heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud

iICT

Labo 1 - VoIP /CCUM

Auteurs : Joris Blatti

Version 1.0, Septembre 2010

Objectifs du laboratoire

Ce laboratoire est composé de le premier d'une suite de manipulations dans laquelle nous allons étudier la configuration d'un réseau VoIP avec Cisco Unified Communications Manager Express CUCME.

Les objectifs de cette partie sont

- *Configuration du réseau LAN pour l'intégration de la VoIP*
- *Configuration des VLAN VoIP et Data*
- *Configuration des mécanismes de sécurité des ports LAN*

Rendu

- Vous pouvez noter les réponses directement dans ce document, dans les cases bleues. Les fichiers de configuration sont à joindre en annexe.
- L'échéance du rapport est avant la prochaine séance.
- Le rapport en PDF est à remettre par email à l'adresse labo.vip.heig _at_ gmail.com

1 Introduction

Ce laboratoire a pour sujet Cisco Unified Communications Manager Express (CUCME), connu également sous le nom de Cisco CallManager Express (CCME). Il vise à implémenter sur routeur, une solution légère et efficace de téléphonie sur IP dans le cadre d'une entreprise, étalée sur plusieurs petits sites (moins de 250 téléphones par site). Cette solution a été préférée à l'installation plus onéreuse d'un cluster de Cisco Unified Communications Manager, offrant néanmoins davantage de fonctionnalités.

Décomposé en 4 parties successives, cette première phase a pour objectif la mise en place, pour chaque groupe, de l'infrastructure réseau nécessaire pour l'utilisation de CallManager Express. Les différents sites sont interconnectés à l'aide d'un Gatekeeper H.323. Ce dernier ne sera pas atteignable lors de ce laboratoire.

1.1 Architecture du réseau

L'architecture du réseau avec un site est montrée Figure 1.

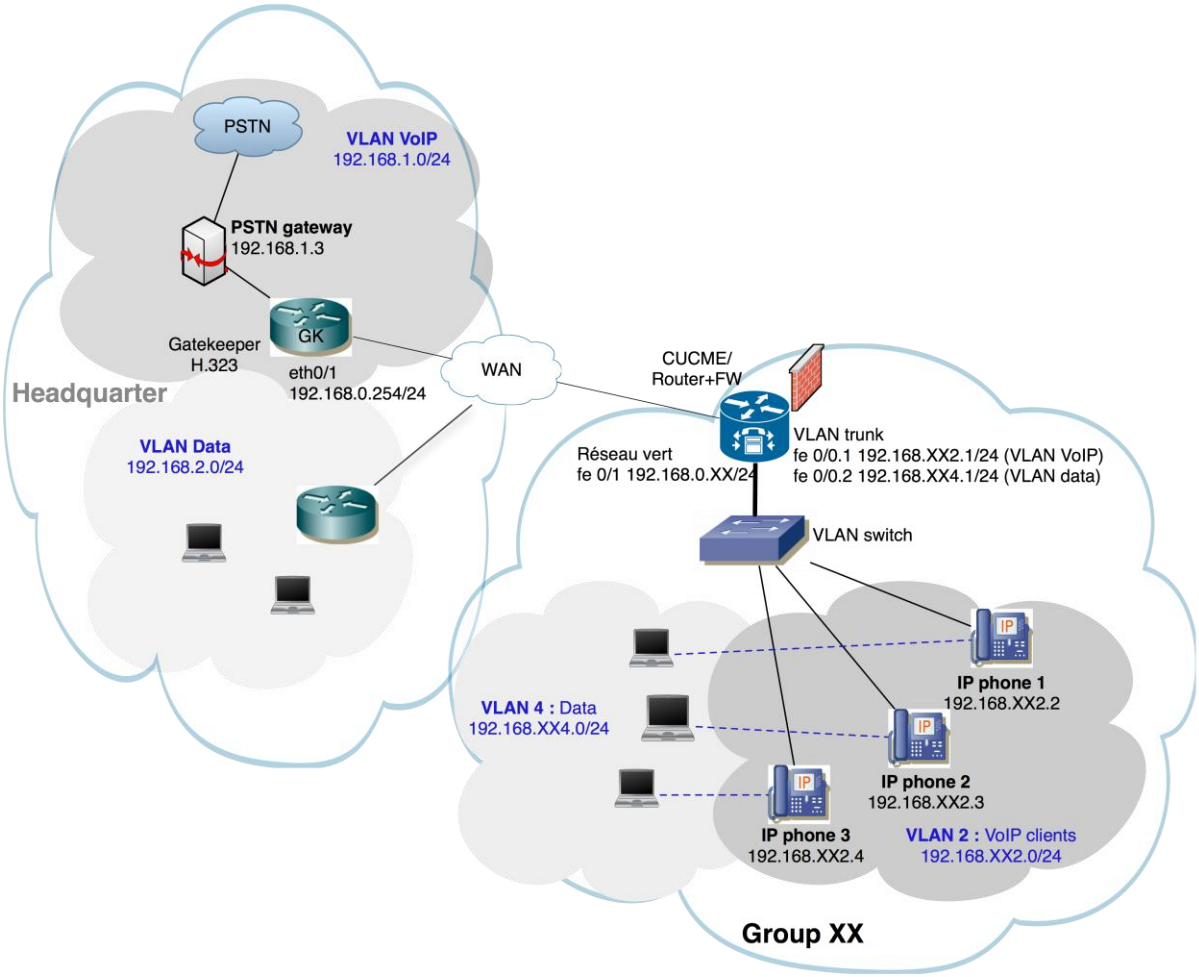

Figure 1 : Architecture du réseau avec un site

Dans cette figure, XX représente le numéro de votre groupe avec deux chiffres, par exemple XX=10.

Les PC et laptops sont connectés sur les ports switches des téléphones IP. Par souci de sécurité, le LAN doit être configuré de telle manière que les PC et laptops ne se trouvent pas dans le VLAN Voice.

1.2 Matériel nécessaire

Les manipulations sont effectuées avec le matériel suivant par site :

- 1 routeur Cisco 2811
- 1 switch VLAN Cisco Catalyst 3560
- 2 téléphones Cisco IP Phone Serie 7906
- 1 téléphone Cisco IP Phone Serie 7960
- 1 hub

2 Configuration de base du réseau

Cette partie concerne la configuration du switch, des différents VLAN nécessaires (Data, VoIP), du serveur DHCP ainsi que les options de routage.

2.1 Configuration VLAN accès

Le câblage physique relie les PC au port switch du téléphone. Les téléphones, quant à eux, sont connectés au port du switch central. Bien que les paquets data et VoIP arrivent sur le même port du switch, les deux types de trafic ne doivent pas, par principe de sécurité, se situer dans le même VLAN.

Les switches Cisco C3560 permet de configurer des ports VLAN en mode « Voice » qui est spécialement conçu pour permettre au téléphone de fonctionner comme switch intermédiaire pour le PC. Un port peut être mis en mode « Voice avec les commandes :

```
Switch(config)# interface fastethernet 0/X
Switch(config-if)# switchport access vlan Y
Switch(config-if)# switchport voice vlan Z
```

où

- x est le numéro de l'interface,
- Y et le VLAN data et
- Z est le VLAN voice.

Configurez les ports 2 à 8 du switch Catalyst 3560 comme port Voice. Le port 1 sera utilisé comme trunk VLAN.

Question 1 (2 points)

Montrez les commandes pour la configuration des ports VLAN voice.

Réponse

2.2 Trunk

Ne pouvant échanger d'informations entre eux, les périphériques des différents VLAN souhaitent néanmoins pouvoir communiquer avec le routeur (qui fait aussi office de CallManager). Le lien entre le switch et le routeur doit donc être configuré comme trunk VLAN, transportant ainsi les trames des deux VLAN data et voice. De son côté, le routeur réceptionnera par la suite les différents VLAN sur autant d'interfaces virtuelles que nécessaires.

La mise en place d'un trunk s'effectue selon les commandes ci-dessous.

```
Switch(config)# interface fastethernet 0/X
Switch(config-if)# switchport
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan Y,Z

Y, Z : VLAN autorisés sur l'interface
```

Configurez le port fastEthernet0/1 du switch 3560 pour qu'il transporte les VLAN « Data » et « VoIP » en mode Trunk.

Question 2 (2 points)

Montrez les commandes pour la configuration du port VLAN trunk.

Réponse

2.3 Interfaces virtuelles

Le routeur doit pouvoir récupérer les différents VLAN transportés par l'interface Trunk du switch 3560. Cette récupération s'effectue à l'aide d'interfaces virtuelles, construites sur l'interface physique connectée au Trunk et correspondant chacune d'entre elles à un VLAN spécifique. La mise en place d'une interface virtuelle s'effectue à l'aide de la commande suivante :

```
Router(config)# interface fastethernet 0/0.X
Router(config-subif)# encapsulation dotq1q Y
Router(config-subif)#    ip    address    <IP_address>    <netmask>
x : numéro de l'interface virtuelle
Y : numéro du VLAN à réceptionner
```

où les paramètres en <…> doivent être remplacés par les valeurs appropriées.

Configurez les interfaces virtuelles nécessaires pour que les VLAN « Data » et « VoIP » aient accès au routeur. N'oubliez pas d'activer l'interface avec « no shutdown ».

Question 3 (2 points)

Montrez les commandes pour la configuration des deux interfaces virtuelles du routeur.

Réponse

2.4 DHCP

L'objectif de cette partie est de mettre en place un serveur DHCP sur le routeur/CallManager Express. La particularité du service souhaité est de pouvoir distribuer des adresses sur les deux VLAN qui ne sont pas censés communiquer entre

elles. L'une des solutions les plus simples est de créer, sur le routeur, un serveur DHCP par VLAN.

La mise en place d'un service DHCP s'effectue selon les commandes suivantes :

```
Router(config)# ip dhcp pool <DHCP_server_name>
Router(dhcp-config)# network <network_IP> <netmask_IP>
Router(dhcp-config)# default-router <router_IP>
```

Question 4 (2 points)

Montrez les commandes pour la configuration des services DHCP pour les deux VLAN.

Réponse

Option TFTP

Le serveur DHCP ne sera pas uniquement à fournir l'adresse IP aux téléphones, mais aussi le masque de sous-réseau, la passerelle par défaut et le serveur DNS. Il permet également d'informer les nouveaux clients de la présence d'un serveur TFTP, qui permettra par exemple dans le cas d'un téléphone IP, de mettre à jour son firmware. L'ajout de l'adresse du serveur TFTP se fait par l'option 150, selon la commande suivante :

```
Router(config)# ip dhcp pool DHCP_server_name
Router(dhcp-config)# option 150 ip TFTP_Server_IP
```

Le service TFTP étant dans ce cas géré par le CallManager Express, l'adresse IP du serveur TFTP est donc celle du routeur.

Exclusion d'adresses

La distribution d'adresses se fait par défaut sur la totalité du sous-réseau spécifié. Il est néanmoins possible d'exclure certaines adresses (celle du routeur !) de la distribution afin de les réserver pour certains services particuliers (gateway, DNS, …). L'exclusion d'adresses s'effectue selon la commande suivante :

```
Router(config)#ip dhcp excluded-address <begin_IP> <end_IP>
```

Mettez en place un serveur DHCP par VLAN, intégrant l'exclusion d'adresses et l'adresse du serveur TFTP.

Question 5 (2 points)

Montrez les commandes pour l'exclusion d'adresses DHCP sur les deux VLAN.

Réponse

2.5 Tests

Dans les manipulations précédentes, les VLAN, le trunk sur le routeur et les services DHCP ont été configurés. Dans cette partie, nous allons tester le bon fonctionnement du réseau.

- Testez d'abord le bon fonctionnement des services DHCP. Branchez les téléphones à un port voice du switch et vérifié qu'il reçoit une adresse IP du VLAN voice.
- Branchez un laptop sur le port « switch » du téléphone. Vérifiez qu'il reçoit une adresse IP du VLAN data.

Question 5 :

Afin d'étudier l'utilisation des VLAN sur le port voice du switch, branchez un hub entre le téléphone et le switch.

a) *Générez du trafic depuis le téléphone, par exemple en le redémarrant. Est-ce que trames envoyées par le téléphone sont marquées avec un VLAN. Quel VLAN est utilisé pour le trafic VoIP ? (2 points)*

Réponse

b) *Générez du trafic depuis le laptop, par exemple à l'aide d'un ping sur le routeur. Est-ce que les trames data sont marquées avec un VLAN. Lequel ? (2 points)*

Réponse

c) *Quelle est la différence, sur le switch, entre un port « Voice » et un port « Trunk VLAN » ? (4 points)*

Réponse

3 Configuration du routage

Arrive maintenant la configuration du routage sur le Cisco 2811. Au-delà de son rôle de routeur, il accueillera également les fonctionnalités du CallManager Express. C'est également sur ce même élément que sera installé, par la suite, le firewall nécessaire pour contrôler le trafic inter-VLAN. Le même matériel remplit donc 3 fonctions essentielles au bon fonctionnement de l'architecture réseau du laboratoire.

En configurant des routes entre tous les sous-réseaux, la séparation VLAN serait compromise, comme un PC pourrait atteindre les téléphones à travers le routeur. Nous avons donc intérêt à interdire certaines communications.

Question 6 :

a) *Les téléphones doivent pouvoir atteindre le gatekeeper et la gateway VoIP. Quelles routes statiques doivent être configurées pour permettre ceci ? (2 points)*

Réponse

b) *Les PC doivent pouvoir atteindre le réseau data du site principale ? Quelles routes statiques doivent être configurées pour permettre ceci ? (2 points)*

Réponse

La création d'une nouvelle route statique s'effectue à l'aide de la commande suivante :

```
Router(config)# ip route network_IP netmask_IP nexthop_IP
```

Question 7 (4 points)

Configurez les routes statiques sur le routeur. Montrez les commandes de configuration. N'oubliez pas la configuration de l'interface du routeur.

Réponse.

(Malheureusement les éléments du site central ne sont pas disponibles pour ce labo. Les routes ne pourront donc pas être testées.)

3.1 Analyse de la connectivité

Avec les VLAN et le routage en place, les éléments du réseau peuvent communiquer. Même si les réseaux Voice et Data sont séparés par des VLAN, ils sont interconnectés au niveau 3 par le routeur. Dans cette étape nous analysons quelles communications sont possibles et quelles communications doivent être interdites par un firewall.

Question 7 :

a) Communications actuellement possibles : remplissez le tableau ci-dessous en mettant un X dans les cases si la communication entre les deux éléments est actuellement possible ? Testez la connectivité, si possible. (5 points)

	Télé-phone	*PC*	*Routeur / CCME*	*GK*	*GW VoIP*	*Routeur site principal*
Téléphone IP	*x*					
PC		*x*				
Routeur / CCME			*x*			
Gatekeeper				*x*		
Gateway VoIP					*x*	
Routeur site principal						*x*

*b) Communications à autoriser : remplissez le tableau ci-dessous en mettant un X dans les cases si la communication entre les deux éléments doit être **authorisée**. (5 points)*

	Télé-phone	*PC*	*Routeur / CCME*	*GK*	*GW VoIP*	*Routeur site principal*
Téléphone IP	*x*					
PC		*x*				
Routeur / CCME			*x*			
Gatekeeper				*x*		
Gateway VoIP					*x*	
Routeur site principal						*x*

4 Sécurisation du réseau

4.1 Firewall

Afin de réaliser la séparation des réseaux VoIP et data au niveau 3, un firewall sera installé sur le routeur.

La notion de firewall est prise en charge par les listes d'accès (Access Control List – ACL) sur Cisco IOS. Les access-list permettent de définir les adresses/ports autorisés ou interdits par le pare-feu. Ils peuvent être spécifiés pour

- une interface donnée,
- une direction donnée (entrée/sortie),
- un protocole défini et
- un port particulier.

La commande « access-list » se construit selon le modèle simplifié ci-dessous. Les access-list-number commencent de préférence à partir de 101.

```
access-list <access-list-number> {deny | permit} <protocol>
<source> <source-wildcard> <destination> <destination-wildcard>
```

Par exemple

```
access-list 101 permit tcp 1.2.3.0 0.0.0.255 any eq 80
access-list deny any
```

pour créer une access-list 101 qui autorise le trafic depuis le sous-réseau 1.2.3.0/24 vers n'importe quelle destination, port 80. La deuxième règle interdit tout autre trafic.

Le lien entre l'access-list et les interfaces réseaux s'effectue de la manière suivante :

```
Switch(config)# interface fastEthernet 0/X
Switch(config)# ip access-group <access-list-numb> {in|out}
```

Définissez les access-lists nécessaires et appliquez-les aux interfaces concernées.

Le filtrage ne doit tenir compte que des adresses IP, pour permettre le bon fonctionnement des services DHCP, TFTP, VoIP, ... Cette méthode ne fournit pas une sécurité optimale. Idéalement, les ports nécessaires devraient être autorisés individuellement.

Question 8 :

Configurez le firewall pour autoriser les communications définies ci-dessus. Appliquez une politique de « Refus par défaut » qui empêche toutes les autres communications. Montrez les commandes de configuration. (6 points)

Réponse

4.2 Port security

La notion de « Port Security » vise à sécuriser les interfaces d'un périphérique réseau par reconnaissance d'adresses physiques. Le principe est d'identifier le périphérique souhaité par son adresse MAC, de mémoriser cette information et de refuser l'accès à toute autre connexion.

Différents modes sont paramétrables pour cette option de sécurité. Le premier est de n'autoriser qu'un seul périphérique à la fois sans se verrouiller sur un appareil unique. Un deuxième mode consiste à n'autoriser qu'un nombre défini d'adresses physiques. Déjà moins permissif, il limite l'accès à une série de périphériques souhaités et refusera toute autre connexion.

Un troisième mode, beaucoup plus restrictif, est basé sur la mémorisation de manière définitive – dans la mesure où le switch n'est pas réinitialisé – de l'adresse physique donnée du périphérique autorisé et ne permet l'accès qu'à ce seul et unique matériel. La mémorisation de l'adresse MAC peut également s'effectuer sur la connexion du premier périphérique connecté (mode sticky).

Les réactions à la violation de la sécurité choisie sont également configurables. La première consiste à informer l'administrateur réseau du problème par message ICMP (restrict). La deuxième ignore la totalité des paquets envoyés par le périphérique non désiré (protect), sans pour autant désactiver le port. La dernière réaction possible désactive de manière instantanée le port Ethernet du switch et seul l'administrateur réseau sera en mesure de le réactiver.

Question 9 :

a) *Supposez que le switch ait été configuré à n'autoriser qu'une seule adresse Mac absolue par port. Décrivez une méthode possible qu'un attaquant pourrait tout de même utiliser pour contourner cette sécurité et accéder au VLAN Voice. (2 points)*

Réponse

b) *Proposez des solutions qui permettraient d'empêcher cette attaque.*

Réponse

Les commandes de l'option « switchport port-security » sont résumées ci-dessous :

```
switchport port-security maximum {max # of MAC addresses allowed}
switchport port-security mac-address {MAC address | sticky}
switchport port-security violation {shutdown|restrict|protect}
```

L'activation du « port-security » sur l'interface Ethernet X, prenant en compte 2 adresses MAC absolues enregistrées sur connexion et avertissant l'administrateur réseau en cas de violation, s'effectue selon l'exemple suivant :

```
Switch(config)# interface fastethernet 0/X
Switch(config-if)# switchport
Switch(config-if)# switchport mode-access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config)# switchport port-security mac-address sticky
Switch(config)# switchport port-security violation restrict
```

Configuration à effectuer

Paramétrez les ports Ethernet du switch à n'autoriser que les adresses MAC des périphériques à connecter (IP Phone + laptop). L'identification des adresses MAC s'effectue à la première connexion des périphériques (mode sticky). La réaction souhaitée est l'extinction du port (shutdown).

Question 10 : (4 points)

Montrez les commandes de configuration pour mettre en place la port-security.

Réponse

Puis tester la configuration :

1. Exécuter la commande « show port-security » pour afficher la configuration.
2. Exécuter la commande « show port-security address » pour afficher les adresses MAC enregistrées.
3. Branchement des périphériques à autoriser (IP Phone + laptop)
4. Affichage des adresses MAC enregistrées
5. Déconnexion du laptop
6. Connexion d'un périphérique non autorisé et réaction à la violation de sécurité

Question 11 : (4 points)

Effectuez les opérations décrites ci-dessus et faites une copie de l'écran avec les résultats des commandes et les messages debug du routeur.

Réponse

La réactivation d'un port sujet à la violation de sécurité s'effectue selon les commandes ci-dessous ; elle ne supprime pas l'option de sécurité :

```
Switch3560(config)# interface fastethernet 0/X
Switch3560(config-if)# shutdown
Switch3560(config-if)# no shutdown
```

5 Fichiers de configuration

Question 12 : (5 points)

Insérez ici le fichier de configuration complet du routeur / CallManager Express.

Fichier de configuration du routeur.