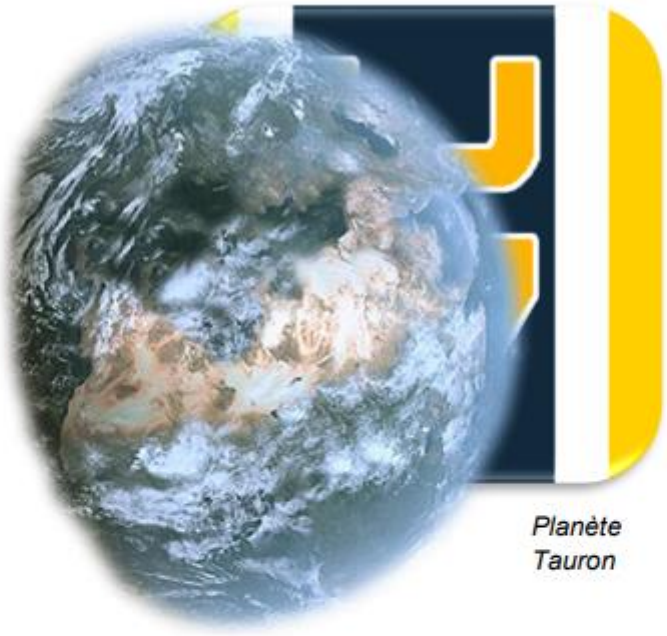
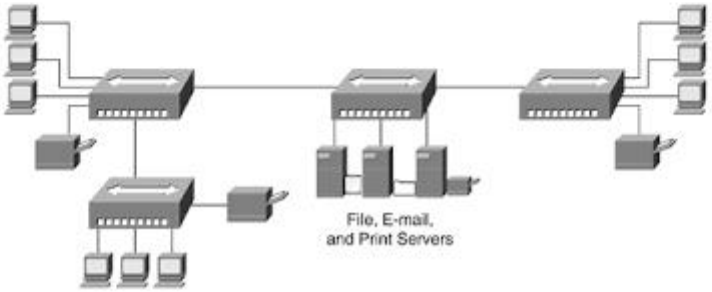
PROJET RÉSEAU

Procédures d'installation et de configuration





Lhinares Tanguy, Simonneau Olivier, Aoustin Quentin, Chauvel Antoine.

FICHE DE CONFIDENTIALITE DES RAPPORTS ET MEMOIRES
CESI ECOLE D'INGENIEURS

Titre du rapport ou du mémoire : Procédures d'installation et de configuration

Nom et prénom des étudiants : AOUSTIN QUENTIN | SIMONNEAU OLIVIER | LHINARES TANGUY | CHAUVEL ANTOINE

Date de la soutenance : 27/03/2020

Confidentialité du rapport ou du mémoire (soutenance)

☐ **Diffusion libre**

Les rapports / mémoires sont conservés en archives et ils peuvent être librement consultés. Ils peuvent être utilisés par les destinataires, les études peuvent faire l'objet de publication …

☒ **Diffusion restreinte**

Les rapports / mémoires **sont restitués aux élèves** à l'issue de la soutenance. Aucune reproduction n'est autorisée. La responsabilité de cette opération est confiée aux étudiants. Dans le cadre de la politique de lutte contre le plagiat, les rapports / mémoires seront susceptibles d'être analysés pour en vérifier les sources et ceci quel que soit le mode de diffusion prévu ci-dessus.

SOMMAIRE :

Introduction

Pour introduire ce rapport de configurations, il convient de présenter brièvement le projet.

Vergis Corporation, entreprise basée sur Tauron a trouvé la clé de l'intelligence artificielle en développant le processeur méta-cognitif (MCP), ce qui en fait un concurrent sérieux de Graystone Industries (Cprica City), pour le contrat militaire des Cyber Combat Units.

En effet, les deux entreprises se livrent une guerre industrielle pour remporter un contrat avec le gouvernement Caprican pour développer des technologies pour des applications militaires. Une partie de ce contrat porte sur l'unité cybernétique de combat.

Muni du MCP, le prototype cybernétique de combat U-87, construit par Graystone, montre des signes d'une intelligence comparable à celle des humains et le gouvernement de Caprica signe le contrat. Graystone lance alors la production des Cybernetic Lifeform Nodes, mieux connus sous le nom de Cylons.

Le PDG de Vergis Corporation, Tomas Vergis, furieux de ce vol des plans de son MCP, souhaite revoir rapidement l'architecture de son réseau informatique et la sécurité de son entreprise. C'est à ce moment que notre équipe intervient. Nous avons la lourde tâche de présenter à Tomas Vergis, dans un délai très court, une maquette de la nouvelle infrastructure informatique.

Tomas souhaite repenser l'ensemble du réseau et mettre l'accent sur la sécurité, nous faisant donc partir d'une feuille vierge.

L'entreprise comporte actuellement 4 bâtiments dans le centre de Tauron City : le bâtiment principal, le bâtiment Est, le bâtiment Ouest et une salle informatique principale. Chaque bâtiment est constitué d'un rez-de-chaussée et de deux étages. Parallèlement à cela, l'entreprise est prospère : elle envisage de faire construire un nouveau site à l'image du site principal (constitué des bâtiments précédemment énoncés).

La société souhaite également disposer d'une agence dans l'idée de développer des gammes de robots grands publics. Pour relier les trois sites, Tomas Vergis envisage un réseau MPLS avec comme point central un datacenter. Ce datacenter sera présente en périphérie de la ville dans des locaux sécurisés.

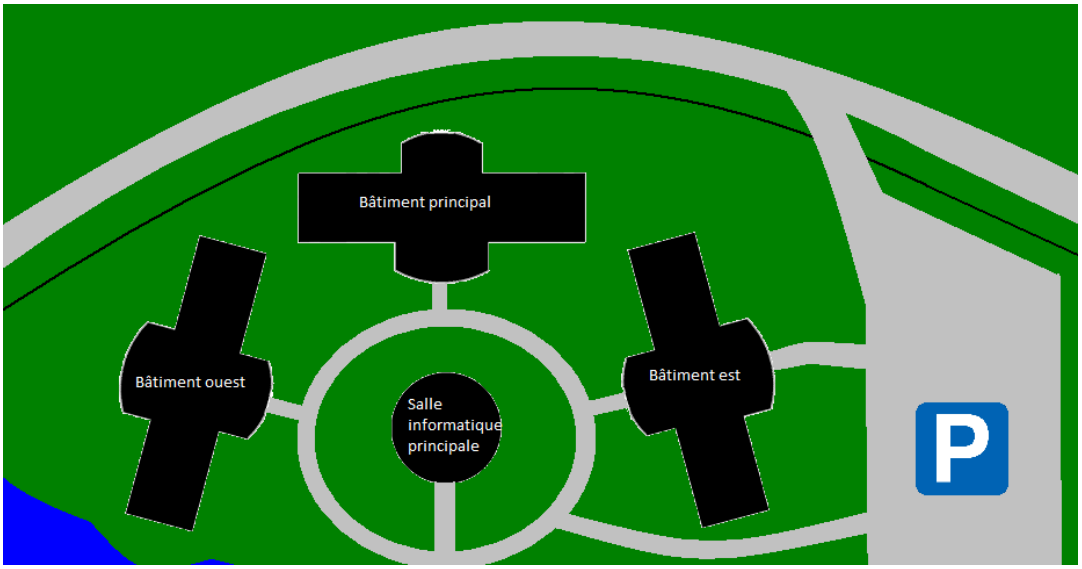
La société nous a fait savoir que le réseau MPLS n'était pas à notre chargé. Nous sommes donc responsables de la constitution d'une architecture réseau pour les sites suivants :

- Site principal
- Site secondaire
- Agence
- Datacenter, épicentre des communications

Il convient de présenter dans le présent document les différentes procédures d'installation et de configuration des équipements utilisés dans l'architecture choisie.

Installation physique des équipements

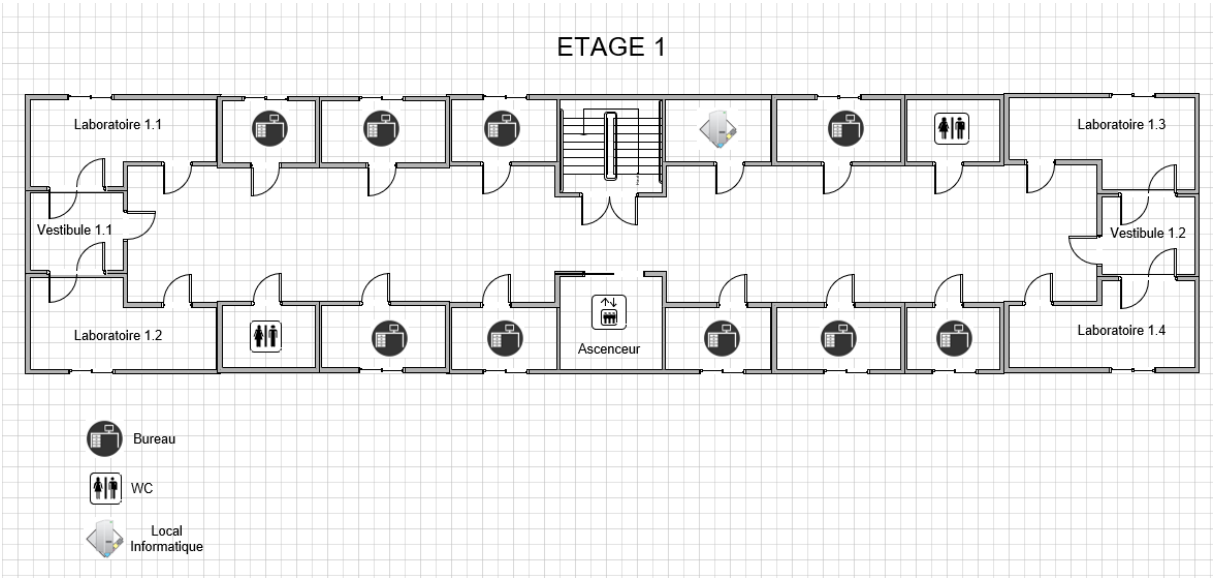
Le site principal et le site secondaire ont le même plan physique :



Chaque bâtiment possède trois niveaux : un rez-de-chaussée et deux étages.

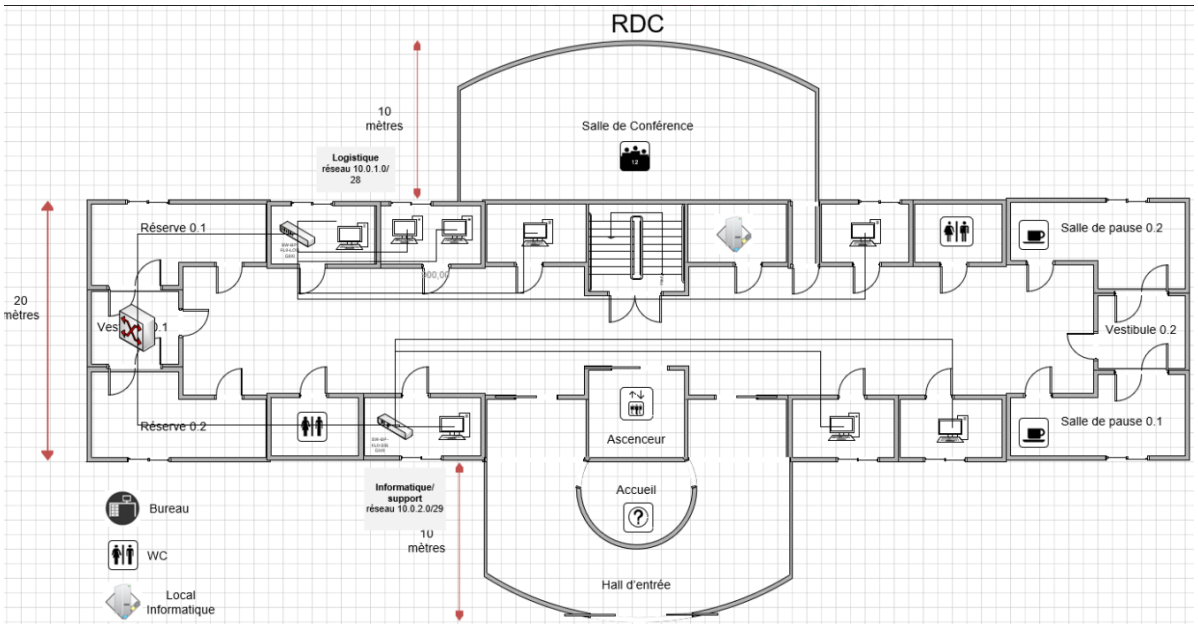
La salle informatique principale connecte les trois autres bâtiments en accueillant les commutateurs de niveau 3 qui agrègent les autres commutateurs des couches Distribution et Access.

Chaque étage des trois autres bâtiments est construit de la sorte :

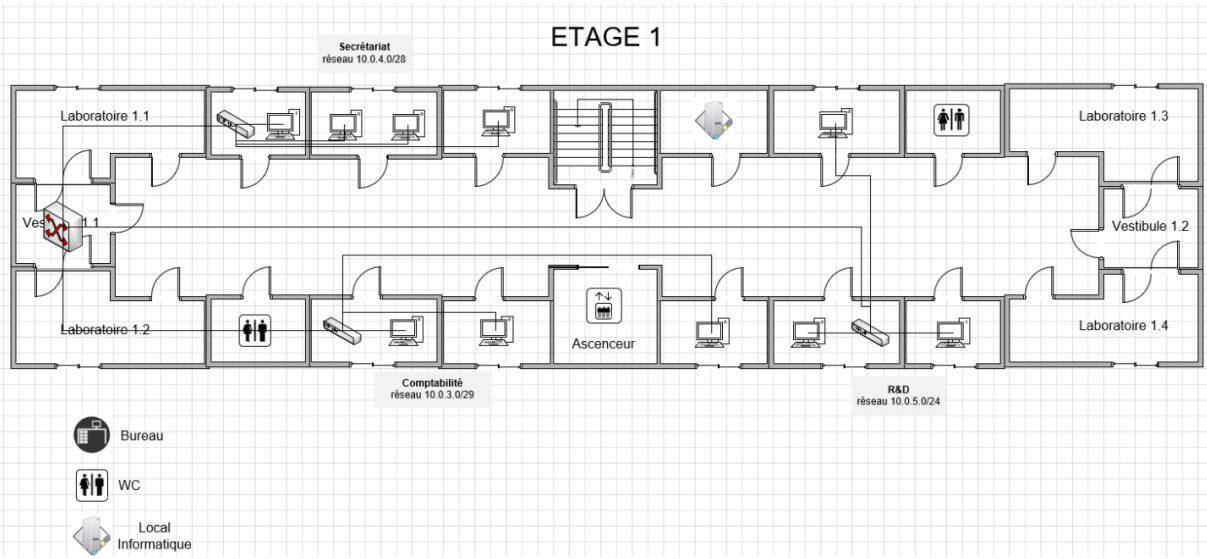


Il convient d'installer dans le local informatique les switchs de niveau 3 qui sont à chaque étage (cf. fichier de spécifications techniques détaillant notre architecture et les choix techniques). Puis, installer physiquement les ordinateurs des employés, avec les commutateurs de niveau 2 dans les vestibules.

Exemple d'installation au rez-de-chaussée du site principal :



Exemple d'installation au premier étage du site principal :



Configuration des équipements

Commandes site principal/site secondaire :

Configuration basique des équipements :

-enable

-conf t

-hostname *nom du switch* (se référer au document sur l'adressage ip et la nomenclature)

Configuration des switchs avec VTP pour propager les VLANs :

En

Conf t

Vtp mode transparent

Vtp version 2

Vtp mode client/server *(le server est le switch de niveau 3 central)*

Vtp domain site-secondaire

Configuration des liens en mode trunk entre les switchs :

Conf t

Interface *interface-type (ex : g0/4)*

Switchport trunk encapsulation dot1q

Switchport mode trunk

Création des VLANs depuis le VTP server :

Conf t

Vlan *numero-vlan* (opération répétée pour l'ensemble des VLANs)

Attribution des IP à chaque VLAN :

Conf t

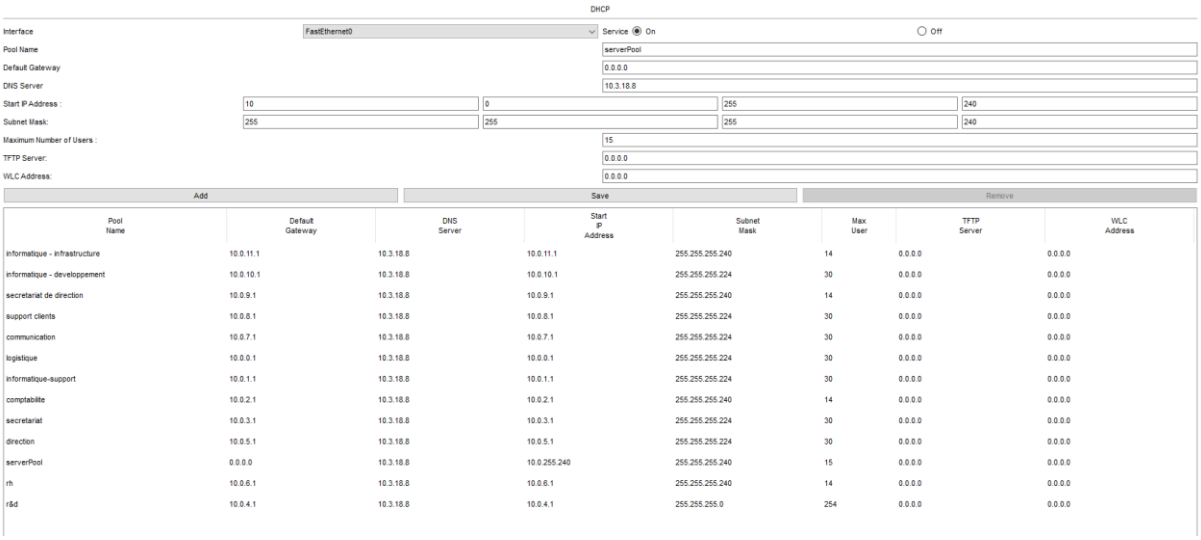
Interface vlan numero-vlan

Ip address X.X.X.X X.X.X.X

No shut

Configuration du DHCP :

Entrée des plages DHCP dans l'onglet « Services » du serveur (selon les plages définies dans l'adressage) :



Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
informatique - infrastructure	10.0.11.1	10.3.18.8	10.0.11.1	255.255.255.240	14	0.0.0.0	0.0.0.0
informatique - developpement	10.0.10.1	10.3.18.8	10.0.10.1	255.255.255.224	30	0.0.0.0	0.0.0.0
secretariat de direction	10.0.9.1	10.3.18.8	10.0.9.1	255.255.255.240	14	0.0.0.0	0.0.0.0
support clients	10.0.8.1	10.3.18.8	10.0.8.1	255.255.255.224	30	0.0.0.0	0.0.0.0
communication	10.0.7.1	10.3.18.8	10.0.7.1	255.255.255.224	30	0.0.0.0	0.0.0.0
logistique	10.0.0.1	10.3.18.8	10.0.0.1	255.255.255.224	30	0.0.0.0	0.0.0.0
informatique-support	10.0.1.1	10.3.18.8	10.0.1.1	255.255.255.224	30	0.0.0.0	0.0.0.0
comptabilite	10.0.2.1	10.3.18.8	10.0.2.1	255.255.255.240	14	0.0.0.0	0.0.0.0
secretariat	10.0.3.1	10.3.18.8	10.0.3.1	255.255.255.224	30	0.0.0.0	0.0.0.0
direction	10.0.5.1	10.3.18.8	10.0.5.1	255.255.255.224	30	0.0.0.0	0.0.0.0
serverPool	0.0.0.0	10.3.18.8	10.0.255.240	255.255.255.240	15	0.0.0.0	0.0.0.0
rh	10.0.6.1	10.3.18.8	10.0.6.1	255.255.255.240	14	0.0.0.0	0.0.0.0
r&d	10.0.4.1	10.3.18.8	10.0.4.1	255.255.255.0	254	0.0.0.0	0.0.0.0

Ou bien entrée des commandes manuelles :

-ip dhcp pool *nom du groupe* (se référer au document sur l'adressage ip et la nomenclature)

-network *adresse ip du réseau* *masque correspondant* (se référer au document sur l'adressage ip)

-default-router *adresse ip de la passerelle* (se référer au document sur l'adressage ip)

-exit

Ne pas oublier de configurer la passerelle par défaut du serveur comme étant l'adresse de l'intervalle vlan 1 du switch de niveau 3 central.

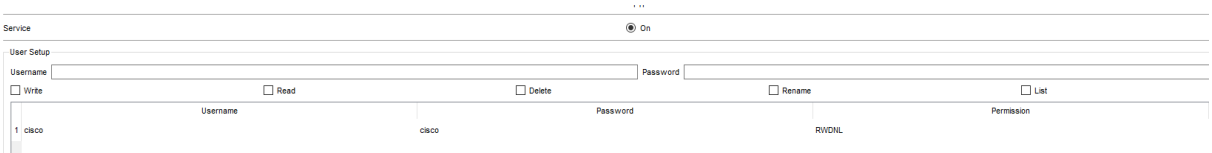
Configuration du FTP :

Configuration de l'adresse IP pour l'interface connectée au switch central de niveau 3 :

-interface *nom de l'interface* (se référer au document sur l'adressage ip et la nomenclature)

-ip address *adresse ip de l'interface (correspond à la passerelle)* *masque correspondant* (se référer au document sur l'adressage ip et la nomenclature)

Configuration d'un login depuis l'interface du serveur FTP :



Configuration du SSH sur les switchs (niveau 2 et 3) :

Etape 1 : Activation du SSH

interface vlan 99

ip address 10.1.254.30 255.255.255.0

exit

ip default-gateway 10.1.254.1

ip domain-name cesi.fr

crypto key generate rsa

2048

ip ssh version 2

username admin password cesi

line vty 0 15

login local

transport input ssh

exit

Etape 2 : Autorisation de l'accès en SSH pour les informaticiens uniquement

access-list 1 permit 10.1.1.0 0.0.0.31 access-list 1 permit 10.1.10.0 0.0.0.31 access-list 1 permit 10.1.11.0 0.0.0.15

access-list 1 remark accept ssh connections from administrators

line vty 0 15

access-class 1 in

Sécurisation de l'accès aux équipements :

En

conf t

enable secret cesi

line console 0

password exia

login

exit

service password-encryption

banner motd #Attention, vous entrez en zone sous securite informatique. Acces reserve aux personnes strictement autorisees. Toute entrave a la securite et connexion de la part d'une personne non autorisee est passible de poursuites.#

Sauvegarde de la configuration :

-exit

-copy run start

« Appuyer sur la touche entrée »

Empêcher le service logistique d'accéder à Internet (site secondaire uniquement) :

Configuration d'une ACL sur le switch layer 3 principal du site secondaire :

access-list 101 permit ip any 10.0.0.0 0.255.255.255

Restriction des accès quant au serveur FTP du site principal :

Doivent y avoir accès : les chercheurs du site principal, du site secondaire, les informaticiens (qui doivent être autorisés à échanger sur l'ensemble des protocoles) :

ip access-list extended CHERCHEUR

ip access-list extended CHERCHEUR

permit tcp 10.0.4.0 0.0.0.255 host 10.0.20.3 eq ftp

permit ip 10.1.4.0 0.0.0.255 host 10.0.20.3

permit tcp 10.0.1.0 0.0.0.31 host 10.0.20.3 eq ftp

permit tcp 10.0.10.0 0.0.0.31 host 10.0.20.3 eq ftp

permit tcp 10.0.11.0 0.0.0.15 host 10.0.20.3 eq ftp

permit ip 10.1.1.0 0.0.0.31 host 10.0.20.3

permit ip 10.1.10.0 0.0.0.31 host 10.0.20.3

permit ip 10.1.11.0 0.0.0.15 host 10.0.20.3

Restriction du trafic SMTP/TFTP pour les chercheurs du site principal :

ip access-list extended BLOCKTRAFIC

deny udp 10.0.4.0 0.0.0.255 any eq tftp

deny tcp 10.0.4.0 0.0.0.255 any eq smtp

permit ip any any

Commandes de configuration datacenter :

Routeur type:

en

conf t

interface GigabitEthernet0/0 *(vers agence)*

ip address 10.2.255.253 255.255.0.0

speed auto

standby 2 ip 10.2.255.254

standby 2 priority 105

standby 2 preempt

standby 2 track GigabitEthernet5/0

standby 2 track GigabitEthernet7/0

standby 2 track GigabitEthernet8/0

standby 2 track GigabitEthernet9/0

interface GigabitEthernet5/0 0 *(vers routeur datacenter backup)*

ip address 10.3.8.2 255.255.255.248

ip ospf cost 65

interface GigabitEthernet6/0 *(vers routeur global backup)*

ip address 10.3.5.2 255.255.255.248

ip ospf cost 65

interface GigabitEthernet7/0 *(vers routeur site secondaire)*

ip address 10.3.7.2 255.255.255.248

interface GigabitEthernet8/0 *(vers routeur site principal)*

ip address 10.3.6.2 255.255.255.248

interface GigabitEthernet9/0 *(vers routeur datacenter)*

ip address 10.3.4.2 255.255.255.248

ex

router ospf 1

passive-interface GigabitEthernet0/0 *(vers agence)*

network 10.3.6.0 0.0.0.7 area 1

network 10.3.7.0 0.0.0.7 area 1

network 10.3.8.0 0.0.0.7 area 1

network 10.3.4.0 0.0.0.7 area 1

network 10.3.5.0 0.0.0.7 area 1

network 10.2.0.0 0.0.255.255 area 1

ex

ip route 0.0.0.0 0.0.0.0 10.3.2.1

ip route 0.0.0.0 0.0.0.0 10.3.3.1 201

enable secret cesi

line console 0

password exia

login

exit

service password-encryption

hostname Agence

Routeur global de backup:

en

conf t

interface GigabitEthernet0/0 *(vers routeur agence)*

ip address 10.3.5.1 255.255.255.248

ip ospf cost 65

interface GigabitEthernet1/0 *(vers routeur site principal)*

ip address 10.3.9.2 255.255.255.248

ip ospf cost 65

interface GigabitEthernet2/0 *(vers routeur datacenter)*

ip address 10.3.12.2 255.255.255.248

ip ospf cost 65

interface GigabitEthernet3/0 *(vers routeur site secondaire)*

ip address 10.3.10.2 255.255.255.248

ip ospf cost 65

interface GigabitEthernet4/0 *(vers routeur datacenter backup)*

ip address 10.3.11.2 255.255.255.248

ip ospf cost 65

interface GigabitEthernet7/0 *(vers site secondaire)*

ip address 10.1.255.252 255.255.0.0

speed auto

standby 4 ip 10.1.255.254

standby 4 preempt

standby 4 track GigabitEthernet0/0

standby 4 track GigabitEthernet1/0

standby 4 track GigabitEthernet2/0

standby 4 track GigabitEthernet4/0

interface GigabitEthernet8/0 *(vers site principal)*

ip address 10.0.255.252 255.255.0.0

speed auto

standby 3 ip 10.0.255.254

standby 3 preempt

standby 3 track GigabitEthernet0/0

standby 3 track GigabitEthernet2/0

standby 3 track GigabitEthernet3/0

standby 3 track GigabitEthernet4/0

interface GigabitEthernet9/0 *(vers agence)*

ip address 10.2.255.252 255.255.0.0

speed auto

standby 2 ip 10.2.255.254

standby 2 preempt

standby 2 track GigabitEthernet1/0

standby 2 track GigabitEthernet2/0

standby 2 track GigabitEthernet3/0

standby 2 track GigabitEthernet4/0

ex

router ospf 1

passive-interface GigabitEthernet7/0 *(vers site secondaire)*

passive-interface GigabitEthernet8/0 *(vers site principal)*

passive-interface GigabitEthernet9/0 *(vers agence)*

network 10.3.9.0 0.0.0.7 area 1

network 10.3.11.0 0.0.0.7 area 1

network 10.3.12.0 0.0.0.7 area 1

network 10.3.10.0 0.0.0.7 area 1

network 10.3.5.0 0.0.0.7 area 1

network 10.0.0.0 0.0.255.255 area 1

network 10.1.0.0 0.0.255.255 area 1

network 10.2.0.0 0.0.255.255 area 1

ex

ip route 0.0.0.0 0.0.0.0 10.3.2.1

ip route 0.0.0.0 0.0.0.0 10.3.3.1 201

enable secret cesi

line console 0

password exia

login

ex

service password-encryption

hostname BU-Global

Firewall:

en

conf t

interface GigabitEthernet1/1 *(vers router datacenter)*

nameif inside

security-level 100

ip address 10.3.2.1 255.255.255.248

interface GigabitEthernet1/2 *(vers roueter datacenter backup)*

nameif buinside

security-level 100

ip address 10.3.3.1 255.255.255.248

ospf cost 65

interface GigabitEthernet1/3 *(vers "l'extérieur", tout autre routeur sur l'internet)*

nameif outside

security-level 0

ip address 157.240.21.36 255.255.255.0

interface GigabitEthernet1/4 *(vers le serveur de la DMZ)*

nameif DMZ

security-level 70

ip address 10.3.1.1 255.255.255.248

ex

object network buinside-net

subnet 10.3.3.0 255.255.255.248

ex

```
object network dmz-server
host 10.3.1.2
ex
object network inside-net
subnet 10.3.2.0 255.255.255.248
ex
route outside 0.0.0.0 0.0.0.0 157.240.21.35 1

access-list OUTSIDE-DMZ extended permit icmp any host 10.3.1.2
access-list OUTSIDE-DMZ extended permit tcp any host 10.3.1.2 eq www
access-group OUTSIDE-DMZ in interface outside

object network buinside-net
nat (buinside,outside) dynamic interface
ex
object network dmz-server
nat (DMZ,outside) static 157.240.21.36
ex
object network inside-net
nat (inside,outside) dynamic interface
ex

class-map inspection_default
match default-inspection-traffic
ex
policy-map global_policy
class inspection_default
inspect icmp
ex
service-policy global_policy global
```

router ospf 1

network 10.3.1.0 255.255.255.248 area 1

network 10.3.2.0 255.255.255.248 area 1

network 10.3.3.0 255.255.255.248 area 1

network 157.240.21.0 255.255.255.0 area 2

ex

ex

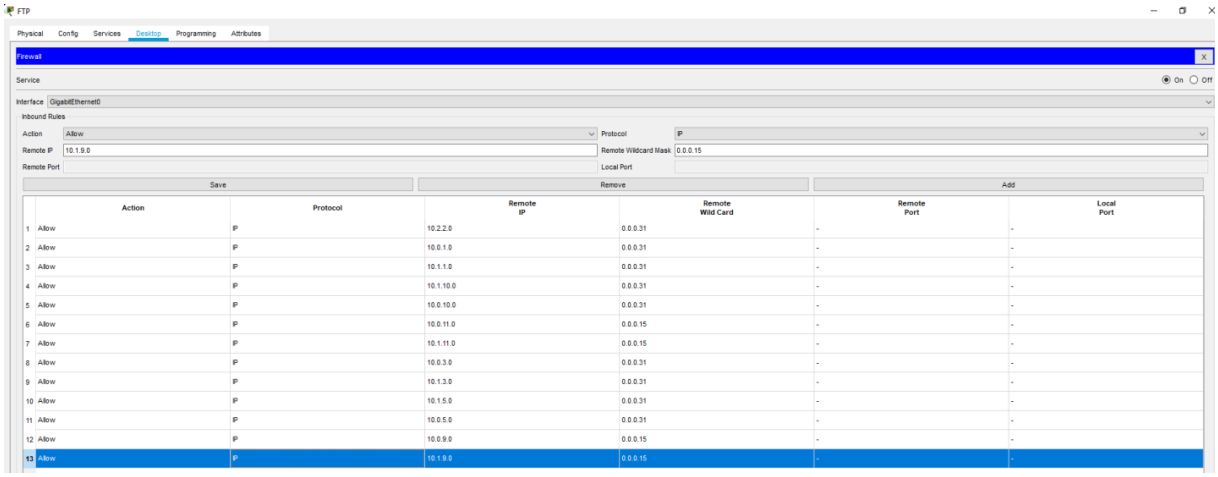
w m

yes

[Press enter]

Serveur FTP:

Configuration des plages restrictives d'accès pour les services considérés :



Commandes pour l’agence :

Switch layer 3:

CONFIGURATION CLASSIQUE

en

conf t

enable secret cesi

line console 0

password exia

login

exit

service password-encryption

hostname SW-AG-DL01

CONFIG DU DHCP

ip dhcp excluded-address 10.2.0.31

ip dhcp excluded-address 10.2.1.31

ip dhcp excluded-address 10.2.2.31

ip dhcp pool 220

 network 10.2.1.0 255.255.255.224

 default-router 10.2.1.1

exit

ip dhcp pool POOL_COMMERCE

 network 10.2.2.0 255.255.255.224

 default-router 10.2.2.1

exit

ASSOCIER VLAN A UNE INTERFACE

interface GigabitEthernet1/0/1

switchport mode access

switchport access vlan 410

exit

interface GigabitEthernet1/0/2

switchport mode access

switchport access vlan 420

exit

interface GigabitEthernet1/0/3

switchport mode access

switchport access vlan 430

exit

interface GigabitEthernet1/0/4

switchport mode trunk

switchport trunk encapsulation dot1q

exit

interface GigabitEthernet1/0/5

switchport mode trunk

switchport trunk encapsulation dot1q

ASSOCIE VLAN A UNE IP

interface Vlan410

ip address 10.2.1.1 255.255.255.224

exit

interface Vlan420

ip address 10.2.2.1 255.255.255.224

exit

interface Vlan430

ip address 10.2.3.1 255.255.255.252

exit

ip default-gateway 10.2.255.254

ip classless

ip route 0.0.0.0 0.0.0.0 10.2.255.254

ip routing

Quelques commandes

```
Vlan1                  10.2.255.250    YES manual up                    down
Vlan410                10.2.1.1        YES manual up                    up
Vlan420                10.2.2.1        YES manual up                    up
Vlan430                10.2.3.1        YES manual up                    up
```

Show ip vlan brief :

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/4, Gig1/0/5, Gig1/0/6,
Gig1/0/7
                                                Gig1/0/8, Gig1/0/9, Gig1/0/10,
Gig1/0/11
                                                Gig1/0/12, Gig1/0/13, Gig1/0/14,
Gig1/0/15
                                                Gig1/0/16, Gig1/0/17, Gig1/0/18,
Gig1/0/19
                                                Gig1/0/20, Gig1/0/21, Gig1/0/22,
Gig1/0/23
                                                Gig1/0/24, Gig1/1/1, Gig1/1/2,
Gig1/1/3
                                                Gig1/1/4
410  support                          active    Gig1/0/1
420  commercial                       active    Gig1/0/2
430  printers                         active    Gig1/0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Switch layer 2 – Commercial :

CONFIGURATION CLASSIQUE

en

conf t

enable secret cesi

line console 0

password exia

login

exit

service password-encryption

hostname SW-AG-SCO

CONFIGURATION INTERFACE / VLAN

interface GigabitEthernet0/1

switchport mode access

switchport access vlan 420

exit

interface GigabitEthernet1/1

switchport mode access

switchport access vlan 420

exit

interface Vlan1

no ip address

exit

vlan 220

name sales

exit

interface Vlan220

no ip address

ip helper-address 10.2.2.1

no shut

exit

Switch layer 2 – Commercial :

CONFIGURATION CLASSIQUE

en

conf t

enable secret cesi

line console 0

password exia

login

exit

service password-encryption

hostname SW-AG-SSC

CONFIGURATION INTERFACE / VLAN

interface GigabitEthernet0/1

```
switchport mode access
switchport access vlan 410
 exit
interface GigabitEthernet1/1
switchport mode access
switchport access vlan 410
exit
interface Vlan1
 no ip address
exit
vlan 210
name support
exit
interface Vlan210
no ip address
ip helper-address 10.2.1.1
no shut
exit
```