

MISSION MAQUETTAGE INFRASTRUCTURE

Préambule

L'objectif de cette maquette est de préparer la mise en place de l'infrastructure réelle que vous utiliserez pour l'épreuve E5 (E6 en 2025 probablement).

Le contexte est celui de l'entreprise CUB. Vous vous référerez au document exposant ce contexte pour plus d'informations, mais vous n'en avez pas strictement besoin pour ce maquetage. Il sera en revanche important pour la mise en œuvre du prototype.

Organisation par groupes

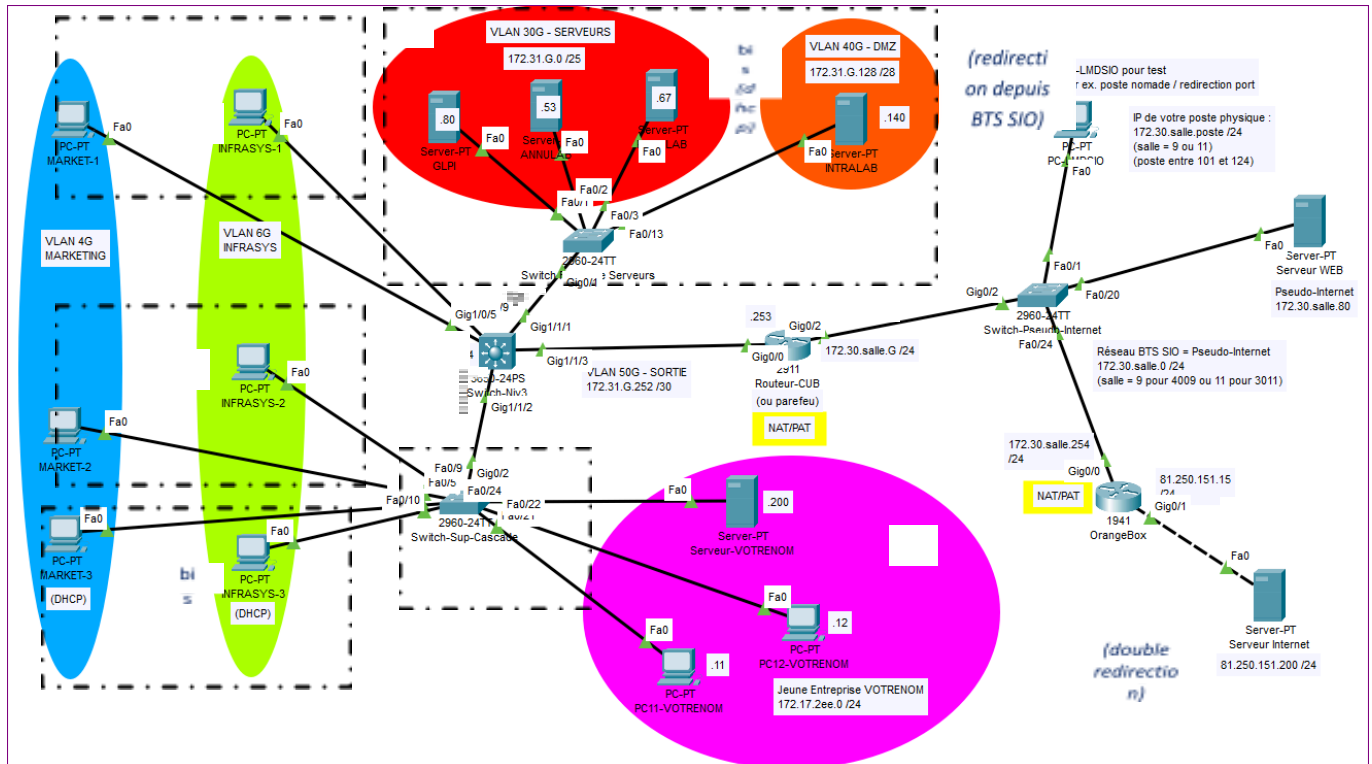
Vous fonctionnerez en PPE par groupe de 2 à 3 étudiants. Cette proposition de constitution des groupes est « aléatoire » et provisoire. Vous utiliserez le n° de groupe indiqué ci-dessous, de manière à ce que vos scripts et notamment vos n° de VLANs et de réseaux soient très proches de la mise en œuvre finale.

Groupe	Etudiant 1	Etudiant 2	Etudiant 3	Etudiant 4	Salle
1	MOTTAKI	EL QANNOUSSI	BEGOT	PIGNARD	3011 – Poteau 1
2	SAHLI	POMMIER	FALI		3011 – Poteau 2
3	RACHDI	FARDEHEB	COULIBALY	BENHAMIDOUCHE	3011 – Poteau 3
4	BLAIZE	BOUNINI GHOURABI	ABDALLA	SAINDOU	4009B - FEN
5	BENABDALLAH	KITTANNEH	SAMUEL		4009B - MUR
6	BESSAS	SID	RAHAIMI	GASSO	4009B - POT

NOTA BENE :

- Chaque fois que la lettre **G** apparaîtra dans la maquette et les explications, vous devrez la remplacer par votre n° de groupe.
- Chaque fois que la double lettre **ee** apparaîtra dans la maquette, vous les remplacerez par votre identifiant étudiant (de '01' à '17').

Maquette à mettre en place



Les pastilles jaunes vous proposent une progression cohérente en 10 étapes : inutile de faire une maquette dans laquelle rien ne fonctionne. Donc commencez par ex. par assurer le routage inter-2-vlan (❶&❷), puis ajouter un commutateur Ferme de Serveurs et un vlan (❸), etc ...

Ne passez à l'étape suivante que les précédentes fonctionnent !

Vous allez utiliser pour la première fois un commutateur de niveau 3 : modèle **3750** en réalité, modèle **3650** sur Packet Tracer.

Les principales spécificités / nouveautés sont les suivantes :

- Pour activer le routage sur un commutateur de niveau 3, la commande est la même que sur un routeur. Attention, contrairement aux routeurs, cette commande n'est pas active par défaut :
`Switch-Niv3(config)#ip routing`
- Les adresses IP qui serviront de passerelle aux postes seront définies au niveau des interfaces vlans.
- On peut définir un agent-relais DHCP au niveau d'une interface vlan, comme pour une interface physique (ou sous-interface) de routeur.
- Pour les ports TRUNK d'un commutateur 3750 ou 3560, il faut définir le type d'encapsulation, car plusieurs protocoles d'encapsulation sont théoriquement possibles, pas seulement DOT1Q :

Exemple

```
interface range Gi1/1/1 - 2
sw trunk encapsulation dot1q
sw mode trunk
```

Il faut définir des interfaces svi (switching virtual interfaces) associées à chaque vlan que l'on veut router. Les adresses IP qui leur sont affectées, serviront d'adresse de passerelle pour les postes associés à chaque VLAN.

Exemple

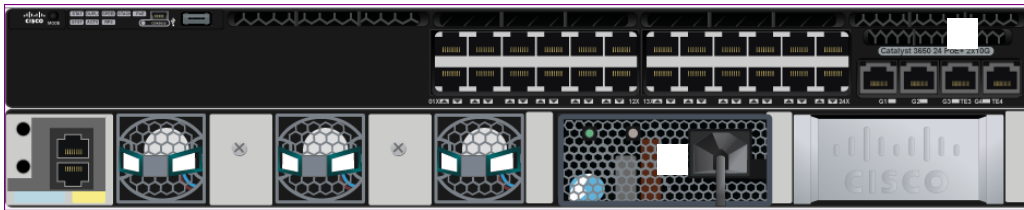
```
interface vlan 69
ip address 192.168.69.254 255.255.255.0
no shutdown
```

Attention ! Ne définir ces interfaces que sur le commutateur de niveau 3 !

Equipements à mettre en place

EQUIPEMENTS ACTIFS

- Un commutateur niveau 3 :
 - **Dans la réalité**, ce sera un commutateur **3750**
 - **Sous Packet Tracer**, ce sera un commutateur **3650 24PS**



- Il faut ajouter un module d'alimentation (AC-POWER-SUPPLY) ❶
- Il faut également ajouter 4 modules GLC-T ❷ qui seront utilisable en Gig1/1/1-4

Respecter l'affectation des ports ci-dessous

Ports Gig1/0/1 à Gig1/0/2	VLAN 1G : DIR-G
Ports Gig1/0/3 à Gig1/0/4	VLAN 3G : COMMU-G
Ports Gig1/0/5 à Gig1/0/6	VLAN 4G : MARKET-G
Ports Gig1/0/7 à Gig1/0/8	VLAN 5G : RDEV-G
Ports Gig1/0/9 à Gig1/0/10	VLAN 6G : INFRASYS-G
Ports Gig1/0/11 à Gig1/0/12	VLAN 9G : MANAGEMENT-G
Ports Gig1/0/13 à Gig1/0/16	VLAN 30G : Serveurs-G
Ports Gig1/0/17 à Gig1/0/18	VLAN 40G : DMZ-G
Ports Gig1/0/19 à Gig1/0/20	VLAN 1 (vlan par défaut)
Ports Gig1/0/21 à Gig1/0/24	VLAN 2EE : JE-2EE (=vlan étudiant)
Ports Gi1/1/1 et Gi1/1/2	TRUNK
Ports Gi1/1/3	VLAN 50G : EXIT-G

- Un 1^{er} commutateur niveau 2 (2960) représentant le commutateur virtuel dans la ferme de serveurs
 - Situé (géographiquement) **au-dessus** du commutateur de niveau 3
 - Cascadé sur le port Gi0/1 depuis le port Gi1/1/1 commutateur niveau 3
 - Desservant uniquement les vlans DMZ & Serveurs, ainsi que les vlans « JE » (= vlans étudiants)

Respecter l'affectation des ports ci-dessous

Ports 1 à 12	VLAN 30G : Serveurs
Ports 13 à 18	VLAN 40G : DMZ
Ports 19 à 24	VLAN 2EE : JE-2EE (=vlan étudiant)
Gi0/1 & Gi0/2	TRUNK

- Un 2^{ème} commutateur niveau 2 (2960) correspondant à une extension du réseau
 - Situé (géographiquement) **au-dessous** du commutateur de niveau 3
 - Cascadé sur le port Gi0/2 depuis le port Gi1/1/2 commutateur niveau 3
 - Desservant les mêmes vlans que le commutateur de niveau 3, même affectation des ports (sauf pour le vlan 50G, non pertinent sur ce commutateur – laisser le vlan par défaut)

- un routeur vers pseudo-internet (réseau BTS SIO en fait)
 - Fonctionnalité Nat/Pat activée
 - Règles de filtrage éventuelles pour n'autoriser que certains services ou que certains protocoles
 - Adresse IP côté interne : 172.31.G.253 /30 (EXIT / SORTIE)
 - Adresse IP côté réseau BTS SIO : 172.30.9.G /24 (4009B) ou 172.30.11.G /24 (3011)
- un commutateur représentant le pseudo-internet (réseau BTS SIO en fait)
- le routeur ORANGE vers le « vrai » INTERNET
 - Fonctionnalité Nat/Pat activée
 - Adresse interne (réseau BTS SIO) : 172.30.salle.254
(dans la réalité, c'est un peu plus compliqué que cela, mais on simplifie par rapport à l'infra réelle)
 - Adresse publique : 81.250.151.15 /24

HÔTES INTERNES

- Trois postes dans chaque service, deux en adressage fixe et un en adressage DHCP
 - Un poste en adressage fixe connecté directement au commutateur niveau 3
 - Un poste en adressage fixe connecté au commutateur cascadié
 - Un poste en adressage DHCP connecté également au commutateur cascadié

Les VLANS présents sont donc les suivants :

- Au moins 2 VLANs utilisateur : MARKET (Marketing), INFRASYS (Infrastructure & Système)
- Les vlans SERVEURS et DMZ
- Un serveur par fonctionnalité (à compléter quand vous aurez choisi vos situations)

Nom serveur	Adresse IP	Fonction(s)	Commentaire
ANNULAB	172.31.G.53 /25	Active directory, DNS	
REZOLAB	172.31.G.67 /25	Serveur DHCP	
GLPI	172.16.G.80	Gestion de parc	
INTRALAB	172.31.G.140	Serveur HTTP	En DMZ

HÔTES EXTERNES

- Un poste sur le réseau du BTS SIO pour tester un accès client depuis le pseudo-internet
 - Permettre par exemple de tester la redirection de port sur le routeur de CUB vers la DMZ
- Un serveur WEB sur le réseau du BTS SIO pour tester un accès vers le pseudo-internet
 - Permettra de tester le bon fonctionnement du nat/pat sur le routeur CUB
 - Permettra de tester les règles de filtrage sortantes éventuelles
- Un serveur d'ORANGE pour tester la connexion vers le « vrai » internet
 - Permettra de tester le bon fonctionnement du double nat/pat en sortie,
 - voire de la double redirection en entrée

Plan d'adressage IP

(limité aux VLANs présents sur la maquette – cf. contexte pour les autres)

N° VLAN	Nom du service / vlan	Réseau	Commentaire
4G	MARKET-G	192.168.4G.0 /24	Pool-MARKET sur REZOLAB : Plage DHCP de .201 à .250 <i>Pour vérifier la maquette 2 postes en adressage fixe, un poste en adressage dynamique sur le commutateur cascade</i>
6G	INFRASYS-G	192.168.6G.0 /24	Pool-INFRASYS sur REZOLAB: Plage DHCP de .201 à .250 <i>Pour vérifier la maquette 2 postes en adressage fixe, un poste en adressage dynamique sur le commutateur cascade</i>
30G	SERVEURS-G	172.31.G.0 /25	Adressage fixe
40G	DMZ-G	172.31.G.128 /28	Adressage fixe
50G	EXIT-G	172.31.G.252 /30	.254 côté Switch niv.3, .253 côté routeur
9G	MANAGEMENT-G	192.168.9G.0 /24	Adressage fixe pour les commutateurs .254 pour sw. Niveau 3 .253 pour sw. Ferme .252 pour sw. Cascade
2ee	JE-VOTRENOM	172.17.2ee.0 /24	

TRAVAIL A FAIRE

Mettre en place la maquette complète.

Effectuer des tests dans le scénario 0 montrant la réussite des communications – **Attention de bien respecter l'ordre indiqué pour ces tests** :

- Depuis un poste du vlan MARKET vers un poste du vlan INFRASYS sur Switch niv. 3 et Switch cascade
 - 2 tests
- Depuis chaque vlan (MARKET-1 ou MARKET-2, INFRASYS-1 ou INFRASYS-2) vers les Serveurs et la DMZ
 - 4 tests
- Depuis chaque poste dynamique (MARKET-3, INFRASYS-3) vers un serveur de SERVEURS ou DMZ
 - 2 tests
- Depuis INFRASYS-1 vers PC LMDSIO
- Depuis MARKET-1 vers Serveur WEB
- Depuis INFRASYS-3, MARKET-3 vers Serveur INTERNET
 - 2 tests : 1 test en ICMP + 1 test en HTTP (Port TCP 80)

Pour les dernières étapes, cf. compléments sur page suivante

- Depuis PC LMDSIO, accès à INTRALAB (DMZ) grâce à la redirection de port
- Depuis PC11-VOTRENOM vers Serveur INTERNET en HTTP (Port TCP 80)
- Depuis serveur INTERNET, accéder à INTRALAB grâce à la double redirection de port
- Depuis INFRASYS-1, connexion en SSH sur SwitchN3 et Switch Cascade
 - 2 tests

Soit 17 tests au total, ni plus ni moins

Nous pourrions relancer les tests facilement. Vous enregistrerez votre maquette en vérifiant bien que les tests sont visibles. Un seul test réussi, aucun échec, dans l'ordre demandé. (Vous pouvez au besoin supprimer les tests du scénario pour en refaire un)

COMPLEMENTS POUR LES DERNIERES ETAPES

Redirections de ports

- Vous ferez une démonstration de redirection sur la DMZ :
 1. Depuis le poste du réseau SIO (port 80 sur port 80)
 2. Depuis le serveur Internet (avec port 10G80 sur port 80)

Nota bene : Les redirections se font :

1. Sur l'interface « pseudo-publique » de Routeur-CUB vers INTRANET
2. Sur l'interface publique de OrangeBox vers l'interface « pseudo-publique » de Routeur-CUB

Administration distante des actifs

- Mots de passe à utiliser pour l'administration des actifs :
 - Mot de passe pour l'accès console : cub_console
 - Mot de passe pour l'accès en mode privilégié : cub_exec
 - Utilisateur pour le ssh : **admincub** / cub_ssh

Mettre en place l'administration distante dans l'ordre suivant :

1. Sur le commutateur de niveau 3
2. Sur le commutateur cascade
3. Sur le routeur CUB
4. Sur le commutateur ferme de serveurs

Faire à minima 1 et 2 pour les tests.