@MeOps20

Bonjour à tous, je me présente @MeOps20, étudiants en cyle DEC réseau et sécurité Informatique, et tutilaire « en cour » d'un CCNAv7 .
Durant mon parcours actuelles de formation j'ai fait le malheureux constat du manque de documentation récent « en Francais tout particulièrement », sur le partie des IT ayant a trait au monde des réseaux actuelles et plus particulièrement en ce qui concerne les ressources d'aide à l'assimilation des différents modules du CCNAv7, donc j'ai décidé de partager avec vous les résultats de mes recherches et les notes qui m'ont moi même aidé à assimiler plus facilement ces derniers (mais bon, ma documentation fût majoritairement en Anglaise mais je la traduirai en Francais pour vous) , je le fais sur un coup de tête donc ne soyez pas trop stricte avec moi les gars.

Pour touts imcompréhensions au quelques formes de requêtes supplémentaires, vous pouvez me contactez sur
linkedIn : launla Ferdlance
Tweeter : @MeOps20
Gmail : launlaferdlance2021@gmail.com
Sur ceux, Bonne lecture à vous

Chapitre 1 : Compréhension complète des Vlans et concepts liés

Sommaire :

@MeOps20 tous droits réservés

Introduction :

Qu’es ce que cette technologie appelé VLAN ?
A quoi ça sert ?
Et En quoi es ce important ?

Voici sûrement les questions que vous devez vous posez , et je m’efforcerai d’y répondre de façon clair et détaillé .

Pour bien comprendre l'importance et le rôle des VLANs, il est essentiel de saisir leur fonction dans l'organisation et la gestion d’un réseau informatique. Nous allons commencer par définir ce qu’est un VLAN et expliquer son utilité à travers l'exemple d’une entreprise.

Définition d’un VLAN et à quoi cela sert :

Un **VLAN** (Virtual Local Area Network) est une technologie permettant de créer plusieurs réseaux locaux virtuels au sein d’une même infrastructure physique. Cela permet de segmenter un réseau en plusieurs sous-réseaux logiques indépendants, même s’ils partagent le même matériel physique. Autrement dit, au lieu de relier tous les dispositifs d’un réseau à une même unité physique, le VLAN permet de créer des groupes logiques au sein de cette infrastructure commune.

Prenons l'exemple d'une entreprise :

Imaginons une **entreprise de taille moyenne**, avec différents départements comme la comptabilité, les ressources humaines et le marketing. Sans VLAN, tous ces départements seraient connectés au même réseau physique, ce qui pourrait rendre difficile la gestion des performances, de la sécurité et de l'administration du réseau. Tout le trafic de données transiterait par les mêmes équipements réseau, ce qui pourrait entraîner une surcharge, une faible performance et une plus grande vulnérabilité en termes de sécurité.

Grâce aux VLANs, chaque département (comptabilité, ressources humaines, marketing) peut être isolé en termes de réseau, même si tout le monde utilise le même matériel physique. Par exemple, le

@MeOps20 tous droits réservés

réseau de la comptabilité pourrait être isolé du réseau des ressources humaines, ce qui signifie que les employés du département comptabilité n'ont pas accès au réseau des ressources humaines et vice versa, à moins que cela ne soit explicitement permis.

En quoi les VLANs sont-ils importants ?

L'importance des VLANs réside dans leur capacité à améliorer la **sécurité**, la **performance** et la **gestion** du réseau. Voici quelques points clés :

1. **Sécurité améliorée** : En segmentant les réseaux, les VLANs permettent de limiter les risques de propagation de menaces entre les différents groupes d'utilisateurs. Par exemple, si un utilisateur du département marketing est infecté par un virus, il ne pourra pas facilement infecter le réseau de la comptabilité, car ces deux départements sont séparés en termes de VLAN.
2. **Gestion simplifiée** : La gestion des réseaux devient plus flexible. Par exemple, un administrateur réseau peut facilement ajouter de nouveaux employés à un VLAN spécifique ou changer un employé de département sans avoir à modifier toute l'infrastructure physique.
3. **Optimisation des performances** : En réduisant la taille des domaines de diffusion (broadcast domains), les VLANs réduisent la congestion sur le réseau, ce qui améliore la performance globale. Les dispositifs qui n'ont pas besoin d'échanger des données peuvent être isolés pour éviter des communications inutiles.

En résumé, un VLAN est un outil puissant qui permet de gérer efficacement les réseaux d'une entreprise, en améliorant la sécurité, la performance et la simplicité d'administration du réseau.

Mais ceci n'est pas son seul cas d'usage, maintenant, prenons le

*** Cas d'une PME cherchant à s'agrandir :**
Imaginons maintenant une **PME** en pleine phase de croissance, avec un petit nombre d'employés répartis dans plusieurs départements : finance, marketing, et développement produit. Cette entreprise commence à croître rapidement et souhaite permettre à ses employés de différents départements de travailler ensemble plus facilement, tout en conservant des réseaux logiques distincts pour chaque équipe, afin d'optimiser la sécurité et les performances du réseau.

Situation :

Dans ce contexte, l'entreprise a besoin d'une infrastructure réseau qui permette aux employés de travailler physiquement dans les mêmes espaces (par exemple, dans un open space) tout en ayant des **réseaux logiques séparés**. C'est là que les **VLANs** entrent en jeu. Bien qu'ils partagent la même infrastructure réseau physique (le câblage, les commutateurs), les employés peuvent être regroupés par **VLAN** en fonction de leur département ou de leurs besoins spécifiques.

Mise en place :

Par exemple :

@MeOps20 tous droits réservés

- Le département **marketing** travaille sur des campagnes de publicité et a besoin d'accéder à des données clients spécifiques, mais il ne doit pas interagir avec les données financières sensibles.
- Le département **finance** gère des informations comptables et des transactions bancaires, nécessitant une protection accrue contre les accès non autorisés.
- Le **développement produit** doit avoir un accès libre aux outils et aux serveurs de développement, mais ne doit pas avoir accès aux données sensibles du département marketing ou financier.

Les VLANs permettent à chaque département de disposer de son propre réseau logique, séparé des autres, tout en permettant à ces départements de collaborer physiquement dans le même espace de travail. Par exemple, grâce à des VLANs, un employé du marketing peut échanger des informations avec un collègue du développement produit sans interférer avec le réseau financier.

Bénéfices pour la PME en expansion :

1. **Collaboration simplifiée tout en préservant la sécurité** : Les VLANs permettent aux employés de travailler ensemble tout en garantissant que les informations sensibles restent protégées. Ils offrent ainsi une séparation logique des données sans entraver la collaboration.
2. **Scalabilité** : Lorsque l'entreprise grandit et de nouveaux départements ou équipes sont ajoutés, il est facile d'ajouter de nouveaux VLANs sans devoir repenser l'ensemble de l'infrastructure physique du réseau.
3. **Flexibilité dans la gestion des employés** : Si un employé change de département, son réseau logique peut être facilement modifié sans devoir déplacer des équipements physiques, rendant le processus de gestion plus fluide et plus rapide.

En résumé, les VLANs apportent à cette PME en expansion une solution efficace pour gérer un réseau qui reste flexible, sécurisé et évolutif, tout en permettant aux employés de collaborer de manière transparente et efficace.

Ceci est tout pour l'introduction, jusqu'ici j'espère ne pas encore vous avoir perdu, bon bon bon maintenant les bases assimilés et le flou légèrement dissipé, entamons avec la suite .

II Concepts liés

Lorsque vous entendrez « VLAN » vous entendrez également et à coup sûr même ces autres termes : VTP(Vlan Trunking Protocol), DTP (Dynamic Trunkin Protocole),

@MeOps20 tous droits réservés

Trunking, ROAS (Router-On-A-stick), routage-inter-vlan, switch-layer-3, vlan hopping etc.… , et ce sera avec raison car il s'agit tous de concepts important en réseau, non seulement en ce qui concerne le Chapitre sur les Vlans, le Module SRWE ou le CCNAv7 mais tout au long de votre carrière donc il est très important de chercher à les comprendre et à les assimiler dès maintenant donc dans cette partie, je m'efforcerai de vous expliquer ce que chacun de ces termes veulent dire et ce qu'ils impliquent concrètement.

A) Le trunking

Le trunking est une technique utilisée pour permettre le passage du trafic de plusieurs VLANs sur un seul lien physique entre deux équipements réseau (comme des **switches** ou des **routeurs**). Cela permet de ne pas multiplier les câbles entre les équipements et d'optimiser l'infrastructure réseau.

a) Lien trunk

Un lien trunk est un lien qui permet de transporter des trames provenant de plusieurs VLANs. Chaque trame qui traverse ce lien est étiquetée avec un identifiant VLAN (**VLAN ID**) afin que l'équipement récepteur sache de quel VLAN elle provient.

(Ca sonne complexe au début mais avec de la pratique et du temps, ceci vous paraîtra tellement simple)

b) Technologies de trunking

Il existe plusieurs protocoles et méthodes pour gérer le trunking :

- IEEE 802.1Q : C'est la méthode standard de balisage des trames VLAN dans Ethernet. 802.1Q insère une balise (tag) VLAN de 4 octets dans l'en-tête Ethernet pour identifier le VLAN.

- ISL (Inter-Switch Link) : Un protocole de Cisco, désormais obsolète, qui encapsule les trames Ethernet pour les transporter entre les équipements. Aujourd'hui, on utilise principalement 802.1Q.

c) Trunking Native Vlan

@MeOps20 tous droits réservés

Lorsque vous configurez un lien trunk, vous devez spécifier un VLAN natif. C’est un VLAN particulier qui n'est pas balisé lorsqu'il traverse le lien trunk. Le VLAN natif est utilisé pour transmettre du trafic qui ne fait pas partie de VLANs spécifiques (trafic sans tag VLAN). Par défaut, sur Cisco, le VLAN 1 est le VLAN natif.

Cependant, il est recommandé de changer le VLAN natif pour des raisons de sécurité, car laisser le VLAN natif sur 1 peut rendre le réseau vulnérable à des attaques comme VLAN hopping

Bon j’imagine que cette explication semble encore superflu, et vous donne une impréssion de « en quoi ceci est ce utile » car c’est moi même la question que je me suis posé donc voici quelques explications supplémentaires, pour que vous en compreniez le principe et le rôle

1. Définition :

Le VLAN natif est le VLAN auquel sont associés les trames non marquées sur un lien trunk (802.1Q). Lorsqu'une trame passe sur un lien trunk sans marquage (sans balise VLAN), elle est associée au VLAN natif.

2. Rôle du VLAN natif : Dans un réseau configuré avec des Vlans, Les trunks permettent à plusieurs VLANs de traverser un même lien entre deux commutateurs (ou entre un commutateur et un routeur), et les trames transmises sur un trunk sont généralement marquées (taguées) avec un identifiant VLAN (via le standard IEEE 802.1Q), et il peut arriver que sur ce liens passent des trames non marquées (géneralement celle transmises par des hubs, ou nées d’une ou plusieurs mauvaises configurations réseau) , et dans ce type de situation, elles (les trames non marquées) seraient tout simplement abandonées, donc n’arriveront jamais à destination, mais si un Vlan natif a étée préalablement défini, et si une trame non marquée traverse cette liaison, elle sera placée dans le VLAN natif par défaut sur le trunk.

- Par défaut, sur les commutateurs Cisco, le VLAN 1 est défini comme le VLAN natif, mais cela peut être modifié.

Vous comprenez donc son importance, et pour cette raison, on dois lui vouer une attention toute particulière et le sécurisé car il pourrai être la cible de ménace.

Le VLAN natif peut poser des risques de sécurité si mal configuré :

- Les attaques de saut de VLAN (VLAN hopping) peuvent exploiter des configurations inadéquates du VLAN natif. Une trame non marquée pourrait accidentellement traverser un trunk et aboutir dans un autre VLAN non désiré.

@MeOps20 tous droits réservés

- Il est recommandé de changer le VLAN natif par défaut (VLAN 1) à un autre VLAN non utilisé pour réduire les risques de sécurité.

4.Bonnes pratiques :

- Évitez d'utiliser le VLAN 1 comme VLAN natif.

- Changez le VLAN natif par défaut et configurez un VLAN natif spécifique sur vos trunks.

- Filtrez le VLAN natif si possible pour éviter les trames non marquées qui pourraient compromettre le réseau.

B) Le Routage inter-VLAN

Dans un réseau avec des VLANs, chaque VLAN agit comme un réseau local isolé. Pour permettre la communication entre les différents VLANs, on utilise le routage inter-VLAN. Cela nécessite un équipement réseau capable d'agir au niveau de la couch 3, notamment un routeur ou un switch de couche 3 (ou switch Layer 3(L3)) (ou multilayer switch) capable de faire du routage entre les VLANs.

Il existe trois méthodes principales pour configurer le routage inter-VLAN :

a) Router-on-a-stick

Dans cette méthode, un **routeur** est utilisé pour gérer le routage entre plusieurs VLANs, mais avec une connexion physique unique entre le routeur et un switch. Cette connexion est configurée en tant que **lien trunk**, permettant au routeur de recevoir et de transmettre le trafic de plusieurs VLANs sur une seule interface physique. Pour permettre le routage, le routeur utilise des **sous-interfaces** virtuelles, chacune associée à un VLAN spécifique. Chaque sous-interface est configurée avec une adresse IP servant de passerelle par défaut pour les périphériques du VLAN correspondant.

Fonctionnement :

- Le routeur distingue les VLANs grâce au marquage de trame (tagging) via le protocole **802.1Q**. Chaque trame est marquée avec un identifiant de VLAN lorsqu'elle traverse le lien trunk.
- Lorsqu'un périphérique d'un VLAN envoie un paquet destiné à un autre VLAN, le paquet est envoyé au routeur via le switch.

@MeOps20 tous droits réservés

- Le routeur effectue le routage entre les VLANs à l'aide de ses sous-interfaces, puis renvoie le paquet au switch, qui le livre au VLAN de destination.

Avantages :

1. **Économique** : Nécessite un seul routeur et un switch, ce qui en fait une solution accessible pour les petits réseaux ou réseaux avec un trafic limité.
2. **Simplicité** : Facile à configurer dans des réseaux simples avec un nombre réduit de VLANs.

Inconvénients :

1. **Goulot d'étranglement** : Tout le trafic inter-VLAN doit passer par une seule interface physique du routeur, ce qui limite les performances dans les environnements à fort trafic.
2. **Scalabilité limitée** : Peu adapté pour les réseaux de grande taille ou complexes, en raison de la surcharge sur l'unique lien trunk.

---

b) Switch de couche 3 (Layer 3 Switch)

Un **switch de couche 3** combine les fonctionnalités d'un switch traditionnel (couche 2) et d'un routeur (couche 3). Il est capable de **router le trafic entre les VLANs** directement en interne, sans nécessiter de routeur externe. Chaque VLAN est associé à une interface virtuelle sur le switch, et le routage se fait directement dans le matériel du switch, ce qui est beaucoup plus rapide que le routage traditionnel effectué par un routeur.

Fonctionnement :

- Le switch de couche 3 prend en charge le routage en utilisant des interfaces virtuelles (SVI) et des tables de routage intégrées.
- Lorsque le trafic inter-VLAN est nécessaire, il est routé directement au sein du switch, sans devoir passer par un périphérique externe.
- Ce routage interne est souvent appelé **routage matériel**, car il est géré par les circuits ASIC du switch, ce qui accélère considérablement le traitement des paquets.

Avantages :

1. **Haute performance** : Le routage est réalisé au niveau du matériel, ce qui réduit la latence et améliore la vitesse, même avec un trafic élevé.
2. **Scalabilité** : Idéal pour les grandes entreprises ou les environnements complexes avec de nombreux VLANs.
3. **Gestion centralisée** : Toutes les fonctions de commutation et de routage sont intégrées dans un seul équipement, simplifiant l'administration.

Inconvénients :

1. **Coût élevé** : Les switches de couche 3 sont généralement plus chers que les switches traditionnels et les routeurs basiques.
2. **Complexité accrue** : Leur configuration peut être plus technique et exigeante, notamment dans les environnements où plusieurs protocoles de routage sont utilisés.

@MeOps20 tous droits réservés

c) Routage inter-VLAN via SVI (Switch Virtual Interface)

Un **Switch Virtual Interface (SVI)** est une interface virtuelle configurée sur un switch (généralement de couche 3) pour fournir une interface logique au VLAN associé. Contrairement au Router-on-a-stick, où tout le trafic transite par un lien trunk unique, le routage inter-VLAN via SVI est réalisé directement au niveau du switch. Chaque VLAN dispose d'une SVI, qui agit comme une passerelle par défaut pour les périphériques appartenant à ce VLAN.

Fonctionnement :

- Chaque VLAN configuré sur le switch est associé à une SVI. Par exemple, si un réseau a trois VLANs (10, 20, 30), trois SVIs seront créées, chacune avec une adresse IP distincte.
- Les périphériques dans un VLAN envoient leur trafic à l'adresse IP de leur SVI, qui le route vers le VLAN de destination si nécessaire.
- Le routage est géré en interne par le switch, utilisant ses capacités de couche 3.

Avantages :

1. **Performance élevée** : Tout comme avec un switch de couche 3, le routage est réalisé en interne, ce qui réduit la latence.
2. **Administration simplifiée** : Permet de centraliser la configuration des VLANs et de leurs passerelles directement sur un seul équipement.
3. **Flexibilité** : Convient aux réseaux de taille moyenne à grande, nécessitant une gestion efficace de plusieurs VLANs.

Inconvénients :

1. **Coût** : Bien que moins cher qu'un switch de couche 3 complet, un switch prenant en charge les SVIs peut être plus onéreux qu'un switch basique.
2. **Dépendance au switch** : Si le switch devient un point de défaillance, tout le routage inter-VLAN est affecté.

Résumé :

Méthode	Performance	Coût	Scalabilité	Complexité
Router-on-a-stick	Moyenne	Bas	Faible	Faible
Switch de couche 3	Élevée	Élevé	Élevée	Moyenne
Routage via SVI	Élevée	Modéré à Élevé	Moyenne à Élevée	Moyenne

Chacune de ces méthodes s'adapte à des besoins spécifiques en termes de budget, de performance, et de complexité réseau.

Nous pratiquerons tout ceci par le biais de deux problématiques et topologies complètes et réel via simulation PT ou GNS3, pour que vous puissiez vous faire une idée.

@MeOps20 tous droits réservés

C) DTP (Dynamic Trunking Protocol)

DTP est un protocole propriétaire de Cisco utilisé pour négocier automatiquement la création d'un trunk VLAN entre deux commutateurs.

1. Fonctionnement de DTP :

- Lorsqu'une interface entre deux commutateurs est configurée pour négocier un trunk, DTP négocie le mode du lien (soit en mode trunk, soit en mode access).

- Il y a plusieurs modes DTP disponibles :

  - Dynamic Auto : L'interface attend que l'autre côté initie une négociation de trunk.

  - Dynamic Desirable : L'interface tente activement de former un trunk avec l'autre côté.

  - Trunk : Le port est forcé en mode trunk.

  - Access : Le port est forcé en mode access (ne supporte qu'un seul VLAN).

- Remarque : DTP ne fonctionne que sur les appareils Cisco ou compatibles avec ce protocole.

2. Sécurité et bonnes pratiques :

- Désactiver DTP sur les interfaces qui ne nécessitent pas de trunk pour éviter des trunkings non autorisés.

- Configurez les interfaces explicitement en mode trunk ou access et désactivez la négociation DTP pour sécuriser votre réseau.

3. Commandes importantes :

- Pour désactiver DTP sur une interface (la forçant en trunk sans DTP) :

```
switchport mode trunk
switchport nonegotiate
```

@MeOps20 tous droits réservés

D) VTP(Vlan Trunking Protocol)

Introduction

Le VTP (VLAN Trunking Protocol) est un protocole propriétaire de Cisco qui permet de gérer de manière centralisée les VLANs dans un réseau. Il simplifie l'administration des VLANs dans les réseaux étendus en synchronisant les informations de VLAN entre plusieurs switchs. Ce protocole fonctionne sur des liaisons trunk, permettant ainsi la propagation des informations de VLAN à travers les switches qui partagent un même domaine VTP.

---

1. Modes de fonctionnement de VTP

VTP offre plusieurs modes de fonctionnement pour gérer la propagation des VLANs. Chaque mode a des rôles et des comportements différents. Les trois principaux modes sont :

1. VTP Server (Serveur VTP) :

- C'est le mode par défaut sur un switch.

- Un switch configuré en mode serveur VTP peut créer, modifier et supprimer des VLANs.

- Il envoie des mises à jour aux autres switches du domaine VTP.

- Le switch serveur peut également recevoir des mises à jour, mais ne peut pas les apporter si des VLANs sont créés ou modifiés localement.

2. VTP Client (Client VTP) :

- Les switches configurés en mode client ne peuvent ni créer, ni modifier, ni supprimer des VLANs.

@MeOps20 tous droits réservés

- Ils reçoivent uniquement les mises à jour de VLAN provenant des serveurs VTP et appliquent ces modifications.

- Ils n’ont pas de base de données VLAN propre ; ils dépendent du serveur VTP pour la configuration des VLANs.

3. VTP Transparent (VTP Transparent) :

- Les switches configurés en mode transparent ne participent pas à la gestion des VLANs dans le domaine VTP.

- Ils ne reçoivent pas les informations de VLAN d'un serveur VTP, mais peuvent quand même ajouter, supprimer ou modifier des VLANs localement. Cependant, ces modifications ne sont pas propagées aux autres switches.

- Ce mode est utile lorsque vous ne voulez pas que certains switches affectent ou reçoivent des mises à jour de VLAN.

J’en suis certain, là, nombre d’entre vous doivent se demander pourquoi donc l’insérer dans notre domaine VTP , s’il ne **fou** strictement rien, donc nous prendrons un petit exemple simple pour que vous assimiliez la chose.

Vous venez d’apprendre les notions donc je parlerai dans cette exemple, donc ce sera un moyen pour vous d’en apprendre un peu plus.

Bon imaginez une domaine VTP constitué d’un Switch server chargé de gérer tout le domaine VTP, et de deux switch client auxquelles sont connectés les PCs hôtes, vous avez permi la communication entre les Vlan de même nature via ds configurations trunk car à ce moment là la société pour laquelle vous travaillez ne voulais pas de communications Inter_Vlan, mais voici que cet Société lance un projet de grande envergure et qu’il vous ai demnader de permettre la communication entre les départements concerné par ce projet, et que par chance, cette société dispose du Switch L3 dans le bâtiment et vous décidez de vous en servir donc, mais vous ne voulez pas qu’il soit affecté par les configurations VLAN du domaine mais il doit pourtant nécéssairement être inclus dans ce domaine pour pouvoir jouer le rôle qu vous attendez de lui, en mode server, ses configurations VLANs actuelles (même vierge) risquent pertuber le domaine, et en mode « client » il recevra des configurations VLAN dont il n’a pas besoin, voici donc oû entre en jeu le mode « transparent »…. J’espère vous avoir un peu plus éclairer à ce sujet

@MeOps20 tous droits réservés

4. VTP Off (Désactivé) :

- Ce mode désactive complètement VTP sur un switch. Il ne reçoit ni ne diffuse d’informations VTP, et ne participe pas à la gestion des VLANs.

- C’est un mode rarement utilisé, mais qui peut être appliqué dans des situations de sécurité où l’on veut empêcher toute propagation de VLAN.

---

2. Fonctionnement de VTP

- Domaines VTP : Un domaine VTP est un groupe de switches qui partagent la même information VTP. Ils échangent des informations de VLAN entre eux. Les switches appartenant à un même domaine VTP doivent utiliser le même mot de passe VTP, si défini.

- Mises à jour VTP : Les informations de VLAN sont envoyées sous forme de trames VTP qui contiennent l’ID de VLAN, son nom, et d'autres attributs. Les mises à jour sont envoyées périodiquement par les switches en mode serveur, mais un changement dans un VLAN (ajout, modification, ou suppression) entraîne une annonce VTP qui est transmise à tous les switches du domaine.

- Numéro de révision : Chaque fois qu'un changement est effectué, un numéro de révision VTP est incrémenté. Ce numéro est utilisé pour déterminer si une mise à jour doit être appliquée. Un numéro de révision plus élevé annule les anciennes informations.

- Trunking : VTP nécessite l’utilisation de liaisons trunk pour échanger les informations de VLAN entre les switches. Les trunks sont utilisés pour transporter plusieurs VLANs en utilisant des protocoles comme **IEEE 802.1Q**.

@MeOps20 tous droits réservés

3. Avantages de VTP

- Simplification de la gestion des VLANs : Permet de centraliser la gestion des VLANs, réduisant ainsi le besoin de configurer chaque switch individuellement.

- Mise à jour automatique : Lorsque de nouveaux VLANs sont ajoutés ou modifiés sur un switch serveur, tous les switches clients sont mis à jour automatiquement.

- Réduction des erreurs humaines : En réduisant le nombre de configurations manuelles sur chaque switch, on minimise le risque d'erreurs dans la configuration des VLANs.

---

4. Inconvénients de VTP

- Risque de propagation d'erreurs : Si une erreur est faite sur un switch serveur (comme la suppression accidentelle d’un VLAN), cette erreur sera automatiquement propagée à tous les switches du domaine.

- Sécurité : Si un switch mal configuré ou non sécurisé est ajouté au domaine VTP, il peut altérer la configuration des VLANs. Cela peut être contourné en utilisant des mots de passe VTP.

- Limitation de contrôle : En mode client, un switch n'a aucun contrôle sur la configuration des VLANs, ce qui peut ne pas être souhaitable dans certaines situations.

---

5. Commandes de configuration VTP

Voici les principales commandes pour configurer VTP sur un switch Cisco :

- VTP version : Cette commande permet de définir la version de VTP (1, 2 ou 3).
  ```

@MeOps20 tous droits réservés
  ```

```
Switch(config)# vtp version 2
```

- VTP mode : Cette commande configure le mode VTP (serveur, client, transparent).

```
Switch(config)# vtp mode server
```

- VTP domain : Cette commande définit le domaine VTP pour un switch.

```
Switch(config)# vtp domain MonDomaine
```

- VTP password : Cette commande configure un mot de passe pour sécuriser les communications VTP.

```
Switch(config)# vtp password MonMotDePasse
```

Le mot de passe VTP (VLAN Trunking Protocol) sert à sécuriser les communications VTP entre les commutateurs d'un même domaine VTP.

Rôle du mot de passe VTP

- Authentification des mises à jour(c’est-à-dire de quelconques modification au nivveau domaine, géneralement les modifications logiques VLAN faites par le serveur, ou des modifications physiques du domaine causées par l’ajout ou le retrait d’un swicth) VTP : Lorsqu'un commutateur envoie des mises à jour VTP à d'autres commutateurs du même domaine, le mot de passe VTP est utilisé pour authentifier la

@MeOps20 tous droits réservés

communication. Cela garantit que seules les mises à jour provenant de commutateurs autorisés (ayant le bon mot de passe) sont acceptées.

- Prévention des modifications non autorisées : Si un mot de passe est configuré, les commutateurs qui n’ont pas le même mot de passe ne peuvent ni envoyer ni recevoir de mises à jour VTP. Cela empêche un commutateur mal configuré ou malveillant de perturber le domaine VTP.

Contexte d'utilisation

1. VTP Domain : Tous les commutateurs dans le domaine VTP doivent avoir le même nom de domaine (ex. `MonDomaine`).

2. VTP Password : Tous les commutateurs doivent partager le même mot de passe pour s'assurer qu'ils échangent des mises à jour.

3. Modes VTP : Cette commande est pertinente pour les commutateurs configurés en **mode client** ou **mode serveur** (pas pour le mode transparent).

Commande VTP password

Exemple : Configuration d'un mot de passe

Switch(config)# vtp domain MonDomaine

Switch(config)# vtp password MonMotDePasse

Switch(config)# vtp mode server

```

Ce qui se passe :

- Le commutateur est configuré pour appartenir au domaine `MonDomaine`.

- Le mot de passe `MonMotDePasse` sécurise les mises à jour VTP.

- En mode serveur, le commutateur peut envoyer et recevoir des mises à jour avec les autres commutateurs du domaine ayant le même mot de passe.

@MeOps20 tous droits réservés
```

Bénéfices

1. Sécurité renforcée : Évite les mises à jour accidentelles ou malveillantes.

2. Cohérence des VLANs : Garantit que seuls les commutateurs autorisés peuvent gérer et synchroniser les informations VLAN.

Si vous avez d'autres questions sur VTP ou des exemples spécifiques, je suis là pour vous aider ! 😊

Nous en avons terminé avec la théorie, enfin, maintenant passons aux cas pratiques…

PRATIQUE :

CONTEXTE :

Imaginez une Entreprise dont les services sont : PAM (Programmation et Application Mobile) et RSI (Réseau et Sécurité Informatique), et vous êtes l'administrateur réseau chargé d'établir l'infrastructure réseau de cette dernière, vous devez :

*Identifier les différents départements et la structure que vous désirez mettre en place

*Établir un plan d'addréssage

*Identifier les besoins « matériels principalement pour ce contexte précis »

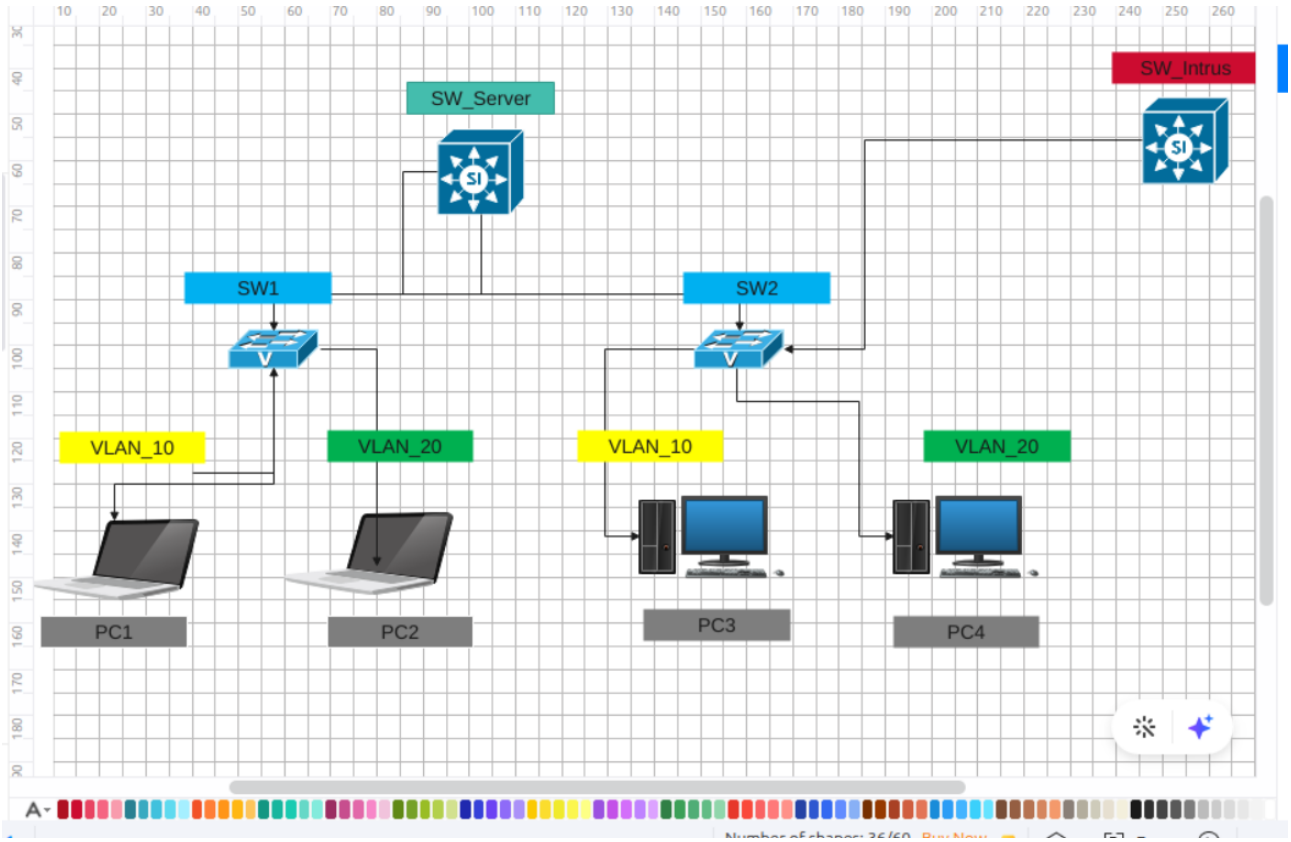
*Concevoir la topologie physique

*Vous munir du matériels adéquat

*Passer à l'action

@MeOps20 tous droits réservés

Pour cette exemple ci, nous dirons que nous venons de terminer l’étape de conception de la topologie physique et qu’il est temps de passer à l’action :



PS : Comme vous pouvez le constater Nous pousserons un peu loin en simulant l’infiltration du menace externe et comment s’en protéger.

Avant de commencer je tiens a préciser que l’émulation ne se que se rapprocher du réel, mais reste en sois incomplet, je dis ceci car lors de vos futurs test sur des équipements réels ou lors de simulations plus poussés, vous constaterez quelques différences au niveau des configurations (bien-sûr ceux qui continuerons avec moi aurons la possibilité d’expérimenter lors des futurs autres mini-manuels, des simulations plus poussées) .

Nous verrons des ici des configurations quelques configurations que vous aurez peut être déjà vu , sans en avoir réellement compris le rôle, ils feront également l’objet de prochain « mini-manuel »

@MeOps20 tous droits réservés

Commençons par les configurations de bases

Configuration de base des Switches

SW_Server

```
en                        # pour entrer en mode privilégié #
conf t                    # pour entrer en mode de configuration
globale #
hostname SW_server        # pour configurer le nom #
enable secret cisco       # pour configurer le mot de passe
privilégié #
line console 0            # pour entrer en mode de configuration
console #
password cisco            # pour définir le mot de passe d’accès
console, c’est celui que vous devrez entrer pour accéder à la
console de l’équipement #
login                     # pour que les configurations prennent
effet #
exit                      # pour sortir du mode actuel #
service password-encryption  # pour chiffrer les identifiants et
mots de passe #
ip domain name xxxx       # pour configurer le nom de domaine #
username xxx privilege 15 secret xxxx  # pour configurer vos
identifiants de connexion #
crypto key generate rsa 1024  # pour définir la clé de chiffrement
#
ip ssh version 2          # pour activer SSH version 2 #
```

SW_client1

```
en                        # pour entrer en mode privilégié #
conf t                    # pour entrer en mode de configuration
globale #
hostname SW1              # pour configurer le nom #
enable secret cisco       # pour configurer le mot de passe
privilégié #
line console 0            # pour entrer en mode de configuration
console #
password cisco            # pour définir le mot de passe d’accès
console, c’est celui que vous devrez entrer pour accéder à la
console de l’équipement #
login                     # pour que les configurations prennent
effet #
exit                      # pour sortir du mode actuel #
```

@MeOps20 tous droits réservés

```
service password-encryption  # pour chiffrer les identifiants et
mots de passe #
ip domain name xxxx      # pour configurer le nom de domaine #
username xxx privilege 15 secret xxxx  # pour configurer vos
identifiants de connexion #
crypto key generate rsa 1024  # pour définir la clé de chiffrement
#
ip ssh version 2         # pour activer SSH version 2 #
line vty 0 15            # pour configurer l'accès distant via les
lignes vty #
password cisco           # pour définir le mot de passe d’accès
distant #
login                    # pour activer la connexion via les
lignes vty #
end                      # pour sortir de la configuration
actuelle #
copy running-config startup-config  # pour sauvegarder la
configuration en cours #
show running-config      # pour visualiser les configurations
actives #
```

SW_client2

```
en                       # pour entrer en mode privilégié #
conf t                   # pour entrer en mode de configuration
globale #
hostname SW2             # pour configurer le nom #
enable secret cisco      # pour configurer le mot de passe
privilégié #
line console 0           # pour entrer en mode de configuration
console #
password cisco           # pour définir le mot de passe d’accès
console, c’est celui que vous devrez entrer pour accéder à la
console de l’équipement #
login                    # pour que les configurations prennent
effet #
exit                     # pour sortir du mode actuel #
service password-encryption  # pour chiffrer les identifiants et
mots de passe #
ip domain name xxxx      # pour configurer le nom de domaine #
username xxx privilege 15 secret xxxx  # pour configurer vos
identifiants de connexion #
crypto key generate rsa 1024  # pour définir la clé de chiffrement
#
ip ssh version 2         # pour activer SSH version 2 #
line vty 0 15            # pour configurer l'accès distant via les
lignes vty #
password cisco           # pour définir le mot de passe d’accès
distant #
login                    # pour activer la connexion via les
lignes vty #
```

@MeOps20 tous droits réservés

```
end                       # pour sortir de la configuration
actuelle #
copy running-config startup-config  # pour sauvegarder la
configuration en cours #
show running-config      # pour visualiser les configurations
actives #
```

SW_Intrus

```
en                        # pour entrer en mode privilégié #
conf t                    # pour entrer en mode de configuration
globale #
hostname Intrus           # pour configurer le nom #
enable secret cisco       # pour configurer le mot de passe
privilégié #
line console 0            # pour entrer en mode de configuration
console #
password cisco            # pour définir le mot de passe d’accès
console, c’est celui que vous devrez entrer pour accéder à la
console de l’équipement #
login                     # pour que les configurations prennent
effet #
exit                      # pour sortir du mode actuel #
service password-encryption  # pour chiffrer les identifiants et
mots de passe #
ip domain name xxxx       # pour configurer le nom de domaine #
username xxx privilege 15 secret xxxx  # pour configurer vos
identifiants de connexion #
crypto key generate rsa 1024  # pour définir la clé de chiffrement
#
ip ssh version 2          # pour activer SSH version 2 #
line vty 0 15             # pour configurer l'accès distant via les
lignes vty #
password cisco            # pour définir le mot de passe d’accès
distant #
login                     # pour activer la connexion via les
lignes vty #
end                       # pour sortir de la configuration
actuelle #
copy running-config startup-config  # pour sauvegarder la
configuration en cours #
show running-config      # pour visualiser les configurations
actives #
```

Infrastructure et Table d’Adressage

Une fois les configurations de base terminées, il est important d’examiner l'infrastructure virtuelle et la table d’adressage de votre réseau. Cela nous permettra

@MeOps20 tous droits réservés

de choisir la meilleure méthode pour réaliser le routage inter-VLAN, comme le **ROAS (Router on a Stick)** et le **Switch Layer 3**.

ROAS (Router on a Stick)

Le **Router on a Stick** est une méthode courante de routage inter-VLAN, où un seul routeur gère plusieurs VLANs. Ce type de configuration utilise une seule interface physique sur le routeur pour gérer plusieurs VLANs, grâce à l'utilisation du sous-routage (subinterfaces).

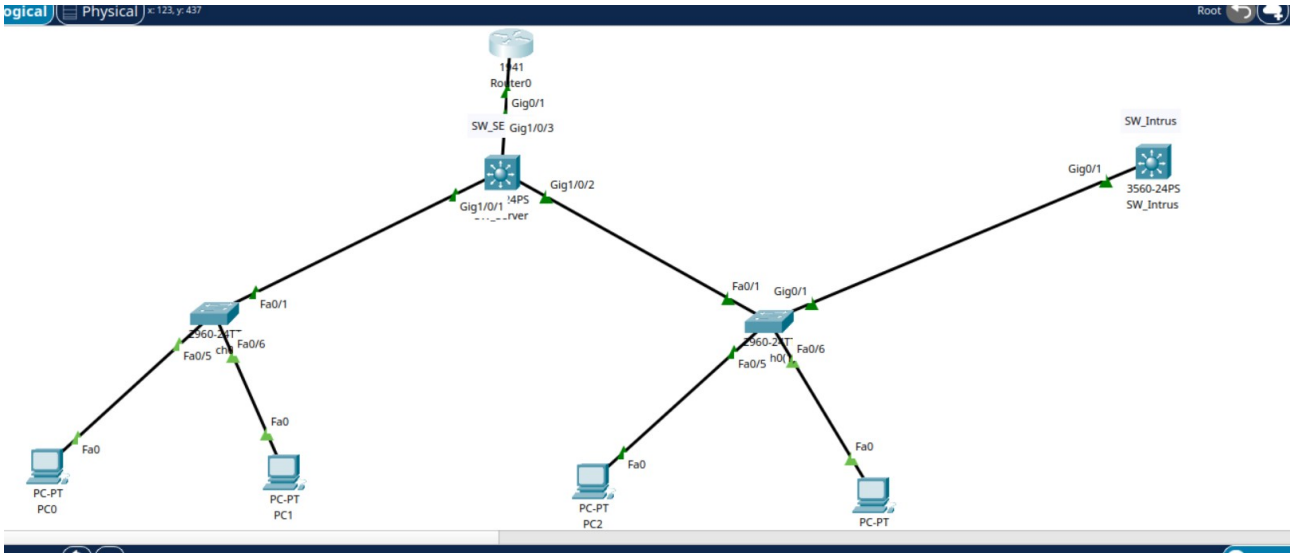
Nous allons maintenant approfondir cette méthode ainsi que la configuration de Switch Layer 3 dans les prochaines étapes.

Cela vous permet d'avoir une configuration de base complète avant de passer à des étapes plus avancées telles que la gestion du routage inter-VLAN.

Bon maintenant que nous en avons terminer avec ceci, examinons notre infrastructure virtuelle et notre table d'adressage

Je vais en profiter pour vous apprendre les deux méthodes de routage inter-Vlan les plus utilisés à savoir le ROAS (Router on a stick) et le Switch Layer 3

Nous commencerons par le ROAS :



@MeOps20 tous droits réservés

Table d’Adressage

Appareil	Interface	Adresse IP	Masque de Sous-Réseau	Passerelle par Défaut
R1	G0/0/1.1	192.168.1.1	255.255.255.0	N/A
R1	G0/0/1.2	192.168.2.1	255.255.255.0	N/A
PC-A	Carte réseau	192.168.1.10	255.255.255.0	192.168.1.1
PC-B	Carte réseau	192.168.2.10	255.255.255.0	192.168.2.1
PC-C	Carte réseau	192.168.1.11	255.255.255.0	192.168.1.1
PC-D	Carte réseau	192.168.2.11	255.255.255.0	192.168.2.1

Table de VLAN

VLAN	Nom	Interface Attribuée
10	RSI	S1 : F0/5, S2 : F0/6
20	PAM	S1 : F0/5, S2 : F0/6
10	Espion	SW_Intrus : Int VLAN 10
20	Intrus	SW_Intrus : Int VLAN 20

PS : Il est recommandé de toujours configurer des interfaces de gestions pour nos équipements Switch (L2 tout particulièrement), mais dans le cadre de cette démonstration, son omission sera volotaire et en rien un problème, mais notez qu’il s’agit d’une bonne pratique .

Configuration de Base

Sw_Server : Configurer le domaine VTP et les VLANs

```
en
conf t
vtp domain domain0
vtp password xxxx
vtp mode server # par défaut, tous les switches d’un
domaine VTP sont des serveurs #
vlan 10
name RSI
exit
vlan 20
name PAM
exit
end
```

@MeOps20 tous droits réservés

```
show vlan brief # Pour vérifier que nos configurations ont bien été prises en compte #
```

Maintenant configurons les liaisons trunk :

- Considérons `g0/1` comme la liaison trunk vers **SW_Client1** et `g0/2` comme la liaison trunk vers **SW_Client2**.

```
en
conf t
int range g0/1-2
switchport encapsulation dot1q  # Pour définir le protocole d’encapsulation. Cela n’est pas nécessaire pour les équipements virtuels, mais c’est une bonne pratique à connaître #
switchport mode trunk
switchport trunk allowed vlan 1,10,20
end
show ip int g0/1
show ip int g0/2
write memory
```

SW_Clients : Configurer le domaine VTP et le mode client

Sur chaque switch client, configurez simplement le domaine VTP, le mot de passe, et le mode client.

SW_Client1 :

```
en
conf t
vtp domain domain0
vtp password xxxx
vtp mode client
end
```

SW_Client2 :

```
en
conf t
vtp domain domain0
vtp password xxxx
vtp mode client
end
```

@MeOps20 tous droits réservés

SW_Intrus : Configurer le domaine VTP et les VLANs

```
en
conf t
vtp domain domain0
vtp password xyyx
vtp mode server # Par défaut, tous les switches d’un
domaine VTP sont des serveurs #
vlan 10
name Espion
exit
vlan 20
name Intrus
exit
end
show vlan brief # Pour vérifier que nos configurations
ont bien été prises en compte #
```

Configurer les liaisons trunk :

- Considérons `g0/1` comme la liaison trunk vers **SW_Client1**.

```
en
conf t
int g0/1
switchport encapsulation dot1q  # Pour définir le
protocole d’encapsulation. Cela n’est pas nécessaire pour
les équipements virtuels, mais c’est une bonne pratique à
connaître #
switchport mode trunk
switchport trunk allowed vlan 1,10,20
end
show ip int g0/1
write memory
```

Note Importante :

- Si nous avions configuré le **bon mot de passe VTP**, **SW1** aurait pris les nouvelles configurations VLANs de l’**Intrus**, et ce dernier aurait propagé cette mise à jour à tout le domaine VTP. **Imaginez l’ampleur des dégâts !**

@MeOps20 tous droits réservés

Routage Inter-VLAN avec ROAS

Pour des projets nécessitant la collaboration entre services, nous allons implémenter le **routage inter-VLAN**.

Configuration du routeur (R1)

```
en # pour entrer en mode privilégié #
conf t # pour entrer en mode de configuration globale #
hostname ROAS # pour configurer le nom #
enable secret cisco # pour configurer le mot de passe
privilégié #
line console 0 # pour entrer en mode de configuration
console #
password cisco # pour définir le mot de passe d’accès
console #
login # pour que les configurations prennent effet #
exit # pour sortir du mode actuel #
service password-encryption # pour chiffrer les
identifiants et mots de passe #
ip domain name xxxx # pour configurer le nom de domaine #
username admin privilege 15 secret xxxx # pour configurer
ses identifiants de connexion #
crypto key generate rsa
1024 # pour définir la clé de chiffrement #
ip ssh version 2
```

Configurer les sous-interfaces pour le routage inter-VLAN

```
en
conf t
int g0/1
no shutdown
int g0/1.1
encapsulation dot1q 10
ip address 192.168.1.1 255.255.255.0
no shutdown
int g0/1.2
encapsulation dot1q 20
ip address 192.168.2.1 255.255.255.0
exit
```

@MeOps20 tous droits réservés

```
ip routing
end
write memory
```

Bon maintenant essayons de voir a quoi ressemble la méthode usant du switch Layer 3

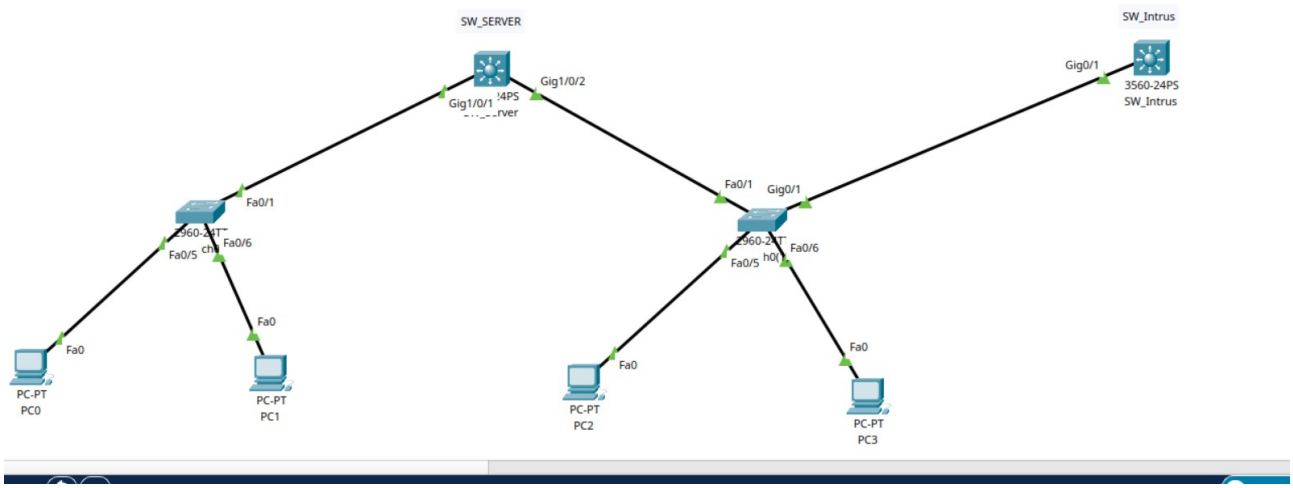


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
Sw_Server	VLAN 10	192.168.1.1	255.255.255.0	N/A
	VLAN 20	192.168.2.1	255.255.255.0	
Sw_Intrus	VLAN 10	192.168.1.1	255.255.255.0	N/A
	VLAN 20	192.168.2.1	255.255.255.0	
PC-A PC-B	Carte réseau	192.168.1.10 192.168.2.10	255.255.255.0 255.255.255.0	192.168.1.1 192.168.2.1
PC-C PC-D	Carte réseau	192.168.1.11 192168.2.11	255.255.255.0 255.255.255.0	192.168.1.1 192.168.2.1

Table de VLAN

VLAN	Nom	Interface attribuée
10	RSI	S1: F0/5 S2 : F0/6
20	PAM	S1: F0/5 S2 : F0/6
10	Espion	Sw_Intrus: Int vlan 10
20	Intrus	Sw_Intrus: Int vlan 20

@MeOps20 tous droits réservés

Comme vous l’aurez sûrement remarqué, j’ai fait exprès de configurer le Switch server et celui Intrus pareillement

Je ne reproduirai pas ces configurations en entier, notamment celles de bases et celles des vlans, nous nous concentrerons uniquement sur le routage inter vlan, pour ce cas de figure, nous considérons que le routeur en question ne sert que de connexion WAN distante, et avec les FAI et que le SWITCH SERVER est un SWICTH L3 et que c’est lui qui sert de liaison MAN entre les différents bâtiments de la société donc il sera celui qui sera utilisé pour le routage inter-VLAN….

Pour ce scénario, nous considérons que le routeur R1 est utilisé uniquement pour la connexion au WAN. Le routage inter-VLAN sera pris en charge par le **SW_Server**, qui est un switch de couche 3.

Configuration du SW_Server

```
en
conf t
int vlan 10 # Interface de gestion pour le VLAN 10 #
ip address 192.168.1.1 255.255.255.0
int vlan 20 # Interface de gestion pour le VLAN 20 #
ip address 192.168.2.1 255.255.255.0
ip routing
end
write memory
```

Validation et Tests

1. **Vérifiez les VLANs sur les switches clients :**

   ```
   show vlan brief
   ```

2. **Testez la connectivité entre VLANs :**

   - Depuis **PC-A** (192.168.1.10), testez la connectivité avec **PC-B** (192.168.2.10).

   ```
   ping 192.168.2.10
   ```

Avec cette configuration, vous avez appris à :

- **Segmenter un réseau avec des VLANs.**
- **Mettre en œuvre un routage inter-VLAN avec un routeur ou un switch L3.**
- **Tester la sécurité du domaine VTP et comprendre ses failles potentielles.**

Félicitations pour votre réalisation ! 🎉

@MeOps20 tous droits réservés

Sur ceux

@MeOps20
Nous voilà à la fin de ce mini-manuel, qui est aussi l’un de mes touts premiers ! J’espère sincèrement qu’il ne sera pas le dernier. 🙌

Pour toutes vos questions ou incompréhensions, retrouvez-moi sur mes réseaux sociaux :

- **Twitter** : @MeOps20, @DevOps2024
- **LinkedIn** : Launla Ferdlance

Je suis conscient que ce manuel n’a pas pu répondre à toutes vos interrogations. C’est pourquoi j’envisage de lancer une chaîne YouTube dédiée, où je partagerai des explications plus détaillées sous forme de présentations PowerPoint. Mais avant tout, mon objectif est de construire une communauté plus large.

Merci encore pour votre intérêt et beaucoup de courage dans vos différents parcours ! 🚀

Si d'autres ajustements sont nécessaires, n'hésitez pas ! 😊

@MeOps20 tous droits réservés

@MeOps20 tous droits réservés