Vlans & Routage Inter-Vlan

Paul NDJE
Expert Réseaux et Sécurité
CCSI, CCNP Route, CCNP Switch, CCNP Tshoot
CCEH, NSE4, PCNSA, MTCNA, CCNA Enterprise
CCNA Security/Cybersecurity, IT Essentials

Email: paul.ndje@epita.fr

2025 - 2026

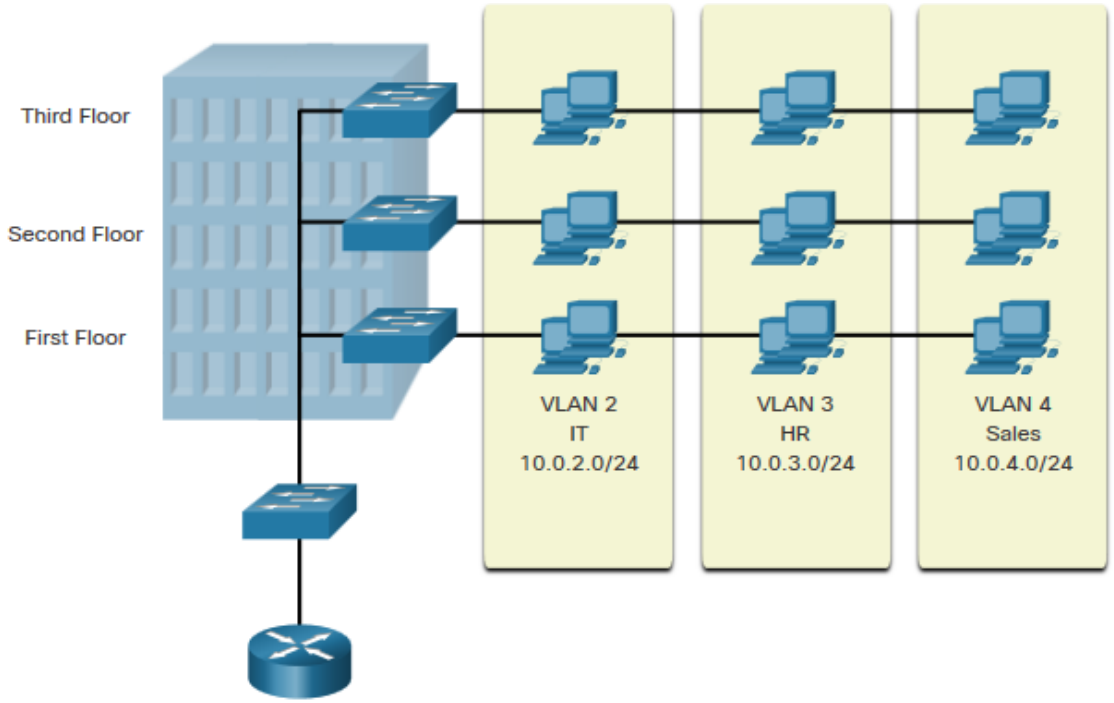
Objectifs du Module

Titre du module: VLANs & Routage Inter-VLAN

Module Objective: Mettre en œuvre des VLAN et des solutions de trunking dans un réseau commuté et dépanner les problèmes de routage entre VLAN sur les périphériques de couche 3.

Titre de Rubrique	Objectif de Rubrique
Vue d'ensemble des VLAN	Expliquer la fonction des VLAN dans un réseau commuté.
VLAN dans un environnement à commutateurs multiples	Expliquer comment un commutateur transmet des trames en fonction de la configuration du VLAN dans un environnement à commutateurs multiples.
Configuration du VLAN	Configurer un port de commutateur à attribuer à un VLAN en fonction des conditions requises.
Trunks de VLAN	Configurer un port trunk sur un commutateur LAN.
Protocole DTP (Dynamic Trunking Protocol)	Configurer le protocole DTP (Dynamic Trunking Protocol).
Fonctionnement du routage inter-VLAN	Décrire les options permettant de configurer le routage inter VLAN
Routage inter-VLAN avec la méthode router-on-a-stick	Configurer le routage Inter-VLAN avec la méthode «Router-on-a-stick».

Définitions des VLAN

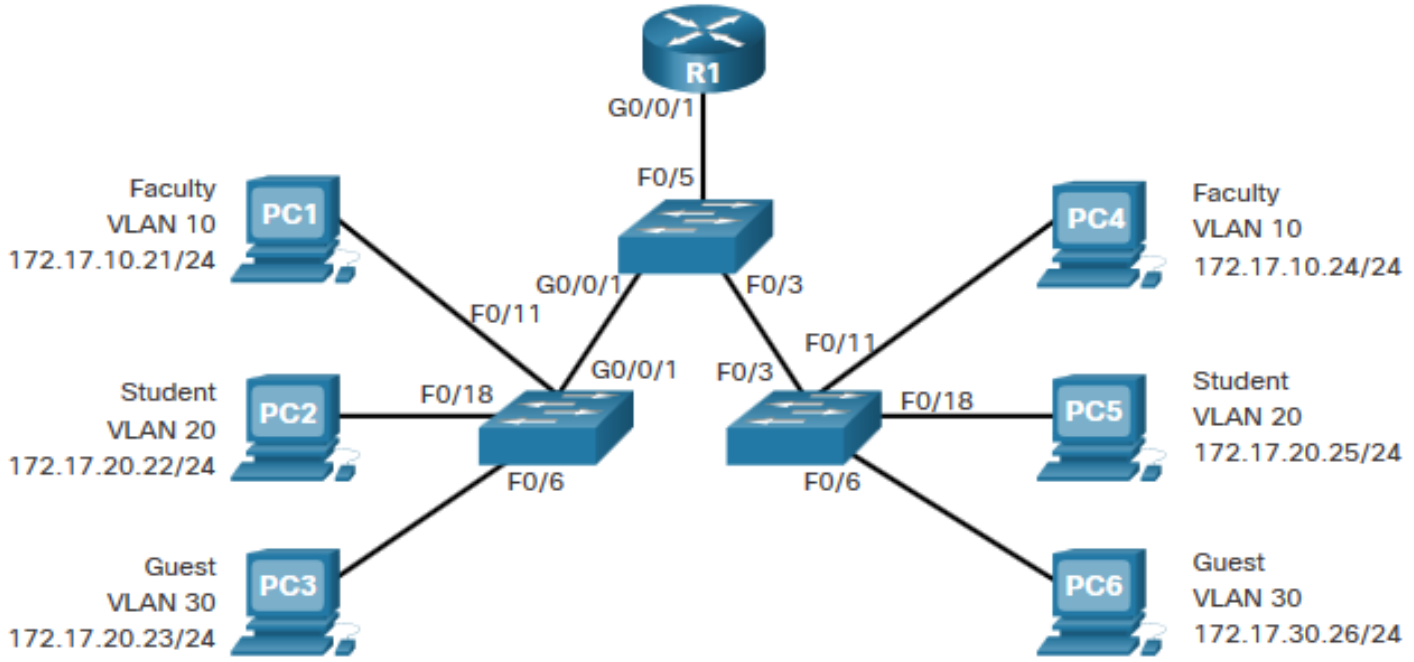


Les VLAN sont des connexions logiques avec d'autres périphériques similaires.
Le placement de périphériques dans divers VLAN présente les caractéristiques suivantes:

- Fournir la segmentation des différents groupes de périphériques sur les mêmes commutateurs
- Fournir une organisation plus facile à gérer
  - Les diffusions, les multidiffusions et les monodiffusions sont isolées dans le VLAN individuel
  - Chaque VLAN aura sa propre plage d'adressage IP unique
  - Domaines de Diffusion Plus Petits

Avantages du concept de VLAN

Les avantages des VLAN sont les suivants:



Avantages	Description
Domaines de Diffusion Plus Petits	La division du réseau local réduit le nombre de domaines de diffusion
Sécurité optimisée	Seuls les utilisateurs du même VLAN peuvent communiquer ensemble
Efficacité accrue des IT	Les VLAN peuvent regrouper des appareils ayant des exigences similaires, par exemple professeurs contre étudiants
Réduction des coûts	Un commutateur peut prendre en charge plusieurs groupes ou VLAN
Meilleures performances	Les domaines de diffusion plus petits réduisent le trafic et améliorent la bande passante
Gestion simplifiée	Des groupes similaires auront besoin d'applications similaires et d'autres ressources réseau

Types de VLAN

VLAN par défaut

VLAN 1 est le suivant:

- Le VLAN par défaut
- Le VLAN natif par défaut
- VLAN de gestion par défaut
- Impossible de supprimer ou de renommer

Remarque : Bien que nous ne puissions pas supprimer VLAN1, Cisco recommandera d'attribuer ces caractéristiques par défaut à d'autres VLAN

```
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
```

Types de VLAN (Suite)

VLAN de données

- Dédié au trafic généré par l'utilisateur (trafic e-mail et web).
- VLAN 1 est le VLAN de données par défaut car toutes les interfaces sont attribuées à ce VLAN.

VLAN natif

- Ceci est utilisé uniquement pour les liaisons de trunk.
- Toutes les trames sont marquées sur une liaison de trunk 802.1Q, à l'exception de celles sur le VLAN natif.

VLAN de gestion

- Ceci est utilisé pour le trafic SSH/TelNet VTY et ne doit pas être transporté avec le trafic d'utilisateur final.
- Généralement, le VLAN qui est le SVI pour le commutateur de couche 2.

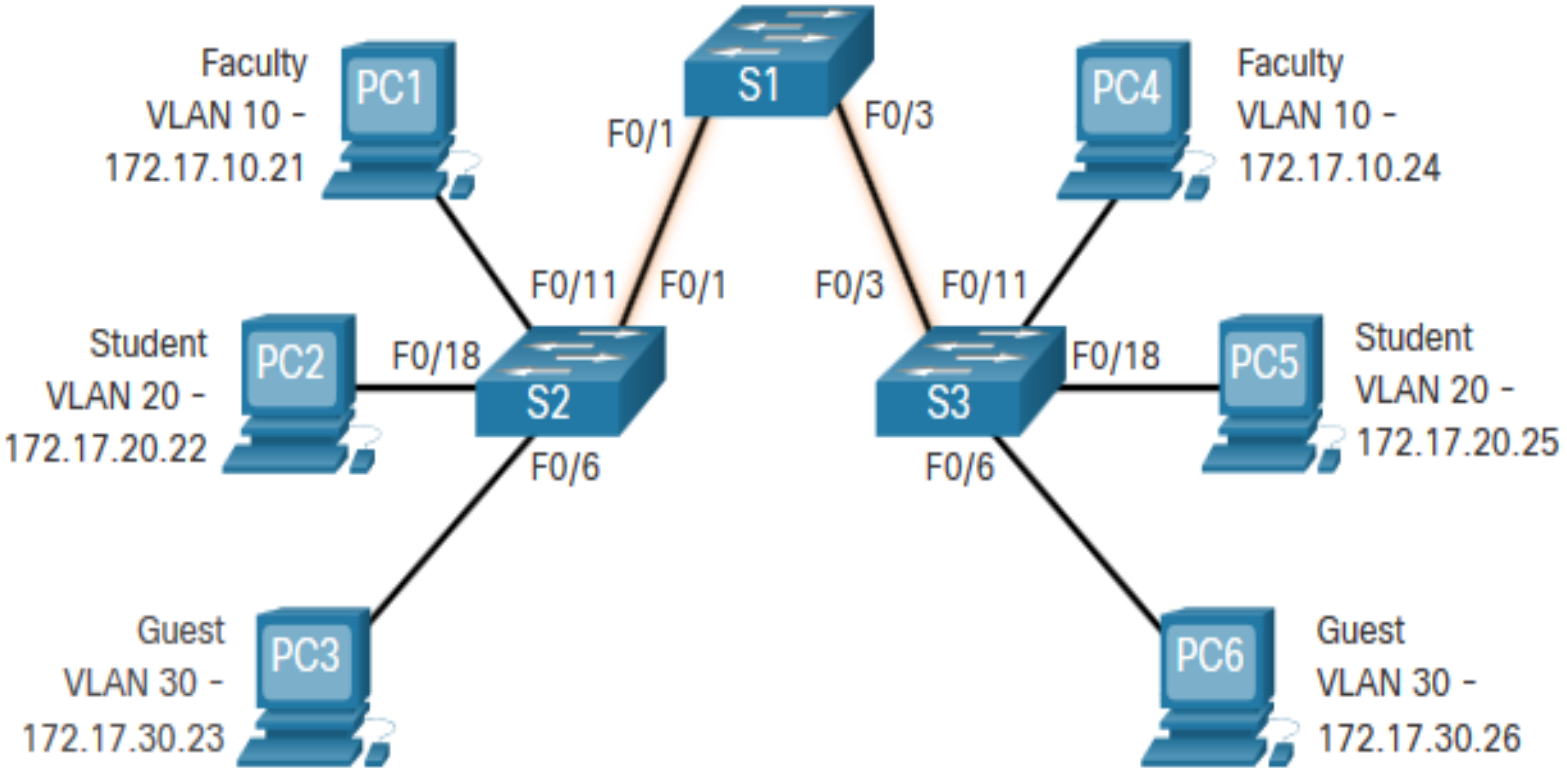
VLAN dans un environnement à plusieurs commutateurs

Définir les trunks de VLAN

Un trunk est une liaison point à point entre deux périphériques réseau.

Fonctions du trunk Cisco :

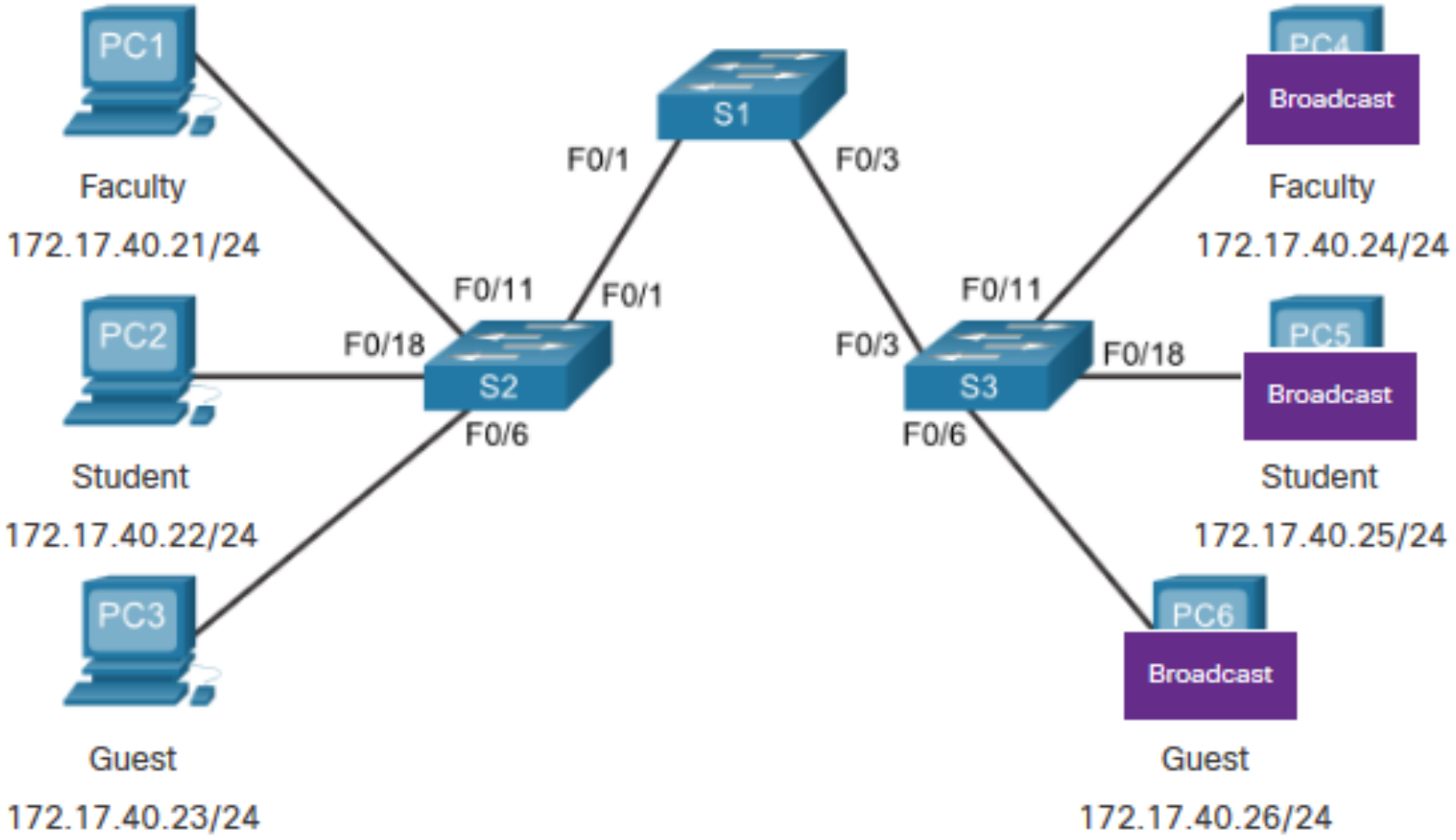
- Autoriser plusieurs VLAN
- Étendre le VLAN sur l'ensemble du réseau
- Par défaut, il prend en charge tous les VLAN
- Il prend en charge trunking 802.1Q



Les VLAN dans un environnement à plusieurs commutateurs

Réseaux sans VLAN

Sans VLAN, tous les périphériques connectés aux commutateurs recevront tout le trafic de monodiffusion, de multidiffusion et de diffusion.

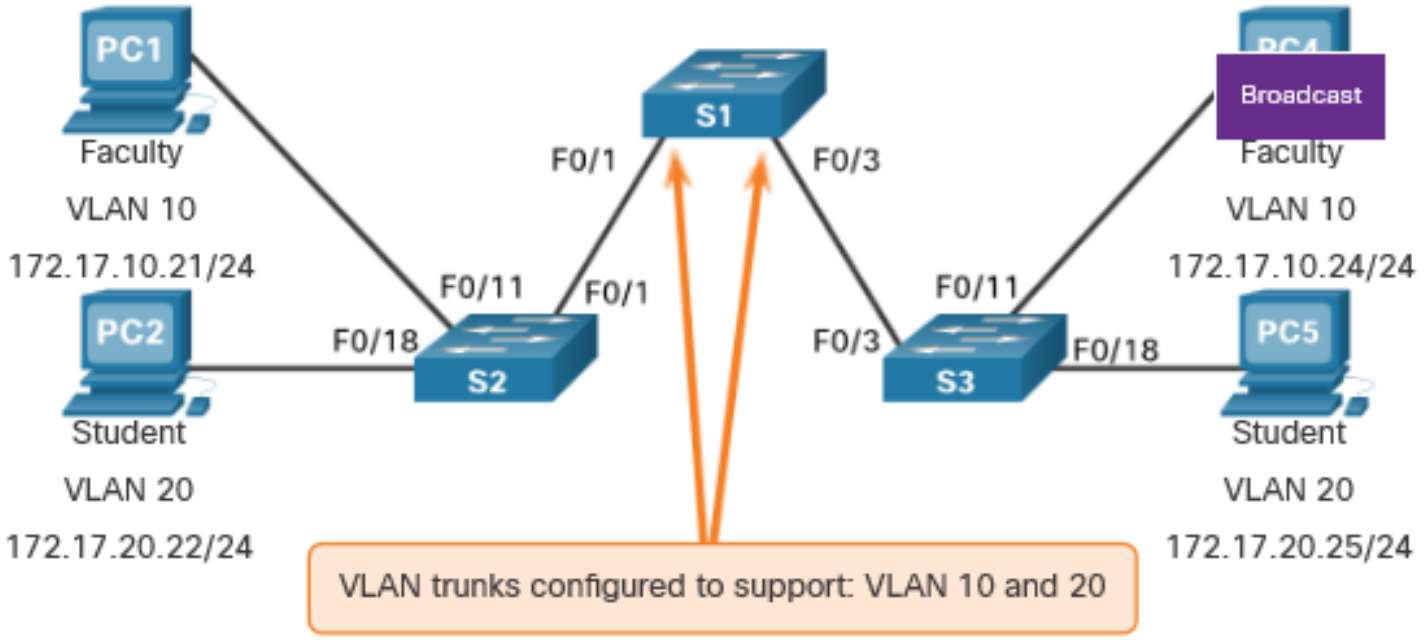


PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame out all available ports.

VLAN dans un environnement à plusieurs commutateurs

Réseaux sans VLAN

Avec les VLAN, le trafic de monodiffusion, de multidiffusion et de diffusion est limité à un VLAN. Sans un périphérique de couche 3 permettant de connecter les VLAN, les périphériques de différents VLAN ne peuvent pas communiquer.

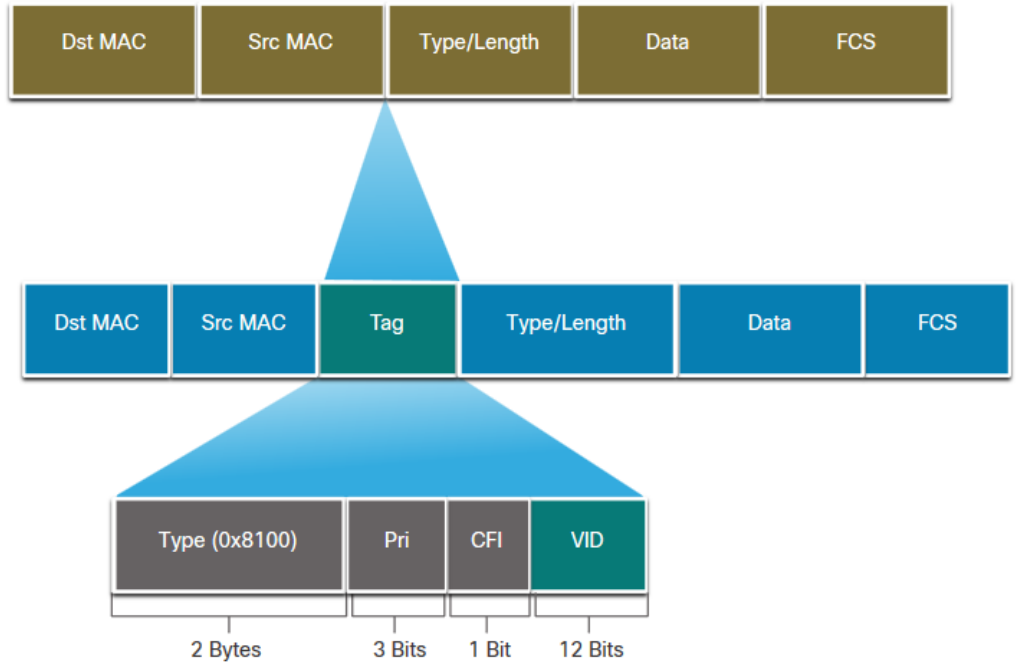


PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

VLAN dans un environnement à plusieurs commutateurs

Identification du VLAN avec une étiquette

- L'en-tête IEEE 802.1Q est de 4 octets
- Lorsque l'étiquette est créée, le FCS doit être recalculé.
- Lorsqu'elle est envoyée aux périphériques terminaux, cette étiquette doit être supprimée et le FCS doit être recalculé pour retourner à son numéro d'origine.



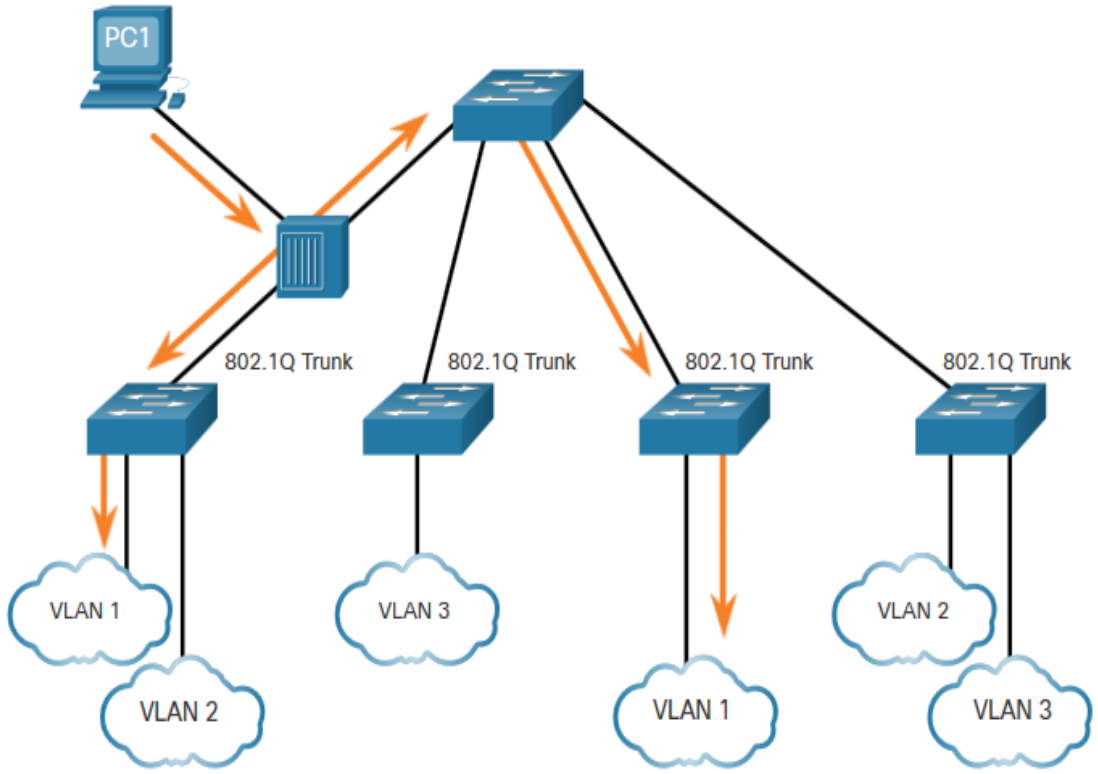
Champ d'étiquette VLAN 802.1Q	Fonction
Type	• Champ de 2 octets avec hexadécimal 0x8100 • Ceci est appelé TPID (Tag Protocol ID)
Priorité Utilisateur	• Valeur de 3 bits prenant en charge
CFI (Canonical Format Identifier)	• Identificateur de 1 bit qui prend en charge les trames Token Ring sur des liaisons Ethernet
ID de VLAN (VID)	• Numéro d'identification VLAN de 12 bits qui prend en charge jusqu'à 4096 ID de VLAN.

VLAN dans un environnement à plusieurs commutateurs

VLAN natifs et étiquetage 802.1Q

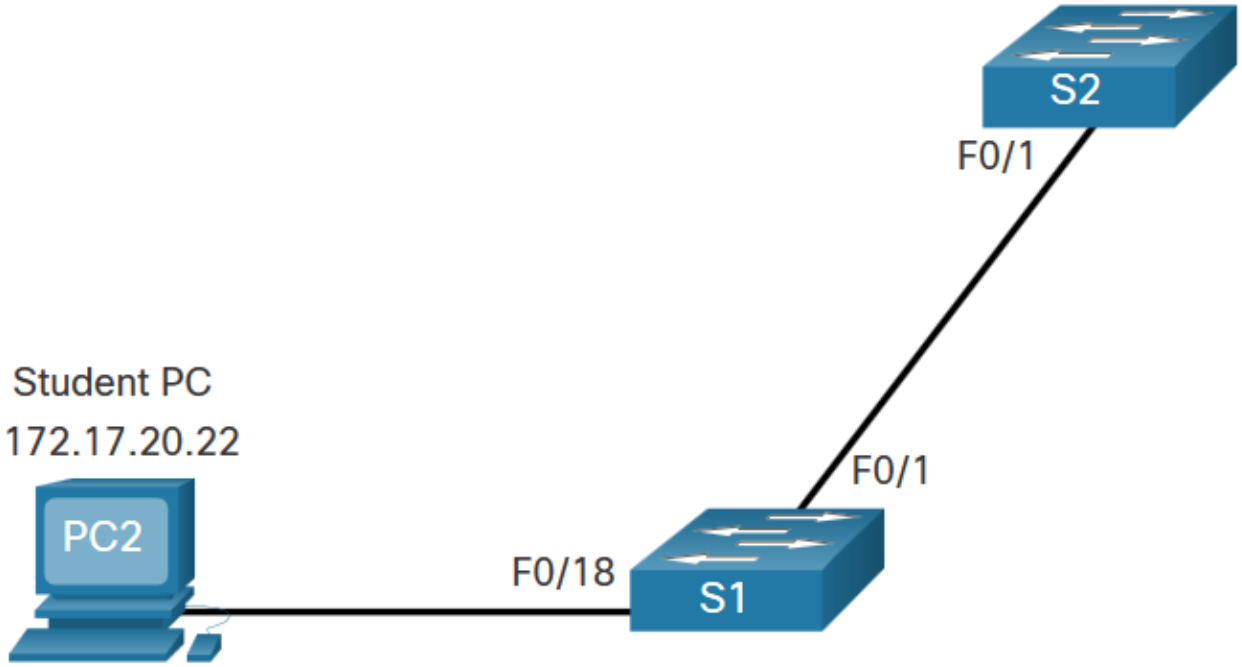
trunk de base 802.1Q:

- Étiquetage est généralement effectué sur tous les VLAN.
- L'utilisation d'un VLAN natif a été conçue pour une utilisation ancienne, comme le concentrateur dans l'exemple.
- Moins qu'il ne soit modifié, VLAN1 est le VLAN natif.
- Les deux extrémités d’une liaison trunk doit être configurées avec le même VLAN natif.
- Chaque trunk est configuré séparément, il est donc possible d'avoir un VLAN natif différent sur des trunks séparés.



Exemple de création de VLAN

- Si le PC d'étudiant doit être en VLAN 20, nous allons d'abord créer le VLAN, puis le nommer.
- Si vous ne le nommez pas, le Cisco IOS lui donnera un nom par défaut de vlan et le numéro à quatre chiffres du VLAN. Par exemple, vlan 0020 pour VLAN 20.

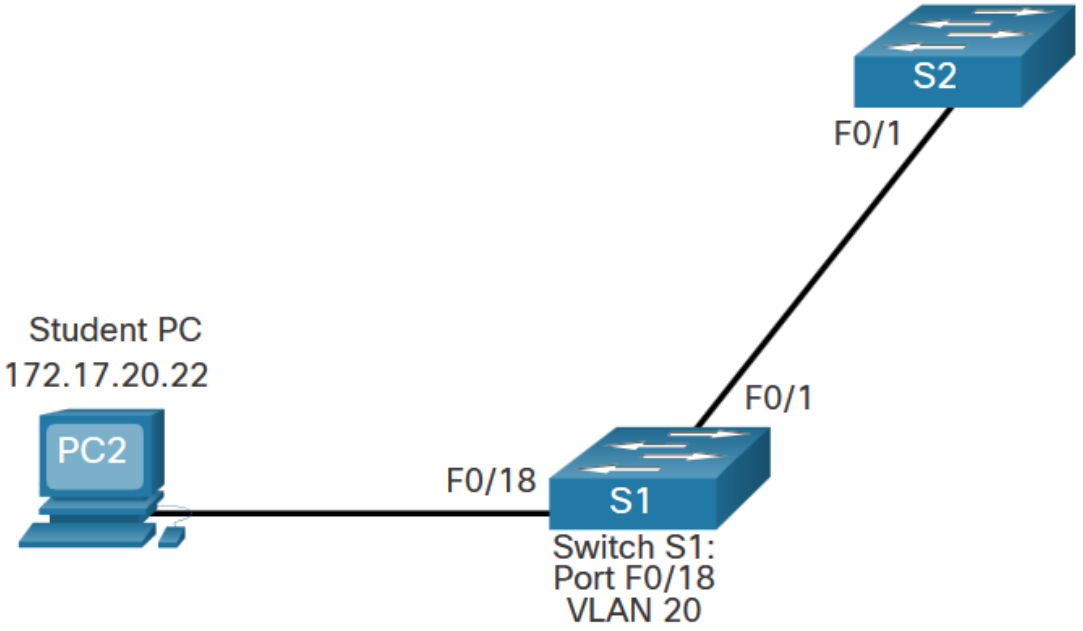


Invite	Commande
S1#	Configure terminal
S1(config)#	vlan 20
S1(config-vlan)#	name student
S1(config-vlan)#	end

Exemples d'attribution de port à des VLAN

Nous pouvons attribuer le VLAN à l'interface du port.

- Une fois le VLAN est attribué au périphérique, le périphérique final aura besoin des informations d'adresse IP pour ce VLAN
- Ici, le PC de l'étudiant reçoit 172.17.20.22



Invite	Commande
S1#	Configure terminal
S1(config)#	Interface fa0/18
S1(config-if)#	Switchport mode access
S1(config-if)#	Switchport access vlan 20
S1(config-if)#	end

Configuration de VLAN

Modification de l’appartenance des ports aux VLAN

Il existe plusieurs façons de modifier l’appartenance des ports aux VLAN:

•saisissez à nouveau la commande **switchport access vlan** *vlan-id*

•utilisez la commande **no switchport access vlan** pour replacer l'interface sur VLAN 1

Utilisez les commandes **show vlan brief** ou **show interface fa0/18 switchport** pour vérifier l'association correcte de VLAN.

```
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)
```

Suppression de VLAN

Supprimez les VLAN avec la commande **no vlan***vlan-id*_.

Attention: Avant de supprimer un VLAN, réaffectez tous les ports membres à un autre VLAN.

•Supprimez tous les VLAN avec les commandes **delete flash:vlan.dat** ou **delete vlan.dat** .

•Rechargez le commutateur lors de la suppression de tous les VLAN.

Remarque: Pour restaurer la valeur par défaut d'usine, débranchez tous les câbles de données, effacez la configuration de démarrage et supprimez le fichier vlan.dat, puis rechargez le périphérique.

Commandes de configuration de trunk

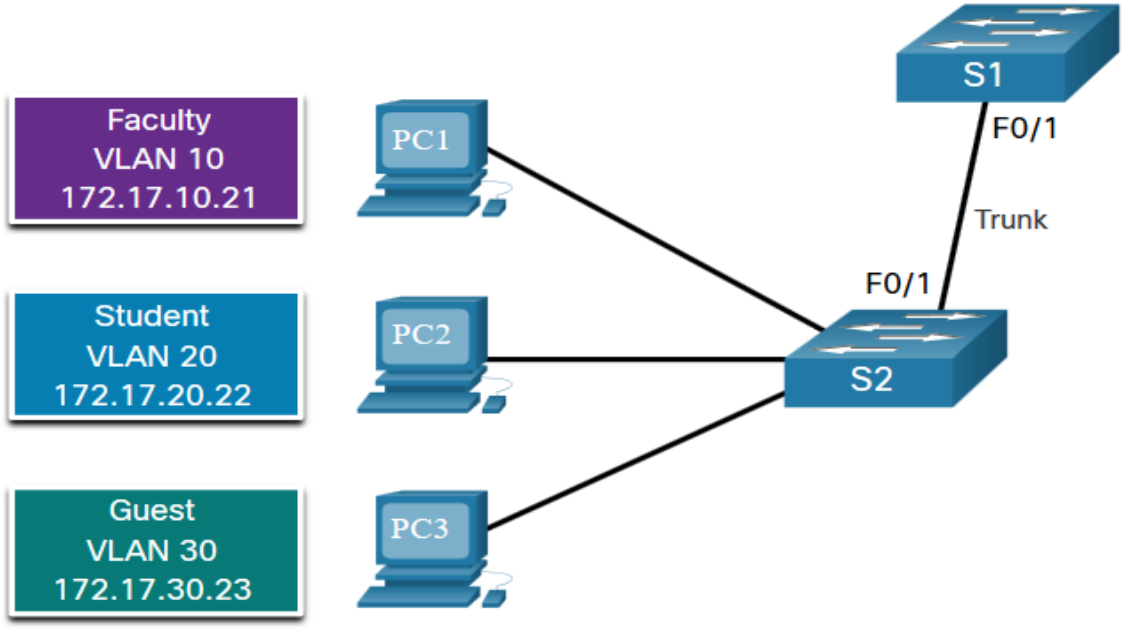
Configurez et vérifiez les trunks VLAN. Les trunks sont de couche 2 et transportent le trafic pour tous les VLAN.

Tâche	Commande IOS
Passez en mode de configuration globale.	Switch# **configure terminal**
Passez en mode de configuration d'interface.	Switch(config)# **interface** *interface-id*
Réglez le port en mode de liaison permanent.	Switch(config-if)# **switchport mode trunk**
Choisissez un VLAN natif autre que le VLAN 1	Switch(config-if)# **switchport trunk native vlan** *vlan-id*
Indiquez la liste des VLAN autorisés sur la liaison trunk.	Switch(config-if)# **switchport trunk allowed vlan** *vlan-list*
Repassez en mode d'exécution privilégié.	Switch(config-if)# **end**

Exemple de configuration de trunk

Les sous-réseaux associés à chaque VLAN sont:

- VLAN 10 - Faculté/Personnel - 172.17.10.0/24
- VLAN 20 - Étudiants - 172.17.20.0/24
- VLAN 30 - Invités - 172.17.30.0/24
- VLAN 99 - Natif - 172.17.99.0/24



Le port F0/1 sur S1 est configuré en tant que port de trunk.

Remarque : Ceci suppose un commutateur 2960 utilisant l'étiquetage 802.1q. Les commutateurs de couche 3 nécessitent que l'encapsulation soit configurée avant le mode trunk.

Invite	Commande
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

Présentation au protocole DTP

Le protocole DTP (Dynamic Trunking Protocol) est un protocole de Cisco propriétaire.
Les caractéristiques de protocole DTP sont les suivantes:

- Activé par défaut sur les commutateurs Catalyst 2960 et 2950
- Dynamic-auto est par défaut sur les commutateurs 2960 et 2950
- Peut être désactivé avec la commande nonegotiate
- Peut être réactivé en réglant l'interface sur dynamic-auto
- La définition d'un commutateur sur un trunk statique ou un accès statique évitera les problèmes de négociation avec la commande **switchport mode trunk** ou **switchport mode access** .

```
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
```

```
S1(config-if)# switchport mode dynamic auto
```

Modes d'interface négociés

La commande **switchport mode** comporte des options supplémentaires.
Utilisez la commande de configuration d'interface **switchport nonegotiate** pour arrêter la négociation DTP.

Option	Description
accès	Mode d'accès permanent et négocie pour convertir le lien voisin en un lien d'accès
Dynamique Automatique	l'interface devient un trunk si l'interface voisine est configurée en mode trunk inconditionnel ou souhaitable.
dynamique souhaitable	Cherche activement à devenir un trunk en négociant avec d'autres interfaces automatiques ou souhaitables
trunk	Mode de trunking permanent avec négociation pour convertir le liaison voisin en liaison trunk

Résultats d'une configuration du protocole DTP

Les options de configuration du protocole DTP sont les suivantes:

	Dynamique Automatique	Dynamique souhaitable	Trunk	Accès
Dynamique Automatique	Accès	Trunk	Trunc	Accès
Dynamique souhaitable	Trunc	Trunc	Trunc	Accès
Trunk	Trunc	Trunc	Trunc	Connectivité limitée
Accès	Accès	Accès	Connectivité limitée	Accès

Vérifier le mode du protocole DTP

La configuration du protocole DTP par défaut dépend de la version et de la plate-forme de Cisco IOS.
Utilisez la commande **show dtp interface** pour déterminer le mode DTP actuel.
La meilleure pratique recommande que les interfaces soient configurées pour l'accès ou le trunk et pour passer au PAO

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```

Routage inter VLAN Router-on-a-Stick

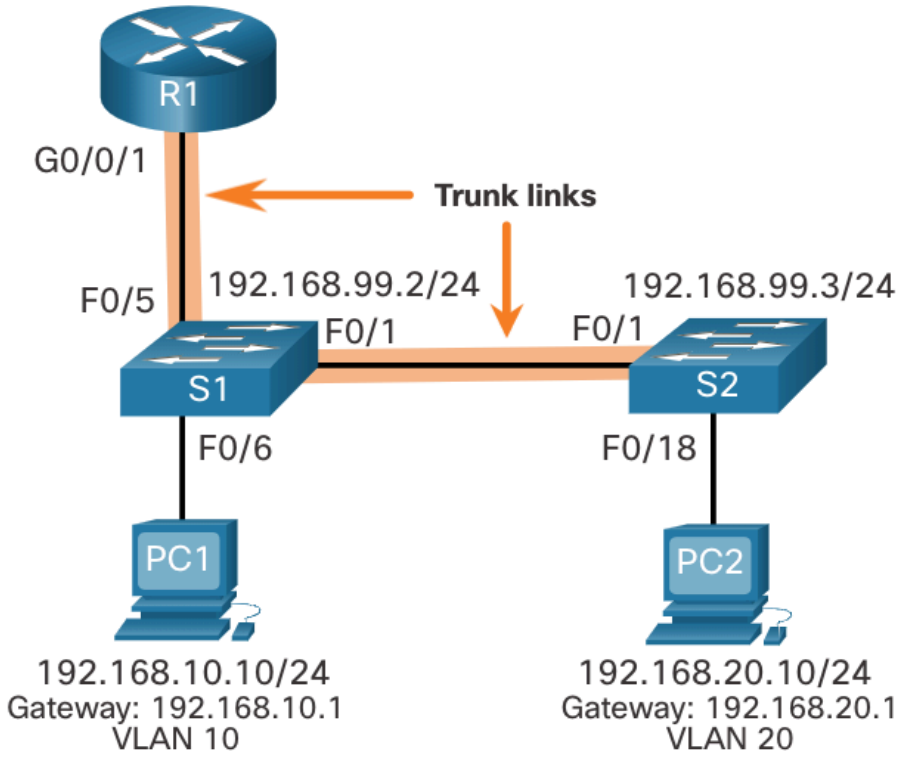
La méthode de routage inter-VLAN 'router-on-a-stick' surmonte la limite de la méthode de routage inter-VLAN héritée. Il ne nécessite qu'une seule interface Ethernet physique pour acheminer le trafic entre plusieurs VLANs sur un réseau.

- Une interface Ethernet de routeur Cisco IOS est configurée comme un trunk 802.1Q et connectée à un port de trunk sur un commutateur de couche 2. Plus précisément, l'interface du routeur est configurée à l'aide de sous-interfaces pour identifier les VLANs routables.
- Les sous-interfaces configurées sont des interfaces virtuelles logicielles. Chacune est associée à une seule interface Ethernet physique. Les sous-interfaces sont configurées dans un logiciel sur un routeur. Chaque sous-interface est configurée indépendamment avec sa propre adresse IP et une attribution VLAN. Les sous-interfaces sont configurées pour différents sous-réseaux correspondant à une attribution VLAN. Cela facilite le routage logique.
- Lorsque le trafic balisé VLAN entre dans l'interface du routeur, il est transféré à la sous-interface VLAN. Une fois qu'une décision de routage est prise en fonction de l'adresse du réseau IP de destination, le routeur détermine l'interface de sortie du trafic. Si l'interface de sortie est configurée en tant que sous-interface 802.1q, les blocs de données sont étiquetés VLAN avec le nouveau VLAN et renvoyés vers l'interface physique

Remarque: la méthode router-on-a-stick de routage inter-VLAN ne va pas au-delà de 50 VLAN.

Router-on-a-Stick Scénario

- Sur la figure, l'interface R1 GigabiteEthernet 0/0/1 est connectée au port S1 FastEthernet 0/5. Le port S1 FastEthernet 0/1 est connecté au port S2 FastEthernet 0/1. Il s'agit de liaisons de trunk qui sont nécessaires pour transférer le trafic au sein des VLANs et entre ceux-ci.
- Pour router entre les VLANs, l'interface R1 GigabitEthernet 0/0/1 est logiquement divisée en trois sous-interfaces, comme indiqué dans le tableau. Le tableau indique également les trois VLANs qui seront configurés sur les commutateurs.
- Supposons que R1, S1 et S2 ont des configurations de base initiales. Actuellement, PC1 et PC2 ne peuvent pas effectuer de **ping** mutuellement parce qu'ils se trouvent sur des réseaux distincts. Seuls S1 et S2 peuvents'envoyer des **pings** mutuellement, mais ils sont inaccessibles par PC1 ou PC2 car ils sont également sur des réseaux différents.
- Pour permettre aux périphériques de s'envoyer des pings, les commutateurs doivent être configurés avec des VLANs et des trunkings, et le routeur doit être configuré pour le routage inter-VLAN.



Sous-interfaces	VLAN	Adresse IP
G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24

Configuration du VLAN S1 et du trunking

Effectuez les étapes suivantes pour configurer S1 avec les VLANs et le trunking :

- **Étape 1**. Créez et nommez les VLANs.
- **Étape 2**. Créez l'interface de gestion.
- **Étape 3**. Configurer les ports d'accès
- **Étape 4**. Configurez les ports trunk.