

TP8-(VLAN) / AR

Responsable du Module : Mr A. BENZERBADJ

1 Objectif

Créer des réseaux locaux virtuels.

2 rappels

- Un ou plusieurs ports d'un switch peuvent être assignés à un VLAN spécifique.
- Des ports assignés à des VLANs différents ne peuvent communiquer que via un routeur (ou switch de niveau 3)
- Par défaut, tous les ports sont dans le VLAN1, considéré comme le VLAN d'administration.

Parmi les avantages de la création de VLANs, on citera :

- Contrôle de broadcast
- D'un point de vue sécurité, il y a séparation logique des utilisateurs et des départements
- Point de vue flexibilité et scalabilité : pas de frontières physiques pour les réseaux.

3 Exercice

- Soit la topologie du réseau et les tableaux d'adressage relatifs à celle-ci représentés dans la Figure 1
- Notons que quatre réseaux locaux virtuels sont considérés : VLAN 10 (faculty/staff), VLAN 20 (students), VLAN 30 (guest) et VLAN 99 (management)

1. **Désactivation de tous les ports non utilisés** (Il est recommandé de désactiver tous les ports non utilisés sur les commutateurs) :

- Switch#conf t
- Switch(config)#interface range fa0/1-24
- Switch(config-if-range)#shutdown
- Switch(config-if-range)#interface range gi0/1-2
- Switch(config-if-range)#shutdown

2. **Réactivation des ports utilisateur sur S2 et S3 :**

- S2(config)#int range fa0/6, fa0/11, fa0/18
- S2(config-if-range)#switchport mode access
- S2(config-if-range)#no shutdown
- S3(config)#int range fa0/6, fa0/11, fa0/18
- S3(config-if-range)#switchport mode access

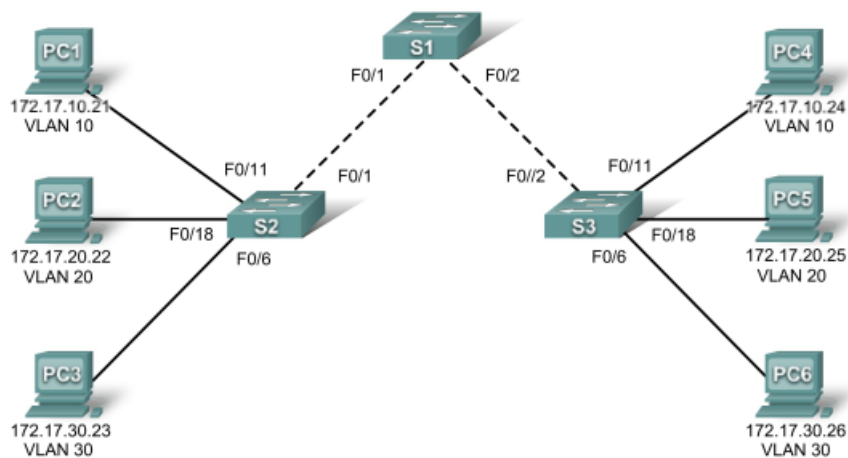


Tableau d'adressage

Périphérique (Nom d'hôte)	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
S1	VLAN 99	172.17.99.11	255.255.255.0	S/O
S2	VLAN 99	172.17.99.12	255.255.255.0	S/O
S3	VLAN 99	172.17.99.13	255.255.255.0	S/O
PC1	Carte réseau	172.17.10.21	255.255.255.0	172.17.10.1
PC2	Carte réseau	172.17.20.22	255.255.255.0	172.17.20.1
PC3	Carte réseau	172.17.30.23	255.255.255.0	172.17.30.1
PC4	Carte réseau	172.17.10.24	255.255.255.0	172.17.10.1
PC5	Carte réseau	172.17.20.25	255.255.255.0	172.17.20.1
PC6	Carte réseau	172.17.30.26	255.255.255.0	172.17.30.1

Affectation initiale des ports (Commutateurs 2 et 3)

Ports	Affectation	Réseau
Fa0/1 – 0/5	Agrégations 802.1q (VLAN 99 natif)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

FIGURE 1 – Topologie et tableaux d'adressage.

— S3(config-if-range)#no shutdown

3. Création de réseaux locaux virtuels sur le commutateur S1.

On utilisera la commande **vlan id-vlan** en **mode de configuration globale** pour ajouter un réseau local virtuel. Après avoir créé le réseau local virtuel, on utilisera le **mode de configuration vlan** pour nommer le réseau local virtuel via la commande **name nom vlan**.

— S1(config)#vlan 10

— S1(config-vlan)#name faculty/staff

— S1(config-vlan)#vlan 20

— S1(config-vlan)#name students

— S1(config-vlan)#vlan 30

- S1(config-vlan)#name guest
 - S1(config-vlan)#vlan 99
 - S1(config-vlan)#name management
 - S1(config-vlan)#end
 - S1#
4. vérification de la création des réseaux locaux virtuels pour S1. Utilisez la commande **show vlan brief**.
 - S1#show vlan brief
 5. configurez et affectez un nom aux réseaux locaux virtuels pour les commutateurs S2 et S3.
 6. Vérifiez la configuration avec la commande **show vlan brief**.
 7. Affectation des ports de commutateur aux réseaux locaux virtuels sur S2 et S3, selon le tableau de la Figure 1. Les ports sont affectés aux réseaux locaux virtuels en **mode de configuration d'interface**, via la commande **switchport access vlan id-vlan**. Vous pouvez affecter chaque port individuellement ou utiliser la commande **interface range** pour simplifier cette tâche :
 - S3(config)#interface range fa0/6-10
 - S3(config-if-range)#switchport access vlan 30
 - S3(config-if-range)#interface range fa0/11-17
 - S3(config-if-range)#switchport access vlan 10
 - S3(config-if-range)#interface range fa0/18-24
 - S3(config-if-range)#switchport access vlan 20
 - S3(config-if-range)#end
 - S3#copy running-config startup-config
 8. détermination des ports ayant été ajoutés : utilisez la commande **show vlan id numéro-vlan** sur S2 pour identifier les ports affectés au VLAN 10 (la commande **show vlan name nom-vlan** affiche la même sortie. Vous pouvez également afficher les informations d'affectation VLAN à l'aide de la commande **show interfaces interface switchport**.
 9. Affectation d'un réseau local virtuel de gestion : Un réseau local virtuel de gestion est un réseau local virtuel que vous configurez pour accéder aux fonctions de gestion d'un commutateur. Si vous ne définissez aucun autre réseau local virtuel, le VLAN 1 fait office de réseau local virtuel de gestion. Affectez une adresse IP et un masque de sous-réseau au réseau local virtuel de gestion. Un commutateur peut être géré via HTTP, Telnet, SSH ou SNMP. Étant donné que la première configuration d'un commutateur Cisco présente le VLAN 1 comme réseau local virtuel par défaut, il n'est pas recommandé d'utiliser le VLAN 1 comme réseau local virtuel de gestion. Vous ne souhaitez pas qu'un utilisateur arbitraire se connectant à un commutateur soit dirigé par défaut vers le réseau local virtuel de gestion. N'oubliez pas que vous avez configuré le réseau local virtuel de gestion en tant que VLAN 99 précédemment dans l'actuel TP. En mode de configuration d'interface, utilisez la commande **ip address** pour affecter l'adresse IP de gestion aux commutateurs.
 - S1(config)#interface vlan 99
 - S1(config-if)#ip address 172.17.99.11 255.255.255.0
 - S1(config-if)#no shutdown

```

— S2(config)#interface vlan 99
— S2(config-if)#ip address 172.17.99.12 255.255.255.0
— S2(config-if)#no shutdown
— S3(config)#interface vlan 99
— S3(config-if)#ip address 172.17.99.13 255.255.255.0
— S3(config-if)#no shutdown

```

L'affectation d'une adresse de gestion permet la communication IP entre les commutateurs, ainsi que la connexion aux commutateurs de n'importe quel hôte connecté à un port affecté au VLAN 99. Étant donné que le VLAN 99 est configuré en tant que réseau local virtuel de gestion, tout port affecté à ce réseau local virtuel est considéré comme un port de gestion et doit être sécurisé pour contrôler les périphériques autorisés à se connecter à ce port.

10. Configuration de l'agrégation et du réseau local virtuel natif pour les ports agrégés sur tous les commutateurs. Les agrégations sont des connexions entre les commutateurs leur permettant d'échanger des informations pour tous les réseaux locaux virtuels. Par défaut, un port agrégé appartient à tous les réseaux locaux virtuels, contrairement à un port d'accès qui ne peut appartenir qu'à un seul réseau local virtuel. Si le commutateur prend en charge l'encapsulation VLAN ISL et 802.1Q, les agrégations doivent spécifier la méthode utilisée. Étant donné que le commutateur 2960 ne prend en charge que l'agrégation 802.1Q, il n'est pas spécifié dans ces travaux pratiques.

Un réseau local virtuel natif est affecté à un port agrégé 802.1Q. Dans la topologie, le réseau local virtuel natif est le VLAN 99. Un port agrégé 802.1Q prend en charge le trafic provenant de plusieurs réseaux locaux virtuels (trafic étiqueté), ainsi que le trafic ne provenant pas d'un réseau local virtuel (trafic non étiqueté). Le port agrégé 802.1Q place le trafic non étiqueté sur le réseau local virtuel natif. Le trafic non étiqueté est généré par un ordinateur connecté à un port de commutateur configuré avec le réseau local virtuel natif. Une des spécifications IEEE 802.1Q pour les réseaux locaux virtuels natifs consiste à conserver la compatibilité amont avec le trafic non étiqueté commun aux scénarios de réseau local existants. Pour les besoins de ces travaux pratiques, un réseau local virtuel natif fait office d'identificateur commun aux extrémités d'un lien agrégé. Il est recommandé d'utiliser un réseau local virtuel autre que le VLAN 1 comme réseau local virtuel natif.

Utilisez la commande `interface range` en mode de configuration globale pour simplifier la configuration de l'agrégation.

```

— S1(config)#interface range fa0/1-5
— S1(config-if-range)#switchport mode trunk
— S1(config-if-range)#switchport trunk native vlan 99
— S1(config-if-range)#no shutdown
— S1(config-if-range)#end
— S2(config)# interface range fa0/1-5
— S2(config-if-range)#switchport mode trunk
— S2(config-if-range)#switchport trunk native vlan 99
— S2(config-if-range)#no shutdown
— S2(config-if-range)#end

```

11. Vérifiez que les agrégations ont été configurées via la commande **show interface trunk** :
 - S1#show interface trunk
12. vérification de la communication entre les commutateurs. À partir de S1, envoyez une requête ping à l'adresse de gestion sur S2 et S3 :
 - S1#ping 172.17.99.12
 - S1#ping 172.17.99.13
13. Envoyez une requête ping de l'hôte PC2 à l'hôte PC1 (172.17.10.21). La tentative de requête ping a-t-elle abouti ?
14. Envoyez une requête ping de l'hôte PC2 à l'adresse IP 172.17.99.12 du commutateur VLAN 99. La tentative de requête ping a-t-elle abouti ?
15. Envoyez une requête ping de l'hôte PC2 à l'hôte PC5. La tentative de requête ping a-t-elle abouti ?
16. Déplacement de PC1 sur le même réseau local virtuel que PC2 Le port connecté à PC2 (S2 Fa0/18) est affecté au VLAN 20, et le port connecté à PC1 (S2 Fa0/11) est affecté au VLAN 10. Affectez de nouveau le port S2 Fa0/11 au VLAN 20. Vous n'avez pas besoin de supprimer un port d'un réseau local virtuel pour modifier son appartenance au réseau local virtuel. Après avoir réaffecté le port à un nouveau réseau local virtuel, il est automatiquement supprimé de son ancien réseau local virtuel.
 - S2#configure terminal
 - S2(config)#interface fastethernet 0/11
 - S2(config-if)#switchport access vlan 20
 - S2(config-if)#end
17. Envoyez une requête ping de l'hôte PC2 à l'hôte PC1. La tentative de requête ping a-t-elle abouti ?
18. Modification de l'adresse IP et du réseau de PC1 Remplacez l'adresse IP de PC1 par 172.17.20.21. Le masque de sous-réseau et la passerelle par défaut peuvent rester identiques. Envoyez de nouveau une requête ping de l'hôte PC2 à l'hôte PC1, en utilisant la nouvelle adresse IP affectée. La tentative de requête ping a-t-elle abouti ? Pourquoi ?