

## MODULE 11 ET 12 CCNA1 : ADRESSAGE IPV4 ET IPV6

A partir de l'adresse 192.168.10.20/16, Segmenter le réseau en utilisant la méthode VLSM.

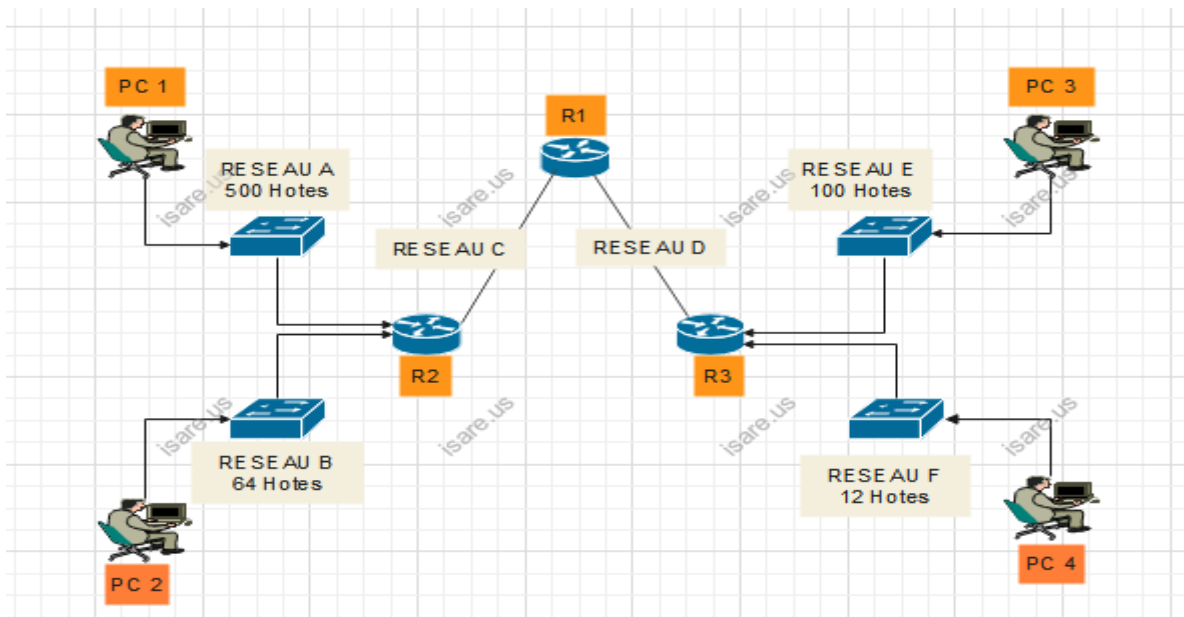
Utilisez l'adresse ipv6 2001 : DB8 : ACAD/64 pour adresser le réseau.

Pour le réseau F : utiliser la 10eme adresse d'hôte

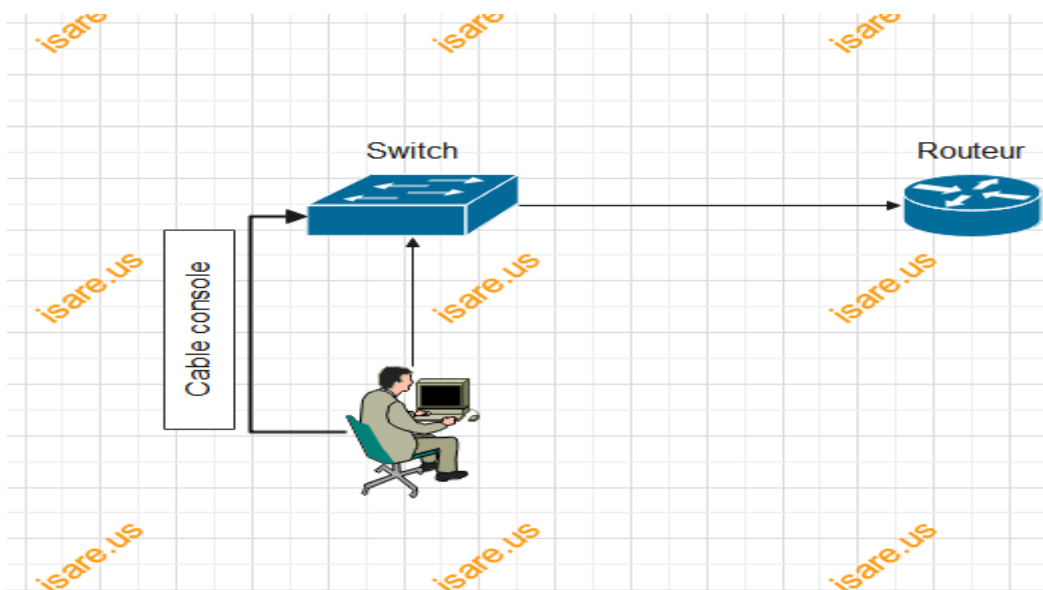
A : 2eme adresse

B : 2eme Adresse

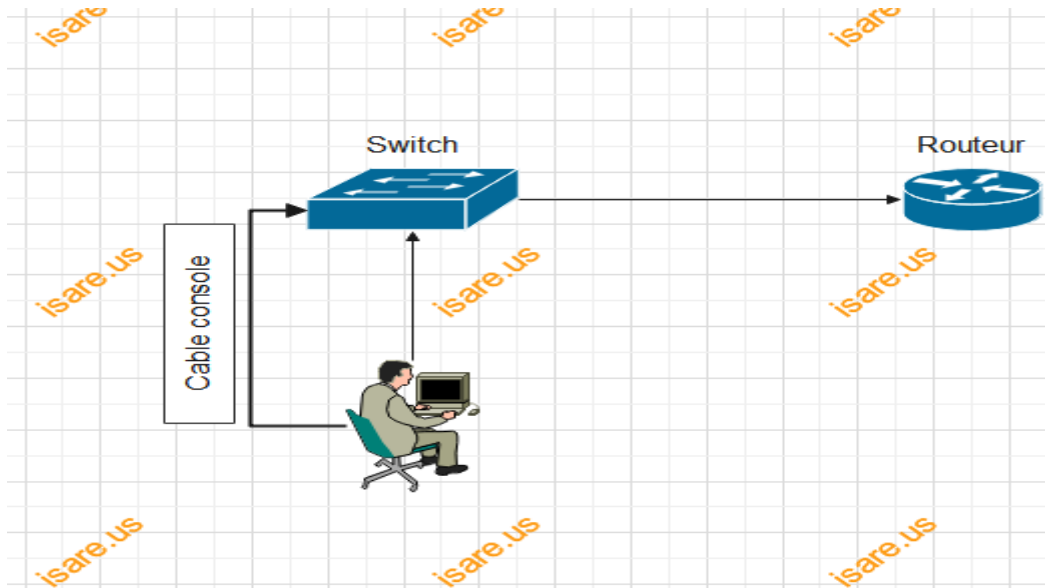
E : 1ere adresse



## SAUVEGARDE DE L'IOS D'UN PERIPHERIQUE CISCO VERS UN PC(SERVEUR) EN UTILISANT LE LOGICIEL TFTP/32/64

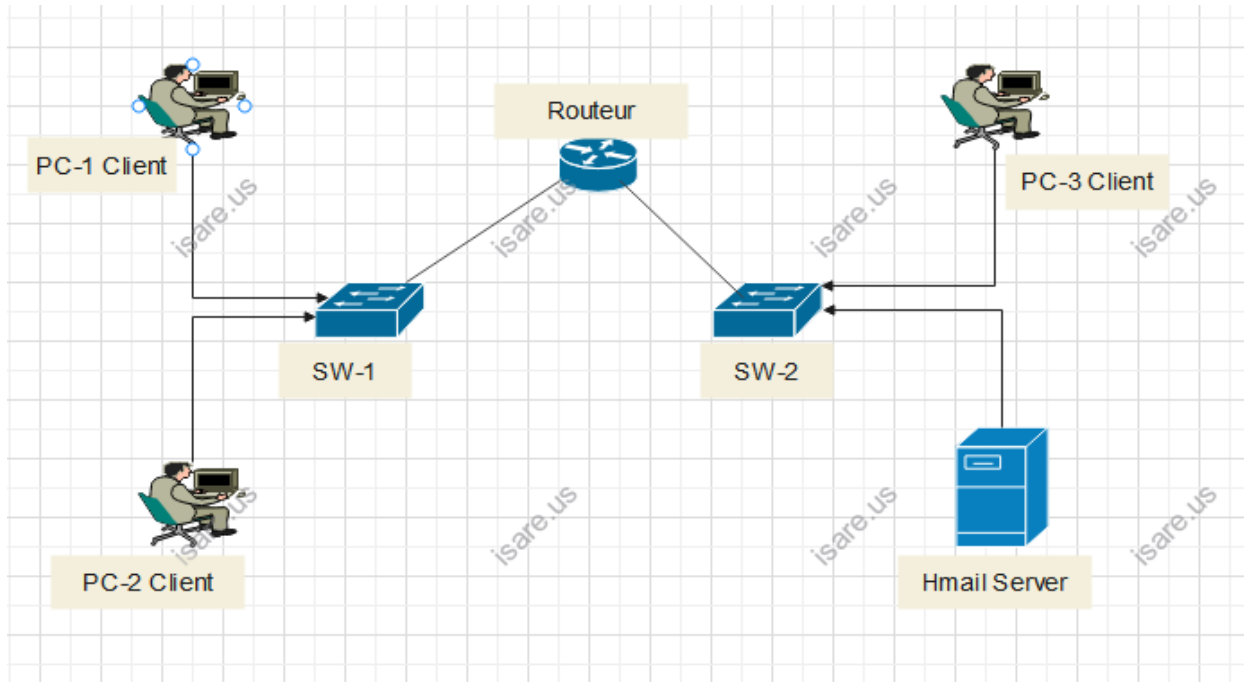


**SAUVEGARDE DE L'IOS D'UN PERIPHERIQUE CISCO DU PC DU VERS UN SERVEUR  
AVEC UN EMULATEUR DE TERMINAL : TERA TERM**



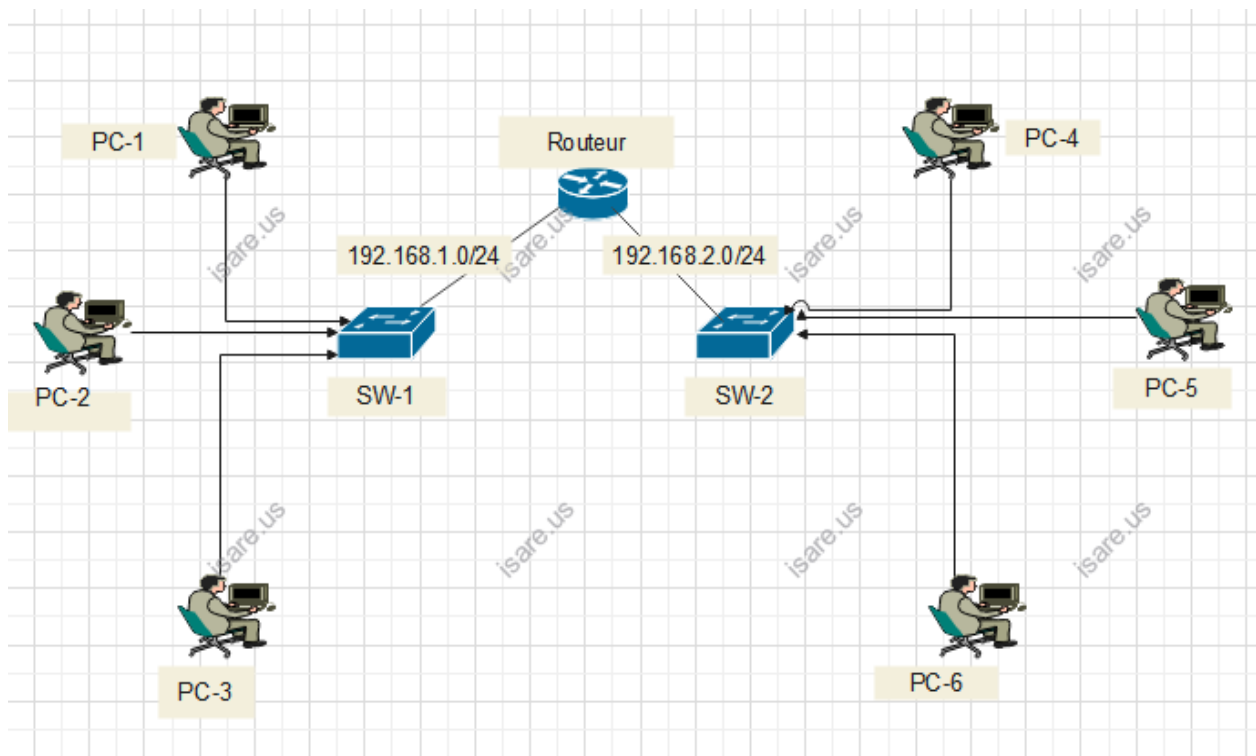
## MODULE 15 COUCHE APPLICATION

Mettre sur pied un serveur Mail utilisant POP avec un client utilisant la messagerie Outlook

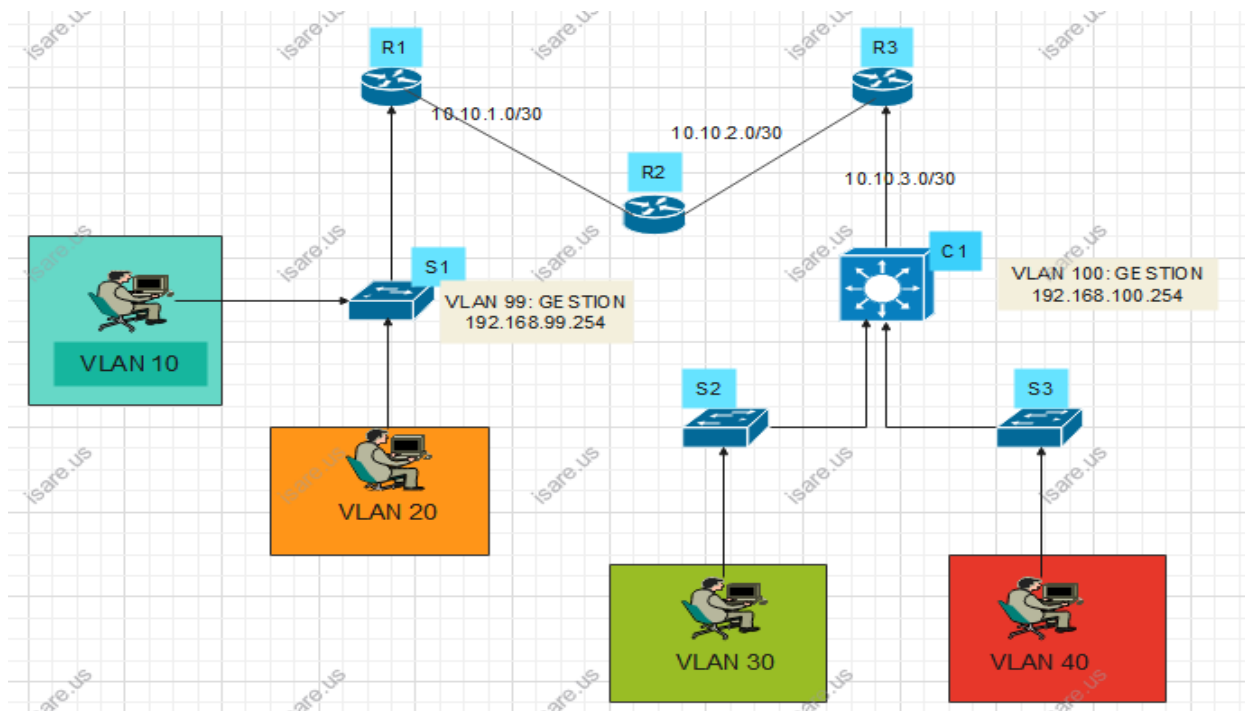


## MODULE 15 COUCHE APPLICATION : Utiliser les pare-feu Windows pour Bloquer des applications

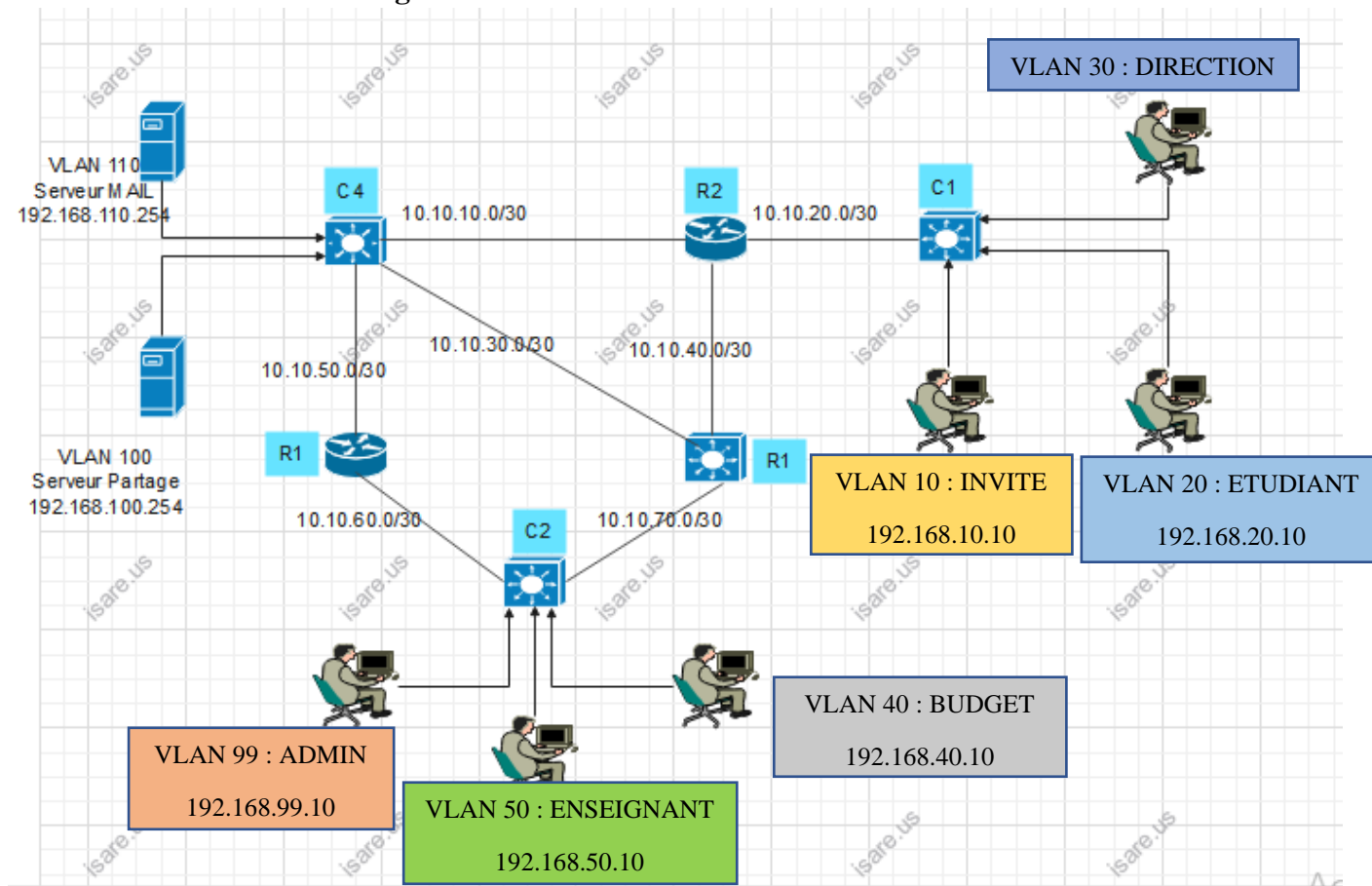
- 1- Configurer le réseau et le partage de fichier Mail
- 2- Utiliser une machine comme serveur de fichier et une autre comme serveur Mail
- 3- Bloquer l'accès à partir de l'adresse IP du client F d'accéder au serveur
- 4- Bloquer l'accès uniquement accès aux partages de fichiers du client F
- 5- Bloquer l'accès au client C d'accéder au serveur Mail seulement
- 6- Le client D n'aura ni accès aux services partages, ni aux serveur mail mais pourra effectuer des requêtes ping aux serveurs



## MODULE 3 CCNA2 : Configurer les VLANS



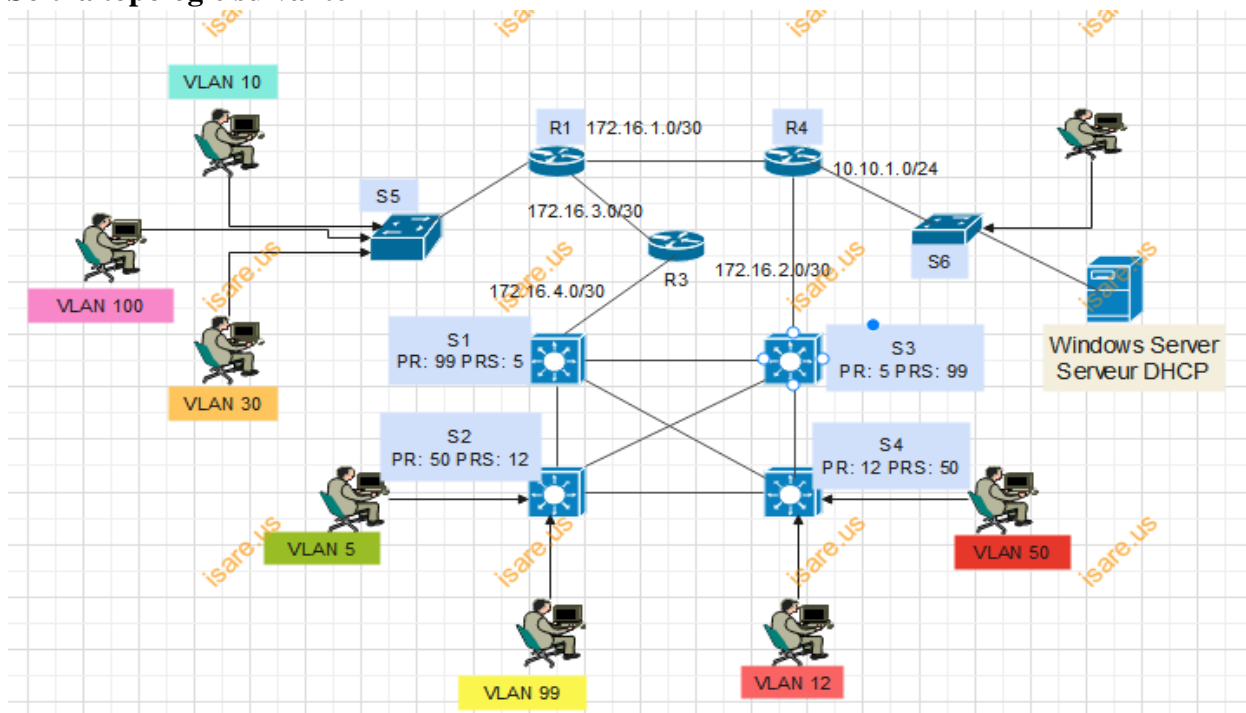
## MODULE 4 CCNA2 : Routage Inter VLAN



## ENSEMBLE DES TP CCNA 1,2,3

- 1- Configurer les noms d'hôtes conformément à la topologie
  - 2- Configurer les adresse IP des interfaces conformément a la topologie
  - 3- Configurer le Routeur R2 avec la méthode Router-on-a-stick
  - 4- Configurer le routage Inter Vlan avec le commutateur de couche 3
  - 5- Configurer une session distante SSH du vlan Admin sur le commutateur C2, Routeur R2 et R1.
  - 6- Configurer les comptes mail conformément aux VLAN. Rassurer vous que les échanges mails fonctionnent dans les différents VLAN.
- Bloquer le service Mail pour le vlan Invite et Etudiant
- 7- Configurer le partage pour l'ensemble de la topologie
  - 8- Bloquer le partage pour le vlan Invite et Etudiant
  - 9- Tester la redondance des liens en déconnectant un câble.

**MODULE 4,5,7 : Routage Inter vlan, DHCP, VTP, STP,  
Soit la topologie suivante**



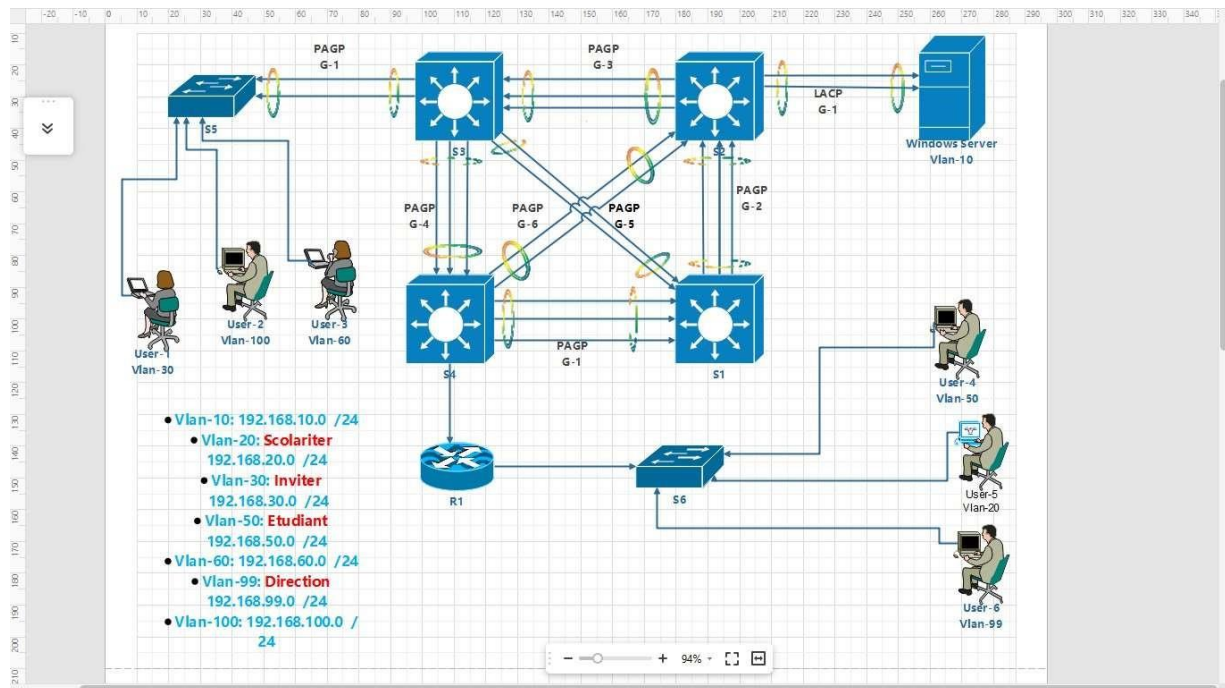
Configurer les noms d'hôtes conformément à la topologie

- 1- Configurer les paramètres d'adressage des interfaces ainsi que le routage
- 2- Définir R1 comme serveur DHCP pour les routeurs R4 et R3
- 3- Configurer linter vlan Router-on-a-stick sur R1
- 4- Configurer le DHCP pour chaque VLAN
- 5- Configurer le serveur DHCPV4 sous Windows server pour les sous réseaux du routeur R4
- 6- Définir S1 comme serveur VTP, le reste (S2, S3, S4) client  
Nom de Domain : isare.com  
Mot de passe : isare1234
- 7- Configurer l'inter vlan sur S2 et S4
- 8- Configurer le DHCP sur le commutateur S2 et S4
- 9- Configurer le trunk entre les liaisons de switch S2, S3, S4

Qui est le pont racine ?

- 10- Activer PVST+ sur l'ensemble du réseau commuté
- 11- Définir les ponts racines et pont racines secondaires pour chaque VLAN
- 12- Intégrez les machines du vlan 99 et 5 dans le domaine du server Windows
- 13- Définir les ports bloqués pour chaque VLAN du réseau commuté

## MODULE 6 : ETHERCHANNEL



- 1) Configurer les noms d'hôtes conformément à la topologie
- 2) Configurer les différents groupes etherchannel de la topologie précisément PAgP entre les commutateurs. Et LACP entre S2 et le serveur Windows
- 3) Préciser l'état des liens etherchannel de l'ensemble du réseau commuté
- 4) Quel est le pont racine de la topologie
- 5) Configurer rpvst+ sur l'ensemble du réseau commuté
- 6) Définir S2 comme pont racine de tous les vlans et S4 comme pont racine secondaire pour tt les vlans
- 7) Déterminer les liaisons etherchannel bloquées et les liaisons de transfert.
- 8) Définir S1 comme nouveau pont racine de l'ensemble du réseau commuté définissant la valeur a 4096, ensuite déterminer les liaisons etherchannel bloquées et les liaisons de transfert.
- 9) Déconnecter les liaisons entre S4 et S1 ainsi que S1 et S2, (S3, S1)
- 10) Déterminer le nouveau pont racine
- 11) Définir S2 comme serveur vtp (activer la version 2) sauf S6, déterminer le numéro de révision,



## ENSEMBLE DES TP CCNA 1,2,3

12) Configurer le routage inter-vlan router-on-stick sur le routeur R1

13) Configurer le serveur DHCP pour les différents vlans

14) Intégrer la machine du vlan 20 dans le domain

15) Paramétrer etherchannel sous Windows server

Configurer hmail server

16) Créer 4 dossiers

-dossier 1 : Direction

-dossier 2 : Etudiant

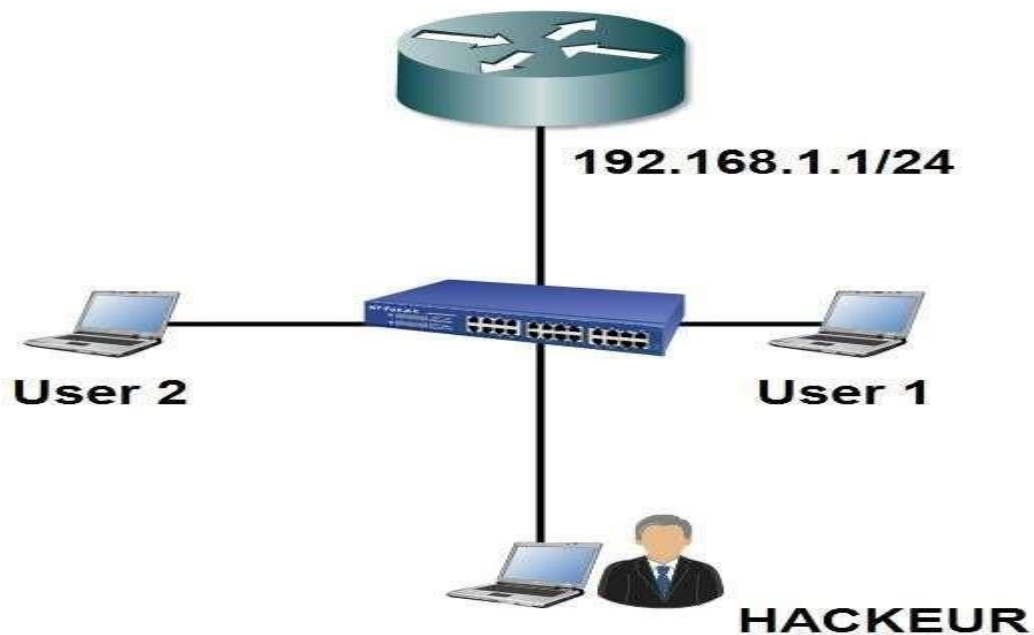
-dossier 3 : Scolarité

-dossier 4 : Invité

Configurer le partage sur Windows server

17) Restreindre l'accès uniquement aux personnes autorisées. Le dossier 1 ne doit pas être accessible aux personnes non autorisées.

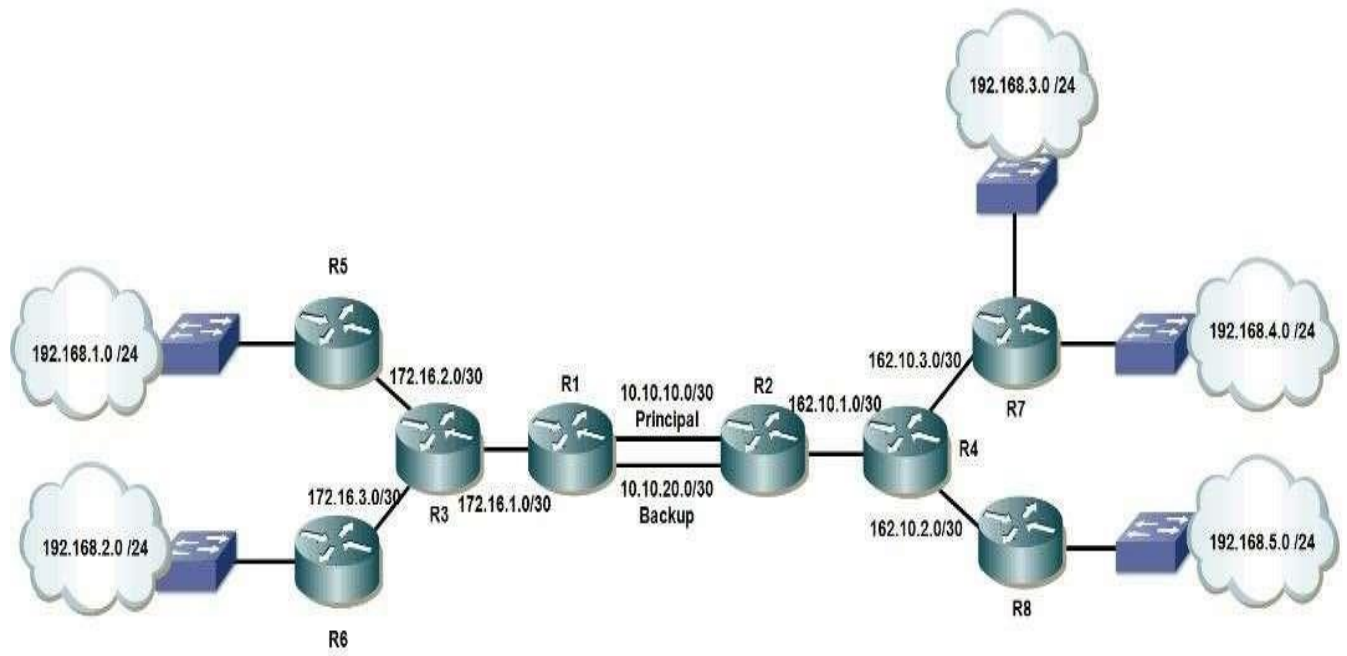
**MODULE 11 : CONFIGURATION DE LA SECURITE DU COMMUTATEUR**



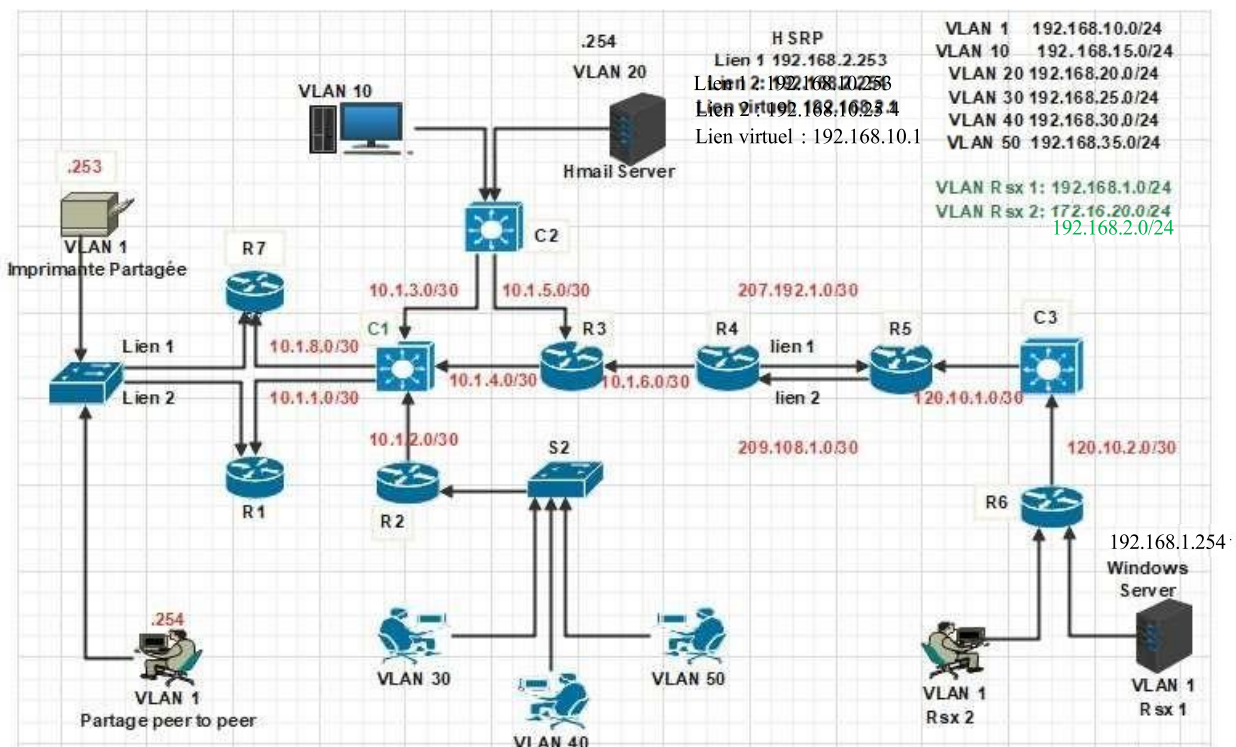
**TP : Sécuriser une attaque d'épuisement DHCP**

- 1) Configurez la topologie conformément au schéma
- 2) Configurez le DHCP sur le routeur avec la plage 192.168.1.0/24
- 3) Rassurez-vous que les utilisateurs légitimes accèdent aux ressources du réseau
- 4) Lancez kali linux sur la machine de l'hacker après avoir déconnecter du réseau les utilisateurs
- 5) Lancez l'outil Yersinia en mode graphique
- 6) Lancez une attaque d'épuisement de ressource DHCP
- 7) Analysez le comportement du réseau après avoir connecter les utilisateurs
- 8) Configurez un serveur DHCP sur la machine de l'hacker et analysez le comportement.
- 9) Sécurisez le réseau contre ce type d'attaque.

**MODULE 15 : ROUTAGE STATIQUE**



## TP GENERAL RESUME COURS 2

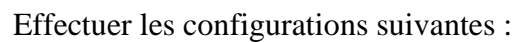


- 1- Configurer les noms d'hôtes conformément à la topologie
  - 2- Configurer l'accès à distance SSH pour les routeurs R4 et R5 pour deux utilisateurs simultanés
  - 3- Adresser les interfaces conformément à la topologie
  - 4- Configurer le protocole HSRP sur le routeur R1
  - 5- Dans le LAN du routeur R1, configurer PC1 pour le partage de fichier Peer to Peer et PC2 pour l'imprimante partagée
  - 6- Configurer le routeur R2 avec la méthode router-on-a-stick. Configurer le DHCP sur le routeur R2
  - 7- Pour chaque PC du réseau local de R2, configurer la sécurité des ports rémanents (sticky) et la sécurité DHCP.
  - 8- Configurer le routage inter vlan avec le commutateur de couche 3 C2
  - Configurer le DHCP sur le commutateur C2 et configurer SSH IPV6 pour ce commutateur.
  - 9- Configurer hmail server pour le vlan 20. Restreindre le service mail dans le vlan 10 et 50(les PC de ces VLAN pourront faire le ping vers le serveur mais pas avoir accès aux services de ce serveur).
- Configurer Filezilla avec la même restriction.

## ENSEMBLE DES TP CCNA 1,2,3

- 10- Configurer le routage statique pour l'ensemble du réseau
- 11- R4 et R5 sont considérés comme des routeurs d'extrémités, configurer de part et d'autre, une route statique récapitulative pour le lien principal et une autre flottante pour le lien redondant
- 12-configurer R4 en tant que serveur DHCP et R5 comme client DHCP pour les deux liens.  
Configurer une route statique d'hôte sur R4 pour atteindre le serveur Windows
- 13-configurer le service DHCP sur Windows de telle sorte que le PC du LAN2 puisse recevoir une adresse IP
- 14-Configurer le service AD dans le serveur Windows de telle sorte que tous les périphériques du réseau se connectent sur le domaine
- 15- Mettre sur pieds une procédure de récupération de mot de passe lorsqu'il est oublié, la récupération et la réinstallation de l'IOS.
- 16- Ajouter sur un PC un logiciel serveur DHCP qui attribuera les adresses aux périphériques de son réseau.

Soit la topologie réseau suivante :

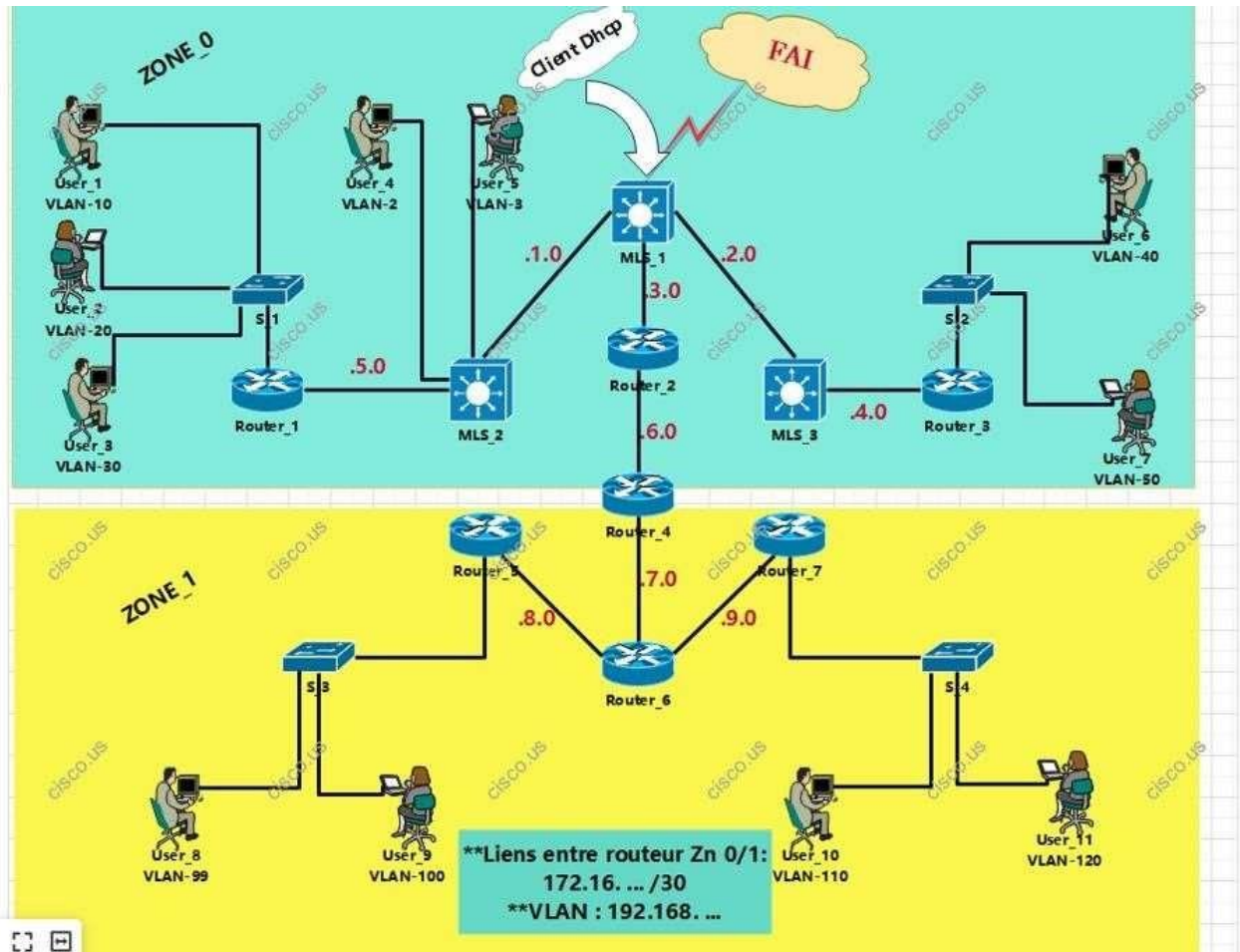


- ☐ Configurer les noms d'hôtes conformément a la topologie.
- ☐ Adresser l'ensemble des équipements conformément au consigne.
- ☐ Configurer les ID de routeur conformément aux nom (ex R1 :1.1.1.1)
- ☐ Configurer OSPF sur l'ensemble de la topologie tout en respectant les zones\*

## ENSEMBLE DES TP CCNA 1,2,3

- ☐ Définissez R5 comme routeur désigné de la zone 10 et R1 comme routeur désigné de la zone 0\*
- ☐ Définissez la priorité a 200 pour R5 et R1
- ☐ Configurer le routage inter vlan avec la méthode routeur onstick sur les routeurs R3 et R4 de la zone 0
- ☐ Configurer le routage inter-vlan avec les commutateurs de couche 3 C1 et C2 de la zone 0\*
- ☐ Configurer le DHCP sur l'ensemble des sous réseaux de la topologie (R8, R9, R3, R4, C1, C2) \*
- ☐ Configurer les interface Wan de R1 entant client DHCP
- ☐ Pour le lien principal utiliser la PAT avec adresse unique
- ☐ Les vlan 10, 20,30 ,60 et le Lan 1 seront autoriser pour la traduction NAT, et les vlan 40,50 ,65 ne seront pas autoriser. \*
- ☐ Configurer la liaison WAN.

## TP2 : SUR ACL, NAT, OSPF



- 1---configurez les noms d'hôtes conformément à la topologie (adressage, ...)
- 2---configurez OSPF a zone multiple tout en respectant les indications du schéma
- 3--configurez R4 comme routeur désigné de la zone 1 (process ID : 20) et C1 comme routeur désigné de la zone 0 (process ID : 10)
- 4--configurez la NAT avec la méthode PAT
- 5--uniquement les VLAN 50,2 et 3 n'auront pas accès à internet.
- 6--bloquez le trafic Https du VLAN 100 vers internet
- 7---bloquez le trafic réseau du VLAN 120 vers le VALN 20

(Utiliser la méthode qui consommera le moins de ressource du réseau)



## ENSEMBLE DES TP CCNA 1,2,3

8---configurez l'accès VTY sur l'ensemble des périphériques de la topologie et restreindre la communication uniquement pour le VLAN management (VLAN 99)

9---le VLAN 100 n'est pas autorisé à communiquer avec les vlan 40 et 50 10---isolez le VLAN 110 de l'ensemble des réseaux de la topologie.

11—Configurer le server SMB et bloquer le service SMB pour le Vlan-40