ASSIZ

Documentation : Mise en place de l'infrastructure informatique nomade

1. Introduction

Cette documentation décrit la mise en place d’une infrastructure informatique, comprenant des réseaux séparés pour les organisateurs et les visiteurs. Elle comprend la configuration des VLANs, du NAT, du DHCP, du filtrage, ainsi que la gestion des points d’accès Wi-Fi.

---

2. Architecture de l'Infrastructure

L'infrastructure réseau est composée des éléments suivants :

- **Routeur ADSL** : Fournit l’accès à Internet.
- **Routeur MDL** : Gère les VLANs, le NAT, et le DHCP.
- **Commutateur réseau** : Gère la séparation des VLANs.
- **Points d'accès Wi-Fi** : Diffusent les SSID pour les visiteurs et les organisateurs.
- **Postes de travail** : Station d’accueil et poste d’organisation.

---

3. Configuration du Routeur MDL

3.1. Activation du NAT (Network Address Translation)

Le NAT est configuré pour permettre aux appareils des VLANs de sortir vers Internet.

```
# Activer le NAT
ip nat inside source list 1 interface Ethernet0 overload

# Créer une liste d'accès pour le NAT
access-list 1 permit 10.10.10.0 0.0.0.255   # Plage IP du VLAN "orga"
access-list 1 permit 172.31.1.0 0.0.0.255   # Plage IP du VLAN "public"

# Appliquer le NAT sur l'interface interne
interface Ethernet1
ip nat inside
exit
```

```
# Appliquer le NAT sur l'interface externe (connectée à Internet)
interface Ethernet0
ip nat outside
exit
```

3.2. Configuration du DHCP pour les VLANs

Définir des plages DHCP distinctes pour chaque VLAN.

```
# Configuration DHCP pour le VLAN 2 (Orga)
ip dhcp pool ORGA
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
dns-server 8.8.8.8
lease 0 2 0  # Durée de la location IP : 2 jours
exit

# Configuration DHCP pour le VLAN 3 (Public)
ip dhcp pool PUBLIC
network 172.31.1.0 255.255.255.0
default-router 172.31.1.1
dns-server 8.8.8.8
lease 0 2 0  # Durée de la location IP : 2 jours
exit
```

3.3. Filtrage des VLANs

Les VLANs doivent être séparés pour éviter toute communication non souhaitée. Voici la configuration du filtrage entre les VLANs.

```
# Créer une ACL pour bloquer la communication entre VLANs
access-list 100 deny ip 172.31.1.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 100 permit ip any any

# Appliquer l'ACL sur l'interface du routeur pour filtrer le trafic
interface Ethernet1
ip access-group 100 in
exit
```

3.4. Sécurisation du Routeur

```
# Configuration du mot de passe pour l'accès administrateur
enable secret <votre_mot_de_passe>

# Activation de l'accès SSH pour une gestion sécurisée
```

```
ip domain-name <nom_de_domaine>
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 4
transport input ssh
login local
exit
```

---

4. Configuration du Commutateur (Switch)

4.1. Création des VLANs

Les VLANs sont configurés sur le commutateur pour isoler les réseaux.

```
# Créer les VLANs
vlan 1
name Gestion
exit
vlan 2
name Orga
exit
vlan 3
name Public
exit
```

4.2. Assignation des Ports aux VLANs

Attribuer des ports spécifiques à chaque VLAN.

```
# Ports VLAN 1 (Gestion)
interface range fa0/1 - 2
switchport mode access
switchport access vlan 1
exit

# Ports VLAN 2 (Orga)
interface range fa0/3 - 10
switchport mode access
switchport access vlan 2
exit

# Ports VLAN 3 (Public)
interface range fa0/11 - 20
switchport mode access
```

```
switchport access vlan 3
exit
```

4.3. Configuration du Trunking

Les points d'accès Wi-Fi doivent être en mode trunk pour supporter plusieurs VLANs.

```
# Configuration du trunking pour les points d'accès
interface range fa0/21 - 22
switchport mode trunk
switchport trunk allowed vlan 2,3
exit
```

---

5. Configuration des Points d'Accès Wi-Fi

5.1. Création des SSID

Les SSID "public" et "orga" sont créés et sécurisés.

```
# SSID public
dot11 ssid public
authentication open
encryption mode ciphers aes-ccm
wpa-psk ascii <clé_wpa2_visiteur>
exit

# SSID orga
dot11 ssid orga
authentication open
encryption mode ciphers aes-ccm
wpa-psk ascii <clé_wpa2_orga>
exit
```

5.2. Associer les SSID aux VLANs

Associer chaque SSID à son VLAN respectif.

```
# Assigner le SSID "public" au VLAN 3
interface dot11radio 0
ssid public
vlan 3
exit

# Assigner le SSID "orga" au VLAN 2
```

```
interface dot11radio 1
ssid orga
vlan 2
exit
```

5.3. Isolement des Clients sur le Réseau Public

Les visiteurs ne doivent pas pouvoir communiquer entre eux sur le réseau Wi-Fi public.

```
# Activer l'isolement des clients sur le réseau public
client-isolation enable
```

---

6. Tests et Validation

6.1. Vérification de la Connectivité Internet

1. Connecter un appareil au SSID "Public" et vérifier qu'il peut accéder à Internet.
2. Connecter un appareil au SSID "Orga" et vérifier qu'il peut accéder à Internet, ainsi qu'aux ressources internes (imprimantes, afficheurs, etc.).

6.2. Test de Séparation des VLANs

1. Tenter de communiquer entre un appareil du VLAN 2 (Orga) et un appareil du VLAN 3 (Public). La communication doit être bloquée.
2. Vérifier que les appareils sur le réseau public ne peuvent pas se communiquer entre eux (test de l'isolement).

---

7. Conclusion

Une fois cette configuration terminée, vous aurez une infrastructure réseau robuste, sécurisée et bien segmentée, permettant aux organisateurs et aux visiteurs d'utiliser Internet tout en protégeant les ressources internes de l'événement. Assurez-vous de tester la configuration avant l'événement pour garantir une expérience fluide.

Notes supplémentaires

- Cette documentation est un guide pour configurer le réseau de l’événement. Les commandes doivent être adaptées aux spécifications de votre matériel (routeurs,

commutateurs, points d’accès).
- Assurez-vous que le firmware de vos équipements est à jour avant de procéder à la configuration.
