SAE 3.03 - Cyber

Concevoir un réseau informatique sécurisé multi-sites

Pierre FROSTIN

BUT Réseaux et Télécommunications – La Rochelle

Introduction

Dans le cadre de cette SAE, nous avons mis en place un réseau fonctionnel avec plusieurs sites interconnectés. L'objectif était de configurer des VLANs pour séparer les différents types de trafic (utilisateurs, administrateurs, VoIP, etc.), tout en assurant une gestion de la qualité de service (QoS) et une connectivité fiable. Nous avons également implémenté des protocoles de routage dynamique comme OSPF et mis en place un VPN pour sécuriser les communications entre les sites. Toutefois, plusieurs défis techniques ont été rencontrés, notamment liés à la configuration des VLANs, la QoS et la connectivité entre certains équipements distants.

Table des matières

Configuration IPv4 des liens et équipements

La première étape a consisté à attribuer des adresses IP à l'ensemble des interfaces, puis à tester la connectivité en effectuant des pings vers les interfaces opposées. Ensuite, les différents VLANs ont été créés sur les switchs de niveau 2 et de niveau 3. J'ai ensuite affectée les différents équipements au bon VLAN sachant qu'il y a une particularité pour la configuration de certains téléphones car ceux-ci sont reliés à un PC, voici la configuration à faire sur un switch :

```
inter fa0/1
switchport mode access
switchport access vlan 112
switchport voice vlan 212
spanning-tree portfast
spanning-tree bpduguard enable
```

```
switchport access vlan 112
```

- Associe le VLAN 112 comme VLAN de données pour cette interface. C'est le VLAN utilisé pour transmettre le trafic réseau de l'ordinateur connecté au téléphone (ou directement au port du switch).

```
switchport voice vlan 212
```

- Associe le VLAN 212 comme VLAN voix, dédié au trafic VoIP. Cela permet de séparer logiquement le trafic voix (téléphonie IP) du trafic données sur un même port, offrant une meilleure gestion du réseau et de la qualité de service (QoS).

Sécurité sur les ports des switchs

Voici la configuration appliquée aux ports des switchs connectés à des équipements :

```
inter fa0/2
switchport mode access
switchport access vlan 112
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security mac-address sticky
```

```
switchport nonegotiate
spanning-tree portfast
spanning-tree bpduguard enable
```

```
switchport port-security
```

- Active la sécurité des ports (*port security*) sur cette interface. Cela limite et contrôle le nombre d'adresses MAC pouvant accéder au réseau via ce port.

```
switchport port-security maximum 3
```

- Configure une limite à **3 adresses MAC** pouvant être apprises dynamiquement ou configurées statiquement sur ce port. Cela empêche la connexion de plus de trois appareils simultanément sur ce port.

```
switchport port-security violation restrict
```

- Définit la politique de violation. En cas de dépassement de la limite (plus de 3 adresses MAC), le port bloquera les nouveaux appareils non autorisés et continuera à permettre le trafic des adresses autorisées :

```
switchport port-security mac-address sticky
```

- Configure le port pour "apprendre" dynamiquement les adresses MAC des appareils connectés et les stocker dans la configuration en tant qu'adresses "statiques". Cela simplifie la gestion, car les adresses MAC apprises sont conservées même après un redémarrage du switch (si la configuration est sauvegardée).

```
switchport nonegotiate
```

- Désactive la négociation DTP (*Dynamic Trunking Protocol*), ce qui empêche le port de tenter de devenir un lien *trunk*. Cela garantit que le port reste en mode *access*.

```
spanning-tree portfast
```

- Active le mode *PortFast*, ce qui permet au port de passer immédiatement à l'état *forwarding* sans les délais habituels du protocole Spanning Tree. Ceci est recommandé pour les ports connectés à des appareils finaux.

```
spanning-tree bpduguard enable
```

- Active la protection *BPDU Guard*. Si le port reçoit des messages *BPDU* (ce qui indiquerait qu'un autre switch est connecté par erreur), le port sera immédiatement désactivé (mis en *err-disabled*). Cela protège contre les boucles réseau accidentelles.

Sécurité mise en place sur un trunk

La première étape consiste à autoriser uniquement les VLANs spécifiques à être transportés sur un lien trunk. De plus, il est essentiel de modifier le VLAN natif sur les trunks afin de sécuriser le réseau contre certaines attaques, telles que le VLAN hopping. Cette attaque permet à un attaquant d'envoyer des trames non étiquetées (sans tag VLAN) en utilisant le VLAN natif pour accéder à d'autres VLANs du réseau. Si un attaquant réussit à se connecter à un switch avec un port configuré sur le VLAN natif par défaut (VLAN 1), il pourrait perturber ou compromettre des VLANs sensibles.

Mise en place d'un DHCP

La configuration d'un service DHCP a été réalisée sur le routeur Call Manager de chaque site, bien qu'il aurait également été possible de l'implémenter sur le switch de niveau 3. Par ailleurs, un seul serveur DHCP a été déployé, alors qu'il était envisageable d'en configurer un second sur le switch de niveau 3 en tant que serveur de secours. Cela aurait permis aux équipements d'obtenir une adresse IP de l'un des deux serveurs disponibles. Cependant, cette configuration n'a pas été mise en place dans ma topologie. Un pool DHCP a été mis en place par VLAN.

Pour ce qui est de la configuration du DHCP voici les étapes à suivre :

Exclure les adresses réservées :

Avant de créer un pool DHCP, il faut exclure les adresses IP réservées pour les appareils critiques, par exemple les adresses des passerelles par défaut ou alors celle du WLC et du serveur radius pour le pool wifi-management.

```
ip dhcp excluded-address [début] [fin]
```

Créer un pool DHCP :

Créez un pool DHCP pour définir les paramètres du réseau. Chaque pool est associé à un sous-réseau ou VLAN.

```
ip dhcp pool LAN_Phones_A
```

Configurer le réseau et le masque de sous-réseau :

```
network 10.102.12.0 255.255.255.0
```

Configurer la passerelle par défaut :

```
default-router 10.102.12.252
```

Concernant la configuration des pools DHCP pour les téléphones et les équipements Wi-Fi, une particularité réside dans l'option suivante :

```
option 150 ip 10.102.12.252
```

L'option 150 fournit l'adresse IP du **TFTP server** (ici **10.102.12.252**) que les téléphones utiliseront pour télécharger leurs configurations, leurs firmwares, ou d'autres fichiers nécessaires.

Vérification des baux DHCP actifs :

```
show ip dhcp binding
```

```
R-CME-A#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.101.12.3      000A.F31A.D591           --                     Automatic
10.101.12.1      000C.855B.0345           --                     Automatic
10.101.12.2      00D0.5839.5017           --                     Automatic
10.102.12.1      00D0.BCA7.93A4           --                     Automatic
10.102.12.2      0060.3EC9.E616           --                     Automatic
10.104.12.1      000B.BE88.2D01           --                     Automatic
10.104.12.3      0001.42E5.9B36           --                     Automatic

R-CME-B#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.201.12.1      0060.7065.1630           --                     Automatic
10.201.12.2      000A.F36D.772B           --                     Automatic
10.201.12.3      0001.630A.CD20           --                     Automatic
10.202.12.2      000C.CF52.73D2           --                     Automatic
10.202.12.1      0002.1772.77D3           --                     Automatic
```

Test de ping intra VLAN dans le VLAN data et Voix :

```
C:\>ping 10.101.12.3

Pinging 10.101.12.3 with 32 bytes of data:

Reply from 10.101.12.3: bytes=32 time<1ms TTL=128
Reply from 10.101.12.3: bytes=32 time<1ms TTL=128
Reply from 10.101.12.3: bytes=32 time<1ms TTL=128
Reply from 10.101.12.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.101.12.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Figure 1 : Ping intra VLAN data

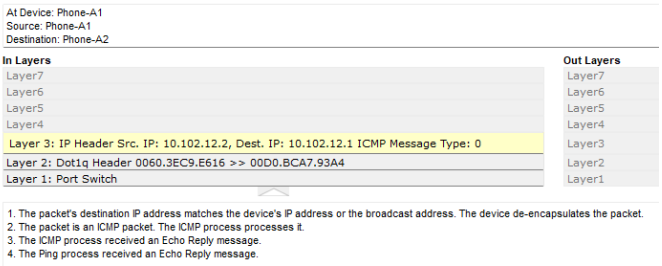

Figure 2 : Ping intra VLAN voix

Test de ping inter VLAN entre le VLAN data et le VLAN voix :

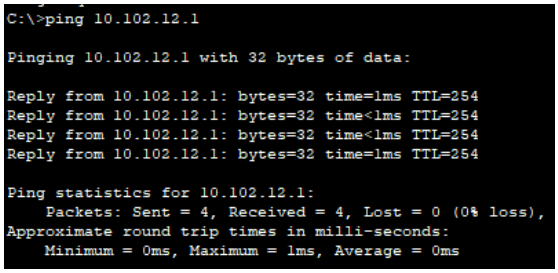

Figure 3 : Ping inter VLAN entre voix et data

La configuration d'un router on a stick, ainsi que des interfaces VLAN sur le switch de niveau 3, a été utilisée pour servir de passerelle par défaut.

Configuration des téléphones

Configuration de base du service de téléphonie

Voici un exemple de configuration d'un téléphone après avoir correctement configuré l'option 150 dans le service DHCP :

```
telephony-service
max-ephones 2
max-dn 2
no auto-reg-ephone
ip source-address 10.102.12.252 port 2000
end
```

`telephony-service` : Active le service de téléphonie sur le routeur pour configurer les téléphones IP.

`max-ephones 2` : Définit un maximum de 2 téléphones pouvant être enregistrés sur le système.

`max-dn 2` : Définit un maximum de 2 numéros de ligne disponibles.

`no auto-reg-ephone` : Désactive l'enregistrement automatique des téléphones. Cela signifie que seuls les téléphones configurés avec une adresse MAC explicite seront autorisés.

`ip source-address 10.102.12.252 port 2000` : Spécifie l'adresse IP du routeur (interface utilisée pour le service) et le port TCP (2000) utilisé par le protocole SCCP (Skinny Client Control Protocol) pour la communication entre les téléphones et le routeur.

Configuration des numéros (ephone-dn)

`ephone-dn 1` : Crée une instance de ligne virtuelle (Directory Number ou DN) pour le téléphone 1.

`number 7120` : Associe le numéro 7120 à cette ligne.

`ephone-dn 2` : Crée une deuxième instance de ligne virtuelle pour le téléphone 2.

`number 7121` : Associe le numéro 7121 à cette ligne.

Ces lignes (DN) seront assignées aux téléphones spécifiques à l'étape suivante.

Configuration des téléphones (ephones)

`ephone 1` : Configure le téléphone 1.

`mac-address 00D0.BCA7.93A4` : Spécifie l'adresse MAC du téléphone pour l'identifier sur le réseau.

`button 1:1` : Associe le bouton 1 du téléphone à la ligne 1 (ephone-dn 1). Cela signifie que ce téléphone utilisera le numéro 7120.

`ephone 2` : Configure le téléphone 2.

`mac-address 0060.3EC9.E616` : Spécifie l'adresse MAC du deuxième téléphone.

`button 1:2` : Associe le bouton 1 du téléphone à la ligne 2 (ephone-dn 2), ce qui correspond au numéro 7121.

Test d'un appel

Figure 4 : Appel depuis le téléphone

Figure 5 : Réponse à l'appel

Nous observons sur le CME que les téléphones ont bien été enregistrés :

```
%IPPHONE-6-REGISTER: ephone-1 IP:10.102.12.2 Socket:2 DeviceType:Phone has registered.
%IPPHONE-6-REGISTER: ephone-2 IP:10.102.12.1 Socket:2 DeviceType:Phone has registered.
```

Figure 6 : Les téléphones enregistrés

Nous constatons que l'appel est fonctionnel. Cependant, nous allons analyser les trames échangées pour comprendre le processus ayant permis ce résultat.

Tout d'abord nous observons que lorsque nous lançons un appel depuis le téléphone celui-ci créé un message SCCP sur le port 2000 (Skinny Client Control Protocol) un protocole propriétaire développé par Cisco, principalement utilisé pour la communication entre les téléphones IP Cisco et les serveurs de téléphonie. SCCP permet aux téléphones de se connecter à un système de gestion centralisé pour le contrôle des appels, l'attribution de numéros de téléphone, ainsi que d'autres fonctions liées à la gestion des téléphones VoIP. :

In Layers	Out Layers
Layer7	Layer 7: SCCP MESSAGE
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: TCP Src Port: 1026, Dst Port: 2000
Layer3	Layer 3: IP Header Src. IP: 10.102.12.1, Dest. IP: 10.102.12.252
Layer2	Layer 2: Dot1q Header 00D0.BCA7.93A4 >> 0000.0C07.AC01
Layer1	Layer 1: Port(s): Switch

Figure 7 : Le téléphone envoie un message au routeur CME pour obtenir des informations sur le téléphone appelé

Cette trame est envoyée au routeur CME, qui doit connaître le chemin vers le téléphone en utilisant le numéro configuré, de plus lorsque nous observons l'en-tête SCCP nous observons le type 6 qui est supposément utilisé pour demander des informations au routeur CME.

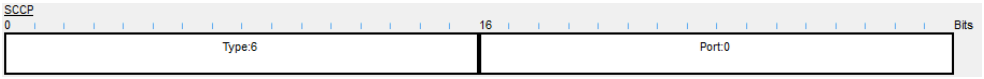

Figure 8 : Le type de l'en-tête SCCP lors du premier envoie vers le routeur CME

In Layers
Layer 7: SCCP MESSAGE
Layer6
Layer5
Layer 4: TCP Src Port: 2000, Dst Port: 1026
Layer 3: IP Header Src. IP: 10.102.12.252, Dest. IP: 10.102.12.1
Layer 2: Dot1q Header 0002.4A82.8401 >> 00D0.BCA7.93A4
Layer 1: Port Switch

Figure 9 : Réponse du routeur CME au message du téléphone composant l'appel

Après cela, le routeur répond au téléphone. Nous remarquons un changement de type dans l'en-tête, qui passe à 273. Cela semble indiquer que le routeur envoie des informations au téléphone ayant fait la demande.

Ensuite, un nouveau message est envoyé par le téléphone vers le routeur CME, qui redirige l'appel vers le téléphone correspondant au numéro configuré initialement, nous observons un changement de type qui passe à 3 peut être une confirmation du téléphone :

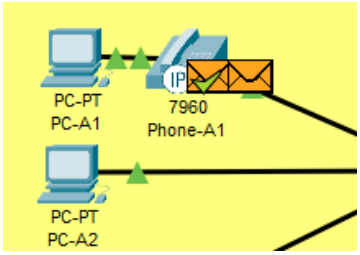

Figure 10 : Le téléphone recevant le premier message du routeur puis lui renvoyant un message

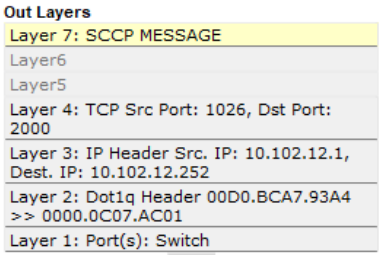

Figure 11 : Le téléphone renvoyant un message au routeur

Enfin, le type change une dernière fois à 133. À ce moment-là, le routeur envoie un message SCCP au téléphone appelé, ainsi qu'à celui ayant composé le numéro, afin de confirmer l'appel :

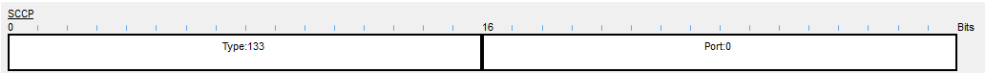

Figure 12 : Le type lorsque le routeur renvoie les appels

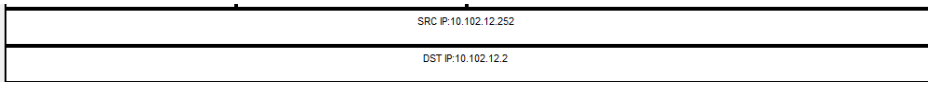

Figure 13 : Le routeur envoyant un message au numéro appelé

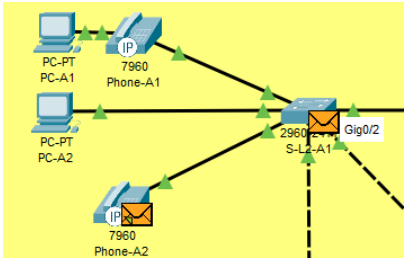

Figure 14 : Le routeur envoyant un message au numéro appelé

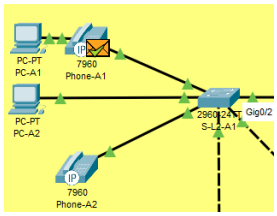

Figure 15 : Le routeur envoyant un message à l'appelant

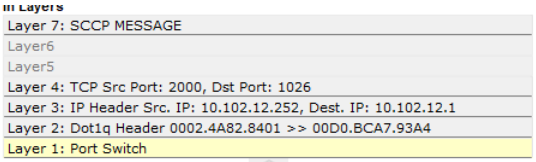

Figure 16 : Le routeur envoyant un message à l'appelant

Routage dynamique

Le protocole de routage dynamique OSPF a été utilisé sur les deux sites ainsi que chez le FAI, bien que, rétrospectivement, cela se soit avéré inutile. Cependant, OSPF a été conservé chez le FAI. Grâce à OSPF, j'ai pu diffuser la route par défaut, tout en veillant à mettre en interface passive les interfaces côté FAI et côté équipements afin d'éviter les messages HELLO. De plus, je n'ai pas diffusé les réseaux privés sur mes routeurs frontières.

Redondance de gateway

Dans cette topologie, le protocole HSRP a été mis en place entre le routeur CME et le switch L3, voici un exemple de configuration utilisé dans cette topologie :

```
interface FastEthernet0/0.112
standby 1 ip 10.101.12.252
standby 1 priority 120
standby 1 preempt
standby 1 ip 10.101.12.252
```

Cette commande configure l'adresse IP virtuelle pour le groupe **HSRP 1**. Dans ce cas, l'adresse IP virtuelle du groupe HSRP sera **10.101.12.252**.

L'IP virtuelle est l'adresse à laquelle les clients du réseau vont se connecter pour accéder à leur passerelle par défaut. Dans un environnement HSRP, cette adresse est partagée entre plusieurs routeurs.

```
standby 1 priority 120
```

Cette commande définit la priorité du routeur pour le groupe HSRP 1. Une priorité plus élevée signifie que ce routeur a plus de chances de devenir le **routeur actif** pour le groupe HSRP.

```
standby 1 preempt
```

La commande **preempt** permet à un routeur de prendre le rôle de routeur actif si sa priorité devient supérieure à celle du routeur actif actuel.

J'ai configuré le système de manière à ce que le CME ne soit pas toujours le routeur principal, afin de répartir le trafic entre les deux équipements de niveau 3. Par exemple, pour le site A, le CME est le routeur principal pour le VLAN data et le VLAN voix (étant donné qu'il possède les informations sur les téléphones). Pour les autres VLANs, le choix de la passerelle a été fait de manière arbitraire. Le switch de niveau 3 est la passerelle par défaut principale pour les autres VLANs.

Test de la redondance de gateway

D’après ce qui a été dit précédemment les équipements du VLAN data, si tout va bien, devrait sortir par le routeur CME :

Nous observons premièrement, lors de l’ouverture du fichier packet tracer que le CME est bien actif pour le 112 (data) :

```
%HSRP-6-STATECHANGE: FastEthernet0/0.112 Grp 1 state Standby -> Active
```

Figure 17 : Le CME est bien le routeur actif

```
%HSRP-6-STATECHANGE: Vlan112 Grp 1 state Speak -> Standby
```

Figure 18 : Le switch de niveau 3 est bien inactif

Vérifions tout de même avec le mode simulation de packet tracer :

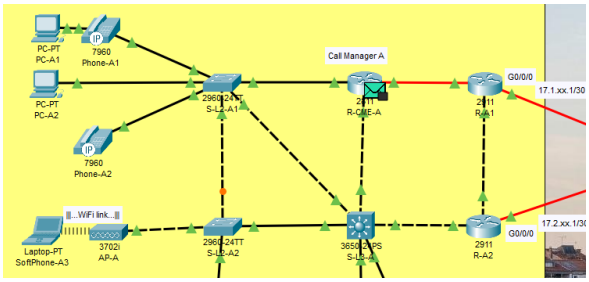

Figure 19 : Le packet passe par le routeur CME

Eteignons maintenant le routeur CME :

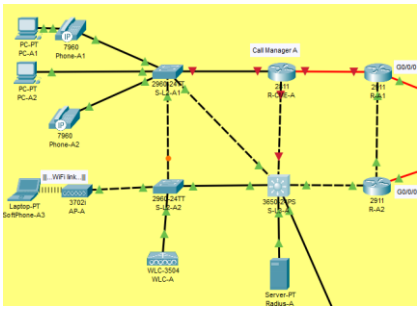

Figure 20 : CME éteint

```
%HSRP-6-STATECHANGE: Vlan112 Grp 1 state Standby -> Active
```

Figure 21 : Le L3 devient actif

Vérifions tout de même avec le mode simulation de packet tracer et un ping :

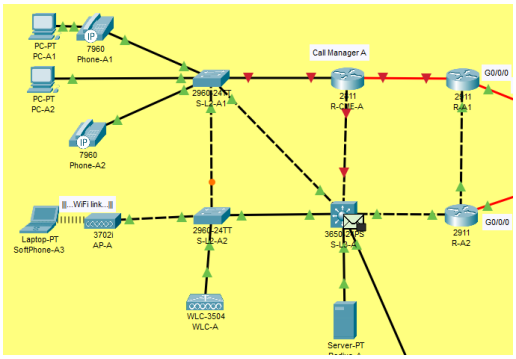

Figure 22 : Ça fonctionne

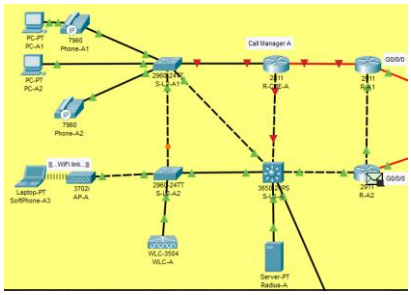

Figure 23: Ça fonctionne x2

Configuration de la NAT

Pour accéder à Internet avec une adresse IP privée, nous utilisons la NAT. Dans notre cas, une PAT (Port Address Translation) est configurée sur les deux routeurs de bordure, car nous disposons d'une seule adresse IP publique pour les deux cas. Nous autoriserons uniquement les équipements des VLANs prédéfinis précédemment à accéder à Internet.

Test de la PAT

Ping du serveur web :

```
C:\>ping 192.0.2.19

Pinging 192.0.2.19 with 32 bytes of data:

Reply from 192.0.2.19: bytes=32 time=1ms TTL=125
Reply from 192.0.2.19: bytes=32 time=1ms TTL=125
Reply from 192.0.2.19: bytes=32 time<1ms TTL=125
Reply from 192.0.2.19: bytes=32 time<1ms TTL=125

Ping statistics for 192.0.2.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure 24 : Ping du serveur web réussi

Nous observons bien que l'adresse IP source change et que la translation d'adresse est fonctionnelle :

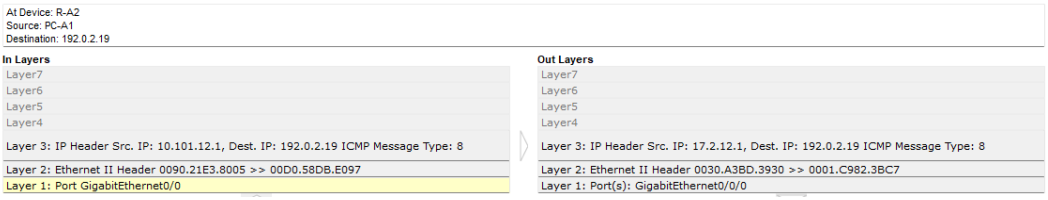

Figure 25 : Translation des adresses IP source sur R-A2

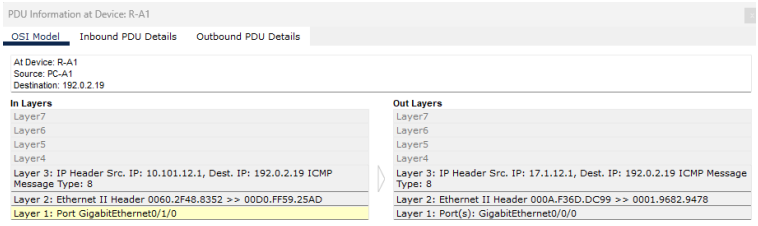

Figure 26 : Translation des adresses IP source sur R-A1

Nous effectuons le même test pour les 2 adresses IP publiques :

```
C:\>ping 69.1.12.1

Pinging 69.1.12.1 with 32 bytes of data:

Reply from 69.1.12.1: bytes=32 time<1ms TTL=251
Reply from 69.1.12.1: bytes=32 time=5ms TTL=251
Reply from 69.1.12.1: bytes=32 time<1ms TTL=251
Reply from 69.1.12.1: bytes=32 time<1ms TTL=251

Ping statistics for 69.1.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 5ms, Average = 1ms

C:\>ping 69.2.12.1

Pinging 69.2.12.1 with 32 bytes of data:

Reply from 69.2.12.1: bytes=32 time=3ms TTL=251
Reply from 69.2.12.1: bytes=32 time<1ms TTL=251
Reply from 69.2.12.1: bytes=32 time<1ms TTL=251
Reply from 69.2.12.1: bytes=32 time<1ms TTL=251

Ping statistics for 69.2.12.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms
```

Figure 27 : Ping publiques

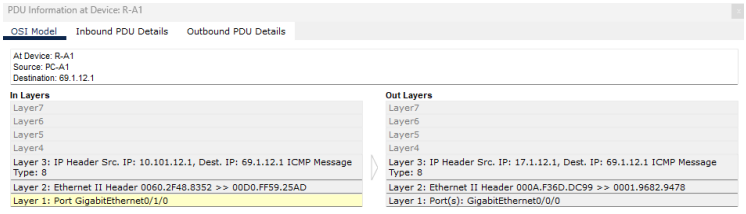

Figure 28 : Trame publique

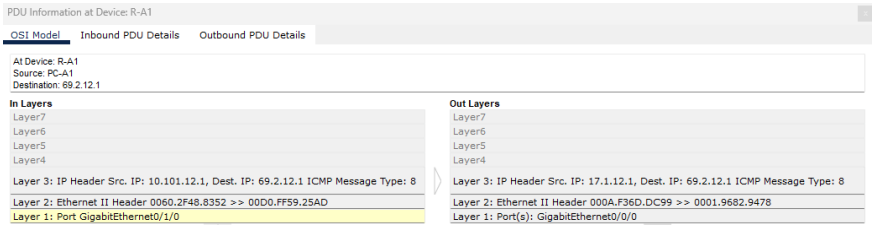

Figure 29 : Trame publique

Configuration du VPN

Le VPN a été configuré sur les routeurs frontières des sites. Pour cela, il a été nécessaire de modifier l'ancienne configuration de la PAT afin qu'elle autorise uniquement le trafic à destination d'Internet, et non celui destiné au site distant.

Sans cette modification, le trafic destiné à passer par le VPN pour atteindre le site distant était transformé par la PAT, ce qui empêchait le bon acheminement du trafic. Voici un exemple de configuration VPN utilisé sur la topologie :

Activation de la licence

```
license boot module c2900 technology-package securityk9
```

Cette commande active la licence nécessaire pour les fonctionnalités de sécurité, telles que le chiffrement IPsec, sur les équipements de la série **Cisco 2900**. La licence **securityk9** est nécessaire pour activer le module de sécurité (cryptographie).

Configuration de base du routeur

```
ip domain-name batman.gotham
crypto key generate rsa general-keys modulus 2048
do write
do reload
```

`ip domain-name batman.gotham` : Définit le nom de domaine pour le routeur. Cela est nécessaire pour la génération des clés RSA et l'établissement des connexions sécurisées.

`crypto key generate rsa general-keys modulus 2048` : Génére une paire de clés RSA (publiques et privées) pour le routeur avec un **modulus de 2048 bits**. Ces clés sont utilisées pour sécuriser les communications.

Configuration de la politique ISAKMP

```
crypto isakmp policy 1
hash sha
authentication pre-share
group 5
lifetime 3600
encryption aes 256
```

`crypto isakmp policy 1` : Crée une politique ISAKMP (Internet Security Association and Key Management Protocol). La politique **1** est la première définition de cette politique.

`hash sha` : Utilise **SHA** (Secure Hash Algorithm) pour le hachage des données.

`authentication pre-share` : Définit l'authentification par clé pré-partagée (PSK), ce qui signifie que le secret partagé doit être configuré sur les deux routeurs pour établir une connexion VPN.

`group 5` : Définit le groupe DH (Diffie-Hellman) utilisé pour l'échange de clés. Le groupe **5** correspond à un échange de clés de **1536 bits**.

`lifetime 3600` : Définit la durée de vie de la session ISAKMP à **3600 secondes** (une heure).

`encryption aes 256` : Utilise **AES 256 bits** pour le chiffrement des données.

Définition de la clé pré-partagée ISAKMP

```
crypto isakmp key WEhAve address 69.1.12.1
```

Cette commande définit la **clé pré-partagée** (PSK) utilisée pour l'authentification entre les routeurs lors de la phase 1 d'ISAKMP. Dans cet exemple, la clé est **"WEhAve"** et l'adresse du pair (peer) est **69.1.12.1**.

Configuration du transform-set IPsec

`crypto ipsec transform-set LR-LYON1` : Crée un ensemble de transformées appelé **LR-LYON1**.

`esp-aes 256 esp-sha-hmac` : Définit les transformées à utiliser pour le chiffrement et l'intégrité des données.

- `esp-aes 256` : Utilise **AES 256 bits** pour le chiffrement.
- `esp-sha-hmac` : Utilise **SHA HMAC** pour garantir l'intégrité des données.

Application de la configuration du crypto map

```
crypto map LR-LYON1 10 ipsec-isakmp
match address ACCES_LR_LYON1
set transform-set LR-LYON1
set peer 69.1.12.1
```

`crypto map LR-LYON1 10 ipsec-isakmp` : Crée une **crypto map** nommée **LR-LYON1** avec un **ID de séquence** de **10**. Ce crypto map est configuré pour utiliser **IPsec avec ISAKMP**.

`match address ACCES_LR_LYON1` : Applique la liste d'accès **ACCES_LR_LYON1** à ce crypto map pour spécifier quel trafic doit être chiffré.

`set transform-set LR-LYON1` : Spécifie l'ensemble de transformées **LR-LYON1** à utiliser pour le chiffrement du trafic.

`set peer 69.1.12.1` : Définit l'adresse IP du pair (le routeur distant) comme **69.1.12.1**.

Test du VPN

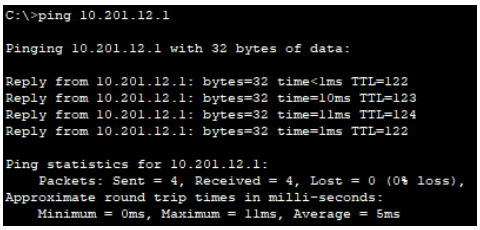

Figure 30 : Ping d'un PC sur le site distant

Nous analysons maintenant une trame passant dans un VPN :

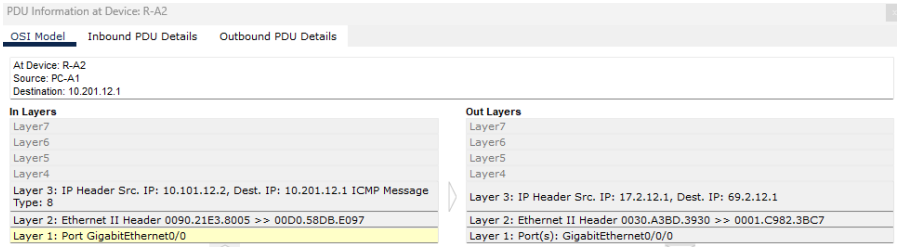

Figure 31 : Packet entrant dans le VPN

Nous observons que l'adresse IP source a été changé par l'adresse IP public du routeur frontière, et que l'adresse source a été changé par l'adresse définie précédemment par le `set peer`.

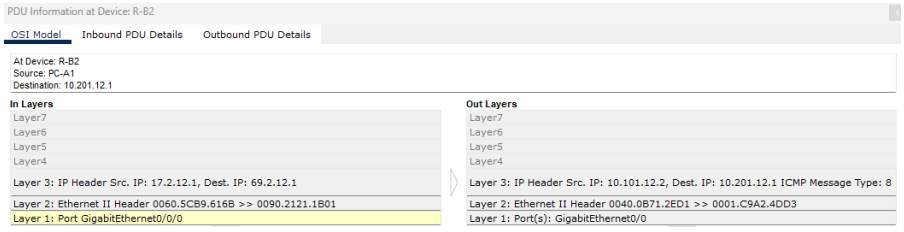

Figure 32 : Packet sortant du VPN

Une fois le packet arrivé dans le réseau privé distant l'adresse source est à nouveau l'adresse privée du PC qui a effectué le ping.

Le protocole utilisé par IPsec pour fournir des services de sécurité aux paquets IP, notamment en garantissant la confidentialité, l'intégrité et l'authenticité des données, est ESP (Encapsulating Security Payload). Voici ce que nous observons lors d'un ping entre deux appareils passant par le tunnel IPsec :

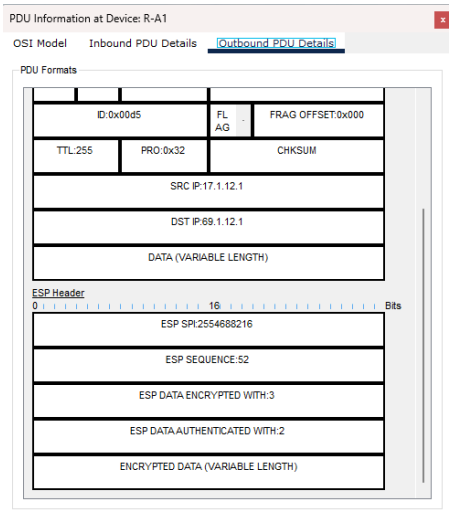

Figure 33 : En-tête ESP

Nous observons un paramètre le SPI qui est un identifiant unique qui figure dans l'en-tête ESP et sert à associer un paquet à un ensemble spécifique de paramètres de sécurité (SA, *Security Association*). En d'autres termes, il permet au destinataire du paquet de savoir comment le traiter (déchiffrement, vérification de l'authenticité, etc.). Lorsqu'un routeur ou un appareil reçoit un paquet ESP avec ce SPI dans son en-tête, il va chercher dans sa base de données de SA pour déterminer comment traiter ce paquet. Les paramètres associés à ce SPI incluent :

- L'algorithme de chiffrement (par exemple, AES).
- L'algorithme d'authentification (par exemple, HMAC-SHA-256).
- Les clés de chiffrement et d'authentification.
- Les options de gestion des séquences pour la protection contre les attaques par rediffusion.

Le SPI va donc être utilisé par le routeur associé au `set peer`. Une fois que le paquet atteint le site distant, l'en-tête ESP disparaît. À partir de ce moment, les adresses IP source et destination normales réapparaissent, permettant une communication classique entre les appareils.

Nous avons l'ESP séquence à 52 qui est utilisé pour assurer l'intégrité des données, le numéro de séquence garantit que les paquets ESP sont reçus dans l'ordre dans lequel ils ont été envoyés et si un paquet arrive avec un numéro de séquence hors de la fenêtre prévue, il est rejeté pour prévenir les attaques.

Nous avons ensuite la mention DATA ENCRYPTED WITH: 3 qui fait référence à l'algorithme ou au mode de chiffrement utilisé pour protéger les données. Enfin nous avons la mention DATA AUTHENTICATED WITH: 2 qui fait référence à l'algorithme utilisé pour l'authentification (HMAC-SHA-256 / SHA-384 / SHA-512…) et l'intégrité des données

encapsulées dans ESP. Ce champ indique le mécanisme choisi pour vérifier que les données n'ont pas été modifiées pendant leur transit.

Le VPN a été appliqué sur les 2 routeurs de bordures des 2 sites ce qui rend l'équilibrage de charge possible :

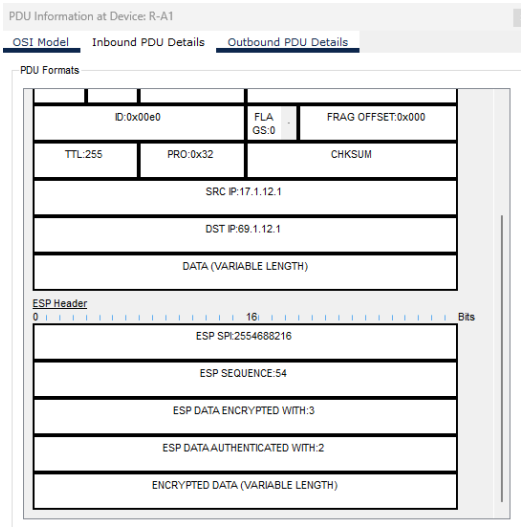

Figure 34 : Packet entrant dans le routeur R-A1

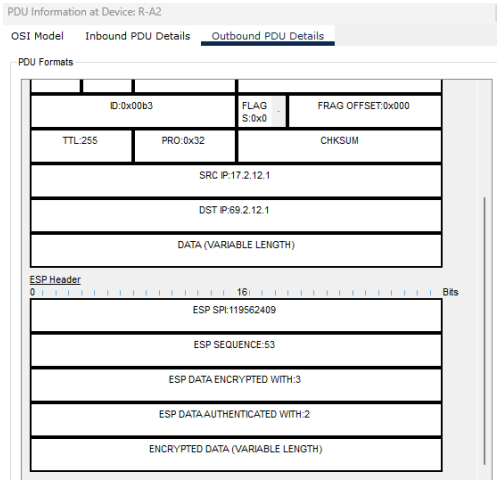

Figure 35 : Packet entrant dans le routeur R-A2

Concernant la partie VPN, il est important de noter un comportement particulier : si je lance un ping depuis le site A vers le site B en premier, les pings depuis le site B vers le site A fonctionnent également par la suite. Cependant, si je commence par effectuer des pings depuis le site B vers le site A, ceux-ci ne passent pas par le VPN. C'est un comportement inhabituel à prendre en compte lors des différents tests.

Appels Inter sites

Exemple de configuration à faire sur les routeurs CME :

```
conf t
dial-peer voice 1 voip
destination-pattern 8...
session target ipv4:10.202.12.252
```

Création d'un dial-peer pour VoIP :

```
dial-peer voice 1 voip
```

Le numéro **1** est simplement un identifiant unique pour ce dial-peer.

voip indique que ce dial-peer concerne des appels VoIP, c'est-à-dire utilisant un réseau IP pour transmettre la voix (et non TDM).

Destination-pattern :

```
destination-pattern 8...
```

Définit les numéros de téléphone ou les modèles de numérotation qui correspondront à ce dial-peer. Les numéros qui commencent par **8** et comportent au total **4 chiffres** (grâce aux 3 points ...) correspondront à ce dial-peer.

```
session target ipv4:10.202.12.252
```

Définit l'adresse IP cible.

J'ai expliqué précédemment comment fonctionnaient les appels intra-sites en utilisant le protocole SCCP, propriétaire de Cisco. Pour les appels inter-sites, le principe est similaire, mais à un moment donné, nous le protocole H.323 (un protocole de signalisation) est utilisé, qui ressemble à SCCP, mais qui est un protocole ouvert.

Comme expliqué précédemment, le protocole utilisé par le téléphone qui lance l'appel est SCCP. Cependant, une fois que le routeur CME a les informations nécessaires, au lieu de renvoyer un message SCCP au téléphone situé localement sur le site, le CME va utiliser le protocole H.323 (port 1720) pour l'appel inter-site. Ce dernier passera par le VPN pour établir la communication entre les sites.

L'adresse IP de destination est celle rentré dans la dialer interface donc l'adresse du routeur CME distant :

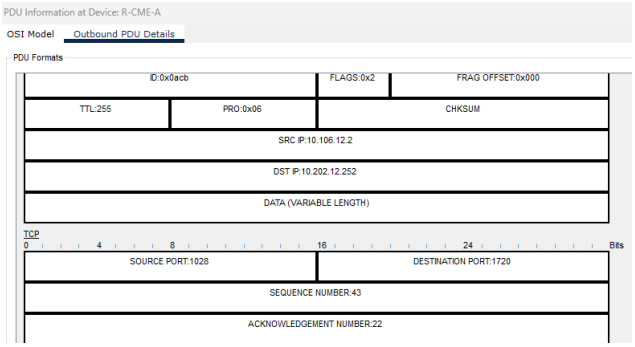

Figure 36 : Préparation du message H.323

Le message va ensuite passer par le VPN comme expliqué précédemment donc en changeant les adresses IPs et en utilisant le protocole ESP etc … :

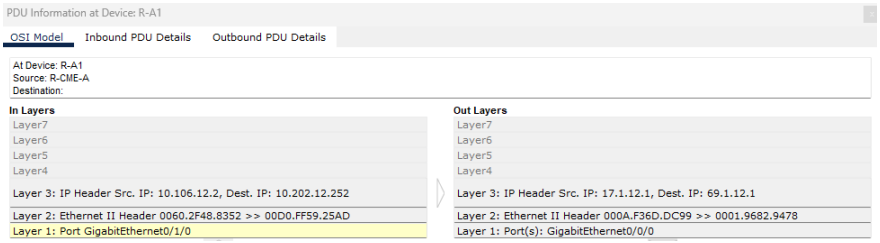

Figure 37 : Rentré dans le VPN

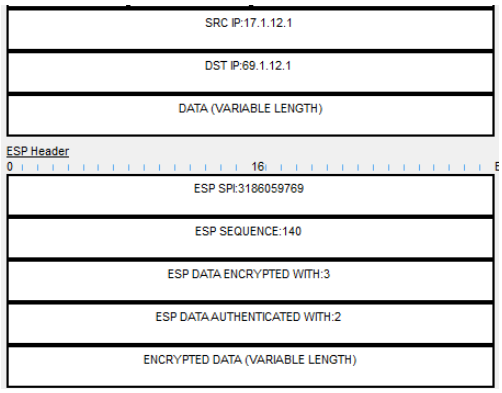

Figure 38 : Nous ne voyons plus le protocole H.323, celui-ci doit être encrypter dans le protocole ESP

Nous observons cependant que l'adresse source n'est pas celle du téléphone effectuant l'appel, ni celle du CME-A, mais plutôt l'une des adresses de l'interface du routeur CME-A. Cela peut être dû au fait qu'avant d'envoyer le message H.323 sur le VPN, celui-ci a effectué un aller-retour via le lien entre le routeur et le switch L3, et a pris l'adresse IP de l'interface entrante :

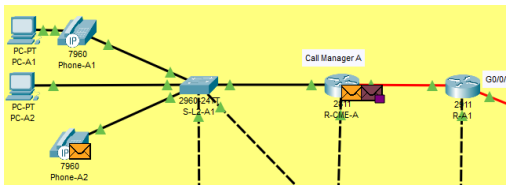

Figure 39 : Création du message H.323

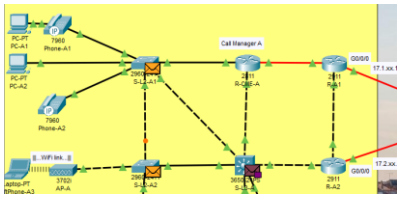

Figure 40 : Envoie sur le switch L3

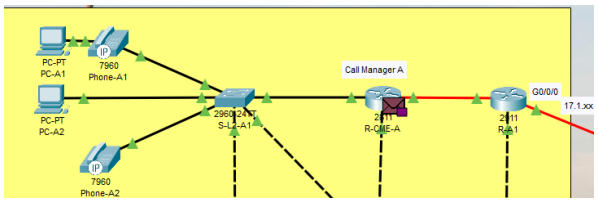

Figure 41 : Retour sur le CME-A en utilisant maintenant l'adresse en face du switch L3

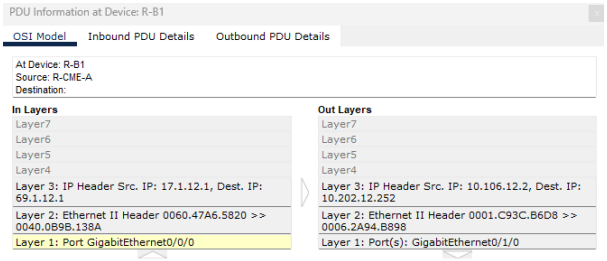

Figure 42 : Sortie du VPN

Nous observons le retour des adresses privées.

Le paquet est envoyé vers le téléphone recevant l'appel, et un nouveau message H.323 est créé. Ce message est ensuite envoyé vers le routeur CME-A du téléphone ayant effectué l'appel, qui lui confirme que l'appel a bien été reçu.

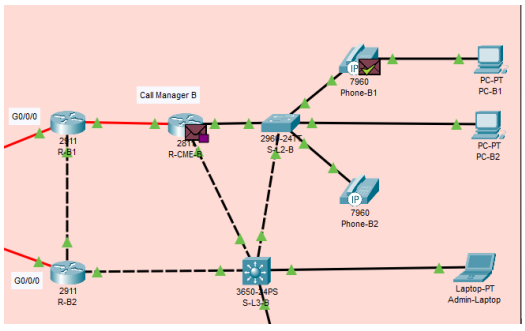

Figure 43 : Le téléphone reçoit l'appel et le routeur envoie un message de bonne réception au routeur CME-A du téléphone ayant effectué l'appel

Figure 44 : Appel reçu

Figure 45 : Appel reçux2

Lorsque nous décrochons cela sera des messages RTP qui seront envoyé directement vers le téléphone distant.

Mise en place de la QOS

QOS de couche 2

Nous devons mettre en place de la QOS pour le VLAN data et ToIP, une priorité CoS de 1 affectée au trafic non tagué (Data) et une priorité CoS de 5 affectée au trafic du VLAN ToIP. Pour cela la QOS a été activé sur le seul switch ayant des équipements dans les VLANs en question.

Nous observons le TCI (Traffic Class Indicator) que nous convertissons en binaire. En prenant les 3 premières valeurs, nous obtenons bien une valeur de priorité de couche 2 CoS (Class of Service) de 1. La QoS de couche 2 disparaît cependant lorsque le paquet quitte le sous-réseau local, car les informations CoS sont généralement perdues ou non utilisées au-delà du réseau local.

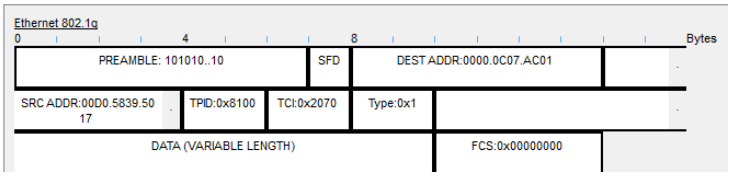

Figure 46 : Ping du serveur WEB et analyse du TCI

La QoS pour les téléphones ne fonctionne pas, que ce soit pour la couche 2 ou la couche 3, en raison d'un bug dans Packet Tracer. Cela empêche l'application correcte des politiques de QoS dans cette simulation.

QOS de couche 3/ basé sur un protocole

Nous devions prioriser les messages échangés dans le VLAN Admin avec une valeur DSCP de 48, et dans le VLAN ToIP avec une valeur DSCP de 46. Cependant, comme mentionné précédemment, la QoS sur les téléphones ne fonctionne pas correctement dans Packet Tracer, ce qui empêche la mise en œuvre effective de ces priorités.

La QoS de niveau 3 doit être appliquée sur un équipement de couche 3, comme un routeur ou un switch L3. Il a été décidé de placer la QoS en sortie des interfaces du switch L3 et du routeur, car j'ai constaté qu'il n'était pas possible de placer une règle de QoS sur une interface virtuelle. Vous trouverez, dans tous les cas, la configuration en annexe.

Nous observons bien une valeur DSCP de 48 si nous convertissons la valeur en hexa en décimale, de plus la priorisation en couche 3 s'applique même en sortant du réseau local, cette priorisation s'applique même dans le réseau du FAI :

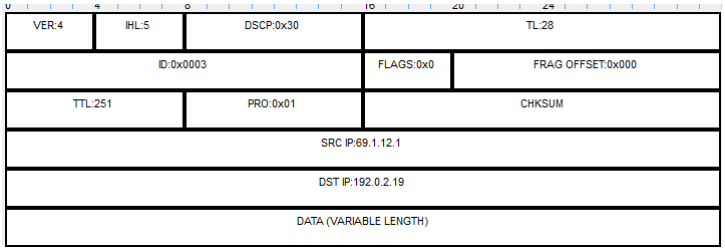

Figure 47 : Ping du PC admin vers le serveur WEB

Nous passons maintenant à la priorisation du protocole H.323 et du protocole RTP :

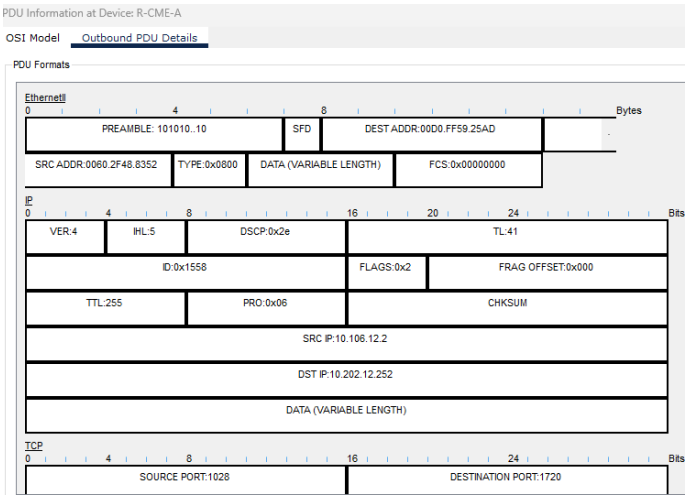

Figure 48 : Priorisation de H.323

Nous observons bien une valeur de priorité de 46 si nous convertissons la valeur en Hexa en décimale.

Voici la même chose pour RTP :

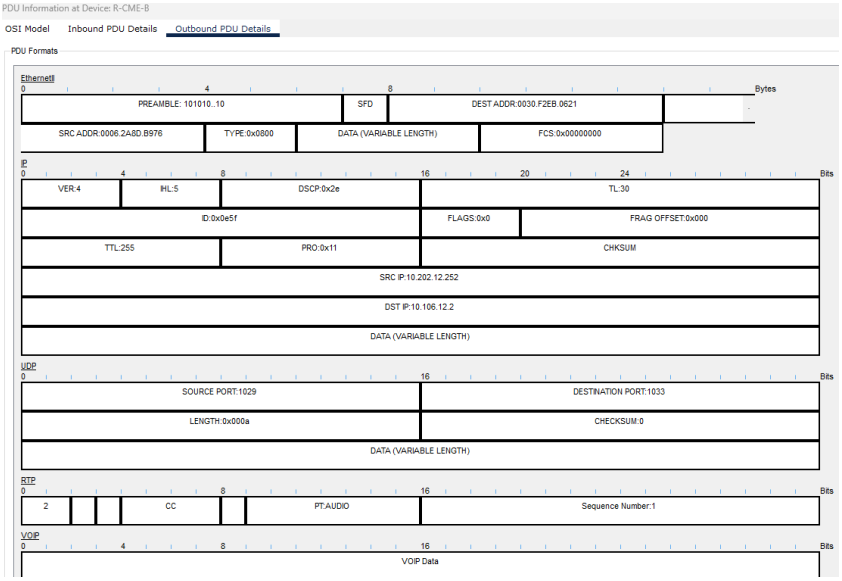

Figure 49 : Priorisation de RTP

Nous observons bien encore une fois la bonne valeur DSCP.

Configuration du WIFI

Le Wi-Fi fonctionne, mais malgré la création d'un WLAN wifi-user et la configuration pour que votre PC client soit associé à ce VLAN, il semble que le PC se connecte au VLAN wifi-management. Malgré la création d'un WLAN spécifique pour les wifi-users et d'une interface dédiée pour ce VLAN, ainsi que l'obligation d'utiliser le pool d'adresses du wifi-user. Cela représente un risque de sécurité, car toute personne connectée à ce PC pourrait

potentiellement accéder au VLAN de gestion du Wi-Fi, ce qui expose le réseau à des vulnérabilités.

Bien que votre PC se connecte au VLAN wifi-management au lieu du VLAN wifi-user, vous obtenez néanmoins une adresse IP et pouvez accéder à Internet. Cela indique que votre serveur RADIUS et votre point d'accès (AP) fonctionnent correctement.

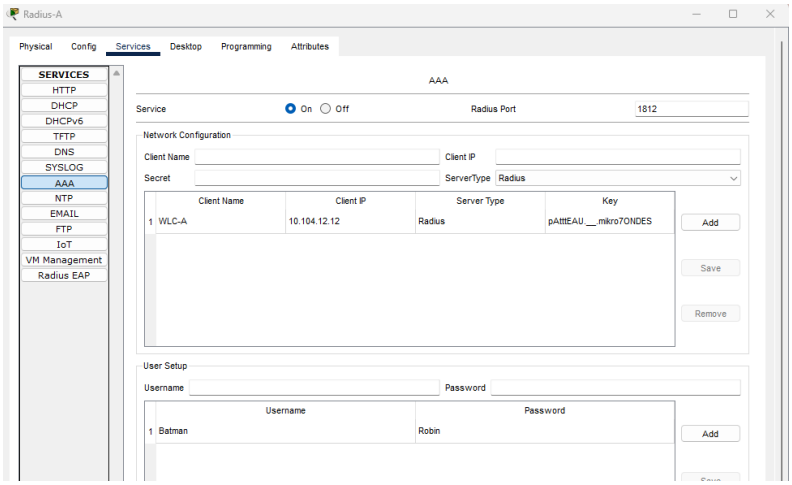

Figure 50 : Serveur Radius

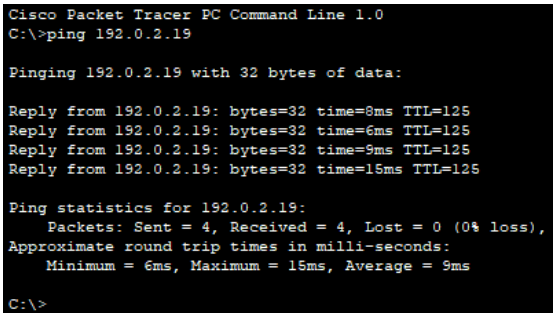

Figure 51 : L'équipement wifi peut ping le serveur WEB

Sécurisation des 2 sites

J'ai dû créer une ACL pour faire en sorte que le VLAN Data ne puisse pas initier de connexion avec les VLANs Admin et WiFi-Mgmt, voici un exemple d'ACL que j'ai appliqué sur les routeurs CME et les switchs L3 :

```
conf t
ip access-list extended BLOCK_DATA_TO_ADMIN_WIFI
remark Bloque les connexions du VLAN Data vers les VLAN Admin et WiFi-Mgmt
deny ip 10.101.12.0 0.0.0.255 10.205.12.0 0.0.0.255
deny ip 10.101.12.0 0.0.0.255 10.104.12.0 0.0.0.255
```

```
permit ip any any
exit

interface FastEthernet0/0.112
ip access-group BLOCK_DATA_TO_ADMIN_WIFI in
```

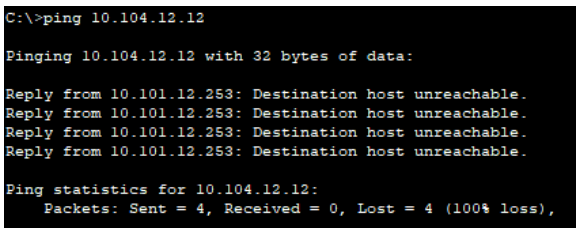

Figure 52 : Impossible d'effectuer un ping vers le VLAN wifi management

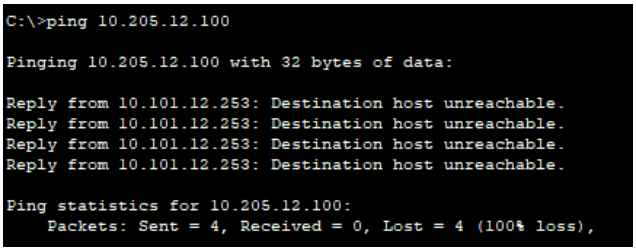

Figure 53 : Impossible d'effectuer un ping vers le VLAN Admin

Le problème est que comme dit précédemment l'appareil connecté au wifi est dans le VLAN wifi management, celui-ci est les PCs ne peuvent pas initier de pings entre eux.

Filtrage des accès sur le routeur frontière

Ce qui a été demandé c'est de de mettre en place, à l'entrée de chacun de nos 2 sites, une ACL interdisant tout trafic non chiffré avec Internet (FTP, Telnet…).

Pour tester cela il suffit d'essayer d'initier une connexion en http depuis un PC pour voir si elle est bloquée, le problème c'est que à chaque fois j'ai ceci ce qui empêche de tester le fonctionnement des ACLs, peu importe si je suis en http ou en https :

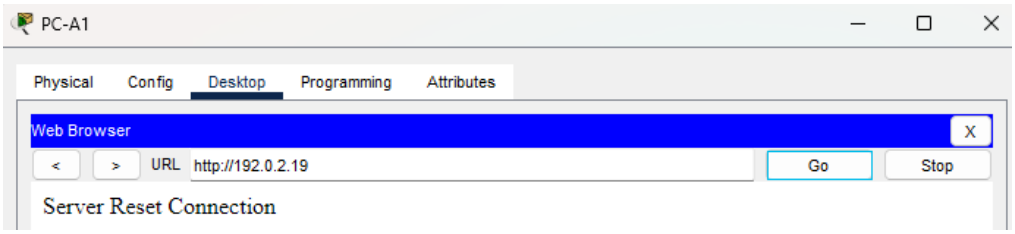

Figure 54 : Impossible de tester en http

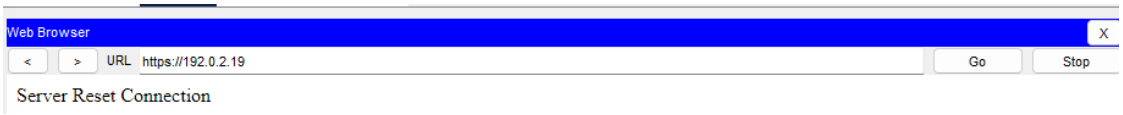

Figure 55 : Impossible de tester en https

Enfin, il reste un point qui ne fonctionne pas : le PC admin peut accéder à de nombreuses ressources, mais il n'arrive pas à pinger les interfaces VLAN des switchs sur le site distant, bien que ces interfaces soient sur le même VLAN.

Conclusion

En conclusion, ce projet m’a permis d’approfondir mes connaissances sur la configuration des VLANs, le routage dynamique avec OSPF et la mise en place de VPN pour interconnecter différents sites. J'ai aussi appris à gérer la qualité de service (QoS) pour prioriser certains types de trafic, et à configurer des équipements tels que les switches de niveau 3 et les routeurs pour assurer une gestion efficace du réseau. Les défis rencontrés, notamment en ce qui concerne la gestion des VLANs sur les points d'accès Wi-Fi et la communication entre les sites, m’ont permis de renforcer ma compréhension de la configuration des réseaux complexes et des protocoles associés. Ce projet m’a ainsi donné une meilleure maîtrise des concepts essentiels pour administrer un réseau d’entreprise.

Annexes

Config LR

R-A1

R-A1 :

Configuration interface FAI :

```
en
conf t
hostname R-A1
inter g0/0/0
ip address 17.1.12.1 255.255.255.252
end
copy run start
```

Configuration interface vers RA-2 :

```
en
conf t
inter
ip address 10.109.12.1 255.255.255.252
end
copy run start
```

Configuration interface vers R-CME-A :

```
en
conf t
inter
ip address 10.107.12.1 255.255.255.252
end
copy run start


!OSPF


conf t
router ospf 1
router-id 1.1.1.1
network 10.107.12.0 0.0.0.3 area 0
network 10.109.12.0 0.0.0.3 area 0
default-information originate
passive-interface g0/0/0

!PAT


conf t
inter g0/1/0
ip nat inside
inter g0/0/0
ip nat outside
exit
ip access-list standard PAT
```

```
permit 10.101.12.0 0.0.0.255
permit 10.102.12.0 0.0.0.255
permit 10.103.12.0 0.0.0.255
permit 10.104.12.0 0.0.0.255
exit
ip nat inside source list PAT interface g0/0/0 overload


!Supprime ancienne PAT
ip access-list standard PAT
no permit 10.101.12.0 0.0.0.255
no permit 10.102.12.0 0.0.0.255
no permit 10.103.12.0 0.0.0.255
no permit 10.104.12.0 0.0.0.255
exit
en
conf t
no ip access-list standard PAT
no ip nat inside source list PAT interface g0/0/0 overload



!IPsec



!Nouvelle PAT
ip access-list extended PAT
```

```
deny ip 10.0.12.0 0.255.0.255 10.0.12.0 0.255.0.255
permit ip 10.0.12.0 0.255.0.255 any
exit
ip nat inside source list PAT interface G0/0/0 overload

exit


!Activer la license
conf t
license boot module c2900 technology-package securityk9




!Début config
en
conf t
ip domain-name batman.gotham
crypto key generate rsa general-keys modulus 2048
do write
do reload

en
conf t
crypto isakmp policy 1
```

```
hash sha
authentication pre-share
group 5
lifetime 3600
encryption aes 256
exit

crypto isakmp key WEhAve address 69.1.12.1
crypto ipsec transform-set LR-LYON1 esp-aes 256 esp-sha-hmac

ip access-list extended ACCES_LR_LYON1
permit ip 10.0.12.0 0.255.0.255 10.0.12.0 0.255.0.255

exit

crypto map LR-LYON1 10 ipsec-isakmp
match address ACCES_LR_LYON1
set transform-set LR-LYON1
set peer 69.1.12.1
exit

int G0/0/0
crypto map LR-LYON1
```

!ACL frontière

conf t

ip access-list extended BLOCK_UNSECURE_TRAFFIC

remark Bloque le trafic non chiffre

deny tcp any any eq 20

deny tcp any any eq 21

deny tcp any any eq 23

deny tcp any any eq 25

deny tcp any any eq 80

deny tcp any any eq 110

deny tcp any any eq 143

remark Autorise le trafic chiffre

permit tcp any any eq 443

permit tcp any any eq 22

permit tcp any any eq 465

permit tcp any any eq 993

permit tcp any any eq 995

permit ip any any

exit

interface g0/0/0

ip access-group BLOCK_UNSECURE_TRAFFIC in

exit

end

copy run start

R-A2

R-A2 :

en

conf t

hostname R-A2

inter g0/0/0

ip address 17.2.12.1 255.255.255.252

no shutdown

end

copy run start

!OSPF

conf t

router ospf 1

router-id 2.2.2.2

network 10.108.12.0 0.0.0.3 area 0

network 10.109.12.0 0.0.0.3 area 0

default-information originate

passive-interface g0/0/0

!PAT

conf t

```
inter g0/0
ip nat inside
inter g0/0/0
ip nat outside
exit
ip access-list standard PAT
permit 10.101.12.0 0.0.0.255
permit 10.102.12.0 0.0.0.255
permit 10.103.12.0 0.0.0.255
permit 10.104.12.0 0.0.0.255
exit
ip nat inside source list PAT interface g0/0/0 overload
```

```
!Supprime ancienne PAT
ip access-list standard PAT
no permit 10.101.12.0 0.0.0.255
no permit 10.102.12.0 0.0.0.255
no permit 10.103.12.0 0.0.0.255
no permit 10.104.12.0 0.0.0.255
exit

en
conf t
no ip access-list standard PAT
no ip nat inside source list PAT interface g0/0/0 overload
```

!IPsec

!Nouvelle PAT

ip access-list extended PAT

deny ip 10.0.12.0 0.255.0.255 10.0.12.0 0.255.0.255

permit ip 10.0.12.0 0.255.0.255 any

exit

ip nat inside source list PAT interface G0/0/0 overload

!Activer la license

license boot module c2900 technology-package securityk9

do write

do reload

!Début config

en

```
conf t
ip domain-name batman.gotham
crypto key generate rsa general-keys modulus 2048
do write
do reload

en
conf t
crypto isakmp policy 1
hash sha
authentication pre-share
group 5
lifetime 3600
encryption aes 256
exit

crypto isakmp key WEhAve address 69.2.12.1
crypto ipsec transform-set LR-LYON2 esp-aes 256 esp-sha-hmac

ip access-list extended ACCES_LR_LYON2
permit ip 10.0.12.0 0.255.0.255 10.0.12.0 0.255.0.255

exit

crypto map LR-LYON2 10 ipsec-isakmp
match address ACCES_LR_LYON2
set transform-set LR-LYON2
set peer 69.2.12.1
```

```
exit

int G0/0/0
crypto map LR-LYON2
end
write
copy run start
```

```
!ACL frontière

conf t
ip access-list extended BLOCK_UNSECURE_TRAFFIC
remark Bloque le trafic non chiffre
deny tcp any any eq 20
deny tcp any any eq 21
deny tcp any any eq 23
deny tcp any any eq 25
deny tcp any any eq 80
deny tcp any any eq 110
deny tcp any any eq 143
```

remark Autorise le trafic chiffre

permit tcp any any eq 443

permit tcp any any eq 22

permit tcp any any eq 465

permit tcp any any eq 993

permit tcp any any eq 995

permit ip any any

exit

interface g0/0/0

ip access-group BLOCK_UNSECURE_TRAFFIC in

exit

end

copy run start

R-CME-A

Config vers R-A1 :

en

conf t

hostname R-CME-A

inter g0/2/0

ip address 10.107.12.2 255.255.255.252

no shut

end

copy run start

Config vers S-L3-A :

```
en
conf t
inter f0/1
ip address 10.106.12.2 255.255.255.252
no shut
end
copy run start


!Routeur on a stick


interface FastEthernet0/0.112
encapsulation dot1Q 112
ip address 10.101.12.253 255.255.255.0
!!!!!!!!


interface FastEthernet0/0.212
encapsulation dot1Q 212
ip address 10.102.12.253 255.255.255.0


interface FastEthernet0/0.312
encapsulation dot1Q 312
ip address 10.103.12.253 255.255.255.0
```

```
interface FastEthernet0/0.412
encapsulation dot1Q 412
ip address 10.104.12.253 255.255.255.0

interface FastEthernet0/0.512
encapsulation dot1Q 512
ip address 10.105.12.253 255.255.255.0



!DHCP

ip dhcp excluded-address 10.101.12.253
ip dhcp excluded-address 10.101.12.252

ip dhcp pool LAN_PCs_A
 network 10.101.12.0 255.255.255.0
 default-router 10.101.12.252

end

conf t
ip dhcp excluded-address 10.102.12.253
ip dhcp excluded-address 10.102.12.252

ip dhcp pool LAN_Phones_A
 network 10.102.12.0 255.255.255.0
```

```
 default-router 10.102.12.252
 option 150 ip 10.102.12.252

end

conf t
ip dhcp excluded-address 10.103.12.253
ip dhcp excluded-address 10.103.12.252

ip dhcp pool LAN_Wifi-Users
 network 10.103.12.0 255.255.255.0
 default-router 10.103.12.252

conf t
ip dhcp excluded-address 10.104.12.253
ip dhcp excluded-address 10.104.12.252
ip dhcp excluded-address 10.104.12.12
ip dhcp excluded-address 10.104.12.212
ip dhcp pool LAN_Wifi-Mng
 network 10.104.12.0 255.255.255.0
 default-router 10.104.12.252
 option 150 ip 10.104.12.252


!Config téléphone
!!!!!!
conf t
telephony-service
```

```
max-ephones 2
max-dn 2
no auto-reg-ephone
ip source-address 10.102.12.252 port 2000
end
conf t
ephone-dn 1
number 7120
exit
ephone-dn 2
number 7121
end
conf t
ephone 1
mac-address 00D0.BCA7.93A4
button 1:1
exit
ephone 2
mac-address 0060.3EC9.E616
button 1:2

!!!!!!!!!!

!HSRP

interface FastEthernet0/0.112
standby 1 ip 10.101.12.252
standby 1 priority 120
```

```
standby 1 preempt
exit
interface FastEthernet0/0.212
standby 1 ip 10.102.12.252
standby 1 priority 120
standby 1 preempt
exit
interface FastEthernet0/0.312
standby 1 ip 10.103.12.252
standby 1 priority 100
standby 1 preempt
exit
interface FastEthernet0/0.412
standby 1 ip 10.104.12.252
standby 1 priority 100
standby 1 preempt
exit
interface FastEthernet0/0.512
standby 1 ip 10.105.12.252
standby 1 priority 120
standby 1 preempt
exit

!OSPF


conf t
router ospf 1
```

router-id 3.3.3.3

network 10.106.12.0 0.0.0.3 area 0

network 10.107.12.0 0.0.0.3 area 0

network 10.101.12.0 0.0.0.255 area 0

network 10.102.12.0 0.0.0.255 area 0

network 10.103.12.0 0.0.0.255 area 0

network 10.104.12.0 0.0.0.255 area 0

passive-interface FastEthernet0/0.112

passive-interface FastEthernet0/0.212

passive-interface FastEthernet0/0.312

passive-interface FastEthernet0/0.412

!Téléphone

conf t

dial-peer voice 1 voip

destination-pattern 8...

session target ipv4:10.202.12.252

end

!QOS

```
conf t

ip access-list extended ToiP_PRIO_2
permit ip 10.102.12.0 0.0.0.255 any
exit

class-map match-any TOIP_2
match access-group name ToiP_PRIO_2
exit
ip access-list extended H323_TRAFFIC
permit tcp any any eq 1720
permit udp any eq 1718 any
permit udp any eq 1719 any
exit

ip access-list extended RTP_TRAFFIC
permit udp any range 16384 32767 any
exit

class-map match-any H323_CLASS
match access-group name H323_TRAFFIC
exit

class-map match-any RTP_CLASS
match access-group name RTP_TRAFFIC
exit
```

```
policy-map QoS_Level3_2

class TOIP_2
set ip dscp ef
bandwidth 80
exit

class H323_CLASS
set ip dscp ef
bandwidth percent 20
class RTP_CLASS
set ip dscp ef
priority percent 40
exit



interface FastEthernet0/1
 service-policy output QoS_Level3_2
exit

interface GigabitEthernet0/2/0
 service-policy output QoS_Level3_2
exit


!ACL data interdit
```

en

conf t

ip access-list extended BLOCK_DATA_TO_ADMIN_WIFI

remark Bloque les connexions du VLAN Data vers les VLAN Admin et WiFi-Mgmt

deny ip 10.101.12.0 0.0.0.255 10.205.12.0 0.0.0.255

deny ip 10.101.12.0 0.0.0.255 10.104.12.0 0.0.0.255

permit ip any any

exit

interface FastEthernet0/0.112

ip access-group BLOCK_DATA_TO_ADMIN_WIFI in

exit

S-L2-A1

R-A1 :

en

conf t

hostname R-A1

inter g0/0/0

ip address 17.1.12.1 255.255.255.252

R-A2 :

en

conf t

hostname R-A2

inter g0/0/0

ip address 17.2.12.1 255.255.255.252

no shutdown

end

copy run start

Config des VLANs :

en

conf t

vlan 112

name Data

exit

vlan 212

name ToIP

exit

vlan 312

name WiFi-Users

exit

vlan 412

name WiFi-Mgmt

exit

vlan 512

name Admin

exit

vlan 666

name poublelle

```
end
copy run start

en
conf t
vlan 666
name Poubelle
end
copy run start
```

ATTRIBUTION DE PORTS DANS LES VLANS :

```
en
conf t
inter fa0/1
switchport mode access
switchport access vlan 112
switchport voice vlan 212
spanning-tree portfast
spanning-tree bpduguard enable

exit
inter fa0/2
switchport mode access
switchport access vlan 112
switchport port-security
switchport port-security maximum 3
```

```
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport nonegotiate
spanning-tree portfast
spanning-tree bpduguard enable
exit
inter fa0/3
switchport mode access
switchport voice vlan 212
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport nonegotiate
spanning-tree portfast
spanning-tree bpduguard enable
end
copy run start

en
conf t
inter fa0/1
no shut
inter fa0/2
no shut
inter fa0/3
no shut
inter fa0/24
```

```
no shut
inter g0/2
no shut
inter g0/1
no shut
end
copy run start
```

config trunk :

```
interface range g0/1 - 2, f0/24
no shut
switchport mode trunk
switchport trunk allowed vlan 112,212,312,412,512
```

!QOS

```
en
conf t
mls qos
int range f0/1-2
mls qos cos 1
int f0/3
mls qos cos 5
int range f0/1-23
mls qos trust cos
```

exit

en

conf t

ip default-gateway 10.105.12.252

S-L2-A2

R-A1 :

en

conf t

hostname R-A1

inter g0/0/0

ip address 17.1.12.1 255.255.255.252

R-A2 :

en

conf t

hostname R-A2

inter g0/0/0

ip address 17.2.12.1 255.255.255.252

no shutdown

end

copy run start

en

conf t

```
vlan 112
name Data
exit
vlan 212
name ToIP
exit
vlan 312
name WiFi-Users
exit
vlan 412
name WiFi-Mgmt
exit
vlan 512
name Admin
exit
vlan 666
name poublelle
end
copy run start

en
conf t
vlan 666
name Poubelle
end
copy run start
```

ACTIVATION DES PORTS ETEINTS :

en

conf t

inter fa0/24

no shut

inter g0/1

no shut

inter f0/23

no shut

inter g1/0/3

no shut

end

copy run start

config trunk :

interface range g0/2, f0/24

no shut

switchport mode trunk

switchport trunk allowed vlan 112,212,312,412,512

!WIFI

en

```
conf t
inter g0/1
switchport mode trunk
switchport trunk allowed vlan 312,412
switchport native vlan 412
end
conf t
inter f0/23
switchport mode access
switchport access vlan 412
end
```

```
en
conf t
ip default-gateway 10.105.12.252
```

S-L3-A

Config vers R-A2 :

```
en
conf t
hostname S-L3-A
inter g1/0/5
no switchport
ip address 10.108.12.1 255.255.255.252
no shut
end
copy run start
```

Config vers R-CME-A :

```
en
conf t
inter g1/0/1
no switchport
ip address 10.106.12.1 255.255.255.252
no shut
end
copy run start
```

```
en
conf t
vlan 112
name Data
exit
vlan 212
name ToIP
exit
vlan 312
name WiFi-Users
exit
vlan 412
name WiFi-Mgmt
exit
```

```
vlan 512
name Admin
exit
vlan 666
name poublelle
end
copy run start
en
conf t
vlan 666
name Poubelle
end
copy run start
```

```
en
conf t
inter g1/0/2
no shutdown
inter g1/0/3
no shutdown
inter g1/0/4
no shutdown
end
copy run start
```

config trunk :

interface range g1/0/2, g1/0/3

no shut

switchport mode trunk

switchport trunk allowed vlan 112,212,312,412,512

!SVI dans les différents VLAN

inter vlan 112

ip address 10.101.12.254 255.255.255.0

inter vlan 212

ip address 10.102.12.254 255.255.255.0

inter vlan 312

ip address 10.103.12.254 255.255.255.0

inter vlan 412

ip address 10.104.12.254 255.255.255.0

inter vlan 512

ip address 10.105.12.254 255.255.255.0

!HSRP

conf t

interface vlan 112

standby 1 ip 10.101.12.252

standby 1 priority 100

standby 1 preempt

exit

interface vlan 212

standby 1 ip 10.102.12.252

standby 1 priority 100

standby 1 preempt

exit

interface vlan 312

standby 1 ip 10.103.12.252

standby 1 priority 120

standby 1 preempt

exit

interface vlan 412

standby 1 ip 10.104.12.252

standby 1 priority 120

standby 1 preempt

exit

inter vlan 512

standby 1 ip 10.105.12.252

standby 1 priority 100

standby 1 preempt

exit

!OSPF

conf t

router ospf 1

router-id 4.4.4.4

network 10.106.12.0 0.0.0.3 area 0

network 10.108.12.0 0.0.0.3 area 0

network 10.101.12.0 0.0.0.255 area 0

network 10.102.12.0 0.0.0.255 area 0

network 10.103.12.0 0.0.0.255 area 0

network 10.104.12.0 0.0.0.255 area 0

passive-interface vlan 112

passive-interface vlan 212

passive-interface vlan 312

passive-interface vlan 412

!Config vers radius

en

conf t

inter g1/0/4

switchport mode access

switchport access vlan 412

```
end

!QOS

conf t

ip access-list extended ToiP_PRIO_2
permit ip 10.102.12.0 0.0.0.255 10.202.12.0 0.0.0.255
exit


class-map match-any TOIP_2
match access-group name ToiP_PRIO_2
exit


policy-map QoS_Level3_2

class TOIP_2
set ip dscp ef
bandwidth 80
exit


interface g1/0/1
 service-policy output QoS_Level3_2
```

exit

interface GigabitEthernet1/0/5

service-policy output QoS_Level3_2

exit

!ACL data interdit

en

conf t

ip access-list extended BLOCK_DATA_TO_ADMIN_WIFI

remark Bloque les connexions du VLAN Data vers les VLAN Admin et WiFi-Mgmt

deny ip 10.101.12.0 0.0.0.255 10.205.12.0 0.0.0.255

deny ip 10.101.12.0 0.0.0.255 10.104.12.0 0.0.0.255

permit ip any any

exit

interface vlan 112

ip access-group BLOCK_DATA_TO_ADMIN_WIFI in

exit

WLC

login : I AM BATMAN

mdp : gralopeKOIRON789==a,,

Shared Secret : pAtttEAU.__.mikro7ONDES

usersname : Batman

password : Robin

Config LY:

R-B1

Configuration interface vers FAI :

```
en
conf t
hostname R-B1
inter g0/0/0
ip address 69.1.12.1 255.255.255.252
no shut
end
copy run start
```

Configuration interface vers RB-2 :

```
en
conf t
inter g0/2
ip address 10.209.12.1 255.255.255.252
no shut
end
copy run start
```

Configuration interface vers R-CME-B :

```
en
conf t
inter g0/1/0
ip address 10.206.12.1 255.255.255.252
no shut
end
copy run start

!OSPF
conf t
router ospf 1
router-id 1.1.1.1
network 10.206.12.0 0.0.0.3 area 0
network 10.209.12.0 0.0.0.3 area 0
default-information originate
passive-interface g0/0/0


!PAT

conf t
inter g0/1/0
ip nat inside
inter g0/0/0
ip nat outside
```

```
exit
no ip access-list standard PAT
no permit 10.201.12.0 0.0.0.255
no permit 10.202.12.0 0.0.0.255
no permit 10.205.12.0 0.0.0.255
exit
no ip nat inside source list PAT interface g0/0/0 overload


!Ancienne PAT
ip access-list standard PAT
no permit 10.201.12.0 0.0.0.255
no permit 10.202.12.0 0.0.0.255
no permit 10.205.12.0 0.0.0.255
exit
en
conf t
no ip access-list standard PAT
no ip nat inside source list PAT interface g0/0/0 overload



!IPsec
```

```
!Nouvelle PAT
ip access-list extended PAT
deny ip 10.0.12.0 0.255.0.255 10.0.12.0 0.255.0.255
permit ip 10.0.12.0 0.255.0.255 any
exit
ip nat inside source list PAT interface G0/0/0 overload



!Activer la license
license boot module c2900 technology-package securityk9


do write
do reload



!Début config
en
conf t
ip domain-name batman.gotham
crypto key generate rsa general-keys modulus 2048
do write
do reload

en
```

```
conf t
crypto isakmp policy 1
hash sha
authentication pre-share
group 5
lifetime 3600
encryption aes 256
exit

crypto isakmp key WEhAve address 17.1.12.1
crypto ipsec transform-set LYON-LR1 esp-aes 256 esp-sha-hmac

ip access-list extended ACCES_LYON_LR1
permit ip 10.0.12.0 0.255.0.255 10.0.12.0 0.255.0.255
exit

crypto map LYON-LR1 10 ipsec-isakmp
match address ACCES_LYON_LR1
set transform-set LYON-LR1
set peer 17.1.12.1
exit

int G0/0/0
crypto map LYON-LR1
end
write
```

!ACL frontière

conf t

ip access-list extended BLOCK_UNSECURE_TRAFFIC

remark Bloque le trafic non chiffre

deny tcp any any eq 20

deny tcp any any eq 21

deny tcp any any eq 23

deny tcp any any eq 25

deny tcp any any eq 80

deny tcp any any eq 110

deny tcp any any eq 143

remark Autorise le trafic chiffre

permit tcp any any eq 443

permit tcp any any eq 22

permit tcp any any eq 465

permit tcp any any eq 993

permit tcp any any eq 995

permit ip any any

exit

interface g0/0/0

ip access-group BLOCK_UNSECURE_TRAFFIC in

exit

end

copy run start

R-B2

Config vers S-L3-B

en

conf t

hostname R-B2

inter g0/0

ip address 10.208.12.2 255.255.255.252

no shutdown

end

copy run start

Config vers R-B1

en

conf t

inter g0/1

ip address 10.209.12.2 255.255.255.252

no shutdown

end

copy run start

Config vers FAI Internet

en

conf t

inter g0/0/0

```
ip address 69.2.12.1 255.255.255.252
no shutdown
end
copy run start


!OSPF
conf t
router ospf 1
router-id 2.2.2.2
network 10.208.12.0 0.0.0.3 area 0
network 10.209.12.0 0.0.0.3 area 0
default-information originate
passive-interface g0/0/0


!PAT
conf t
inter g0/0
ip nat inside
inter g0/0/0
ip nat outside
exit
ip access-list standard PAT
permit 10.201.12.0 0.0.0.255
permit 10.202.12.0 0.0.0.255
permit 10.205.12.0 0.0.0.255
exit
```

```
ip nat inside source list PAT interface g0/0/0 overload



!Ancienne PAT
ip access-list standard PAT
no permit 10.201.12.0 0.0.0.255
no permit 10.202.12.0 0.0.0.255
no permit 10.205.12.0 0.0.0.255
exit
en
conf t
no ip access-list standard PAT
no ip nat inside source list PAT interface g0/0/0 overload



!IPsec



!Nouvelle PAT
ip access-list extended PAT
deny ip 10.0.12.0 0.255.0.255 10.0.12.0 0.255.0.255
permit ip 10.0.12.0 0.255.0.255 any
exit
```

```
ip nat inside source list PAT interface G0/0/0 overload
```

```
!Activer la license
license boot module c2900 technology-package securityk9

do write
do reload
```

```
!Début config
en
conf t
ip domain-name batman.gotham
crypto key generate rsa general-keys modulus 2048
do write
do reload

en
conf t
crypto isakmp policy 1
hash sha
authentication pre-share
```

```
group 5
lifetime 3600
encryption aes 256
exit

crypto isakmp key WEhAve address 17.2.12.1
crypto ipsec transform-set LYON-LR2 esp-aes 256 esp-sha-hmac

ip access-list extended ACCES_LYON_LR2
permit ip 10.0.12.0 0.255.0.255 10.0.12.0 0.255.0.255
exit

crypto map LYON-LR2 10 ipsec-isakmp
match address ACCES_LYON_LR2
set transform-set LYON-LR2
set peer 17.2.12.1
exit

int G0/0/0
crypto map LYON-LR2
end
write
copy run start



!ACL frontière
```

conf t

ip access-list extended BLOCK_UNSECURE_TRAFFIC

remark Bloque le trafic non chiffre

deny tcp any any eq 20

deny tcp any any eq 21

deny tcp any any eq 23

deny tcp any any eq 25

deny tcp any any eq 80

deny tcp any any eq 110

deny tcp any any eq 143

remark Autorise le trafic chiffre

permit tcp any any eq 443

permit tcp any any eq 22

permit tcp any any eq 465

permit tcp any any eq 993

permit tcp any any eq 995

permit ip any any

exit

interface g0/0/0

ip access-group BLOCK_UNSECURE_TRAFFIC in

exit

end

copy run start

R-CME-B

Config vers R-B1 :

```
en
conf t
hostname R-CME-B
inter g0/0/0
ip address 10.206.12.2 255.255.255.252
no shut
end
copy run start
```

Config vers S-L3-B :

```
en
conf t
inter f0/1
ip address 10.207.12.2 255.255.255.252
no shut
end
copy run start
```

```
en
conf t
interface f0/0
no shut
switchport mode trunk
```

```
switchport trunk allowed vlan 112,212,312,412,512
```

```
!Routeur on a stick

conf t

interface FastEthernet0/0.112
encapsulation dot1Q 112
ip address 10.201.12.253 255.255.255.0

interface FastEthernet0/0.212
encapsulation dot1Q 212
ip address 10.202.12.253 255.255.255.0

interface FastEthernet0/0.512
encapsulation dot1Q 512
ip address 10.205.12.253 255.255.255.0

end

!DHCP
```

```
conf t

ip dhcp excluded-address 10.201.12.253
ip dhcp excluded-address 10.201.12.252
ip dhcp pool LAN_PCs_B
 network 10.201.12.0 255.255.255.0
 default-router 10.201.12.252

end

conf t
ip dhcp excluded-address 10.202.12.253
ip dhcp excluded-address 10.202.12.252

ip dhcp pool LAN_Phones_B
 network 10.202.12.0 255.255.255.0
 default-router 10.202.12.252
 option 150 ip 10.202.12.252

end

conf t
ip dhcp excluded-address 10.205.12.253
ip dhcp excluded-address 10.205.12.252

ip dhcp pool PCs_Admin
 network 10.205.12.0 255.255.255.0
 default-router 10.205.12.252
```

```
!Config téléphone
!!!!!!
conf t
telephony-service
max-ephones 2
max-dn 2
no auto-reg-ephone
ip source-address 10.202.12.252 port 2000
end
conf t
ephone-dn 1
number 8120
exit
ephone-dn 2
number 8121
end
conf t
ephone 1
mac-address 000C.CF52.73D2
button 1:1
exit
ephone 2
mac-address 0002.1772.77D3
button 1:2
```

!HSRP

interface FastEthernet0/0.112

standby 1 ip 10.201.12.252

standby 1 priority 100

standby 1 preempt

exit

interface FastEthernet0/0.212

standby 1 ip 10.202.12.252

standby 1 priority 120

standby 1 preempt

exit

interface FastEthernet0/0.512

standby 1 ip 10.205.12.252

standby 1 priority 120

standby 1 preempt

exit

!OSPF

conf t

router ospf 1

router-id 3.3.3.3

network 10.207.12.0 0.0.0.3 area 0

network 10.206.12.0 0.0.0.3 area 0

network 10.201.12.0 0.0.0.255 area 0

```
network 10.202.12.0 0.0.0.255 area 0
network 10.205.12.0 0.0.0.255 area 0

passive-interface FastEthernet0/0.112
passive-interface FastEthernet0/0.212
passive-interface FastEthernet0/0.512
```

```
!Téléphone VPN
conf t
dial-peer voice 1 voip
destination-pattern 7...
session target ipv4:10.102.12.252
end
```

```
!QOS
```

```
conf t
ip access-list extended ADMIN_PRIO
 permit ip 10.205.12.0 0.0.0.255 any
exit
ip access-list extended ToiP_PRIO
permit ip 10.202.12.0 0.0.0.255 any
```

```
exit
ip access-list extended H323_TRAFFIC
permit tcp any any eq 1720
permit udp any eq 1718 any
permit udp any eq 1719 any
exit

ip access-list extended RTP_TRAFFIC
permit udp any range 16384 32767 any
exit

class-map match-any H323_CLASS
match access-group name H323_TRAFFIC
exit

class-map match-any RTP_CLASS
match access-group name RTP_TRAFFIC
exit


class-map match-any TOIP
match access-group name ToiP_PRIO
exit

class-map match-any ADMIN
 match access-group name ADMIN_PRIO
exit
```

```
policy-map QoS_Level3
 class ADMIN
  set ip dscp cs6

class TOIP
set ip dscp ef
bandwidth 80
exit
class H323_CLASS
set ip dscp ef
bandwidth percent 20
class RTP_CLASS
set ip dscp ef
priority percent 40
exit

interface FastEthernet0/1
 service-policy output QoS_Level3
exit

interface GigabitEthernet0/0/0
 service-policy output QoS_Level3
exit
```

!ACL data interdit

ip access-list extended BLOCK_DATA_TO_ADMIN_WIFI

remark Bloque les connexions du VLAN Data vers les VLAN Admin et WiFi-Mgmt

deny ip 10.201.12.0 0.0.0.255 10.205.12.0 0.0.0.255

deny ip 10.201.12.0 0.0.0.255 10.104.12.0 0.0.0.255

permit ip any any

exit

interface FastEthernet0/0.112

ip access-group BLOCK_DATA_TO_ADMIN_WIFI in

exit

S-L2-B

R-A1 :

en

conf t

hostname R-A1

inter g0/0/0

ip address 17.1.12.1 255.255.255.252

R-A2 :

en

conf t

```
hostname R-A2
inter g0/0/0
ip address 17.2.12.1 255.255.255.252
no shutdown
end
copy run start


en
conf t
vlan 112
name Data
exit
vlan 212
name ToIP
exit
vlan 312
name WiFi-Users
exit
vlan 412
name WiFi-Mgmt
exit
vlan 512
name Admin
exit
vlan 666
name poublelle
end
```

copy run start

en

conf t

vlan 666

name Poubelle

end

copy run start

en

conf t

inter fa0/1

no shut

inter fa0/2

no shut

inter fa0/3

no shut

inter g0/1

no shut

inter g0/2

no shut

ATTRIBUTION DE PORTS DANS LES VLANS :

en

conf t

```
inter fa0/1
switchport mode access
switchport access vlan 112
switchport voice vlan 212
spanning-tree portfast
spanning-tree bpduguard enable

exit
inter fa0/2
switchport mode access
switchport access vlan 112
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport nonegotiate
spanning-tree portfast
spanning-tree bpduguard enable
exit
inter fa0/3
switchport mode access
switchport voice vlan 212
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport nonegotiate
spanning-tree portfast
```

spanning-tree bpduguard enable

end

copy run start

config trunk :

en

conf t

interface range g0/1 - 2

no shut

switchport mode trunk

switchport trunk allowed vlan 112,212,312,412,512

!QOS

en

conf t

mls qos

int range f0/1-2

mls qos cos 1

int f0/3

mls qos cos 5

int range f0/1-23

mls qos trust cos

exit

S-L3-B

Config vers R-B2 :

```
en
conf t
hostname S-L3-B
inter g1/0/22
no switchport
ip address 10.208.12.1 255.255.255.252
no shut
end
copy run start
```

Config vers R-CME-B :

```
en
conf t
inter g1/0/23
no switchport
ip address 10.207.12.1 255.255.255.252
no shut
end
copy run start
```

```
en
conf t
```

```
vlan 112
name Data
exit
vlan 212
name ToIP
exit
vlan 312
name WiFi-Users
exit
vlan 412
name WiFi-Mgmt
exit
vlan 512
name Admin
end
copy run start

en
conf t
vlan 666
name Poubelle
end
copy run start

en
conf t
inter g1/0/1
switchport mode access
```

```
switchport access vlan 512
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security mac-address sticky
switchport nonegotiate
spanning-tree portfast
spanning-tree bpduguard enable
```

```
en
conf t
interface g1/0/24
no shut
switchport mode trunk
switchport trunk allowed vlan 112,212,312,412,512

en
copy run start
```

```
inter vlan 112
ip address 10.201.12.254 255.255.255.0
inter vlan 212
ip address 10.202.12.254 255.255.255.0
inter vlan 512
```

```
ip address 10.205.12.254 255.255.255.0



!HSRP


conf t
interface vlan 112
standby 1 ip 10.201.12.252
standby 1 priority 120
standby 1 preempt
exit
interface vlan 212
standby 1 ip 10.202.12.252
standby 1 priority 100
standby 1 preempt
exit
interface vlan 512
standby 1 ip 10.205.12.252
standby 1 priority 100
standby 1 preempt
exit



!OSPF


conf t
```

```
router ospf 1
router-id 4.4.4.4
network 10.207.12.0 0.0.0.3 area 0
network 10.208.12.0 0.0.0.3 area 0

network 10.201.12.0 0.0.0.255 area 0
network 10.202.12.0 0.0.0.255 area 0
network 10.205.12.0 0.0.0.255 area 0

passive-interface vlan 112
passive-interface vlan 212
passive-interface vlan 512
```

!QOS

```
conf t
ip access-list extended ADMIN_PRIO
 permit ip 10.205.12.0 0.0.0.255 any
exit
ip access-list extended ToiP_PRIO
permit ip 10.202.12.0 0.0.0.255 any
exit
```

```
class-map match-any TOIP
match access-group name ToiP_PRIO
exit

class-map match-any ADMIN
 match access-group name ADMIN_PRIO
exit

policy-map QoS_Level3
 class ADMIN
  set ip dscp cs6

class TOIP
set ip dscp ef
bandwidth 80
exit




interface g1/0/22
 service-policy output QoS_Level3
exit

interface GigabitEthernet1/0/23
 service-policy output QoS_Level3
exit
```

```
interface GigabitEthernet1/0/24
 service-policy output QoS_Level3
exit



!ACL data interdit



ip access-list extended BLOCK_DATA_TO_ADMIN_WIFI
remark Bloque les connexions du VLAN Data vers les VLAN Admin et WiFi-Mgmt
deny ip 10.201.12.0 0.0.0.255 10.205.12.0 0.0.0.255
deny ip 10.201.12.0 0.0.0.255 10.104.12.0 0.0.0.255
permit ip any any
exit

interface vlan 112
ip access-group BLOCK_DATA_TO_ADMIN_WIFI in
exit
```

Config FAI

R-FAI-LR

Config vers le routeur R-A1 :

```
en
conf t
inter g0/1/0
ip address 17.1.12.2 255.255.255.252
no shut
end
copy run start
```

Config vers le routeur R-A2 :

```
en
conf t
inter g0/2/0
ip address 17.2.12.2 255.255.255.252
no shut
end
copy run start
```

```
!OSPF

conf t
router ospf 1
router-id 1.1.1.1
network 17.1.12.0 0.0.0.3 area 0
network 17.2.12.0 0.0.0.3 area 0
network 192.0.2.0 0.0.0.255 area 0
passive-interface g0/1/0
passive-interface g0/2/0
```

R-FAI-LY

Config vers le routeur R-B1 :

```
en
conf t
hostname R-FAI-LY
inter g0/1/0
ip address 69.1.12.2 255.255.255.252
no shut
end
copy run start
```

Config vers le routeur R-B2 :

```
en
conf t
inter g0/2/0
ip address 69.2.12.2 255.255.255.252
no shut
end
copy run start
```

```
conf t
router ospf 1
router-id 2.2.2.2
network 69.1.12.0 0.0.0.3 area 0
network 69.2.12.0 0.0.0.3 area 0
```

network 192.0.2.0 0.0.0.255 area 0

passive-interface g0/1/0

passive-interface g0/2/0

Switch6

R-A1 :

en

conf t

hostname R-A1

inter g0/0/0

ip address 17.1.12.1 255.255.255.252

R-A2 :

en

conf t

hostname R-A2

inter g0/0/0

ip address 17.2.12.1 255.255.255.252

no shutdown

end

copy run start