Projet Cisco

Documentation infrastructure réseau

Table des matières

[2 Introduction 2](#_Toc119518631)

[2.1 Contexte 2](#_Toc119518632)

[2.2 Contraintes 2](#_Toc119518633)

[2.3 Objectif document 2](#_Toc119518634)

[3 Matériel 3](#_Toc119518635)

[3.1 Présentation des composants 3](#_Toc119518636)

[3.2 Modifications 3](#_Toc119518637)

[3.3 Câbles 3](#_Toc119518638)

[3.4 Configurations initiales 4](#_Toc119518639)

[3.4.1 Configuration initiale des switches 4](#_Toc119518640)

[3.4.2 Configuration initiale des routeurs 4](#_Toc119518641)

[4 Architecture 5](#_Toc119518642)

[4.1 Agence 5](#_Toc119518643)

[4.2 FAI 6](#_Toc119518644)

[4.3 Siège social 6](#_Toc119518645)

[5 Adressage 7](#_Toc119518646)

[5.1 Tableau 7](#_Toc119518647)

[5.2 Règle d’adressage 7](#_Toc119518648)

[6 Routage 8](#_Toc119518649)

[6.1 Agence 8](#_Toc119518650)

[6.2 FAI 8](#_Toc119518651)

[6.3 Siège social 8](#_Toc119518652)

[7 Plan de sécurité 9](#_Toc119518653)

[7.1 Switch 9](#_Toc119518654)

[7.2 Router 9](#_Toc119518655)

[7.3 Commandes 9](#_Toc119518656)

# 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

## 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

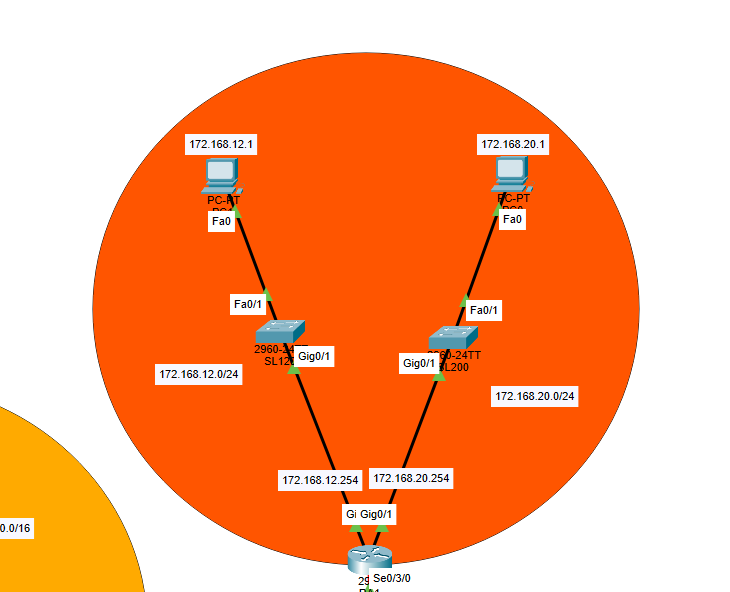
Router(config-if-range)#exit

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

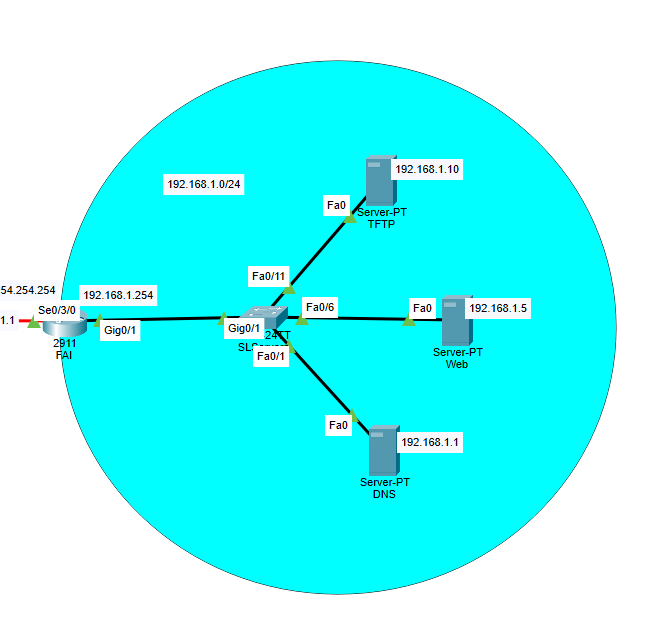
Router(config-if)#no shutdown

# Architecture

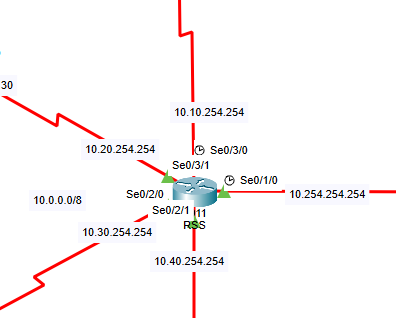
## Agence



## FAI



## 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.

Côté FAI, chaque type de serveur doit ce trouve sur un réseau différent des autres serveurs afin de prévoir l’ajout possible en cas de volonté de redondance.

# Routage

## Agence

RAX(config)#ip route 0.0.0.0 0.0.0.0 10.XX.254.254

## FAI

FAI(config)#ip route 0.0.0.0 0.0.0.0 10.254.254.254

## Siège social

RSS(config)#ip route 0.0.0.0 0.0.0.0 10.10.20.243

RSS(config)#ip route 0.0.0.0 0.0.0.0 10.20.30.130

RSS(config)#ip route 0.0.0.0 0.0.0.0 10.30.45.162

RSS(config)#ip route 0.0.0.0 0.0.0.0 10.40.230.43

RSS(config)#ip route 0.0.0.0 0.0.0.0 10.254.1.1

# Plan de sécurité

## Switch

* Interface non utiliser shutdown
* Mot de passe mode enable (ESGI)
* Désactivation du VTP
* 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

Désactivation du CDP (Cisco Discovery Protocol) - switch et routeur

Permet de trouver d’autre périphérique voisin directement connecter via SNMP

XXXXX(config-if)#no cdp enable

Sécurisation des opérations STP (Spanning Tree Protocol) - switch

XXXXX(config-if)#spanning-tree bpduguard enable

Désactivation VTP - switch

Permet d’administrer les VLAN de plusieurs switches depuis un seul

XXXXX(config)#vtp mode transparent

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