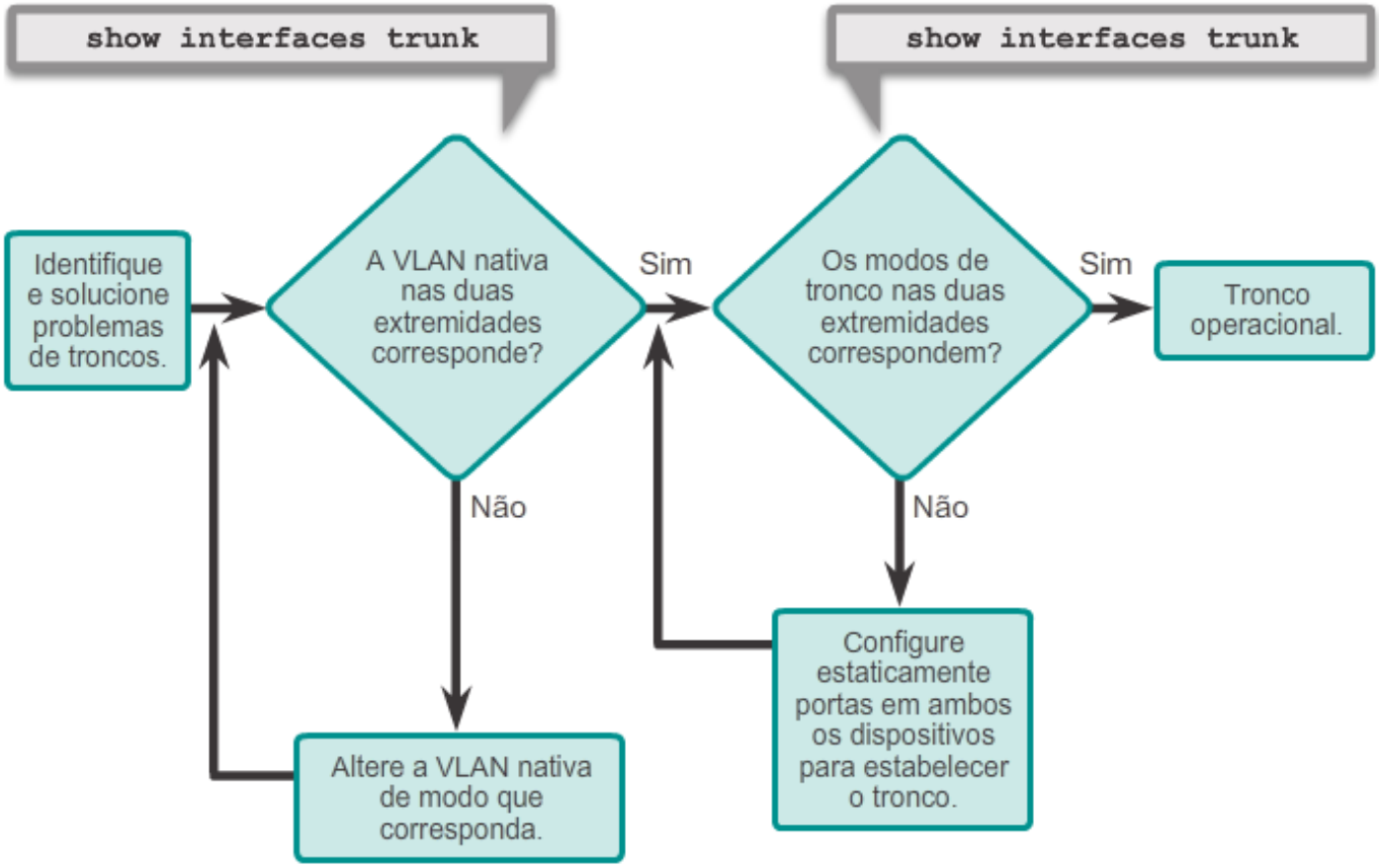


VLANs ausentes

- Se todas as incompatibilidades de endereço IP foram resolvidas, mas o dispositivo ainda não puder se conectar, verifique se a VLAN existe no switch.



Introdução à solução de problemas de troncos



Problemas comuns com troncos

- Os problemas de entroncamento são geralmente associados às configurações incorretas.
- Estes são os tipos mais comuns de erros de configuração de tronco:
  1. Incompatibilidades de VLANs nativas
  2. Incompatibilidades do modo de tronco
  3. VLAN autorizadas em troncos
- Se um problema de tronco for detectado, as práticas recomendadas orientam que os problemas devem ser solucionados na ordem indicada acima.

Incompatibilidades de modos de tronco

- Quando uma porta em um link de tronco é configurada com um modo de tronco que seja inconsistente com a porta de tronco vizinha, um link de tronco não se forma entre os dois switches
- Verifique o status das portas de tronco nos switches usando o comando **show interfaces trunk**
- Para corrigir o problema, configure as interfaces nos modos apropriados de tronco.

	Dynamic Auto	Dynamic Desirable	Tronco	Acesso
Dynamic Auto	Acesso	Tronco	Tronco	Acesso
Dynamic Desirable	Tronco	Tronco	Tronco	Acesso
Tronco	Tronco	Tronco	Tronco	Conectividade limitada
Acesso	Acesso	Acesso	Conectividade limitada	Acesso

Lista de VLANs incorretas

- As VLANs devem ser permitidas no tronco antes que os quadros possam ser transmitidos pelo link
- Use o comando **switchport trunk allowed vlan** para especificar quais VLANs são permitidas em um link de tronco
- Para assegurar que as VLANs corretas sejam permitidas em um tronco, use o comando **show interfaces trunk**

Ataque de spoofing do switch

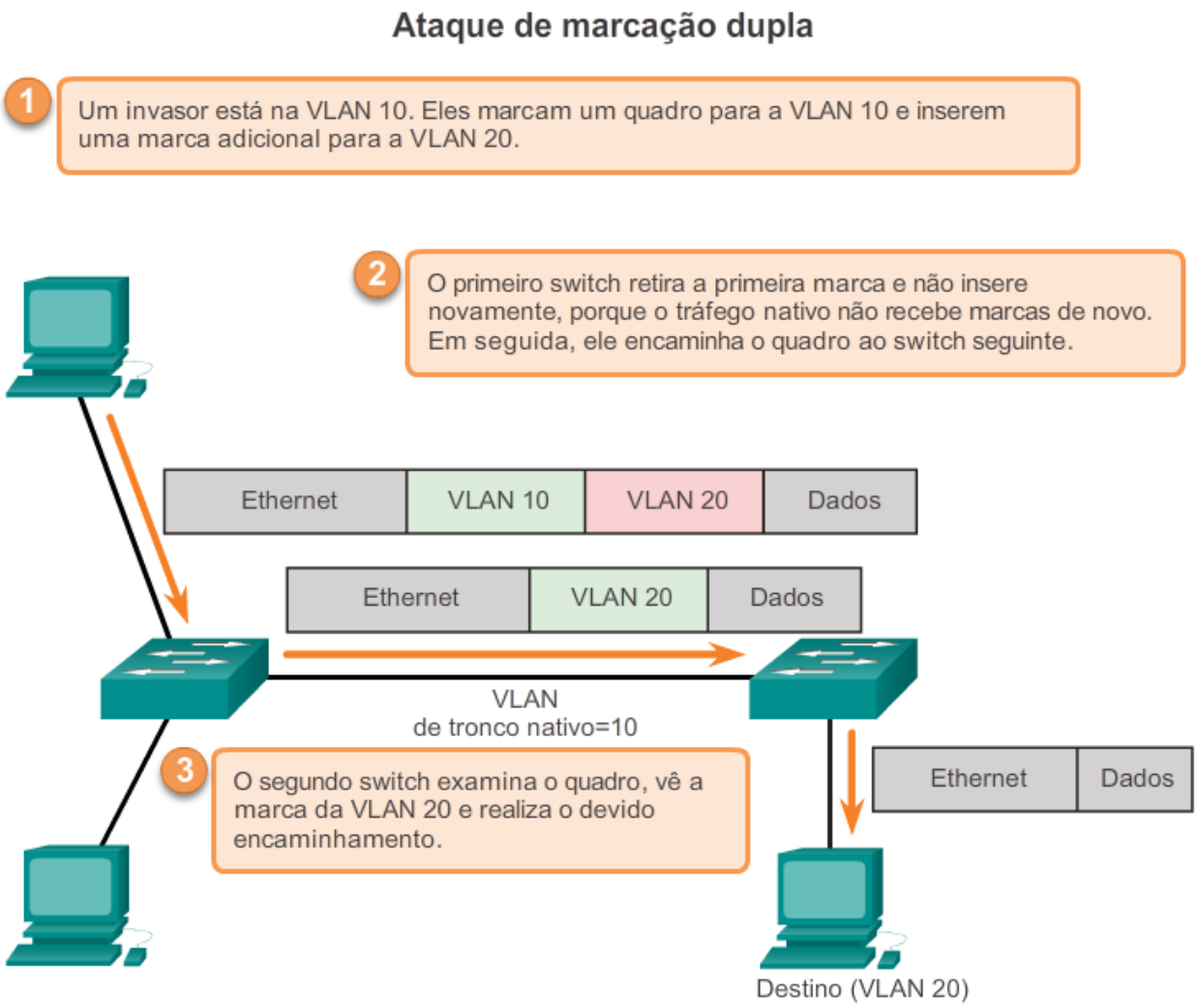
- Há diversos tipos diferentes de ataques a VLANs nas redes comutadas modernas. Um deles se chama salto de VLAN.
- A configuração padrão da porta do switch é dynamic auto
- Ao configurar um host para atuar como um switch e formar um tronco, um invasor pode obter acesso a qualquer VLAN na rede.
- Como o invasor pode acessar outras VLANs, isso é denominado ataque de salto de VLAN
- Para impedir um ataque de spoofing do switch básico, desative todo o entroncamento em todas as portas, exceto aquelas que exigem o entroncamento especificamente

Ataque de Marcação Dupla

- O ataque de marcação dupla aproveita a maneira como o hardware na maioria dos switches desencapsula marcas 802.1Q
- A maioria dos switches executa somente um nível de desencapsulamento 802.1Q, que permite a um invasor inserir um segundo cabeçalho de ataque não autorizado no quadro.
- Depois de remover o primeiro e legítimo cabeçalho 802.1Q, o switch encaminha o quadro à VLAN especificada no cabeçalho 802.1Q não autorizado
- A melhor abordagem para atenuar ataques de marcação dupla é garantir que a VLAN nativa das portas de tronco seja diferente da VLAN das portas de qualquer usuário

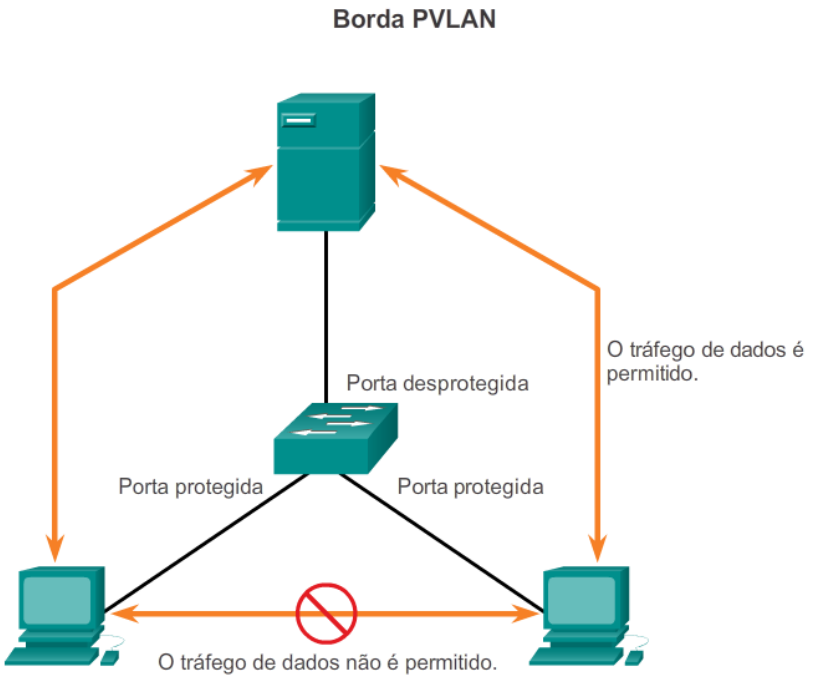
Ataques em VLANs

Ataque de Marcação Dupla



PVLAN Edge

- O recurso Private VLAN (PVLAN) Edge, também conhecido como portas protegidas, assegura que não haja nenhuma troca de tráfego unicast, broadcast ou multicast entre portas protegidas no switch
- Relevância local apenas
- Uma porta protegida somente troca tráfego com portas não protegidas
- Uma porta protegida não trocará tráfego com outra porta protegida



Diretrizes de Design da VLAN

- Mover todas as portas da VLAN1 e atribuí-las a uma VLAN que não esteja em uso
- Desligue todas as portas de switch não utilizadas
- Separe o tráfego de dados de gerenciamento e usuário
- Altere a VLAN de gerenciamento para uma VLAN diferente da VLAN1. O mesmo vale para a VLAN nativa
- Verifique se apenas os dispositivos na VLAN de gerenciamento podem se conectar aos switches
- O switch só deve aceitar conexões SSH
- Desative a autonegociação nas portas de tronco
- Não use os modos de porta de switch automáticos ou desejáveis

Capítulo 3: Resumo

- Este capítulo introduziu VLANS e seus tipos.
- Também abordou a conexão entre VLANs e domínio de broadcast
- O capítulo também aborda a marcação de quadro IEEE 802.1Q e como permite diferenciação entre os quadros Ethernet associados a VLANs distintas à medida que atravessam os links comuns de tronco.
- Este capítulo também examinou a configuração, a verificação e a resolução de problemas de VLANs e troncos usando o IOS Cisco CL e explorou as considerações básicas de segurança e design no contexto das VLANs.