Chapitre 3 : implémentation de la sécurité VLAN

Routage et commutation

Cisco | Networking Academy®
Mind Wide Open™

Chapitre 3

3.1 Segmentation VLAN

3.2 Mise en œuvre d'un VLAN

3.3 Sécurité et conception d'un VLAN

3.4 Résumé

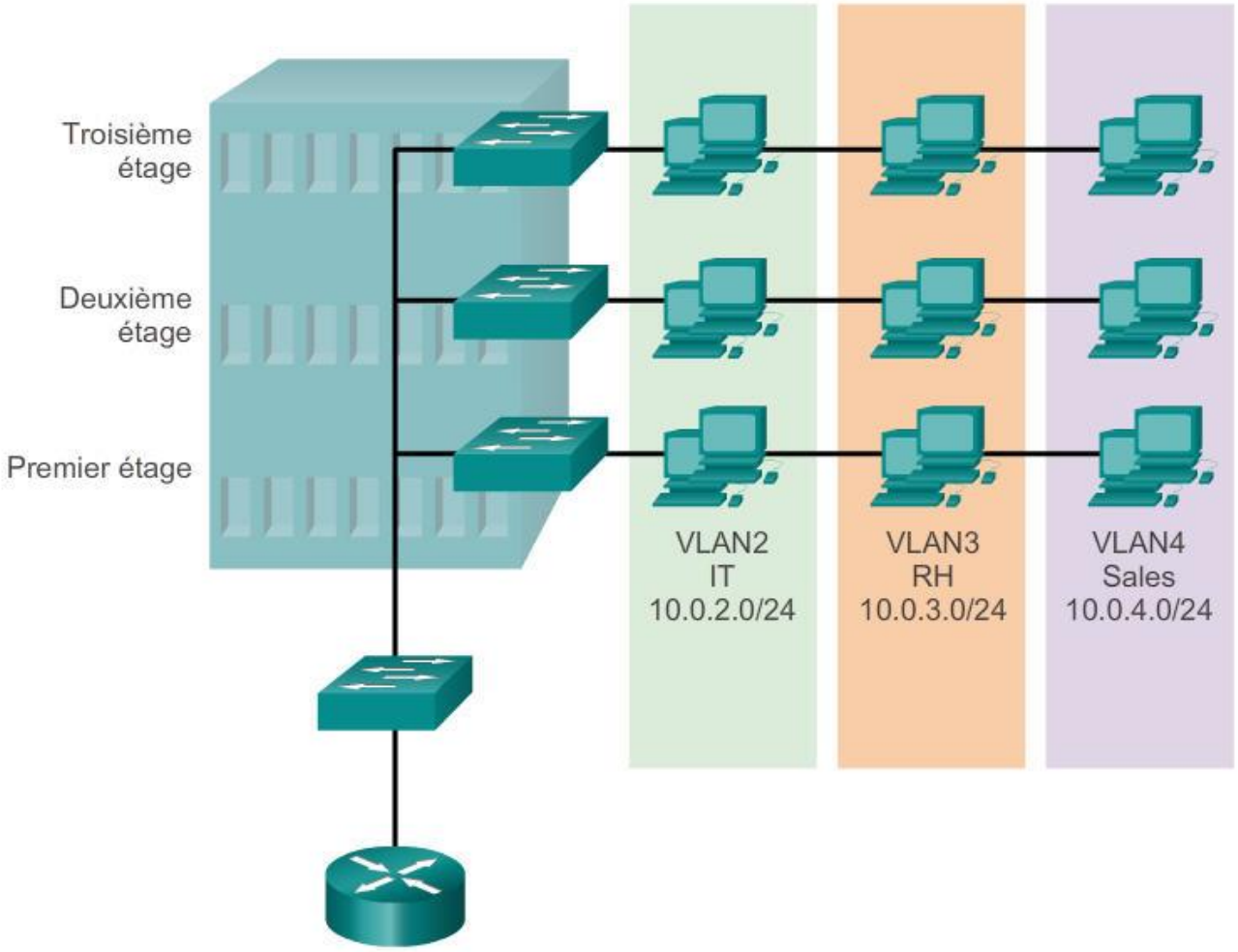
Chapitre 3 : objectifs

- Expliquer la fonction des VLAN dans un réseau commuté
- Analyser comment un commutateur transfère les trames en fonction de la configuration VLAN dans un environnement à commutateurs multiples
- Configurer un port de commutateur à attribuer à un VLAN en fonction des conditions requises
- Configurer un port trunk sur un commutateur LAN
- Configurer le protocole DTP
- Dépanner des configurations de VLAN et de trunk dans un réseau commuté
- Configurer les fonctions de sécurité pour limiter les attaques dans un environnement segmenté VLAN
- Expliquer les meilleures pratiques de sécurité pour un environnement segmenté VLAN

Définitions des VLAN

- Un VLAN (réseau local virtuel) est une partition logique d'un réseau de couche 2.
- Plusieurs partitions peuvent être créées, de sorte qu'il est possible de faire coexister plusieurs VLAN.
- Chaque VLAN constitue un domaine de diffusion, généralement avec son propre réseau IP.
- Les VLAN sont isolés les uns des autres et les paquets ne peuvent circuler entre eux qu'en passant par un routeur.
- La segmentation du réseau de couche 2 a lieu à l'intérieur d'un périphérique de couche 2, généralement un commutateur.
- Les hôtes regroupés dans un VLAN ignorent l'existence de celui-ci.

Définitions des VLAN



Avantages des VLAN

- Sécurité
- Réduction des coûts
- Meilleures performances
- Diminution des domaines de diffusion
- Efficacité accrue des équipes informatiques
- Simplification de la gestion des projets et des applications

Types de VLAN

- VLAN de données
- VLAN par défaut
- VLAN natif
- VLAN de gestion

Types de VLAN

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
```

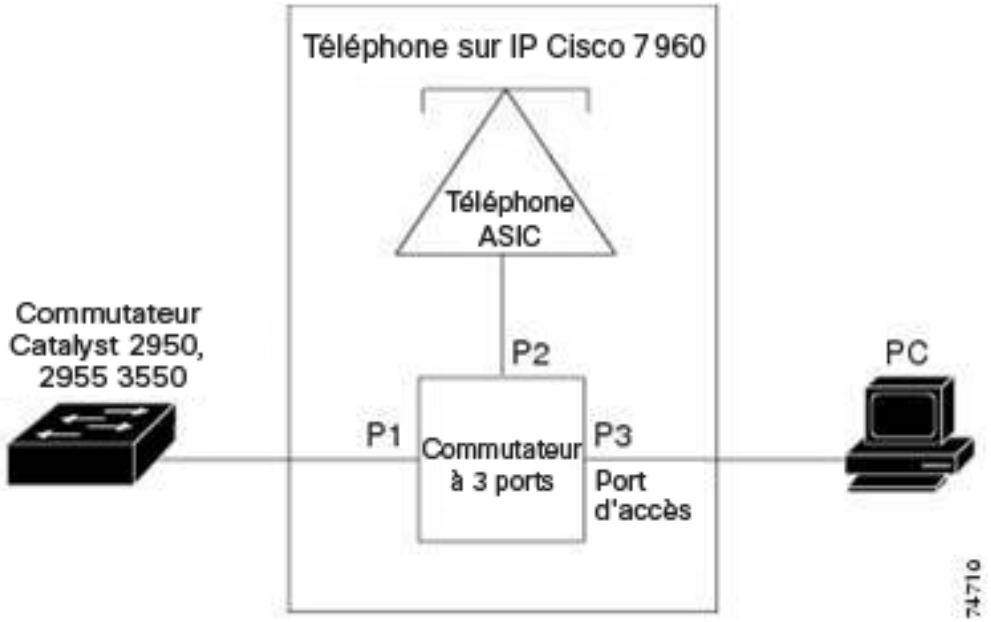
- Tous les ports affectés au VLAN 1 pour acheminer les données par défaut.
- Le VLAN natif est le VLAN 1 par défaut.
- Le VLAN de gestion est le VLAN 1 par défaut.
- Le VLAN 1 ne peut pas être renommé ni supprimé.

VLAN voix

- Le facteur temps est très important pour le trafic VoIP. Cela nécessite :
  - bande passante consolidée pour garantir la qualité de la voix ;
  - priorité de transmission par rapport aux autres types de trafic réseau ;
  - possibilité de routage autour des zones encombrées du réseau ;
  - Délai inférieur à 150 ms sur tout le réseau.
- La fonction VLAN voix permet aux ports du commutateur d'acheminer le trafic VoIP (voix sur IP) provenant d'un téléphone IP.
- Le commutateur peut être connecté à un téléphone IP Cisco 7960 et transmettre le trafic VoIP.
- Puisque la qualité audio de la téléphonie IP peut se détériorer si la transmission des données est inégale, le commutateur prend en charge la qualité de service (QS).

VLAN voix

- Le téléphone IP Cisco 7960 comporte un commutateur 10/100 intégré à 3 ports :
  - Le port 1 est relié au commutateur.
  - Le port 2 est une interface 10/100 interne chargée de la transmission du trafic de la téléphonie IP.
  - Le port 3 (port d'accès) est connecté à un ordinateur ou autre périphérique.



Trunks de VLAN

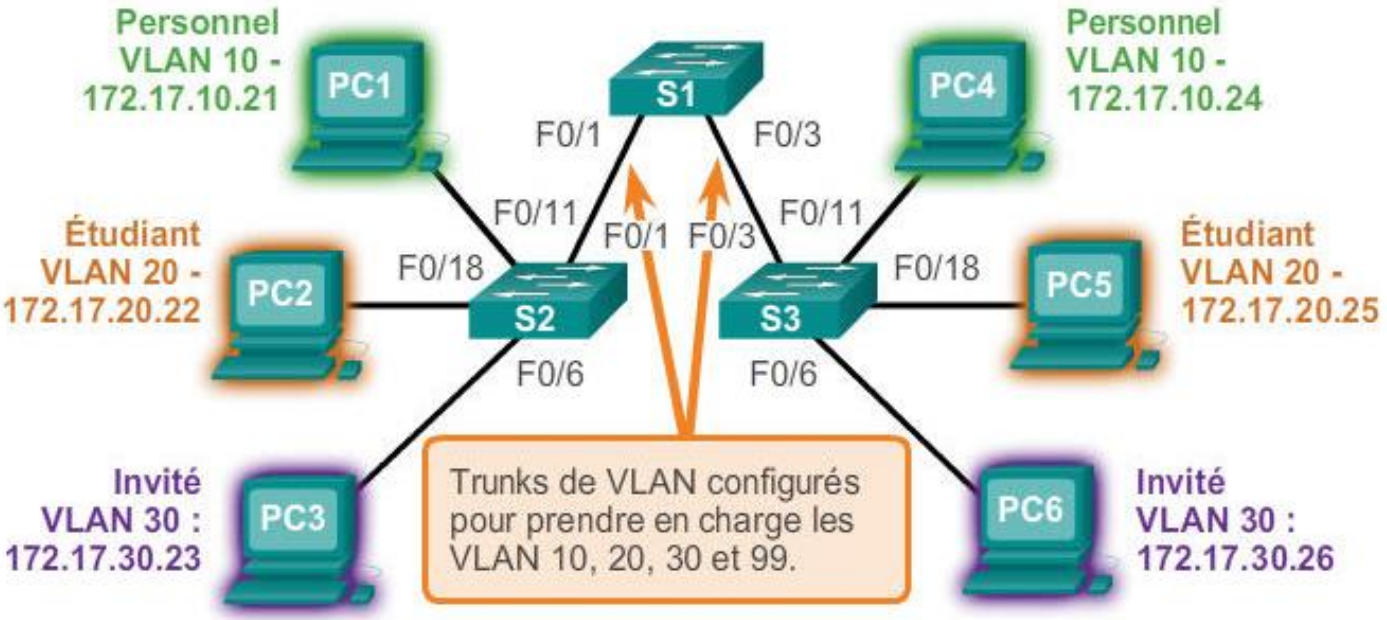
- Un trunk de VLAN achemine le trafic de plusieurs VLAN.
- Il est généralement établi entre des commutateurs pour permettre aux périphériques du même VLAN de communiquer même s'ils sont physiquement connectés à des commutateurs différents.
- Un trunk de VLAN n'est associé à aucun VLAN. Aucun port trunk n'est utilisé pour établir la liaison trunk.
- Cisco IOS prend en charge la norme IEEE802.1q, un protocole de trunk de VLAN très répandu.

VLAN dans un environnement à commutateurs multiples

Trunks de VLAN

VLAN 10 Personnel - 172.17.10.0/24
VLAN 20 Étudiants - 172.17.20.0/24
VLAN 30 Invité - 172.17.30.0/24
VLAN 99 Gestion et natif - 172.17.99.0/24

F0/1-5 sont des interfaces de trunk 802.1Q avec le VLAN 99 comme VLAN natif.
F0/11-17 se trouvent dans le VLAN 10
.F0/18-24 se trouvent dans le VLAN 20.
F0/6-10 se trouvent dans le VLAN 30.



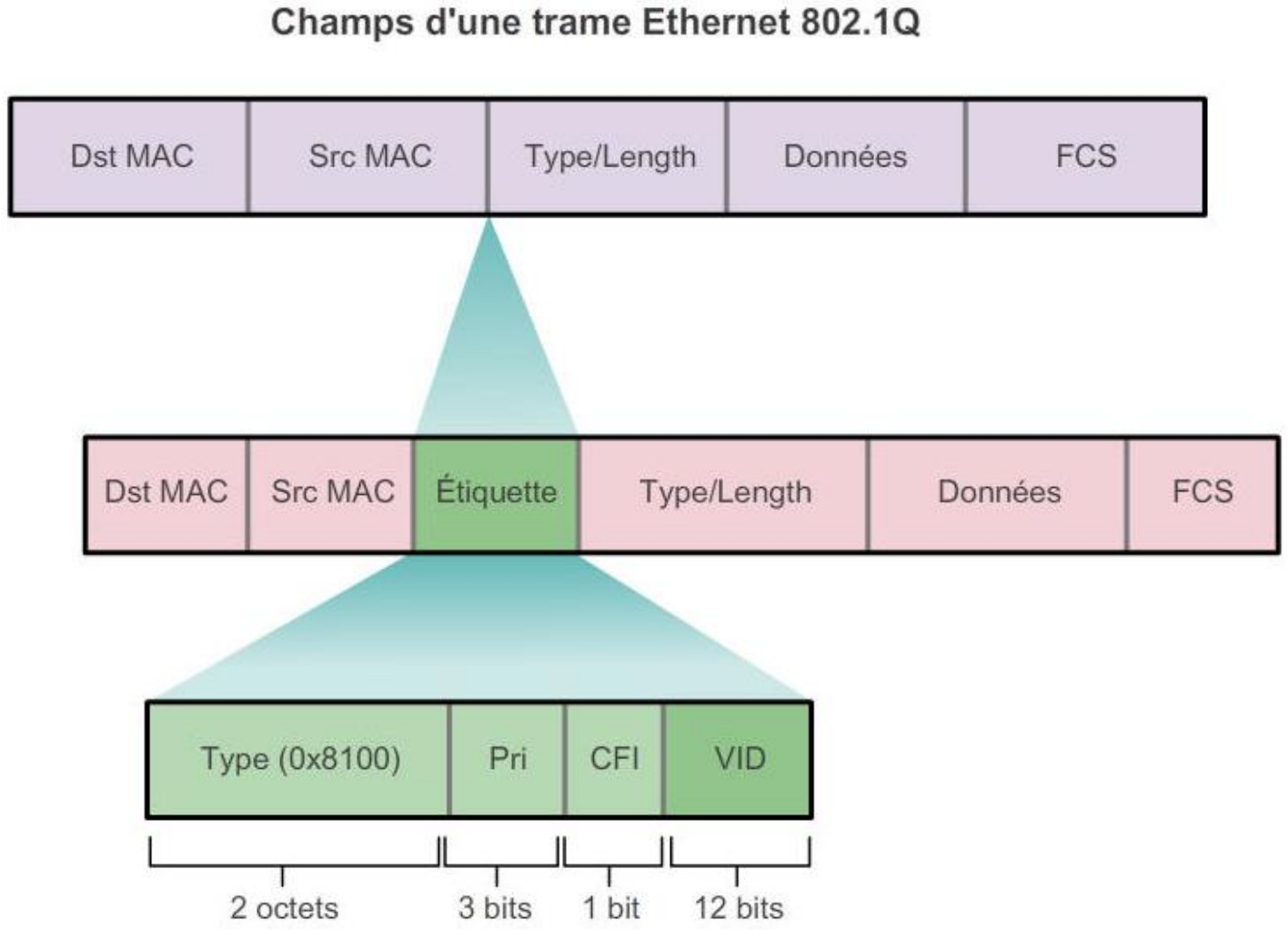
Contrôle des domaines de diffusion à l'aide des VLAN

- Les VLAN peuvent être utilisés pour limiter la portée des trames de diffusion.
- Un VLAN est un domaine de diffusion à part entière.
- Par conséquent, une trame de diffusion envoyée par un périphérique d'un VLAN donné est transmise au sein de ce VLAN uniquement.
- Cela permet de contrôler la portée des trames de diffusion et leur impact sur le réseau.
- Les trames de monodiffusion et de multidiffusion sont également transmises dans le VLAN d'où elles ont été émises.

Étiquetage des trames Ethernet pour l'identification des VLAN

- L'étiquetage des trames est utilisé pour transmettre correctement plusieurs trames VLAN via une liaison trunk.
- Les commutateurs étiquettent les trames pour identifier le VLAN auquel elles appartiennent. Il existe différents protocoles d'étiquetage, IEEE 802.1q étant le plus répandu.
- Le protocole définit la structure de l'en-tête d'étiquetage ajouté à la trame.
- Les commutateurs ajouteront des étiquettes VLAN aux trames avant de les placer dans les liaisons trunk. Ils les enlèveront avant de transmettre les trames via les autres ports (non trunk).
- Une fois qu'elles sont correctement étiquetées, les trames peuvent traverser n'importe quel nombre de commutateurs via les liaisons trunk. Elles resteront dans le VLAN approprié pour atteindre leur destination.

Étiquetage des trames Ethernet pour l'identification des VLAN

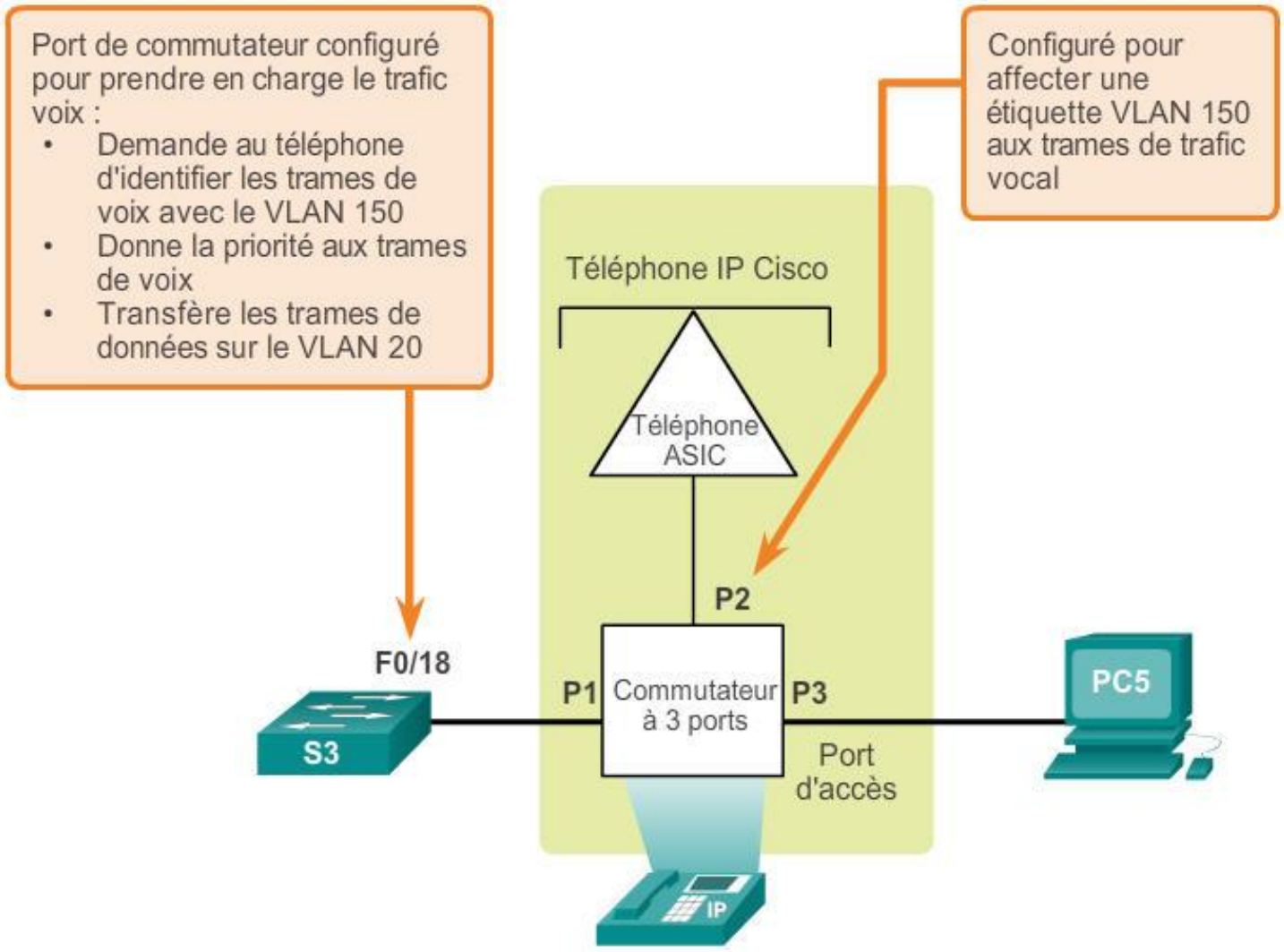


VLAN natifs et étiquetage 802.1q

- Une trame qui appartient au VLAN d'origine n'est pas étiquetée.
- Une trame reçue sans étiquette reste sans étiquetage et est placée dans le VLAN natif lors de la transmission.
- S'il n'y a pas de ports associés au VLAN natif et en l'absence de liaison trunk, une trame non étiquetée est ignorée.
- Dans les commutateurs Cisco, le VLAN natif est le VLAN 1 par défaut.

VLAN dans un environnement à commutateurs multiples

Étiquetage VLAN voix



Plages VLAN sur les commutateurs Catalyst

- Les commutateurs Catalyst 2960 et 3560 prennent en charge plus de 4 000 VLAN.
- Ces VLAN se répartissent dans 2 catégories :
- VLAN de la plage normale
  - Ce sont les VLAN du numéro 1 au numéro 1 005.
  - Les configurations sont stockées dans le fichier vlan.dat (dans la mémoire flash).
  - VTP peut uniquement « apprendre » et stocker les VLAN de la plage normale.
- Les VLAN de la plage étendue
  - Ce sont les VLAN du numéro 1 006 au numéro 4 096.
  - Les configurations sont stockées dans la configuration en cours (dans la mémoire NVRAM).
  - Le protocole VTP ne prend pas en compte les VLAN appartenant à la plage étendue.

Création d'un VLAN

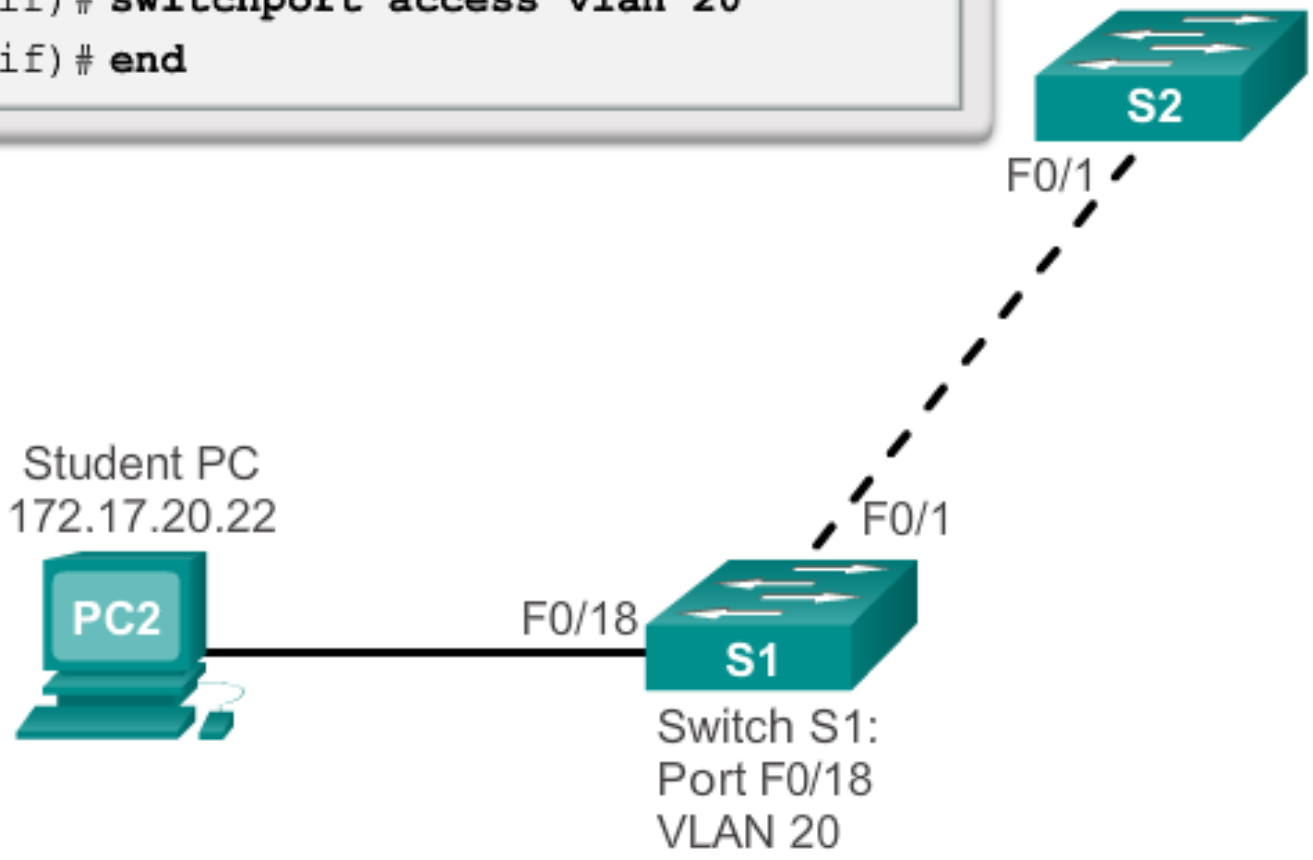
Commandes IOS de commutateur Cisco	
Passez en mode de configuration globale.	`S1#configure terminal`
Créez un VLAN avec un numéro d'identité valide.	`S1(config)# vlan vlan-id`
Indiquez un nom unique pour identifier le VLAN.	`S1(config-vlan)# name vlan-name`
Repassez en mode d'exécution privilégié.	`S1(config-vlan)# end`

Attribution de ports aux VLAN

Commandes IOS de commutateur Cisco	
Passez en mode de configuration globale.	`S1#configure terminal`
Passez en mode de configuration d'interface pour SVI.	`S1(config)# interface` *interface_id*
Définissez le port en mode d'accès.	`S1(config-if)# switchport mode access`
Affectez le port à un réseau local virtuel.	`S1(config-if)# switchport access vlan` *vlan_id*
Repassez en mode d'exécution privilégié.	`S1(config-if)# end`

Attribution de ports aux VLAN

```
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
```



Modification de l'appartenance des ports aux 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#
```

Modification de l'appartenance des ports aux 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#
```

Attribution VLAN

Suppression de VLAN

```
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#
```

Attribution VLAN

Vérification des informations 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#
```

Attribution VLAN

Vérification des informations 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
```

Attribution VLAN

Configuration des liaisons trunk IEEE 802.1q

Commandes IOS de commutateur Cisco	
Passer en mode de configuration globale.	`S1#configure terminal`
Passer en mode de configuration d'interface pour SVI.	`S1(config)# interface interface_id`
Forcer la liaison à devenir une liaison trunk.	`S1(config-if)# switchport mode trunk`
Indiquer un VLAN natif pour les trunks 802.1Q non étiquetés.	`S1(config-if)# switchport trunk native vlan vlan_id`
Indiquer la liste des VLAN autorisés sur la liaison trunk.	`S1(config-if)# switchport trunk allowed vlan vlan-list`
Repasser en mode d'exécution privilégié.	`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 10,20,30,99
S1(config-if)# end
```

Réinitialisation du trunk à l'état par défaut

Exemple de réinitialisation de liaison trunk

```
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>
```

Réinitialisation du trunk à l'état par défaut

Redéfinition de port en mode d'accès

```
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>
```

Attribution VLAN

Vérification de la configuration du trunk

Vérification de la configuration du 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
<resultado omitido>
```

Introduction au protocole DTP

- Les ports de commutateur peuvent être configurés manuellement pour créer les trunks.
- Ils peuvent également être configurés pour négocier et établir une liaison trunk avec un homologue connecté.
- DTP (Dynamic Trunking Protocol) est un protocole qui gère la négociation de trunk.
- C'est un protocole propriétaire de Cisco et il est activé par défaut sur les commutateurs Cisco Catalyst 2960 et 3560.
- Si le port du commutateur voisin est configuré dans un mode trunk qui prend en charge le protocole DTP, il gère la négociation.
- La configuration DTP s'effectue en mode dynamique automatique par défaut sur les commutateurs Cisco Catalyst 2960 et 3560.

Protocole DTP

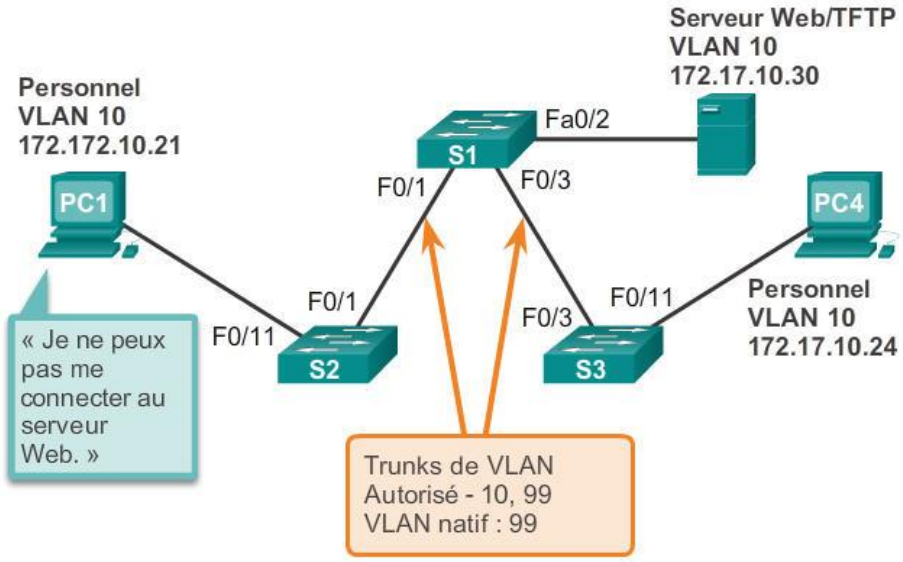
Modes d'interface négociés

- Les commutateurs Cisco Catalyst 2960 et 3560 prennent en charge les modes trunk suivants :
  - switchport mode dynamic auto
  - switchport mode dynamic desirable
  - switchport mode trunk
  - switchport nonegotiate

	Dynamique automatique	Dynamique souhaitable	Trunk inconditionnel	Accès
Dynamique automatique	Accès	Trunk inconditionnel	Trunk inconditionnel	Accès
Dynamique souhaitable	Trunk inconditionnel	Trunk inconditionnel	Trunk inconditionnel	Accès
Trunk inconditionnel	Trunk inconditionnel	Trunk inconditionnel	Trunk inconditionnel	Connectivité limitée
Accès	Accès	Accès	Connectivité limitée	Accès

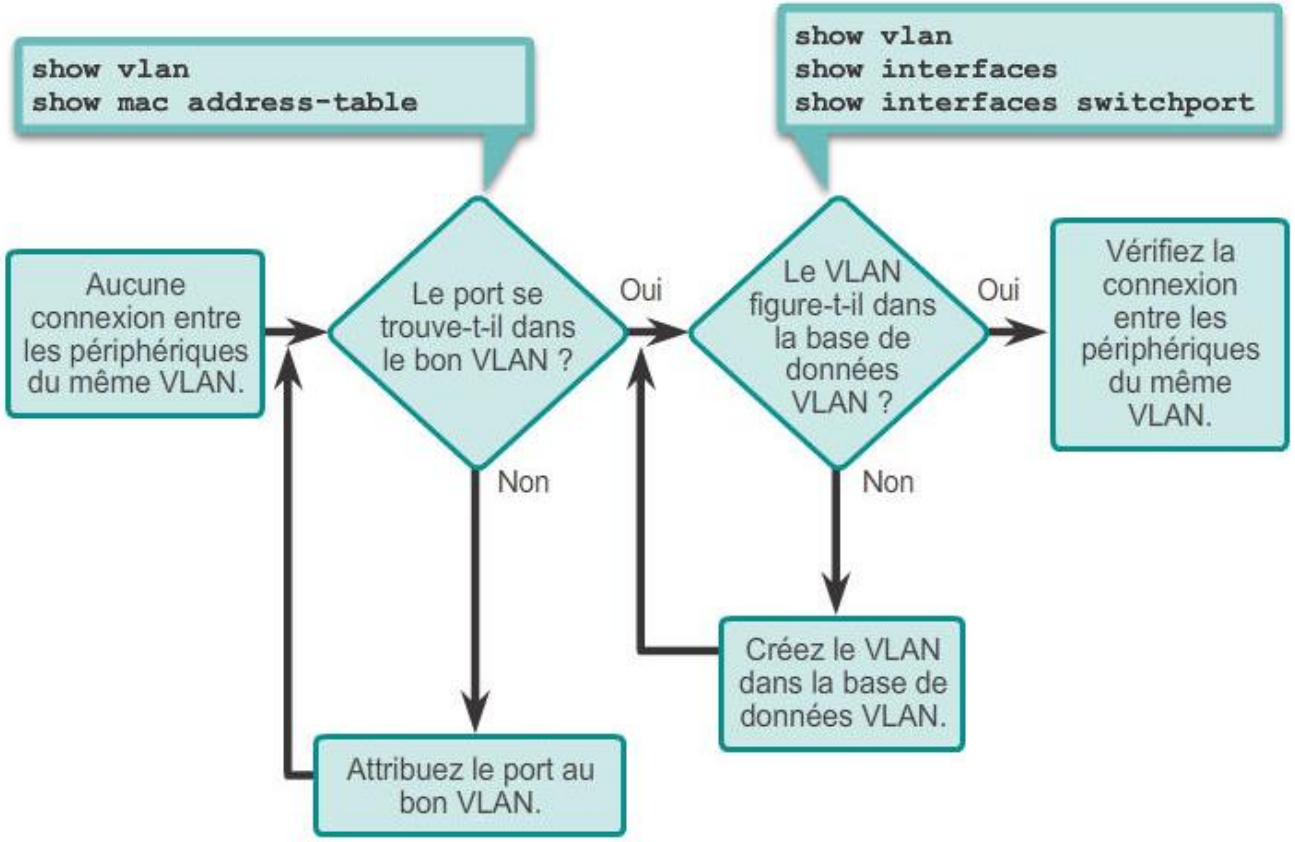
Résolution des problèmes liés aux VLAN

- Il est très fréquent d'associer un VLAN à un réseau IP.
- Comme les différents réseaux IP communiquent uniquement via un routeur, tous les périphériques d'un VLAN doivent appartenir au même réseau IP pour communiquer.
- Dans l'illustration ci-dessous, le PC1 ne peut pas communiquer avec le serveur parce que son adresse IP est incorrecte.

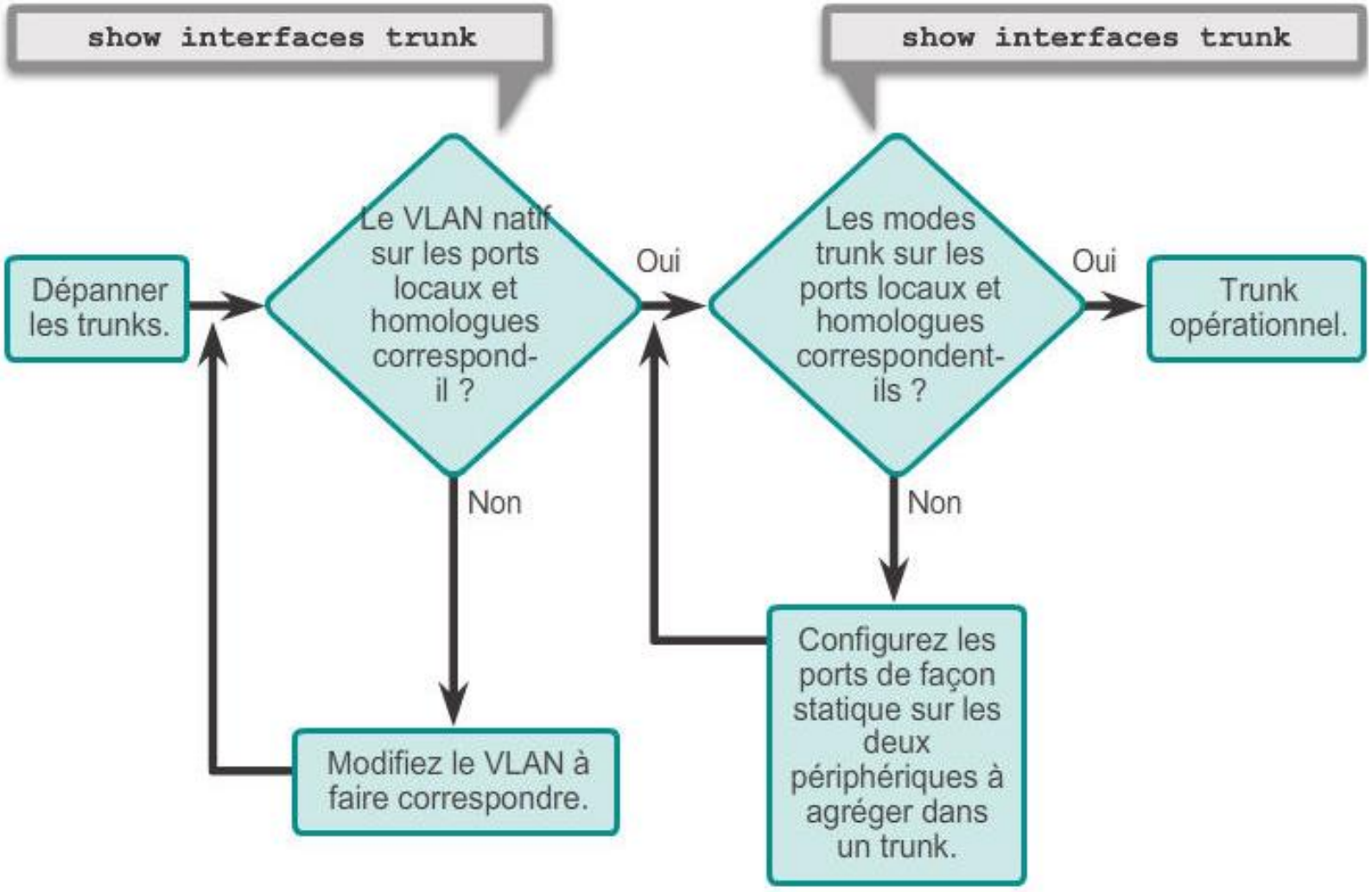


VLAN manquants

- Si tous les problèmes de concordance des adresses IP ont été résolus et que le périphérique ne peut toujours pas se connecter, vérifiez que le VLAN existe dans le commutateur.



Introduction au dépannage des trunks



Problèmes courants avec les trunks

- Les problèmes de trunking sont généralement associés à des configurations incorrectes.
- Le plus souvent, les erreurs de configuration des trunks sont les suivantes :
  1. Non-concordance du VLAN natif
  2. Non-concordance du mode trunk
  3. VLAN autorisés sur les trunks
- En cas de problème sur un trunk, il est recommandé de faire les vérifications dans l'ordre ci-dessus.

Non-concordance du mode trunk

- Lorsqu'un port sur une liaison trunk est configuré avec un mode trunk qui n'est pas compatible avec le port trunk voisin, la liaison en question ne peut pas être établie entre les deux commutateurs.
- Vérifiez l'état des ports trunk sur les commutateurs à l'aide de la commande **show interfaces trunk**.
- Pour résoudre ce problème, configurez les interfaces avec les modes trunk appropriés.

	Dynamique automatique	Dynamique souhaitable	Trunk inconditionnel	Accès
Dynamique automatique	Accès	Trunk inconditionnel	Trunk inconditionnel	Accès
Dynamique souhaitable	Trunk inconditionnel	Trunk inconditionnel	Trunk inconditionnel	Accès
Trunk inconditionnel	Trunk inconditionnel	Trunk inconditionnel	Trunk inconditionnel	Connectivité limitée
Accès	Accès	Accès	Connectivité limitée	Accès

Liste de VLAN incorrecte

- Les VLAN doivent être autorisés dans le trunk avant que leurs trames puissent être transmises sur la liaison.
- Utilisez la commande **switchport trunk allowed vlan** pour indiquer quels VLAN sont admis dans une liaison trunk.
- Pour garantir que les VLAN appropriés sont autorisés dans un trunk, utilisez la commande **show interfaces trunk**.

Attaque par usurpation de commutateur

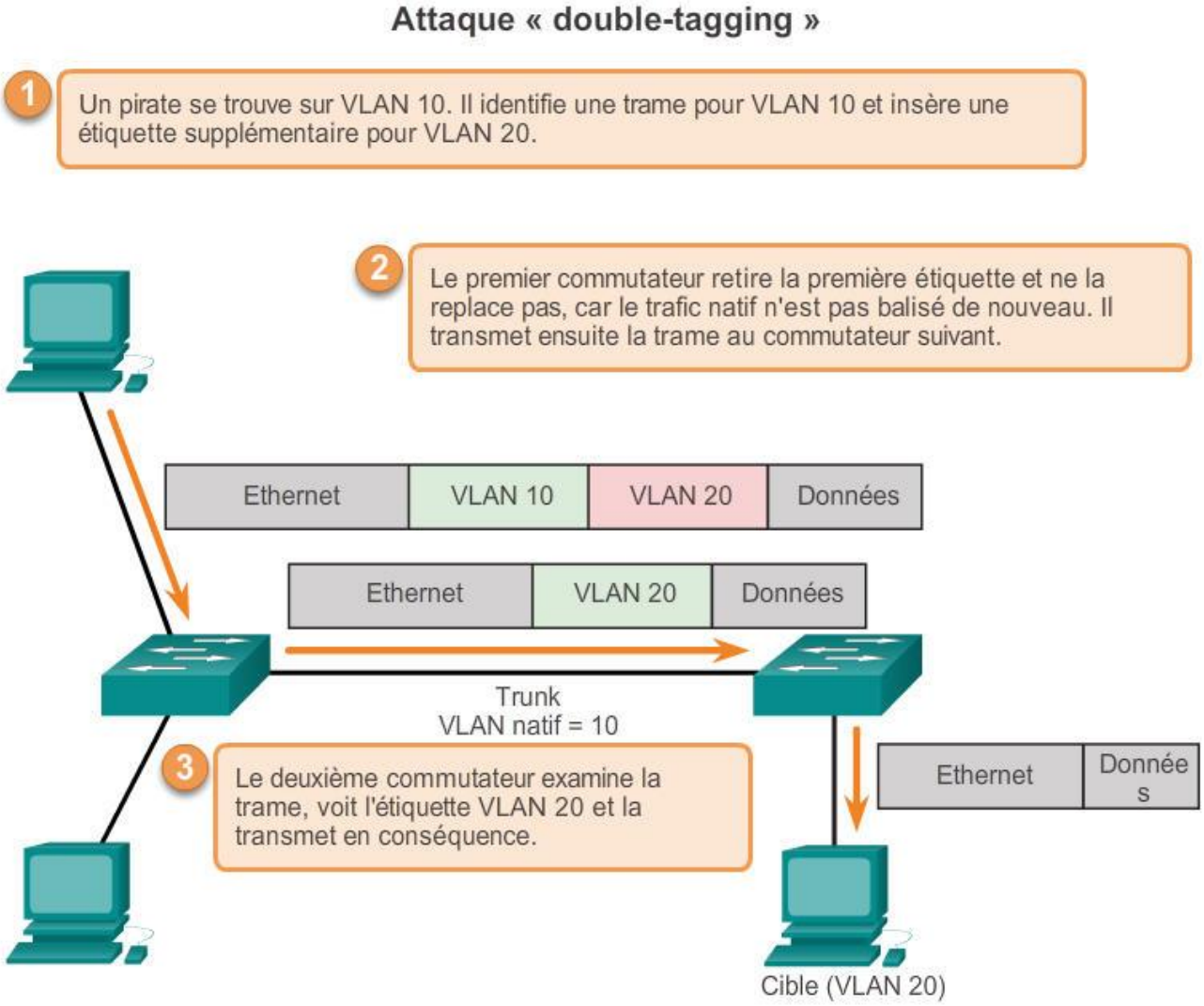
- Il existe différents types d'attaque VLAN dans les réseaux commutés modernes. L'attaque « VLAN hopping » en est une.
- Par défaut, le port du commutateur est configuré en mode dynamique automatique.
- En configurant un hôte pour qu'il fasse office de commutateur et forme un trunk, le pirate peut accéder à n'importe quel VLAN du réseau.
- Il peut ensuite accéder aux autres VLAN.
- Pour éviter une attaque de base, désactivez le trunking sur tous les ports, sauf sur ceux qui l'utilisent.

Attaque Double-Tagging

- L'attaque « Double-Tagging » tire parti de la façon dont les composants matériels de la plupart des commutateurs désencapsulent les étiquettes 802.1Q.
- Le plus souvent, les commutateurs effectuent un seul niveau de désencapsulation 802.1Q, ce qui permet au pirate d'incorporer un deuxième en-tête, non autorisé celui-là, dans la trame.
- Après avoir supprimé le premier en-tête 802.1Q légitime, le commutateur transmet la trame au VLAN spécifié dans le faux en-tête 802.1Q.
- La meilleure façon de parer ces attaques consiste à vérifier que le VLAN natif des ports trunk est différent de celui de tous les autres ports.

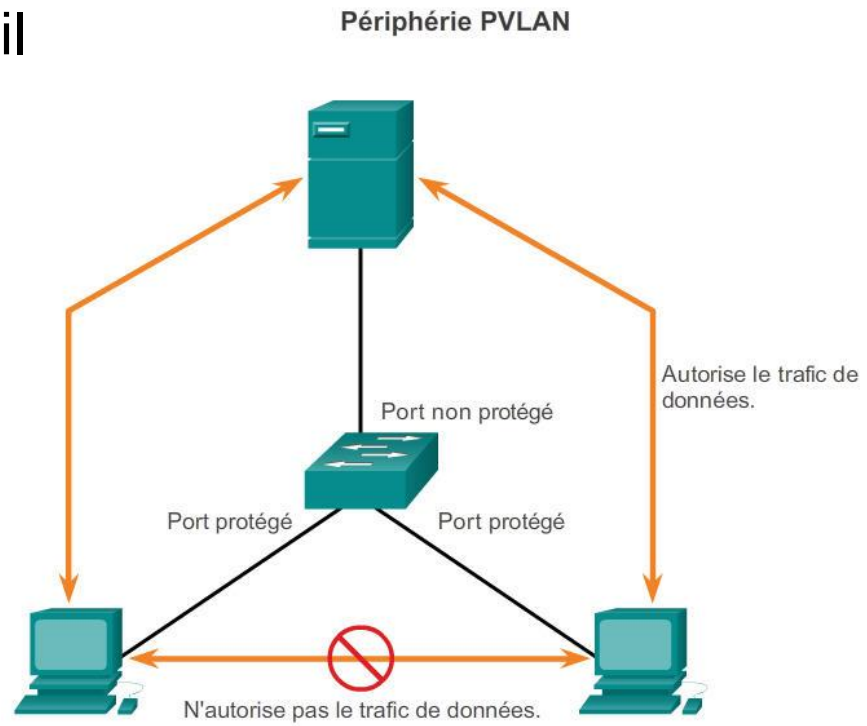
Attaques sur les VLAN

Attaque Double-Tagging



Périphérie PVLAN

- La fonction PVLAN (VLAN privé), ou « ports protégés », garantit qu'il n'y a aucun échange de trafic de monodiffusion, de diffusion ou de multidiffusion entre les ports protégés du commutateur.
- Cette protection n'est pertinente qu'en local.
- Un port protégé échange du trafic uniquement avec les ports non protégés.
- Un port protégé n'échange pas de trafic avec un autre port protégé.



Meilleures pratiques de conception pour les VLAN

Conseils pour la conception d'un VLAN

- Déplacez tous les ports du VLAN1 et attribuez-les à un VLAN qui n'est pas utilisé.
- Arrêtez tous les ports non utilisés du commutateur.
- Séparez le trafic de gestion et le trafic des données des utilisateurs.
- Remplacez le VLAN de gestion par un VLAN autre que VLAN1. Faites de même pour le VLAN natif.
- Assurez-vous que seuls les périphériques du VLAN de gestion peuvent se connecter aux commutateurs.
- Le commutateur doit accepter uniquement les connexions SSH.
- Désactivez l'autonégociation sur les ports trunk.
- N'utilisez pas les modes « auto » ni « desirable » pour les ports des commutateurs.

Chapitre 3 : résumé

- Dans ce chapitre, vous avez découvert les différents types de VLAN, ainsi que la connexion entre les VLAN et le domaine de diffusion.
- Vous connaissez maintenant les détails de l'étiquetage IEEE 802.1Q et comment cette méthode permet de différencier les trames Ethernet associées aux différents VLAN lorsqu'elles parcourent les liaisons trunk courantes.
- Vous avez également observé la configuration, la vérification et le dépannage des VLAN et des trunks en utilisant la ligne de commande de Cisco IOS et exploré les notions de base de la sécurité et de la conception dans le contexte des VLAN.