■ VLAN, Routage Inter-VLAN & Sécurité

Corrigé commenté · Partie 1 + Partie 2 · BTS SIO SISR · Christophe Beaudenon · E2SE Digital IT Caen

PARTIE 1 — Atelier VLAN et routage inter-VLAN

Plan d'adressage complet

■ **Pourquoi ?** Avant toute configuration, on établit un plan d'adressage clair. Chaque VLAN correspond à un sous-réseau IP isolé : les machines d'un VLAN ne peuvent pas communiquer directement avec celles d'un autre sans passer par le routeur. Ce cloisonnement améliore la sécurité et les performances (moins de broadcasts parasites).

Réseau	VLAN	Plage IP	Masque	Gateway	DHCP
SN_Tech	VLAN 11	192.168.1.0	/28 — 14 hôtes	192.168.1.1	✓
SN_Serveurs	VLAN 12	192.168.1.16	/29 — 6 hôtes	192.168.1.17	✗ statique
SN_Direction	VLAN 21	192.168.2.0	/29 — 6 hôtes	192.168.2.1	✓
SN_Marketing	VLAN 22	192.168.2.8	/29 — 6 hôtes	192.168.2.9	✓
SN_Production	VLAN 23	192.168.2.16	/28 — 14 hôtes	192.168.2.17	✓

Étape 1 — Nommage des équipements

■ **Pourquoi ?** Le hostname identifie l'équipement dans l'invite de commande (ex: RT_Dis_1#). C'est indispensable pour ne pas se tromper d'équipement lors d'une session en console ou SSH, surtout quand plusieurs fenêtres sont ouvertes en même temps.

Équipement	Commandes IOS

RT_Dis_1	`enable`
	`configure terminal`
	`hostname RT_Dis_1`

SW_Acc_1	`enable`
	`configure terminal`
	`hostname SW_Acc_1`

SW_Acc_2	`enable`
	`configure terminal`
	`hostname SW_Acc_2`

Étape 2 — Création des VLANs sur les switchs

■ **Pourquoi ?** Un VLAN (Virtual LAN) crée une séparation logique du réseau sur un même switch physique. Sans VLAN, toutes les machines seraient dans le même domaine de broadcast et pourraient se voir. Ici on crée les VLANs et on leur donne un nom lisible pour faciliter l'administration.

Équipement	Commandes IOS

SW_Acc_1	`configure terminal`
	`vlan 11`
	`name SN_Tech`
	`vlan 12`
	`name SN_Serveurs`
	`exit`

SW_Acc_2	`configure terminal`
	`vlan 21`
	`name SN_Direction`
	`vlan 22`
	`name SN_Marketing`
	`vlan 23`
	`name SN_Production`
	`exit`

Étape 3 — Ports en mode access

> ■ **Pourquoi ?** Un port en mode access appartient à un seul VLAN. Les trames qui arrivent sur ce port sont automatiquement taggées avec le numéro de VLAN correspondant. C'est le mode utilisé pour connecter les PC et serveurs : ils n'ont pas à gérer les tags 802.1Q eux-mêmes.

Équipement	Commandes IOS

SW_Acc_1	`interface range Fa0/1 - 14`
	`switchport mode access`
	`switchport access vlan 11`
	`interface range Fa0/17 - 23`
	`switchport mode access`
	`switchport access vlan 12`

SW_Acc_2	`interface range Fa0/1 - 6`
	`switchport mode access`
	`switchport access vlan 21`
	`interface range Fa0/9 - 14`
	`switchport mode access`
	`switchport access vlan 22`
	`interface range Fa0/17 - 23`
	`switchport mode access`
	`switchport access vlan 23`

Étape 4 — Liaison trunk vers le routeur

> ■ **Pourquoi ?** Un port trunk transporte les trames de plusieurs VLANs simultanément en ajoutant un tag 802.1Q dans l'en-tête Ethernet. C'est obligatoire sur la liaison switch → routeur pour que le routeur puisse distinguer à quel VLAN appartient chaque trame et appliquer le bon routage inter-VLAN.

Équipement	Commandes IOS

SW_Acc_1	`interface Gi0/1`
	`switchport mode trunk`
	`switchport trunk allowed vlan 11,12`

SW_Acc_2	`interface Gi0/1`
	`switchport mode trunk`
	`switchport trunk allowed vlan 21,22,23`

■■ On n'autorise que les VLANs nécessaires sur chaque trunk (principe du moindre privilège) — inutile de laisser passer le trafic VLAN 11 vers SW_Acc_2 par exemple.

Étape 5 — Sous-interfaces routeur (Router-on-a-Stick)

■ **Pourquoi ?** Le routeur ne possède que deux interfaces physiques (Gi0/0 et Gi0/1) mais doit router entre 5 VLANs. La technique Router-on-a-Stick crée des sous-interfaces logiques (Gi0/0.11, Gi0/0.12…) sur une seule interface physique. Chaque sous-interface est associée à un VLAN via 'encapsulation dot1Q' et possède l'adresse IP qui servira de passerelle aux machines de ce VLAN.

Équipement	Commandes IOS

RT_Dis_1	`interface Gi0/0`
	`no shutdown`
	`interface Gi0/0.11`
	`encapsulation dot1Q 11`
	`ip address 192.168.1.1 255.255.255.240`
	`interface Gi0/0.12`
	`encapsulation dot1Q 12`
	`ip address 192.168.1.17 255.255.255.248`
	`interface Gi0/1`
	`no shutdown`
	`interface Gi0/1.21`
	`encapsulation dot1Q 21`
	`ip address 192.168.2.1 255.255.255.248`
	`interface Gi0/1.22`
	`encapsulation dot1Q 22`
	`ip address 192.168.2.9 255.255.255.248`
	`interface Gi0/1.23`
	`encapsulation dot1Q 23`
	`ip address 192.168.2.17 255.255.255.240`

Étape 6 — Pools DHCP sur le routeur

■ **Pourquoi ?** Le DHCP (Dynamic Host Configuration Protocol) permet aux PC d'obtenir automatiquement une IP, un masque et une passerelle sans configuration manuelle. On configure les pools sur le routeur car c'est lui qui connaît tous les sous-réseaux. Les adresses statiques (passerelles, serveurs) doivent être exclues des pools pour éviter les conflits d'adressage.

Équipement	Commandes IOS

RT_Dis_1	`! Exclusion des adresses statiques`
	`ip dhcp excluded-address 192.168.1.1`
	`ip dhcp excluded-address 192.168.1.17 192.168.1.19`
	`ip dhcp excluded-address 192.168.2.1 192.168.2.2`
	`ip dhcp excluded-address 192.168.2.9`
	`ip dhcp excluded-address 192.168.2.17`
	
	`! Pool SN_Tech (VLAN 11)`
	`ip dhcp pool SN_Tech`
	`network 192.168.1.0 255.255.255.240`
	`default-router 192.168.1.1`
	
	`! Pool SN_Direction (VLAN 21)`
	`ip dhcp pool SN_Direction`
	`network 192.168.2.0 255.255.255.248`
	`default-router 192.168.2.1`
	
	`! Pool SN_Marketing (VLAN 22)`
	`ip dhcp pool SN_Marketing`
	`network 192.168.2.8 255.255.255.248`
	`default-router 192.168.2.9`
	
	`! Pool SN_Production (VLAN 23)`
	`ip dhcp pool SN_Production`
	`network 192.168.2.16 255.255.255.240`
	`default-router 192.168.2.17`

■■ SN_Serveurs (VLAN 12) n'a pas de pool DHCP : les serveurs ont des adresses IP statiques fixes (SV_IT_1 : .18, SV_IT_2 : .19). Un serveur doit toujours être joignable à la même adresse.

PARTIE 2 — Atelier VLAN Natif et Sécurité

Étape 1 — Sécurisation des accès console et exec

■ **Pourquoi ?** Par défaut, les équipements Cisco ne demandent aucun mot de passe : n'importe qui branché en console peut tout reconfigurer. Le mot de passe console protège l'accès physique au port série. Le 'enable secret' protège le passage en mode privilégié (EXEC). 'service password-encryption' chiffre les mots de passe stockés en clair dans la running-config pour éviter qu'ils soient lisibles lors d'un 'show running-config'.

Équipement	Commandes IOS

RT_Dis_1 / SW_Acc_1 / SW_Acc_2	`configure terminal`
	`! Mot de passe accès console`
	`line console 0`
	`password cisco`
	`login`
	`exit`
	`! Mot de passe mode privilégié (hashé MD5)`
	`enable secret cisco`
	`! Chiffrement des mots de passe en clair`
	`service password-encryption`

■■ En production, remplacez 'cisco' par un mot de passe fort. 'enable secret' est préférable à 'enable password' car il est stocké en MD5 et non en clair.

Étape 2 — VLAN 999 comme VLAN natif

■ **Pourquoi ?** Le VLAN natif est le VLAN utilisé sur un trunk pour les trames qui n'ont PAS de tag 802.1Q. Par défaut c'est le VLAN 1 — ce qui est un risque de sécurité car le VLAN 1 est aussi le VLAN de gestion par défaut sur beaucoup d'équipements. En dédiant le VLAN 999 (vide, sans machines) au rôle de VLAN natif, on empêche les attaques de type 'VLAN hopping'. Forcer le tagging des trames natives renforce encore cette protection.

Équipement	Commandes IOS

SW_Acc_1 / SW_Acc_2	`configure terminal`
	`! Création du VLAN 999 dédié au rôle natif`
	`vlan 999`
	`name NATIF`
	`exit`
	`! Application sur le port trunk et forçage du tag`
	`interface Gi0/1`
	`switchport trunk native vlan 999`
	`switchport trunk tagging native vlan`

Étape 3 — VLAN 998 pour les accès à distance (SN_Equipements)

■ **Pourquoi ?** Les équipements réseau (switchs, routeur) ont besoin d'une adresse IP pour être administrés à distance via SSH. On crée un VLAN dédié à cet usage (VLAN 998) séparé des VLANs utilisateurs : si un PC utilisateur est compromis, il ne peut pas directement attaquer l'interface de gestion. Deux sous-réseaux distincts sont nécessaires car le routeur sépare les deux plateaux — il ne peut pas avoir le même sous-réseau sur deux interfaces différentes.

Équipement	Interface	Adresse IP	Masque	Passerelle
RT_Dis_1	Gi 0/0.998	192.168.1.254	/29	—
RT_Dis_1	Gi 0/1.998	192.168.2.254	/29	—
SW_Acc_1	Vlan 998	192.168.1.249	/29	192.168.1.254
SW_Acc_2	Vlan 998	192.168.2.249	/29	192.168.2.254

Équipement	Commandes IOS

SW_Acc_1	`! Ajout du VLAN 998 dans la base locale`
	`vlan 998`
	`name SN_Equipements`
	`exit`
	`! Autoriser le VLAN 998 à transiter sur le trunk`
	`interface Gi0/1`
	`switchport trunk allowed vlan add 998`
	`exit`
	`! Interface virtuelle de gestion avec IP`
	`interface vlan 998`
	`ip address 192.168.1.249 255.255.255.248`
	`no shutdown`
	`exit`
	`! Passerelle par défaut pour atteindre le réseau`
	`ip default-gateway 192.168.1.254`

SW_Acc_2	`vlan 998`
	`name SN_Equipements`
	`exit`
	`interface Gi0/1`
	`switchport trunk allowed vlan add 998`
	`exit`
	`interface vlan 998`
	`ip address 192.168.2.249 255.255.255.248`
	`no shutdown`
	`exit`
	`ip default-gateway 192.168.2.254`

RT_Dis_1	`! Sous-interface plateau 1 – accès gestion SW_Acc_1`
	`interface Gi0/0.998`
	`encapsulation dot1Q 998`
	`ip address 192.168.1.254 255.255.255.248`
	`! Sous-interface plateau 2 – accès gestion SW_Acc_2`
	`interface Gi0/1.998`
	`encapsulation dot1Q 998`
	`ip address 192.168.2.254 255.255.255.248`

Étape 4 — Vérifications

■ **Pourquoi ?** Les vérifications permettent de confirmer que chaque étape est correctement appliquée avant de passer à la suivante. Un ping réussi prouve la connectivité bout en bout à travers les VLANs et le routage.

- ✓ **ping 192.168.1.254 — depuis SW_Acc_1 vers sa passerelle (plateau 1)**
- ✓ **ping 192.168.2.254 — depuis SW_Acc_2 vers sa passerelle (plateau 2)**
- ✓ **ping 192.168.1.249 — depuis RT_Dis_1 vers SW_Acc_1**
- ✓ **ping 192.168.2.249 — depuis RT_Dis_1 vers SW_Acc_2**
- ✓ **show vlan brief — vérifier la présence des VLANs 998 et 999**
- ✓ **show interfaces trunk — vérifier native vlan 999, VLANs autorisés et mode trunk**
- ✓ **show ip interface brief — vérifier que toutes les sous-interfaces sont UP/UP**

BONUS — Configuration SSH (optionnel)

■ **Pourquoi ?** Telnet transmet les mots de passe en clair sur le réseau — n'importe quelle capture Wireshark les révèle. SSH chiffre intégralement la session grâce à un échange de clés RSA. C'est la norme en production. Le VLAN 998 sera l'interface de gestion utilisée pour les connexions SSH.

Équipement	Commandes IOS

RT_Dis_1 / SW_Acc_1 / SW_Acc_2	`! Nom de domaine requis pour générer les clés RSA`
	`ip domain-name sn-tech.local`
	`! Génération des clés RSA 2048 bits (recommandé)`
	`crypto key generate rsa modulus 2048`
	`! Compte local pour l'authentification SSH`
	`username admin privilege 15 secret cisco`
	`! Lignes VTY : SSH uniquement, auth locale`
	`line vty 0 4`
	`transport input ssh`
	`login local`
	`exit`
	`! Forcer SSH version 2 (v1 est vulnérable)`
	`ip ssh version 2`

■■ Pour se connecter : ssh -l admin 192.168.1.249 (vers SW_Acc_1) ou ssh -l admin 192.168.2.249 (vers SW_Acc_2) depuis un PC du VLAN 998 ou via le routeur.