Projet Cisco

Documentation infrastructure réseau

Table des matières

[2 Introduction 2](#_Toc120171534)

[2.1 Contexte 2](#_Toc120171535)

[2.2 Contraintes 2](#_Toc120171536)

[2.3 Objectif document 2](#_Toc120171537)

[3 Matériel 3](#_Toc120171538)

[3.1 Présentation des composants 3](#_Toc120171539)

[3.2 Modifications 3](#_Toc120171540)

[3.3 Câbles 3](#_Toc120171541)

[3.4 Configurations initiales 4](#_Toc120171542)

[3.4.1 Configuration initiale des switches 4](#_Toc120171543)

[3.4.2 Configuration initiale des routeurs 4](#_Toc120171544)

[4 Architecture 5](#_Toc120171545)

[4.1 Agence 5](#_Toc120171546)

[4.2 FAI 5](#_Toc120171547)

[4.3 Siège social 6](#_Toc120171548)

[5 Adressage 7](#_Toc120171549)

[5.1 Tableau 7](#_Toc120171550)

[5.2 Règle d’adressage 7](#_Toc120171551)

[6 Vlans 8](#_Toc120171552)

[6.1 Explications 8](#_Toc120171553)

[6.2 Commandes 8](#_Toc120171554)

[6.2.1 VTP : 8](#_Toc120171555)

[6.2.2 Router DHCP 8](#_Toc120171556)

[7 Routage OSPF 9](#_Toc120171557)

[7.1 Agence 9](#_Toc120171558)

[7.2 FAI 9](#_Toc120171559)

[7.3 Siège social 9](#_Toc120171560)

[8 Liaison VPN IPSec 10](#_Toc120171561)

[9 Plan de sécurité 11](#_Toc120171562)

[9.1 Switch 11](#_Toc120171563)

[9.2 Router 11](#_Toc120171564)

[9.3 Commandes 11](#_Toc120171565)

# Introduction

## Contexte

Vous participez dans une équipe réseau/sécurité à la mise en place d’un réseau pour DevOpsSecurity. Vous devez concevoir ce réseau en IPv4 pour configuration des machines/hôtes et du routage OSPF avec proposition d’un plan de sécurité.

Ce réseau est constitué de quatre agences connectées à un routeur au siège de la société situé à Paris. Le siège de la société est connecté à son tour à un routeur de FAI par souci de centralisation.

Votre tâche consiste à créer un plan d’adressage afin d’accueillir le nombre d’hôtes requis et de proposer votre plan de sécurité pour l’infrastructure.

## Contraintes

* Réseau en IPv4
* Routage OSPF avec plan de sécurité
* 4 agences connectées via un routeur au siège de la société
* Une connexion du routeur du siège au routeur de FAI

## Objectif document

Ce document a pour objectif de présenter les différents aspects du projet et d’entrer dans le détail de certains éléments importants.

Dans ce document, nous présenterons également les différents composants permettant la mise en place de l'infrastructure réseau, dans cette situation, les différents appareils (switch, router…) ainsi que les câbles utilisés pour les connecter entre eux.

De plus, il y sera détaillé l’architecture du réseau, à savoir comment ceux-ci sont organisés au sein des différents LAN, les adresses IPv4 ainsi que les interfaces de connexion.

# Matériel

## Présentation des composants

 PC Fixe

Server

Router 2911

Switch 2960

## Modifications



Ajout du module HWIC-2T sur chaque routeur afin de les connecté entre eux via câble Serial DCE

## Câbles

Serial DCE

Ces câbles permettront de connecter les routeurs sur de longues distances.

Droits

Ces câbles serviront à connecter le reste des composant de l’infrastructure entre eux, exemple : PC - Switch – Router

 Croisé

Ces câbles seront utilisés pour les connexions switch à switch

## Configurations initiales

### Configuration initiale des switches

Switch(config)#interface range fastEthernet 0/1-24

Switch(config-if-range)#shutdown

Switch(config-if)#exit

Switch(config)#interface GigabitEthernipet0/2

Switch(config-if)#shutdown

### Configuration initiale des routeurs

Router(config)#interface gigabitEthernet 0/1

Router(config-if-range)#no shutdown

Router(config-if-range)#exit

Router(config)#interface serial 0/3/0

Router(config-if)#no shutdown

# Architecture

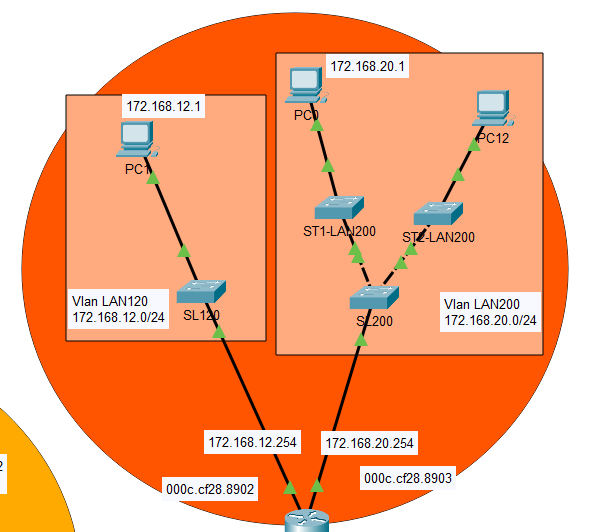
## Agence

Exemple avec l’agence 1 :

Les lans avec plus de 192 (8\*24 ports) machines connectées demande une multiplication des stacks de switch.

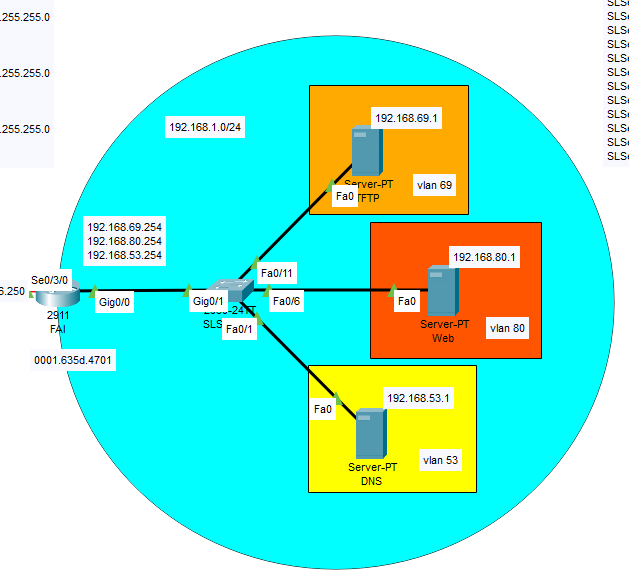
Idéalement le cœur de réseau (ici SL200) devrait être un 4500 afin de pouvoir relier tous les switch enfant par fibre et évité des lenteurs sur le réseau avec un grand nombre de machines connectées.

Pour le reste, un simple stack de switch suffit.

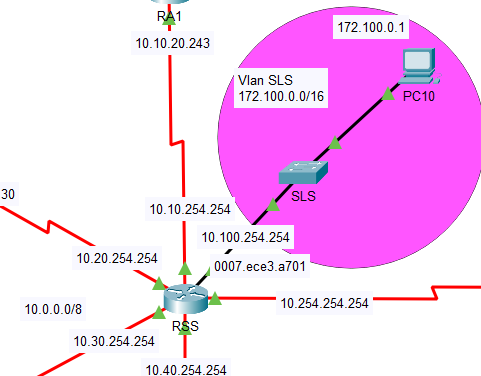


## FAI

Chaque type de service ce trouve dans une vlan et réseau différent.



## Siège social



# Adressage

## Tableau

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Routeurs** | **Lan (G0/0)** | **Lan (G0/1)** | **Lan (G0/2)** | **LAN RSS** |
| RA1 | Off | 172.168.12.0/24 | 172.168.20.0/24 | 10.10.0.0/16 |
| RA2 | Off | 172.1.0.0/16 | 172.2.0.0/16 | 10.20.0.0/16 |
| RA3 | Off | 172.168.8.0/24 | 172.168.80.0/24 | 10.30.0.0/16 |
| RA4 | Off | 172.168.3.0/24 | 172.168.6.0/24 | 10.40.0.0/16 |
| FAI | 192.168.53.254  192.168.80.254  192.168.69.254 | 192.168.1.0/24 | Off | 10.254.0.0/26 |

## Règle d’adressage

Afin de faciliter la compréhension et l’utilisation de l'infrastructure, certaines règles d’adressage ont été appliquées.

Côté LAN agence, chaque ip d’interface finie en .254.

Cette règle sera également appliquée pour réseaux connectant les agences.

Les PC quant à eux sont tous configurer via leur DHCP respectif configurer à partir de leur routeur.

# Vlans

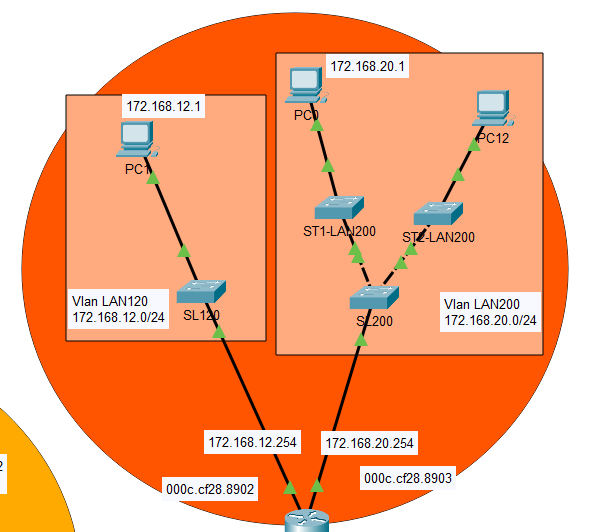
## Explications

Chaque LAN est composé d’au moins un vlan numéroté selon le nombre de machines demander.

Par exemple, le LAN pour 120 postes sera configuré en vlan 120.

Pour les réseaux demandant plus de 192 machines et donc qui requièrent un cœur de réseau, le cœur est configuré comme VTP server et les stack (ST1-ST2) en client.

Le routeur d’agence sert quant à lui de DHCP pour chaque vlan.



## Commandes

### VTP :

STX(config)#vtp domain LANXXX

STX(config)#vtp mode client

STX(config)#vtp password ESGI

### Router DHCP

RAX(config)#ip dhcp pool XXX

RAX(dhcp-config)#network 172.168.XXX.0 255.255.255.0

RAX(dhcp-config)#default-router 172.168.XXX.254

RAX(dhcp-config)#dns-server 192.168.53.1

# Routage OSPF

## Agence

FAI(config)#router ospf 10

FAI(config-router)#network 10.XX.254.254.0 0.0.255.255 area 0

FAI(config-router)#network 192.168.XX.0 0.255.255.255 area 0

FAI(config-router)#network 192.168.XX.0 0.255.255.255 area 0

## FAI

FAI(config)#router ospf 10

FAI(config-router)#network 10.254.254.0.0 0.0.255.255 area 0

FAI(config-router)#network 192.168.0.0 0.0.255.255 area 0

## Siège social

RSS(config)#router ospf 10

RSS(config-router)#network 10.10.0.0 0.0.255.255 area 0

RSS(config-router)#network 10.20.0.0 0.0.255.255 area 0

RSS(config-router)#network 10.30.0.0 0.0.255.255 area 0

RSS(config-router)#network 10.40.0.0 0.0.255.255 area 0

RSS(config-router)#network 10.254.0.0 0.0.255.255 area 0

# Liaison VPN IPSec

Activation de la license securityk9

license boot module c2900 technology-package securityk9

yes

do reload

yes

Configuration du VPN

no ip domain-lookup

crypto isakmp enable

crypto isakmp policy 10

encryption aes 256

authentication pre-share

hash sha

group 5

ex

crypto isakmp key ESGI address 10.XX.XX.XX

crypto ipsec transform-set VPN esp-aes 256 esp-sha-hmac

ip access-list extended VPNACL

permit ip 172.XX.XX.0 0.0.XX.255 172.XX.XX.0 0.0.XX.255

ex

crypto map VPNMAP 10 ipsec-isakmp

set peer 10.20.30.130

set transform-set VPN

match address VPNACL

ex

int s0/X/0

crypto map VPNMAP

ex

# Plan de sécurité

## Switch

* Interface non utiliser shutdown
* Mot de passe mode enable (ESGI)
* Ajout d’une bannière de prévention
* Filtrage vers le routeur par adresse mac et extinction en cas de mauvaise mac
* DHCP snooping

## Router

* Interface non utiliser shutdown
* Mot de passe mode enable (ESGI)
* Ajout d’une bannière de prévention

## Commandes

Ajout d’un mot de passe pour passer en enable – switch et routeur

XXXXX(config)#enable secret ESGI

XXXXX(config)#service password-encryption

Ajout d’une bannière au mode console – switch et routeur

XXXXX(config)#banner motd #

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

PROPERTY OF Quentin Hlion

Paris, France

USE OF THIS SYSTEM, AUTHORIZED OR UNAUTHORIZED,

CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE

MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE

COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL

OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO

MONITORING FOR THESE PURPOSE

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#

Filtrage de la connexion entre switch et router par mac adresse

XXXXX(config)#interface G0/1

XXXXX(config-if)#switchport mode access

XXXXX(config-if)#switchport port-security

XXXXX(config-if)#switchport port-security mac-address XXXX

XXXXX(config-if)#switchport port-security violation shutdown

XXXXX(config-if)#do wr

DHP Snooping – switch

Mise en place du DHCP snooping pour l’ensemble des switchs d’agences, check que le l’appareil connecté au switch est bien passé par le DHCP pour récupérer une IP

XXXXX(config)#ip dhcp snooping vlan XXX

XXXXX(config)#interface g0/1

XXXXX(config-if)#ip dhcp snooping trust

XXXXX(config)#interface range fastEthernet 0/1-24

XXXXX(config-if-range)#ip dhcp snooping limit rate 10