| **Équipement** | **Fonction** | **VLAN** | **IP attribuée** |
| --- | --- | --- | --- |
| PC1 | Poste de travail | VLAN 10 | 10.10.10.12 |
| PC2 | Poste de travail | VLAN 10 | 10.10.10.13 |
| PC3 | Poste de travail | VLAN 10 | 10.10.10.14 |
| PC4 | Poste de travail | VLAN 10 | 10.10.10.15 |
| PC5 | Poste de travail | VLAN 10 | 10.10.10.16 |
| Imprimante | Impression | VLAN 13 | 10.10.13.11 |
| Téléphone IP | VoIP | VLAN 12 | 10.10.12.10 |
| Point d'accès | AP Wi-Fi | VLAN 11 | 10.10.11.10 |
| Smartphone 1 | Wi-Fi | VLAN 11 | 10.10.11.20 |
| Smartphone 2 | Wi-Fi | VLAN 11 | 10.10.11.21 |
| Laptop | Wi-Fi | VLAN 11 | 10.10.11.30 |

Etage 1 :

| **Équipement** | **Fonction** | **VLAN** | **IP attribuée** |
| --- | --- | --- | --- |
| PC1 | Poste de travail | VLAN 20 | 10.10.20.12 |
| PC2 | Poste de travail | VLAN 20 | 10.10.20.13 |
| PC3 | Poste de travail | VLAN 20 | 10.10.20.14 |
| PC4 | Poste de travail | VLAN 20 | 10.10.20.15 |
| PC5 | Poste de travail | VLAN 20 | 10.10.20.16 |
| Imprimante | Impression | VLAN 23 | 10.10.23.10 |
| Téléphone IP | VoIP | VLAN 22 | 10.10.22.10 |
| Point d'accès | AP Wi-Fi | VLAN 21 | 10.10.21.10 |
| Laptop 1 | Wi-Fi | VLAN 21 | 10.10.21.20 |
| Laptop 2 | Wi-Fi | VLAN 21 | 10.10.21.21 |
| Laptop 3 | Wi-Fi | VLAN 21 | 10.10.21.22 |
| Serveur NAS Info | Stockage | VLAN 40 | 10.10.40.2 |
| Serveur NAS Accueil | Stockage | VLAN 40 | 10.10.40.3 |
| Serveur NAS Admin | Stockage | VLAN 40 | 10.10.40.4 |
| Serveur AD | Annuaire | VLAN 40 | 10.10.40.5 |

Etage 2 :

| **Équipement** | **Fonction** | **VLAN** | **IP attribuée** |
| --- | --- | --- | --- |
| PC1 | Poste de travail | VLAN 30 | 10.10.30.10 |
| PC2 | Poste de travail | VLAN 30 | 10.10.30.11 |
| PC3 | Poste de travail | VLAN 30 | 10.10.30.12 |
| PC4 | Poste de travail | VLAN 30 | 10.10.30.13 |
| PC5 | Poste de travail | VLAN 30 | 10.10.30.14 |
| Imprimante | Impression | VLAN 33 | 10.10.33.10 |
| Téléphone IP | VoIP | VLAN 32 | 10.10.32.10 |
| Point d'accès | AP Wi-Fi | VLAN 31 | 10.10.31.10 |
| Laptop 1 | Wi-Fi | VLAN 31 | 10.10.31.20 |
| Laptop 2 | Wi-Fi | VLAN 31 | 10.10.31.21 |
| Laptop 3 | Wi-Fi | VLAN 31 | 10.10.31.22 |

Config router pour dhcp :

***ip dhcp excluded-address 10.10.10.1 10.10.10.20***

***ip dhcp pool VLAN10\_PC\_RDC***

***network 10.10.10.0 255.255.255.0***

***default-router 10.10.10.1***

***dns-server 8.8.8.8***

***PS: Bien penser à mettre dhcp sur chaque pc (desktop>ip config> dhcp)***

Ensuite il faut créer les vlan sur chaque switch ex :

***vlan 10 vlan 11 vlan 12***

***name PC\_RDC name WIFI\_RDC name VOIP\_RDC***

La prochaine étape sera d’affecter un port à chaque vlan, exemple sur le switch de l’étage 1 :  
***int range fa0/4 - 8***

***switchport mode access***

***switchport access vlan 20***

***int fa0/10***

***switchport mode access***

***switchport access vlan 21***

***PS: Ne pas oublier de configurer les ports entre switch en mode trunk.***

Syslog + honeypot :

A screenshot of a computer

AI-generated content may be incorrect.

Je vais rajouter un switch qui sera lié au serveur ainsi que mon point d’accès pour wifi visiteurs. Afin de bien l’isoler du reste du réseau je le connecte directement au router.

Identifier les vlan sur tous les switchs

vlan 21

name VLAN\_WIFI1

vlan 20

name VLAN\_PC1

vlan 22

name VLAN\_VOIP1

vlan 23

name VLAN\_PRINT1

vlan 40

name VLAN\_SERVER

vlan 10

name VLAN\_RDC\_PC

vlan 11

name VLAN\_RDC\_WIFI

vlan 12

name VLAN\_RDC\_VOIP

vlan 13

name VLAN\_RDC\_PRINT

vlan 30

name VLAN\_PC2

vlan 31

name VLAN\_WIFI2

vlan 32

name VLAN\_VOIP2

vlan 33

name VLAN\_PRINT2

Pour configurer les VoIP, le router utilisé à a base n’étant pas compatible avec telephony-service.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Configurer CallManager Express (CME) :

***telephony-service***

***max-ephones 3***

***max-dn 3***

***ip source-address 192.168.10.1 port 2000***

configurer les VoIP :

***ephone-dn 1***

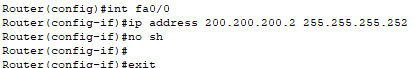
***number 1001***

***ephone 1***

***mac-address 001D.452D.50BD***

***button 1:1***

Configuration router fai :



Sur router entreprise :



Les 2 routers pourront se ping entre eux

Une image contenant texte, logiciel, Icône d’ordinateur, nombre

Le contenu généré par l’IA peut être incorrect.

J’ai une topologie bien riche en VLANs internes et une connexion entre mon RouterEntreprise (avec Gig0/1 en 200.200.200.1/30) et mon RouterFAI (Fa0/0 en 200.200.200.2/30). Je veux maintenant configurer le NAT sur mon RouterEntreprise pour masquer mes VLANs internes derrière cette IP publique (200.200.200.1) et simuler un accès Internet via mon RouterFAI.

**Etapes de configuration du NAT**

1. Marquer les interfaces inside et outside :

Une image contenant texte, capture d’écran, Police, document

Le contenu généré par l’IA peut être incorrect.

1. Créer une ACL qui couvre toutes les IP privées à masquer :

***access-list 1 permit 10.10.0.0 0.0.255.255***

1. Configurer NAT Overload (PAT) :

***ip nat inside source list 1 interface GigabitEthernet0/1 overload***

1. Configurer une route par défaut vers RouterEntreprise (200.200.200.1) :

***ip route 10.10.0.0 255.255.0.0 200.200.200.1***

En faisant un ping d’un pc du vlan 10 je vois :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

**Serveur dans un réseau privé derrière routeur FAI + NAT**

1. Configurer interfaces sur routeur FAI :

Une image contenant texte, Police, capture d’écran, reçu

Le contenu généré par l’IA peut être incorrect.

1. Configurer le serveur :

Une image contenant texte, capture d’écran, logiciel, nombre

Le contenu généré par l’IA peut être incorrect.

1. Configurer NAT sur routeur FAI :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Ces ACL définissent les plages d’adresses IP privées qui seront concernées par la traduction NAT.

***access-list 1 cible la plage 192.168.1.0/24***

***access-list 10 cible la plage 10.10.0.0/16***

Cela sert à filtrer précisément quelles adresses sont considérées “inside” (réseau interne à masquer) pour NAT.

***interface FastEthernet0/1***

***ip nat inside***

***interface FastEthernet0/0***

***ip nat outside***

Cette distinction est indispensable pour que le routeur sache dans quelle direction traduire les adresses IP.

***ip nat inside source list 1 interface FastEthernet0/0 overload***

Cette commande active le NAT dynamique avec surcharge (PAT), qui permet à plusieurs IP privées (définies par la liste 1) de partager une seule IP publique, ici l’IP de l’interface fa0/0. Overload signifie que le routeur utilise des ports différents pour distinguer chaque session, ce qui permet à plusieurs machines internes d’accéder simultanément à Internet via la même IP publique.

***ip nat inside source static tcp 192.168.1.2 80 200.200.200.2 80***

Cette règle fixe une traduction statique pour le trafic TCP sur le port 80 (HTTP) :

* Toute requête arrivant sur l’IP publique 200.200.200.2 sur le port 80 sera redirigée vers l’adresse privée 192.168.1.2 sur le port 80.
* Cela permet d’exposer un serveur web interne au réseau externe, tout en maintenant la sécurité du reste du réseau privé.

1. Configurer routage sur routeur entreprise :

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

La dernière commande permet d’ajouter route vers réseau serveur privé via routeur FAI.

1. Configurer routage sur routeur FAI :



Une image contenant texte, capture d’écran, logiciel, affichage

Le contenu généré par l’IA peut être incorrect.

**Configuration d’un tunnel GRE simple**

Je vais créer un tunnel GRE entre mon routeur entreprise et mon routeur FAI, comme si ce dernier était un autre site distant.

L’interface physique sera utilisée pour l’IP publique (par exemple : 200.200.200.1 / 200.200.200.2).

L’interface tunnel aura une adresse privée simulant le lien VPN.

Une fois le tunnel monté, je pourrai faire passer du trafic entre les réseaux internes via ce tunnel

1. Configuration du router Entreprise :

Une image contenant texte, capture d’écran, Police, document

Le contenu généré par l’IA peut être incorrect.

La dernière commande simule le site distant.

1. Configuration du router FAI :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

1. Points clés

10.10.100.0/30 → réseau du tunnel (virtuel)

10.10.0.0/16 → LAN entreprise (tous tes VLAN)

192.168.100.0/24 → LAN distant simulé derrière le FAI

En testant un ping d’un pc d’un vlan je retrouve bien l’ip du vlan distant simulé derrière le FAI.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

**Lier routeurVoice au RouteurEntreprise**

J’ai décidé de créer un lien point-à-point routé en /30 entre le Router Entreprise (RE) et le Router Voice (RV), sans VLAN trunk sur cette liaison, juste du routage simple.

| **Equipement** | **Interface** | **IP** | **Masque** |
| --- | --- | --- | --- |
| Router Entreprise | GigabitEthernet0/2 | 10.10.99.1 | 255.255.255.252 |
| Router Voice | FastEthernet0/1 | 10.10.99.2 | 255.255.255.252 |

Configuration sur RouteurEntreprise :

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

J’affecte l’adresse ***10.10.99.1*** à l’interface physique du router, avec un masque /30 qui crée un sous réseau avec 4 adresses ip (donc 2 utilisables). Ce qui est parfait pour une liaison point-à-point entre les 2 routeurs.  
Les commandes suivantes indiquent au routeur entreprise comment atteindre les réseaux 10.10.12.0/24, 10.10.22.0/24, et 10.10.32.0/24 en passant par la prochaine hop 10.10.99.2 — qui est l’adresse IP de l’interface du routeur voice côté liaison point-à-point. Sans ces routes statiques, le routeur entreprise ne saurait pas comment envoyer le trafic destiné à ces VLANs voice. Elles permettent donc la communication IP entre les VLANs voice et le reste du réseau via la liaison point-à-point.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Je fais pareil du côté du routeur Voice. En faisant un ping entre RE et RV, aucun ne répond.

Après plusieurs recherches, les interfaces réseau utilisent un mécanisme appelé auto-négociation pour s’accorder automatiquement sur la vitesse (ex : 10/100/1000 Mbps) et le mode duplex (half/full) du lien physique. Idéalement, ça marche bien, mais parfois :

* L’auto-négociation échoue.
* Cela provoque un protocole down (la liaison tombe).
* Ou un mismatch duplex (par exemple un côté en full duplex, l’autre en half duplex), ce qui génère des collisions, pertes de paquets, ralentissements.

A l’aide de ces 2 commandes, ces problèmes ont pu être résolu :

***speed 100 :*** fixe la vitesse de l’interface à 100 Mbps, sans laisser l’auto-négociation décider.

***duplex full :*** force le mode duplex à full, c’est-à-dire que la communication peut se faire simultanément dans les deux sens.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Le ping RV vers Re répond. Avec la commande ***show ip route*** sur RV :

Une image contenant texte, Police, capture d’écran, ligne

Le contenu généré par l’IA peut être incorrect.

* Le RouterVoice a bien la route vers son propre réseau voix 192.168.10.0/24 en local (connecté via FastEthernet0/0).
* Il a la sous-réseau point-à-point 10.10.99.0/30 connecté sur FastEthernet0/1, avec son adresse locale 10.10.99.2.
* Il a une route par défaut (0.0.0.0/0) pointant vers 10.10.99.1, ce qui est l’adresse du RouterEntreprise côté de la liaison point-à-point.

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Le ping RE vers RV répond. La commande ***show ip route*** sur RE montre :

Une image contenant texte, capture d’écran, Police, document

Le contenu généré par l’IA peut être incorrect.

Il y a une interface point-à-point sur 10.10.99.0/30 (donc vers 10.10.99.1 et 10.10.99.2). Mais il n'y a aucune route pour 192.168.10.0/24 dans la table de routage de RouterEntreprise.

Pour router du trafic vers 192.168.10.0/24 (réseau voix), RouterEntreprise doit savoir où envoyer les paquets. Actuellement, RouterEntreprise n'a pas de route statique ni dynamique pointant vers 192.168.10.0/24 via 10.10.99.2. Sans cette route, RouterEntreprise ne sait pas comment atteindre le réseau voix.

La solution la plus simple sera de rajouter statiquement cette route via la commande :

***ip route 192.168.10.0 255.255.255.0 10.10.99.2***

Après cette modification voici a quoi ressemble le show ip route sur RE :

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

**Configurer honeypot + acces wifi visiteurs et les isoler**

Je veux que le honeypot et l’accès Wi-Fi soient dans mon réseau (même infrastructure), mais isolés logiquement du reste pour éviter tout risque.  
Je peux le faire sans ajouter de port au routeur, en utilisant un VLAN dédié + ACL.

* Nouveau VLAN 50 → “Honeypot” (honeypot + AP + ses clients Wi-Fi)
* Le switch L2 est relié en trunk au switch du 1er étage
* Le routeur entreprise fait le routage inter-VLAN, mais ACL bloque toute communication du VLAN 50 vers les autres VLAN
* VLAN 50 n’a accès qu’à Internet (via le FAI)

Configuration du switch L2 :

Une image contenant texte, capture d’écran, Police, document

Le contenu généré par l’IA peut être incorrect.

Configuration du swicth 1 er étage :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Configuration du routeur Entreprise :

Une image contenant texte, capture d’écran, Police, ligne

Le contenu généré par l’IA peut être incorrect.

Configuration ACL pour isoler le honeypot :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Grace à cette ACL, le ***deny ip*** bloque tout accès du VLAN 50 vers les autres VLAN internes. Le ***permit ip*** autorise tout accès vers Internet.

En faisant un ping d’un laptop connecté au wifi visiteurs vers le router FAI:

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

En faisant un ping d’un laptop connecté au wifi visiteurs vers un PC du vlan 20:

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

**Configuration HSRP sur une nouvelle topologie**

Une image contenant texte, diagramme, ligne, carte

Le contenu généré par l’IA peut être incorrect.

Vlan 222 : PC 10/12/14

Vlan 223 : PC 11/13/15

Voir le rôle d’un distribution switch et d’un corps switch

DSW1

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

En donnant une adresse physique (172.22.0.100 et 172.23.0.100) et ne autre virtuelle (172.22.0.1 et 172.23.0.1) avec laquelle ils vont répondre avec HSRP. En augmentant la priorité de la gw du vlan 222, cette dernière sera prise en compte pour le HSRP.

DSW2 :

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

Pareil pour ce switch en donnant la priorité à la gw du vlan 223.

Bien penser à rajouter la commande « ip routing » sur les 2 DSW afin que ces derniers s’occupent du routage inter-vlan.