

Sommaire :

Sommaire :	1
Introduction.....	1
Configuration du switch :	2
Configuration du routeur :	5
Configuration de la borne Wifi :	6
Tests de conclusion :	9
ANNEXE – Nos configurations :	13

Introduction

Objectif : L'objectif est de réaliser une maquette d'infrastructure réseau contenant des VLAN, un point d'accès sans fil, un service DHCP, etc.

Pré-requis : Nous commençons par réinitialiser le matériel : le bouton reset et la mise sous tension sur la borne Wifi, et la commande « ***erase nvram:*** » sur le switch et « ***erase startup-config*** » suivi d'un « ***reload*** » sur le routeur.

Norme : Toutes les commandes issues d'une machine avec un système d'exploitation Debian ou Windows sont écrites ***en gras et en italique***.

Configuration du switch :

Il faut maintenant créer les VLAN sur le switch. Il y aura donc :

Le VLAN 10 :	192.168.10.0	255.255.255.0
Le VLAN 20 :	192.168.20.0	255.255.255.0
Le VLAN 40 :	192.168.40.0	255.255.255.0
Le VLAN Invité :	192.168.100.0	255.255.255.0

enable

(config) conf t

(config) vlan 10

(config-vlan) name employes11

(config-vlan) ex

(config) vlan 20

(config-vlan) name direction11

(config-vlan) ex

(config) vlan 40

(config-vlan) name bdd11

(config-vlan) ex

(config) vlan 50

(config-vlan) name admin11

(config-vlan) ex

(config) vlan 100

(config-vlan) name invites11

(config-vlan) ex

Nous affectons les VLAN aux ports :

(config) interface fastEthernet 0/3

(config-if) switchport mode access

(config-if) switchport access vlan 10

(config-if) ex

(config) interface fastEthernet 0/4

(config-if) switchport mode access

(config-if) switchport access vlan 20

(config-if) ex

```
(config) interface fastEthernet 0/5  
(config-if) switchport mode access  
(config-if) switchport access vlan 40  
(config-if) ex
```

```
(config) interface fastEthernet 0/6  
(config-if) switchport mode access  
(config-if) switchport access vlan 50  
(config-if) ex
```

Nous assignons maintenant les ports du routeur et de la borne wifi en mode trunk :

```
(config) interface fastEthernet 0/1  
(config-if) switchport mode trunk  
(config-if) ex
```

```
(config) interface fastEthernet 0/2  
(config-if) switchport mode trunk  
(config-if) ex
```

Nous affectons une adresse IP au VLAN 20 pour administrer à distance le switch :

```
(config) interface vlan 20  
(config-vlan) ip address 192.168.20.250 255.255.255.0  
(config-vlan) ex
```

Nous activons ensuite le SSH :

```
(config) ip domain-name archupontroz.local  
(config) end
```

```
(config) crypto key generate rsa general-keys modulus 1024
```

```
(config) ip ssh version 2
```

```
(config) username admin secret Password1234
```

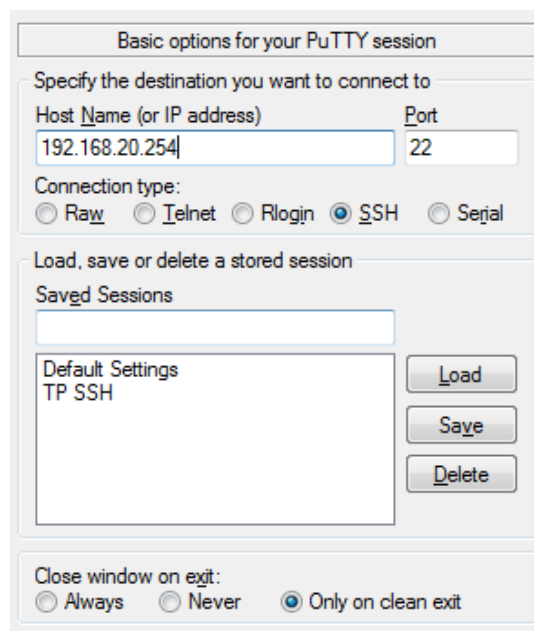
```
(config) line vty 0 15  
(config-line) login local  
(config-line) transport input ssh
```

```
show ip ssh
```

On attribue un mot de passe à la commande enable, avec un :

enable password Root1

Il faut ensuite mettre notre PC administrateur sur le même réseau que notre switch, soit le 192.168.20.1 par exemple. Nous pouvons ensuite accéder au switch en SSH :



Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address)	Port
192.168.20.254	22

Connection type:

Raw Telnet Rlogin SSH Serial

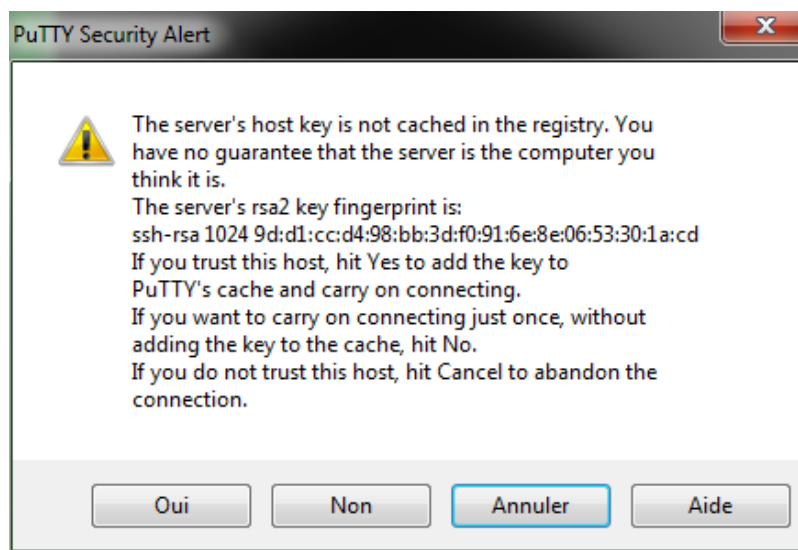
Load, save or delete a stored session

Saved Sessions

Default Settings TP SSH	<input type="button" value="Load"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
----------------------------	-------------------------------------	-------------------------------------	---------------------------------------

Close window on exit:

Always Never Only on clean exit



Nous passons maintenant à la configuration du routeur.

Configuration du routeur :

Nous allons maintenant créer les sous-interfaces attribuées à leur VLAN :

Interface	VLAN	Adresse IP
FastEthernet 0/0.10	Vlan 10 (employes11)	192.168.10.254 255.255.255.0
FastEthernet 0/0.20	Vlan 20 (direction11)	192.168.20.254 255.255.255.0
FastEthernet 0/0.40	Vlan 40 (bdd11)	192.168.40.254 255.255.255.0
FastEthernet 0/0.50	Vlan 50 (admin11)	192.168.50.254 255.255.255.0
FastEthernet 0/0.100	Vlan 100 (invites11)	192.168.100.254 255.255.255.0

```
(config) interface fastEthernet 0/0.10
(config-if) description *VLAN10*
(config-if) encapsulation dot1Q 10
(config-if) ip address 192.168.10.254 255.255.255.0
(config-if) no shut
```

```
(config) interface fastEthernet 0/0.20
(config-if) description *VLAN20*
(config-if) encapsulation dot1Q 20
(config-if) ip address 192.168.20.254 255.255.255.0
(config-if) no shut
```

```
(config) interface fastEthernet 0/0.40
(config-if) description *VLAN40*
(config-if) encapsulation dot1Q 40
(config-if) ip address 192.168.40.254 255.255.255.0
(config-if) no shut
```

```
(config) interface fastEthernet 0/0.50
(config-if) description *VLAN50*
(config-if) encapsulation dot1Q 50
(config-if) ip address 192.168.50.254 255.255.255.0
(config-if) no shut
```

```
(config) interface fastEthernet 0/0.100
(config-if) description *VLAN100*
(config-if) encapsulation dot1Q 100
(config-if) ip address 192.168.100.254 255.255.255.0
(config-if) no shut
```

Nous pouvons maintenant définir les pools DHCP :

```
(config) ip dhcp pool employes11
(config-dhcp) network 192.168.10.0 255.255.255.0
(config-dhcp) default-router 192.168.10.254
```

```
(config) ip dhcp pool direction11
(config-dhcp) network 192.168.20.0 255.255.255.0
(config-dhcp) default-router 192.168.20.254
```

```
(config) ip dhcp pool invites11
(config-dhcp) network 192.168.100.0 255.255.255.0
(config-dhcp) default-router 192.168.100.254
```

Nous pouvons maintenant configurer la borne Wifi.

Configuration de la borne Wifi :

Pour accéder à la borne Wifi via une interface Web, il faut paramétrer l'interface BVI1 :

```
conf t
(config) interface bvi1
(config-if) ip address 192.168.1.250 255.255.255.0
(config-if) no shut
```

Il faut alors créer les VLAN :

Create VLAN		Define SSIDs	
VLAN ID:	<input type="text" value="10"/>	(1-4094)	
VLAN Name (optional):	<input type="text" value="employes 11"/>		
	<input type="checkbox"/>	Native VLAN	
	<input type="checkbox"/>	Enable Public Secure Packet Forwarding	

Puis créer les SSID et les associer aux VLAN :

SSID:
VLAN: [Define VLANs](#)
 Backup 1:
 Backup 2:
 Backup 3:
Interface: Radio0-802.11G
Network ID: (0-4096)

Il faut ensuite configurer l'interface Radio :

Cisco Aironet 1200 Series Access Point

Hostname ap

Home: Summary Status		
Association		
Clients: 0	Infrastructure clients: 0	
Network Identity		
IP Address	192.168.1.250	
MAC Address	0012.d940.e435	
Network Interfaces		
Interface	MAC Address	Transmission Rate
FastEthernet	0012.d940.e435	100Mb/s
Radio0-802.11G	0013.194f.ec10	54.0Mb/s
Event Log		
Time	Severity	Description

World Mode
 Multi-Domain Operation:

Disable

Legacy

Country Code:

Indoor Outdoor

- CCK Transmitter Power (mW): 1 5 10 20 30 50 Max
- OFDM Transmitter Power (mW): 1 5 10 20 30 Max
- Client Power Local: Enable
- Limit Client Power (mW): 1 5 10 20 30 50 Max

Diffuser les SSID :

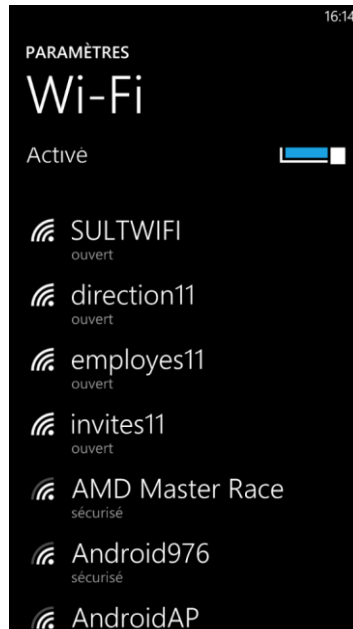
Guest Mode/Infrastructure SSID Settings

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID:

Multiple BSSID

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

Et voici nos réseaux Wifi, direction11, employes11 et invites11, pour l'instant avec une connexion ouverte :



Tests de conclusion :

Nous avons mis en place le chiffrement de nos SSID selon la consigne :

Hostname ap

Security: Encryption Manager

Set Encryption Mode and Keys for VLAN: 10 ▼

Encryption Modes

None
 WEP Encryption Optional ▼
 Cipher WEP 128 bit ▼

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

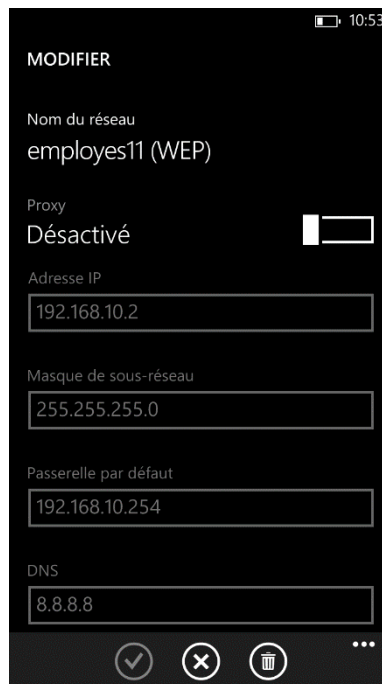
Encryption Keys

	Transmit Key	
Encryption Key 1:	<input checked="" type="radio"/>	Encryption Key (Hexadecimal)
		<input style="width: 100%;" type="text"/>

Et nous nous connectons bien sur nos réseaux protégés :



En récupérant une adresse IP du bon pool. Ici, le VLAN 10 reçoit bien une adresse en 192.168.10.0 :



Nous pouvons maintenant activer le NAT/PAT sur le routeur pour permettre à tous les VLAN d'accéder à Internet. Nous devons d'abord fixer l'interface FastEthernet 0/1 vers le réseau SIO :

```
interface FastEthernet 0/1  
ip address 192.168.1.116 255.255.255.0  
no shut
```

Puis nous créons le pool de NAT :

```
ip nat pool POOLNAT 192.168.1.116 192.168.1.116 prefix-length 24  
ip nat inside source liste 1 pool POOLNAT overload
```

Puis nous devons l'activer sur toutes les sous interfaces :

```
interface FastEthernet 0/0.10  
ip nat inside
```

```
interface FastEthernet 0/0.20  
ip nat inside
```

```
interface FastEthernet 0/0.40  
ip nat inside
```

```
interface FastEthernet 0/0.50  
ip nat inside
```

```
interface FastEthernet 0/0.100  
ip nat inside
```

Puis nous créons des ACL pour permettre à nos VLAN d'utiliser le NAT/PAT :

```
access-list 1 permit 192.168.10.0 0.0.0.255  
access-list 1 permit 192.168.20.0 0.0.0.255  
access-list 1 permit 192.168.40.0 0.0.0.255  
access-list 1 permit 192.168.50.0 0.0.0.255  
access-list 1 permit 192.168.100.0 0.0.0.255
```

Nous pouvons ensuite rajouter les ACL sur le router, afin d'autoriser les communications des VLAN suivants :

Employés peut communiquer avec BDD.
Direction peut communiquer avec BDD.
Admin peut communiquer avec BDD.
Invité ne peut communiquer avec personne.

```
access-list 110 permit ip 192.168.10.0 0.0.0.255 host 192.168.10.254  
access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255  
access-list 110 deny ip any any
```

```
interface FastEthernet 0/0.10  
ip access-group 110 in
```

```
access-list 120 permit ip 192.168.20.0 0.0.0.255 host 192.168.20.254  
access-list 120 permit ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255  
access-list 120 deny ip any any
```

```
interface FastEthernet 0/0.20  
ip access-group 120 in
```

```
access-list 150 permit ip 192.168.50.0 0.0.0.255 host 192.168.50.254  
access-list 150 permit ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255  
access-list 150 deny ip any any
```

```
interface FastEthernet 0/0.50  
ip access-group 150 in  
access-list 150 permit ip 192.168.100.0 0.0.0.255 host 192.168.100.254
```

ARCHAMBAULT Aimeric
DUPONT Anthony
DETROZ Sébastien

Version 1

10/03/2017

```
access-list 100 permit ip 192.168.40.0 0.0.0.255 192.168.100.0 0.0.0.255  
access-list 100 deny ip any any
```

```
interface FastEthernet 0/0.100  
ip access-group 100 in
```

ANNEXE – Nos configurations :

*Jan 1 03:42:11.335: %SYS-5-CONFIG_I: Configured from console by console

Current configuration : 2139 bytes

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Router  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
memory-size iomem 15  
ip cef  
!  
!  
no ip dhcp use vrf connected  
ip dhcp excluded-address 192.168.10.254  
ip dhcp excluded-address 192.168.20.254  
ip dhcp excluded-address 192.168.100.254  
!  
ip dhcp pool employes11  
  network 192.168.10.0 255.255.255.0  
  default-router 192.168.10.254  
  dns-server 8.8.8.8  
!  
ip dhcp pool direction11  
  network 192.168.20.0 255.255.255.0  
  default-router 192.168.20.254  
  dns-server 8.8.8.8  
!  
ip dhcp pool invites11  
  network 192.168.100.0 255.255.255.0  
  default-router 192.168.100.254  
  dns-server 8.8.8.8  
!  
!  
ip auth-proxy max-nodata-conns 3
```

```
ip admission max-nodata-conns 3
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/0.10
description *VLAN10*
encapsulation dot1Q 10
ip address 192.168.10.254 255.255.255.0
ip access-group 110 in
ip nat inside
!
interface FastEthernet0/0.20
description *VLAN20*
encapsulation dot1Q 20
ip address 192.168.20.254 255.255.255.0
ip access-group 120 in
ip nat inside
!
interface FastEthernet0/0.40
description *VLAN40*
encapsulation dot1Q 40
ip address 192.168.40.254 255.255.255.0
ip access-group 140 in
ip nat inside
!
interface FastEthernet0/0.50
description *VLAN50*
encapsulation dot1Q 50
ip address 192.168.50.254 255.255.255.0
ip access-group 150 in
ip nat inside
!
interface FastEthernet0/0.100
```

ARCHAMBAULT Aimeric
DUPONT Anthony
DETROZ Sébastien

Version 1

10/03/2017

```
description *VLAN100*
encapsulation dot1Q 100
ip address 192.168.100.254 255.255.255.0
ip access-group 100 in
ip nat inside
!
interface FastEthernet0/1
ip address 192.168.1.116 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/0/0
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface Serial0/1/0
no ip address
shutdown
clock rate 125000
!
interface Serial0/1/1
no ip address
shutdown
clock rate 125000
!
interface Vlan1
no ip address
!
ip forward-protocol nd
!
!
ip http server
no ip http secure-server
ip nat pool POOLNAT 192.168.1.116 192.168.1.116 prefix-length 24
ip nat inside source liste 1 pool POOLNAT overload
!
!
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
```

```
access-list 1 permit 192.168.50.0 0.0.0.255
access-list 1 permit 192.168.100.0 0.0.0.255
access-list 110 permit ip 192.168.10.0 0.0.0.255 host 192.168.10.254
access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny ip any any
access-list 120 permit ip 192.168.20.0 0.0.0.255 host 192.168.20.254
access-list 120 permit ip 192.168.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 120 deny ip any any
access-list 150 permit ip 192.168.50.0 0.0.0.255 host 192.168.50.254
access-list 150 permit ip 192.168.40.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 150 deny ip any any
access-list 150 permit ip 192.168.100.0 0.0.0.255 host 192.168.100.254
access-list 100 permit ip 192.168.40.0 0.0.0.255 192.168.100.0 0.0.0.255
access-list 100 deny ip any any
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
  login
!
scheduler allocate 20000 1000
end
```