Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE
Diplôme Universitaire de Technologie
Spécialité Réseaux et Télécommunications

ETUDE D'UNE SOLUTION MULTICAST

Henrik HOVSEPYAN

EDF

Responsable entreprise : William MODENESE

Responsable académique : Nadir BOUSSOUKAIA

2017

Remerciements

Dans un premier temps, je tiens à remercier toutes les équipes aux seins de la DAIP qui ont fait preuve d'une réelle attention, d'écoute et d'aide lors de mon stage.

Je tiens à remercier Marc PIANELLI pour son humanité et sa sincérité mais aussi pour les nombreux conseils et l'aide qu'il a pu m'apporter lors de ces 10 semaines.
Je remercie également Gilles LANDUCCI pour avoir proposer ma candidature au sein de son équipe et surtout m'avoir permis de réaliser ce stage riche en expériences et en connaissances .
J'adresse un grand merci à mon tuteur de stage William MODENESE qui m'a proposé un sujet très pertinent, je le remercie pour la confiance qu'il m'a porté sur un projet conséquent et également pour tous ses conseilles et idées.
Je remercie Francois TREVISIOL ainsi que Régis BOUSSION, tout d'abord pour leurs accueille et leur sympathie mais également pour m'avoir soutenue pour mon choix d'école et de carrier professionnelle. Leur proposition d'un poste en alternance me témoigne de la confiance qu'ils portent à mon travaille.
Je remercie Richard GUILLELMET qui m'as permis de travailler à ses coté et avec qui j'ai a partagé de très bon moment lors d'un déplacement à la centrale hydraulique de l'Argentière.
Enfin je voudrais remercier Nadir BOUSSOUKAIA ainsi que toute l'équipe pédagogique de l'IUT R&T pour leur suivi et de leur attention.

SOMMAIRE

Projet RGV

1.Introduction

Ce document est une étude d'opportunité concernant l'implémentation du multicast dans les réseaux vidéo de responsabilité UNITEP, dans les centrales nucléaires de productions d'électricités. Le but de ce document est de trouver une solution multicast qui sera dans un premier temps fonctionnel et évolutive, puis on présentera les avantages et inconvénients qui seront prouvés lors de multiples analyses et tests.
Cette étude intervient suite à l'émergence et l'engagement de STEP dans deux projets vidéo : vidéo RGV et TES. Une solution convergence doit alors être apportée pour permettre à ces deux projets de s'additionner à l'infrastructure vidéo (S2M) existante.

Le projet S2M a pour objectif de filmer les activités d'arrêt de tranche. La retransmission en temps réel est utilisée par la cellule COPAT comme un outil de pilotage, outil d'aide à la décision, au diagnostic et outil de détection de situation dangereuse. Les prises de vue se situent essentiellement dans et autour du Bâtiment Réacteur.
Cette étude présentera pour le projet RGV mais aussi pour tout le projet de convergence de service vidéo, le choix optimal d'un routage multicast. En effet, ce document aura pour objectif de présenter le fonctionnement théorique mais aussi une solution multicast avec les avantages et les inconvénients qui lui sont liées.

2.Présentation de l'entreprise

Historique

La société Électricité de France a été créée **le 8 avril 1946**, suite à la loi de nationalisation des 1450 entreprises françaises de production, de transport et de distribution d'électricité et de gaz. EDF est alors un établissement public à caractère industriel et commercial (EPIC).

Dès le lendemain de la guerre, 90% des foyers français profitent déjà de l'électricité pour l'éclairage et le branchement de petits appareils électroménagers. Dans les années 1960, les appareils électriques se généralisent et la demande énergétique augmente.

Actuellement le groupe emploie 154.845 personnes dans le monde, est présent dans plus de 30 pays. Il a réalisé un chiffre d'affaires de 71 milliards d'euros dont 662 million son consacré au recherche et développements.

DAIP

La Division Appui Industriel à la Production (DAIP) du Groupe EDF a pour mission d'assurer les prestations de services internes pour les unités de production. Elle assure une partie de la maintenance spécialisée sur des segments d'actions stratégiques et doit donc faire face aux enjeux de disponibilité, de sûreté et de pérennité des installations du producteur (nucléaire, hydraulique et thermique).

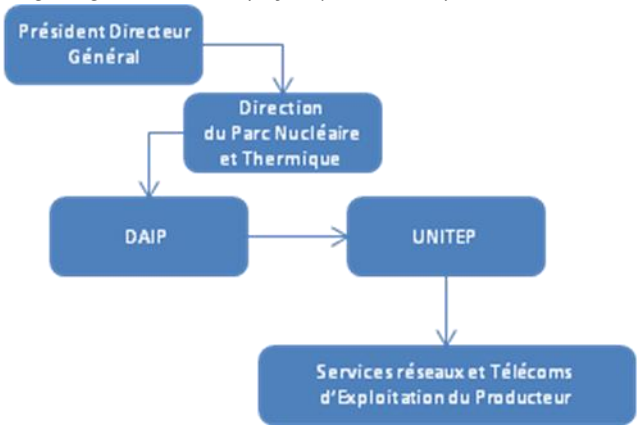
UNITEP

Au sein de la DAIP, l'UNITEP (Unité Nationale systèmes d'Information et Télécoms d'Exploitation du Producteur) intervient notamment dans le domaine du développement et de la maintenance des SI métiers.

STEP

Au sein de l'UNITEP, le Département STEP (Service Télécoms d'Exploitation du Producteur) assure l'ingénierie de conception, l'intégration et le déploiement, l'administration, l'exploitation et la maintenance des télécommunications d'exploitation des producteurs.

Organigramme simplifié (Annexe 7):



3 Introduction au multicast

Bien que la majorité des applications (ex: web/mail/ftp) utilise le mode « Unicast » pour échanger les données sur le réseau, le multicast reste la technologie la mieux adaptée pour les besoins nécessitant de diffuser une même information à plusieurs destinations. L'exemple d'usage le plus fréquent de la technologie Multicast est la diffusion de la vidéo sur IP (ex : Caméra sur IP, IP TV, ..).

3.1 Généralités

Ce mode de transmission est adapté pour les échanges de données entre « une source » vers « plusieurs destinations » souhaitant recevoir la même donnée. La « source » envoie une seule fois le flux vers une adresse multicast et les destinations souhaitant recevoir ce flux s'abonnent à cette adresse.

3.2 Avantages / Inconvénients

- Les avantages du routage Multicast sur les réseaux :

- Optimiser la bande passante sur le réseau : Contrairement à la diffusion en Unicast, un flux émis en Multicast n'est émis qu'une seule fois par la source vers de multiples destinations.

- Optimiser le traitement (cpu, mémoire) sur les équipements actifs du réseau : Une seule copie du flux est émise et traitée par l'ensemble des équipements réseaux situés entre la source et destination.

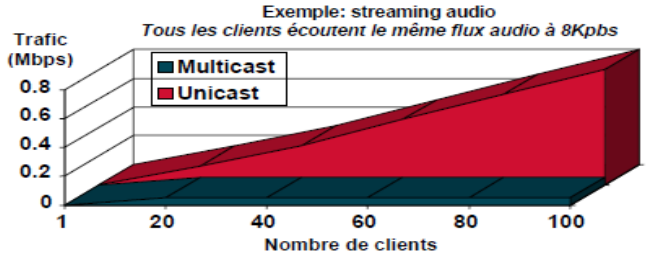
- Optimiser la scalabilité du réseau : L'extension du nombre de clients situés à différents endroits géographique et souhaitant recevoir le flux n'engendre pas une surcharge des liens.

- Les inconvénients du routage Multicast sur les réseaux :

Le multicast ne permet cependant en aucune façon le contrôle de la participation au groupe par la source : la source ne peut déterminer ni qui participe, ni qui peut participer ou non au groupe.
L'identification et l'authentification des participants doivent être prises en charge au niveau applicatif si elles sont souhaitées

3.3 Gains potentiels

Dans le cadre d'une extension du service de vidéo surveillance, le gain en bande passante est une de nos priorités. Le projet pourrait impliquer près d'une quinzaine de caméras de surveillance par tranche, un flux de données conséquent qu'il faudra acheminer dans un réseau composé de connexion physique parfois trop ancien et de faible débit ,surtout a l'intérieur de la centrale nucléaire ou une opération de remplacement de câbles n'est pas envisageable.



4 Les différentes implémentations du multicast

Tout d'abord il est important de préciser quels sont les composants du multicast. La technologie Multicast s'appuie sur les briques fonctionnelles ci-dessous :
IGMP (Internet Group Management Protocol) : ce protocole permet au client d'indiquer au réseau le groupe multicast pour lequel il souhaite s'abonner et recevoir le flux.
PIM (Protocol Independent Multicast) : ce protocole permet définir le chemin réseau pour la diffusion d'un flux depuis une source (émetteur) jusqu'à sa destination (récepteur).

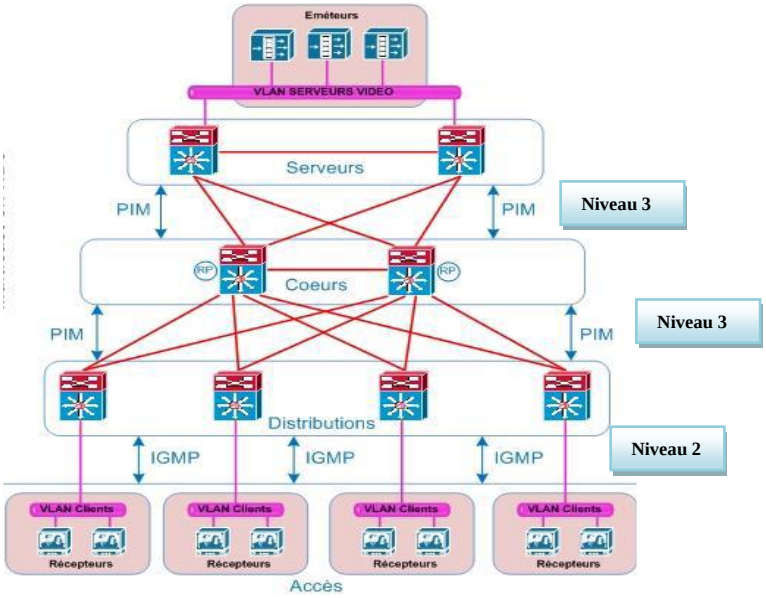


Figure 1 : Exemple de réseau implémenter avec PIM et IGMP

4.1 IGMP (Interne Group Management Protocol)

IGMP est le protocole le plus répandu en termes d'adhésion aux groupes multicast et se présente sous trois versions. Dans le cadre de notre étude on se concentrera sur la version 2 qui est la plus stable car la version 1 est obsolète et la version 3 n'est pas encore disponible sur tous les équipements actuels. IGMP comporte deux phases :

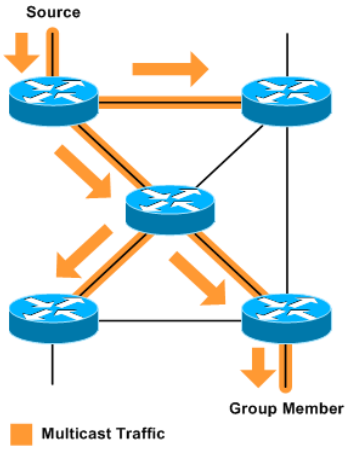
- Un hôte qui rejoint un groupe de diffusion pour la première fois diffuse un rapport IGMP informant les équipements connectés au réseau (ce rapport est réémis une ou deux fois au cas où il s'est perdu ou arrivé endommagé). Les routeurs de groupe locaux reçoivent le message, déterminent le routage nécessaire et communiquent ces informations aux autres routeurs de groupe.

- Les routeurs de groupe interrogent périodiquement les machines du réseau local pour savoir s'il y a des machines appartenant encore à des groupes (l'appartenance change dynamiquement). Les machines appartenant à des groupes répondent à des instants différés. Une seule réponse d'une machine appartenant à un groupe suffit, les autres machines du même groupe n'ont pas alors à répondre. De cette façon on évite la saturation du réseau.

4.2 PIM (Protocol Independent Multicast)

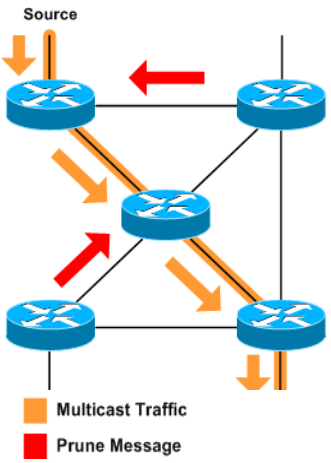
D'après des recherches effectuées sur les différents types de routages multicast, le protocole PIM (Protocole Independent Multicast) semble être le plus complet dans le domaine du routage multicast. Néanmoins le protocole PIM se présente sous plusieurs modes de fonctionnement qui demandent une réflexion avant d'effectuer un choix d'implémentation.

4.2.1 Implémentation PIM Dense Mode



La diffusion en DENSE MODE permet l'envoie du flux vers tous les equipements actifs du réseau. Chaque equipement redistribue les flux sur toutes les interfaces sauf celle de l'entrée du flux, ce qui engendre une surconsomation de la bande passante.
Ce mode de diffusion n'est pas adapté à des architectures qui depasse la taille d'une maquette de test ou d'un petit site. De plus la diffusion en DM n'est pas evolutive car n'existe pas en IPV6. On peut tout de même noter que le protocole PIM en DM est facile d'implémenter.

4.2.2 Implémentation PIM Sparse Mode



La diffusion en SPARSE MODE, ou mode clairsemé en français, permet contrairement au DM de distribuer les flux seulement aux équipements intéressés. Ce mode de diffusion permet alors de gagner en bande passante. Le fonctionnement de ce mode est basé sur la présence d'un Point de Rendez-vous (RP) et son point fort est qu'il possède de nombreuses options et des techniques de mise en place qui peuvent être un atout de taille. De plus, on notera que la diffusion en SM est la plus présente de nos jours et est la plus évolutive car il est possible de l'implémenter en IPv6.

4.2.3 Implémentation PIM Specific Source Mode

Ce mode de diffusion a été pensé pour améliorer le mode SM et s'applique d'ailleurs en appliquant quelques modifications à celui-ci. L'idée de ce mode de diffusion est d'éliminer la phase de la construction de l'arbre partagé. Ce mécanisme permettra alors aux routeurs de connaitre l'adresse du groupe et celle de la source. L'atout majeur du mode SSM est l'apport en sécurité au SM. Néanmoins, malgré les multiples avantages que peut offrir le SSM il n'est pas encore présent sur tout les équipements et modèles actuels.

4.3 Bilan / Synthèse

	AVANTAGES	INCOVENEANTS
PIM DM	-PIM-DM est un protocole efficace quand les récepteurs sont distribués de manière dense au niveau du réseau. -PIM-DM est indépendant du protocole de routage unicast sous-jacent. -PIM-DM ne met pas en œuvre de RP, ce qui fait de lui un protocole plus simple à configurer, mettre en œuvre et déployer que PIM SM.	-Tous les routeurs PIM, à la fois ceux qui **font partie des arbres** de distribution comme ceux qui n'en **font pas partie**, doivent maintenir et conserver des états par source, et ce **pour chaque source** dans le domaine. -Le déploiement à l'échelle de PIM-SM pose problème dans des topologies réseau où la plupart des terminaux ne sont pas intéressés par recevoir les flux de diffusion.
PIM SM	-PIM-SM est indépendant du protocole de routage unicast sous-jacent et fonctionne quel que soit le type d'IGP employé. -PIM-SM ne pose pas de problèmes de déploiement à l'échelle dans des réseaux multicast de grande taille et étendus. -PIM-SM est un protocole en mode épars. Les informations de routage multicast relatives à un groupe sont uniquement créées et maintenues sur les seuls routeurs	-**Collisions d'adresse de groupe** entre plusieurs applications concurrentes sélectionnant la même adresse de groupe. -PIM-SM ne met en œuvre aucun mécanisme pour contrôler ou empêcher un terminal IP d'émettre du trafic multicast sur un groupe de diffusion donné. -PIM-SM est vulnérable aux attaques par déni de service où une source malveillante.
PIM SSM	-Empêcher des récepteurs de joindre un arbre partagé pour des adresses de groupe dans l'espace SSM. -Interdire toute source d'émettre du trafic multicast dont l'adresse de destination est dans l'espace SSM sur un arbre partagé. -La complexité mais aussi l'installation, la gestion et la maintenance d'un réseau multicast SSM est plus simple que celle d'un réseau PIM-SM. -Sécurité et contrôle d'accès renforcés.	-Nécessité de disposer dans les terminaux récepteurs d'une implantation du protocole IGMPv3 ou MLDv2. Cette pile protocolaire **IGMPv3/MLDv2 n'est pas encore disponible dans tous les types de terminaux multicast.**

5 PIM sparse mode (SM)

La diffusion en mode clairsemé (SM) est la plus prometteuse dans le cadre de nos études. En effet le SM présente le plus de critères d'évolutivités tout en étant stable en ce qui concerne le routage multicast. Les défauts qu'il présente seront étudiés et limités au maximum, pour cela il est essentiel de comprendre son fonctionnement afin de mettre en évidence les points à améliorer.

5.1 PIM SM en détail

Le protocole PIM SM créé un arbre de diffusion partagé et unidirectionnel. Le point de Rendez-vous (RP) est considéré comme la racine de cet arbre et sera le point de convergences si plusieurs sources émettent pour un même groupe multicast. Le routeur étant le RP redistribue les flux qui partagent alors l'arbre qui correspond à leur groupe. Le protocole PIM SM se fait en trois phases :

Phase 1 : Construction de l'arbre partagé du RPT (Rendez-vous Point Tree)
Les chemins RPT (RPT : Rendez-vous Point Tree) sont créés par les routeurs dits DR qui sont en tête de chaque sous réseau. Les récepteurs envoient des messages IGMP au DR pour notifier qu'ils souhaitent participer à un groupe multicast et recevoir tous les flux de ce groupe. Le DR signale cette information à tous les routeurs voisins qui ont rejoint le routage multicast.

Phase 2 : L'acheminement spécifique.
Si l'on résume cette phase, elle a pour but de stopper un message spécifique que le routeur lié a la source (DR de la source) et le RP s'échange, le message « PIM Register »

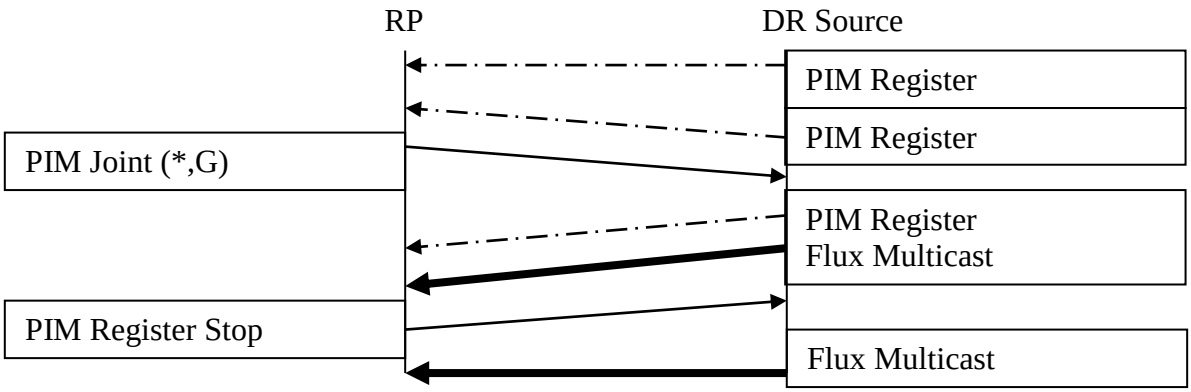


Figure 2: Fonctionnement de PIM Register Stop

Remarque : Cette phase permet de stopper les messages « PIM Register » et d'éviter un trafic inutile une fois la source enregistrée.

Lorsque les deux phases sont terminées nous avons l'acheminassions de flux suivant :

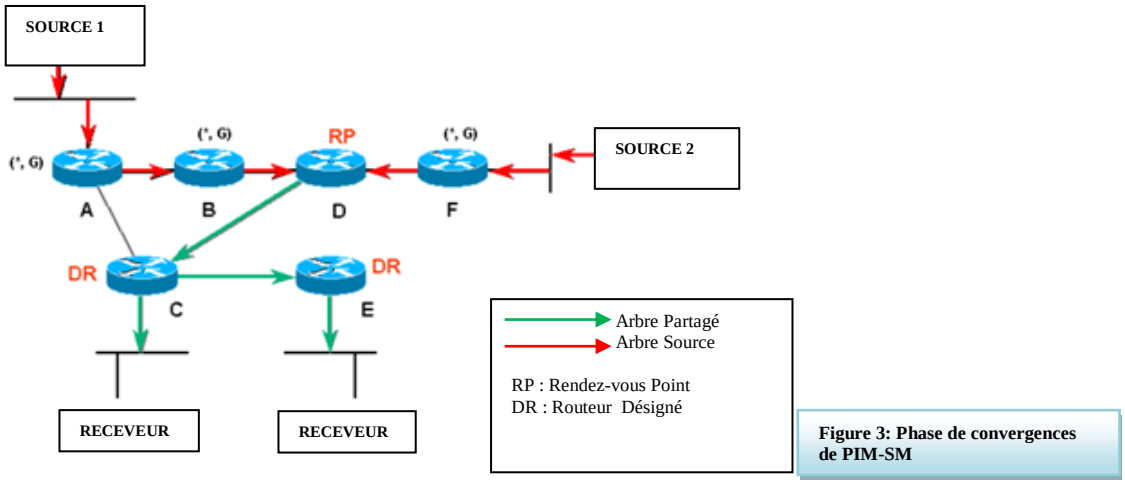


Figure 3: Phase de convergences de PIM-SM

Phase 3 : L'arbre du plus court chemin STP (Shortest Path Tree)
En effet on parle de chemins SPT lorsque les routeurs reçoivent les flux directement des sources par ces chemins. Cette phase permet d'éviter les détours par le RP. Dans le cas ou le DR a un état (Source,Groupe) il peut alors , émettre un message Joint (S,G) vers la source pour recevoir les flux avec le chemin le plus court et envoyer un message Prune (S,G) vers le RP pour fermer le chemin le plus long.

Les trois phases vont donner le résultat suivant :

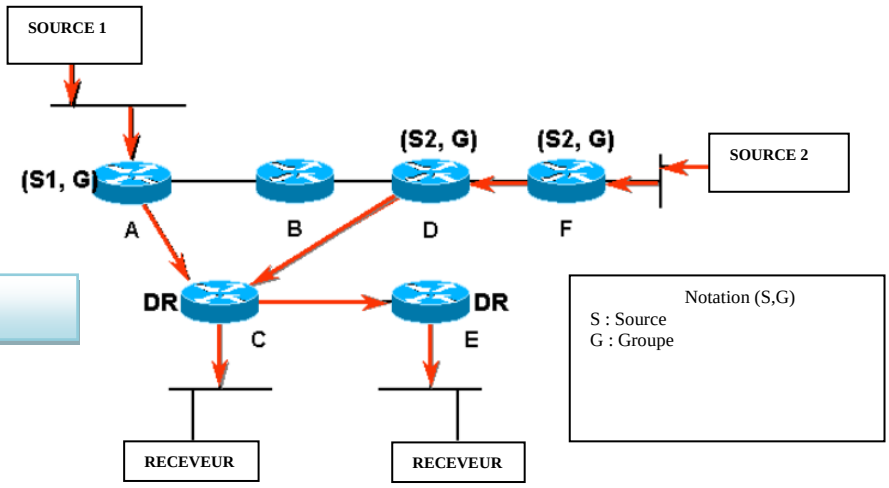


Figure 4: Phase finale de la convergence avec PIM-SM

5.2 Différents Mécanismes de PIM

5.2.1 Bootstrap Router (BSR)

Le protocole BSR est le standard qui permet d'annoncer dynamiquement les RP à l'ensemble des équipements de la topologie Multicast. Le mécanisme BSR garantit une tolérance en cas de panne du RP et permet le partage de charges entre différents routeurs RP, en attribuant à chacun des plages d'adresses multicast distinctes à gérer. L'inconvénient majeur de BSR consiste en un allongement des temps de convergence, en cas de panne d'un RP, mais tient aussi à sa complexité technique.

5.2.2 Anycast-RP

Anycast-RP est un moyen de contourner la restriction d'avoir un seul RP par groupe multicast. Il permet de partager la charge et la tolérance aux fautes. Contrairement au protocole BSR, il n'est plus nécessaire de répartir la gestion des groupes multicast. De plus, le temps de restauration en cas de panne sur un des deux RP est bien plus court. Afin que tous les RP aient connaissance de toutes les sources du domaine émettant sur les groupes de diffusion, des séssions MSDP (Multicast Source Discovery Protocol), doivent être établies entre les RP afin qu'ils s'échangent des informations sur leurs sources respectives.

5.3 Bilan des choix pour l'étude

Le protocole IGMPv2 sera choisi dans le cadre de l'abonnement d'un récepteur à un flux diffusé en multicast par un émetteur et sera implémenté sur tous les routeurs possédant des groupes multicast.
Le protocole PIM-SM sera choisi dans le cadre du routage multicast et sera appliqué sur tous les routeurs et en parallèle avec le routage unicast OSPF. Le RP sera fixé manuellement dans notre cas en raison de la taille (trop petit) de notre réseau de test en revanche il sera préférable de favoriser le mécanisme Anycast-RP avec MSDP dans le cadre d'un réel déploiement.

6 Tests et résultats

Pré-requis et configuration avant les tests.
Plan d'adressage (Annexe 1)
Routage OSPF (Annexe 2)
Routage PIM-SM (RPadd : 20.20.20.2)(Annex 3)
Switching (Annex 4)
Configuration Caméra AXIS (Annexe 5)
Configuration du poste de visualisation avec VLC (Annexe 6)
Configuration SNMP monitoring

Pour notre étude, nous avions à disposition des routeurs Cisco 1841, des Switchs Cisco Catalyse 2960, une caméra AXIS, et des postes sous différentes versions de Windows (xp 7, 10). Sur tous les équipements choisis, la configuration du protocole IGMP était alors disponible tout comme les trois modes de fonctionnement du protocole PIM. Les topologies réalisables sont multiples, on se basera dans un premier temps sur la topologie de test suivant :

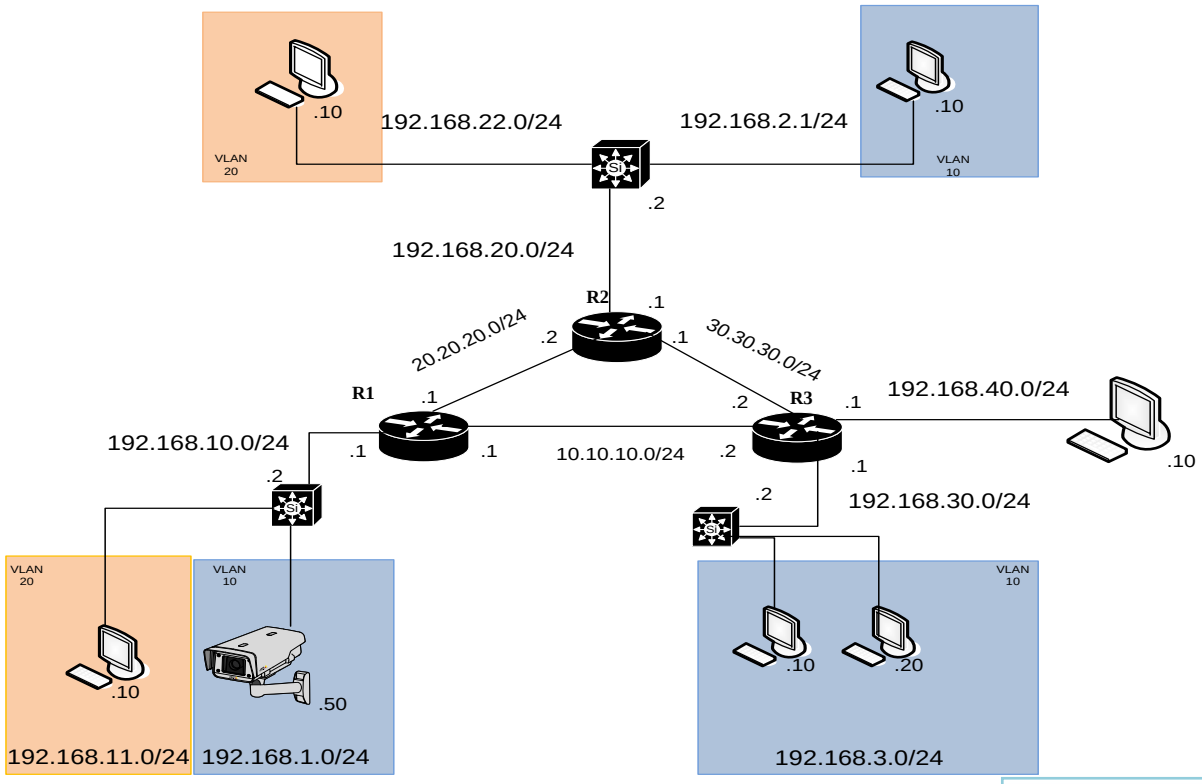


Figure 5 : Topologie de test des configurations

En effet, cette topologie va nous permettre de tester plusieurs aspects du multicast :

Test 1 : Le test de connexion, récupération et distribution des flux aura pour but de créer des accès multicast et unicast vers la source depuis un même poste afin d'observer la cohabitation entre eux.

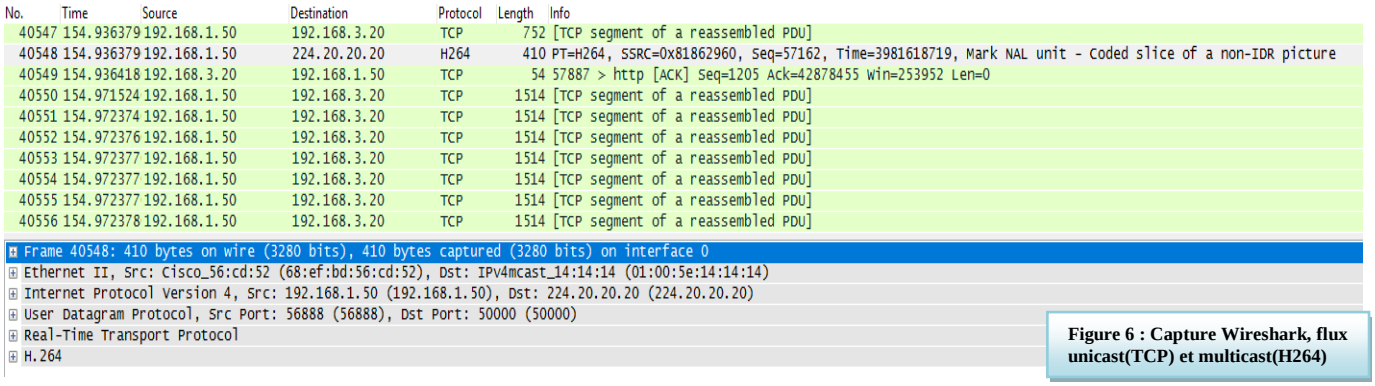


Figure 6 : Capture Wireshark, flux unicast(TCP) et multicast(H264)

On peut, en effet, observer la présence d'un flux TCP (Unicast). Une fois la connexion effectuée, on reçoit le trafic depuis la source. Le protocole H264 présent ici est en réalité un paquet acheminé en UDP et on peut observer que le multicast est en marche car la destination n'est plus l'IP du poste mais celui du groupe multicast (224.20.20.20).

Remarque : On notera ici particulièrement l'atout que peut apporter la caméra AXIS. Son paramètre d'utilisateur enregistré renforce l'aspect sécurité du protocole PIM-SM qui est dépourvu d'option d'authentification. La connexion se fait donc en HTTP (TCP), peu importe le type de diffusion (Mcast ou Unicast).

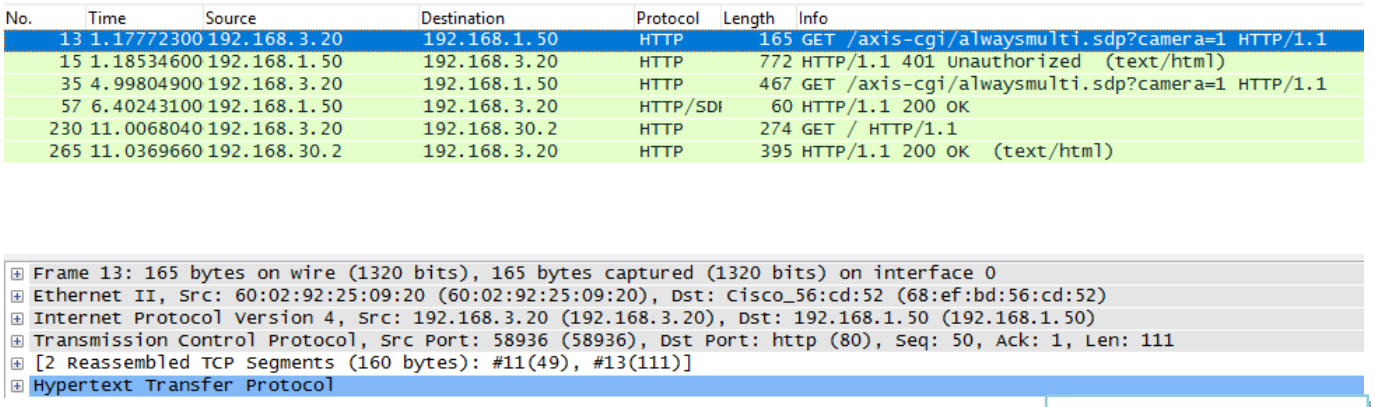


Figure 7: Capture Wireshark , Phase d'authentification HTTP

Test 2 : Lors de ce test on vérifie que le routage unicast se fait bien en OSPFv2 et que le multicast se fait bien par IGMP et PIM-SM.

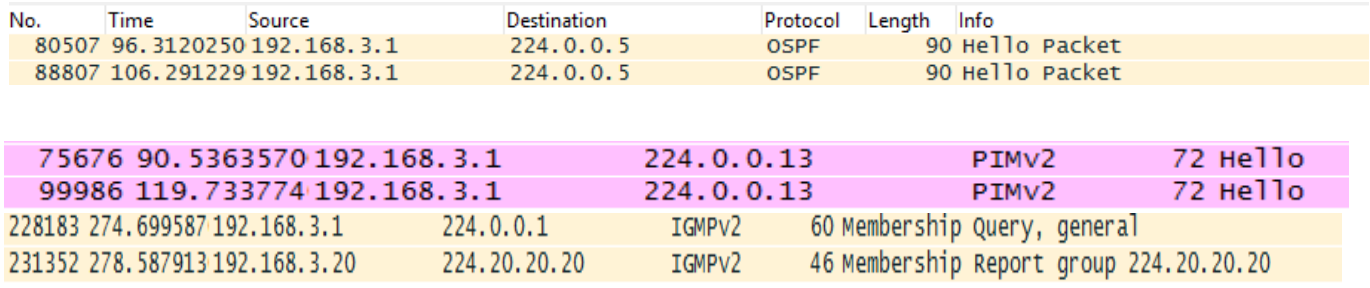


Figure 8: Capture Wireshark des protocoles OSPF, PIM et IGMP

Toutes les étapes de routages unicast et multicast sont respectées. On notera tout de même que l'on ne peut pas observer le mode de fonctionnement, ni même le RP du protocole PIM, pour ces informations il est nécessaire de regarder la configuration des routeurs.
Remarque : Suite à ce test un nouveau problème concernant IGMP a fait surface. En effet, on a pu observer une tendance à l'inondation au niveau 2. Des postes qui n'ont pas répondu à la requête

d'adhésion une première fois, continuent à recevoir régulièrement un message diffusé comme un Broadcast par le commutateur. Il existe tout de même une solution à ce problème **(uniquement pour les équipements CISCO)** qui permet au commutateur d'acquérir une compétence de niveau 3 afin de pouvoir participer et optimiser le trafic IGMP grâce à **IGMP Snooping**.

Test 3 : Vérifier l'étanchéité du vlan consacré à la télésurveillance (Vlan 10) :
Ici nous allons tester d'accéder au groupe multicast de diffusion vidéo 224.20.20.20 depuis un poste externe au Vlan's puis depuis un vlan autre que le vlan de diffusion vidéo (vlan 10)

Figure 9 : Erreur lors d'un accès extérieur

Les résultats obtenus sont très convainquant car les accès sont bloqués dans le deux cas, et cela même après une authentification réussie. Ce test est très important, en effet le Vlan contenant le vidéo doit être complètement isolé de tous les autres trafics sans quoi la sécurité d'accès au flux serait inefficace. Un poste quelconque ayant en sa possession un compte et mot de passe dérobé pourrait alors accéder aux images. Dans notre cas une gestion des ports participant au vlan video est possible et cette aspect renfoncera donc la sécurité du réseau.

Test 4 : Faire un filtrage multicast avec une ACL dans un Vlan. Le but est d'interdire l'inscription au groupe multicast 224.20.20.20 avec l'adresse IP 192.168.2.10 (Vlan 10).

Dans ce cas, l'idée était alors de mettre en place une ACL étendue bloquant les messages IGMP pour un poste en particulier. L'idée reste à être exploitée car dans mon cas cela n'a pas fonctionné, alors que l'adresse IP du poste n'apparaissait plus dans la table des membres IGMP le poste continuait à recevoir des flux multicast.

TOPOLOGIE MODIFIEE POUR LA SUITE DES TESTS

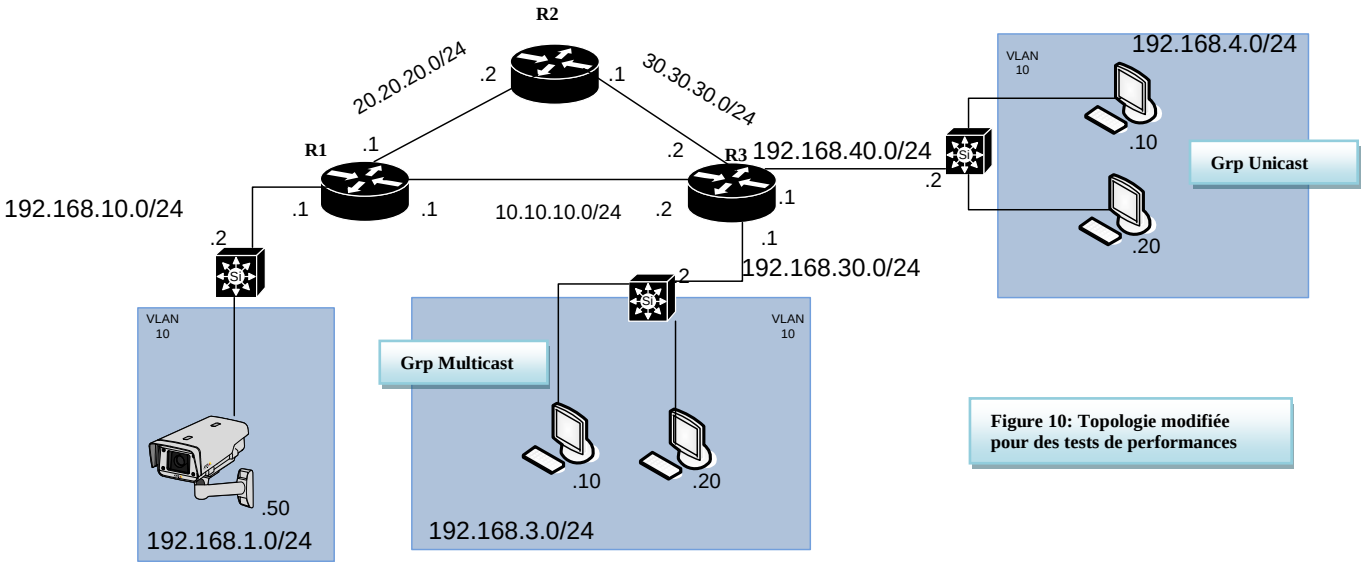


Figure 10: Topologie modifiée pour des tests de performances

Remarque : Dans cette configuration les équipements utilisés sont identiques à la configuration précédente.

Test 5 : Les modifications apportées vont nous permettre de vérifier que le multicast montre davantage de performances dans le cas suivant. Les flux seront acheminés vers R3, on se place alors sur les interfaces de celui-ci pour observer les performances. On notera que le groupe Multicast aura deux membres, de même que le groupe Unicast.

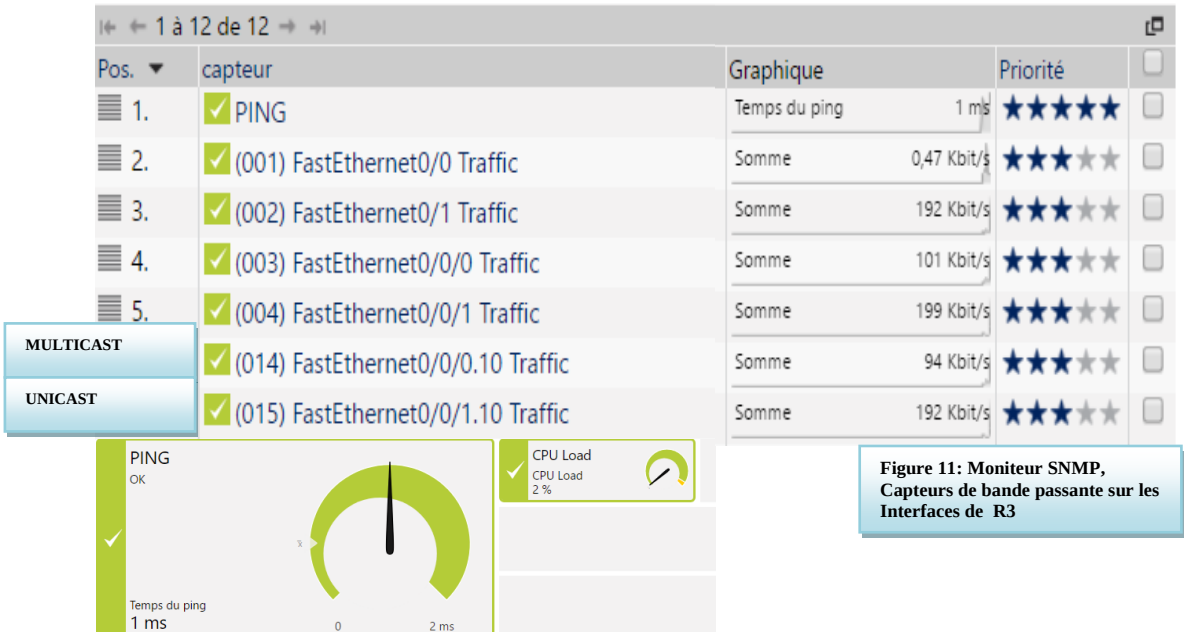
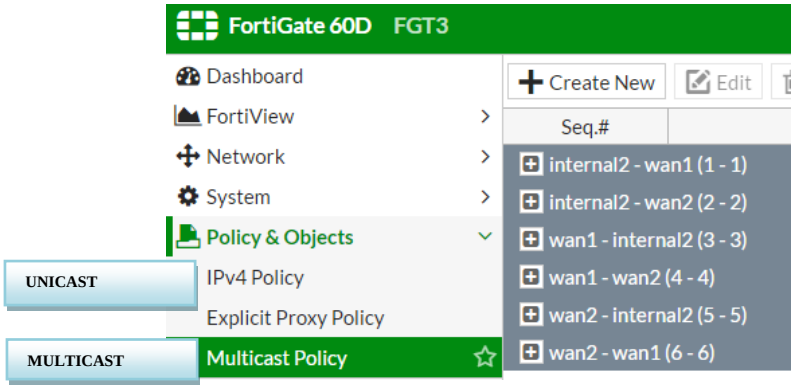


Figure 11: Moniteur SNMP, Capteurs de bande passante sur les Interfaces de R3

Test 6 : Le dernier test consistera à mettre en place une configuration où l'on remplacera les routeurs CISCO par des firewalls Fortinet.
Le résultat qui en découle est très prometteur, en effet le routage PIM est présent sur ces équipements. Néanmoins l'interface de configuration du routage multicast n'est pas présent par défaut ni même celui d'OSPFv2, il faut donc débloquer ces options depuis le terminale avec les commandes suivantes :
#config system settings
#(settings)set gui-multicast-policy enable (Activation du multicast)
#(settings) set gui-dynamic-routing enable (Activation du routage dynamique)
La configuration d'IGMP est implicite sur le firewall, l'implémentation fonctionne correctement et semble plus simple que sur les routeurs CISCO.
Remarque : La redirection des flux est une étape primordiale sur les firewalls Fortinet et dois donc être pris en compte sur tous les interfaces une fois les routages en places, dans le cas contraire aucun des routages (unicast et multicast) n'est fonctionnels. Dans de réelles conditions des stratégies peuvent être mis en place pour filtrer le trafic. Pour les tests nous avons permis tous les trafics.



7 Bilan synthèse conclusion

Lors de cette étude, on a pu observer les différents aspects du multicast dans le domaine de la vidéosurveillance. À ce jour, le protocole PIM-SM est le protocole de routage multicast le plus largement déployé et est, d'après notre étude, le plus favorable au projet RGV.
Les tests ont prouvé qu'il est possible d'implémenter le multicast en parallèle avec un routage unicast OSPF sans problèmes. L'implémentation d'un Vlan spécialement conçue pour le multicast pourrait alors permettre de traiter le multicast indépendamment de l'unicast. Le point sur le multi RP abordé en théorie, mais pas mis en place en pratique reste tout de même un point important dans le cadre d'un réel déploiement car il peut permettre une meilleure disponibilité en cas de pannes.
En ce qui concerne la sécurité d'accès, PIM-SM ne permet pas de solution d'authentification, il est donc primordial d'avoir des paramètres d'authentifications supplémentaires comme par exemple, les paramètres d'authentification de la caméra AXIS dans notre cas. Un problème très important lié à l'utilisation de l'IGMP a été relevé. En effet, l'inondation des paquets IGMP peut être très coûteuse, c'est pourquoi une solution IGMP Snooping doit être implémentée. La dernière étape de notre étude prouve qu'une solution multicast peut être déployée sur de différents équipements tels que des firewalls Fortigates. La configuration d'un réseau en multicast peut avoir de très nombreux avantages, néanmoins, seule une personne qui maîtrise le multicast sous tous ses aspects, peut tirer le maximum de profit de cette technologie. À ce stade des tests, on remarque tout de même dans notre cas, malgré le manque de postes de visualisation, que le multicast montre des performances supérieures à l'unicast.

8 Missions secondaires

8.1 Durcissement et pré configurations

Objectifs de l'activité :
- Brancher, configurer, et Tester les Commutateurs Cisco 3650.
- Réaliser un durcissement des commutateurs et les tester avec d'autres commutateurs avec une génération et versions antérieurs.

Réalisation de l'activité :
Le but de cette activité était de mettre en place une maquette pour tester la compatibilité de 4 nouveaux équipements Cisco en s'assurant de leur compatibilité avec les versions antérieures.
L'intérêt de cette mission était de permettre une utilisation optimale et sécurisé dans les normes, dans une architecture déjà en place, pour but de diminuer les risques d'incompréhension entre deux équipements.

Les tâches réalisées sont :
- Vérification de la version et d'éventuelles restrictions qui lui sont liée.
- Configuration du durcissement de l'équipement (utilisateur, mdp, accès Telnet).
- Test de connexion, version et port fibre optique avec deux commutateurs Cisco 2960.
- Récupération de la configuration en Ftp.

Difficultés rencontrées :
L'un des commutateurs n'avait pas été remis à zéro et le mot de passe n'était pas renseigné.
Il pouvait être remis à zéro avec le bouton de changement de mode sur ce modèle.

8.2 Test de migration d'une camera AXIS

Objectifs de l'activité :
- Brancher, configurer, et Tester la camera AXIS.
- Réaliser une migration vers un autre réseau et tester le fonctionnement.
- Réaliser revenir à la configuration de base avant de quitter la centrale hydraulique.

Réalisation de l'activité :
Le but de cette activité était de migrer une camera AXIS d'un réseau à un autre en s'assurant qu'aucuns problèmes n'étais causés par ce changement. La camera avait pour but de surveiller le canal de fuite du barrage de l'Argentier, c'est pourquoi il était essentiel de procéder à ce test rapidement.

Les tâches réalisées sont :
- Une pré configuration du logiciel de visionnage EDF (codé en xml/Annexe 8)
- Modifier l'adresse IP, masque et passerelle par défaut de la camera (migration vers le réseau cible)
- Tester la connexion depuis le local de visualisation.
- Ramener toutes les modifications et configurations à leur état initial.

Difficultés rencontrées :
Le câble à la sortie de l'injecteur de la camera était en très mauvais état, il a fallu le remplacer.
Un accès privilégié était configuré sur la camera, nous avons dû appeler le bureau pour avoir ces informations.

9 ANNEXES

ANNEXE 1 : Plan d'adressage

	Interface	Adresse IP /Masque
R1	Fa0/0	192.168.10.0/24
	Fa0/0.10	192.168.1.1/24
	Fa0/1	10.10.10.1/24
	Se0/0/0	20.20.20.1/24
R2	Fa0/0	192.168.20.0/24
	Fa0/0.10	192.16.2.1/24
	Fa0/1	30.30.30.1/24
	Se0/0/0	20.20.20.2/24
R3	Fa0/0	10.10.10.2/24
	Fa0/1	30.30.30.30.2/24
	Fa0/0/0	192.168.30.1/24
	Fa0/0/1	192.168.40.1/24
	Fa0/0/0.10	192.168.3.1/24
	Fa0/0/1.10	192.168.4.1/24

ANNEXE 2 : Routage OSPFv2

R1	R2	R3
router ospf 1 router-id 1.1.1.1 log-adjacency-changes auto-cost reference-bandwidth 10000 timers throttle spf 10 100 5000 timers throttle lsa all 10 100 5000 timers lsa arrival 80 passive-interface FastEthernet0/0 network 10.10.10.0 0.0.0.255 area 0 network 20.20.20.0 0.0.0.255 area 0 network 192.168.1.0 0.0.0.255 area 0 network 192.168.10.0 0.0.0.255 area 0	router ospf 1 router-id 2.2.2.2 log-adjacency-changes auto-cost reference-bandwidth 10000 timers throttle spf 10 100 5000 timers throttle lsa all 10 100 5000 timers lsa arrival 80 passive-interface FastEthernet0/0 network 20.20.20.0 0.0.0.255 area 0 network 30.30.30.0 0.0.0.255 area 0 network 192.168.2.0 0.0.0.255 area 0 network 192.168.20.0 0.0.0.255 area 0	router ospf 1 router-id 3.3.3.3 log-adjacency-changes auto-cost reference-bandwidth 10000 timers throttle spf 10 100 5000 timers throttle lsa all 10 100 5000 timers lsa arrival 80 passive-interface FastEthernet0/0/0 passive-interface FastEthernet0/0/1 network 10.10.10.0 0.0.0.255 area 0 network 30.30.30.0 0.0.0.255 area 0 network 192.168.3.0 0.0.0.255 area 0 network 192.168.4.0 0.0.0.255 area 0 network 192.168.30.0 0.0.0.255 area 0 network 192.168.40.0 0.0.0.255 area 0

ANNEXE 3: Routage PIM-SM et Configuration IGMP

Pour activer le routage multicast :
Router (config) #**ip multicast-routing**
PIM (Protocol Independent Multicast) est le protocole de routage multicast retenu dans les architectures de référence.
Sur tous les liens d'interconnexions niveau 3 le protocole PIM est activé.
Pour activer PIM sur une interface routée :
Router (config) #**interface Fa<Numéro Int>**
Router (config-if) #**ip pim sparse-mode**
Pour accélérer la convergence du multicast en cas de défaillance d'un équipement de l'architecture :
Router (config-if) #**ip pim query-interval 900 msec**
Pour fixer de façon manuelle le Rendez-vous Point (RP)
Router (config-if) #**ip pim rp-address <@ip_du_RP>**
IGMP sera la solution retenue dans l'architecture de référence, on activera IGMP sur toutes les interfaces accueillant des postes de visualisation
Pour limiter l'accès à certains groupes multicast :
Router (config) #**interface Fa<Numéro Int>**
Router (config-if) #**ip igmp access-group <Numéro Access List >**

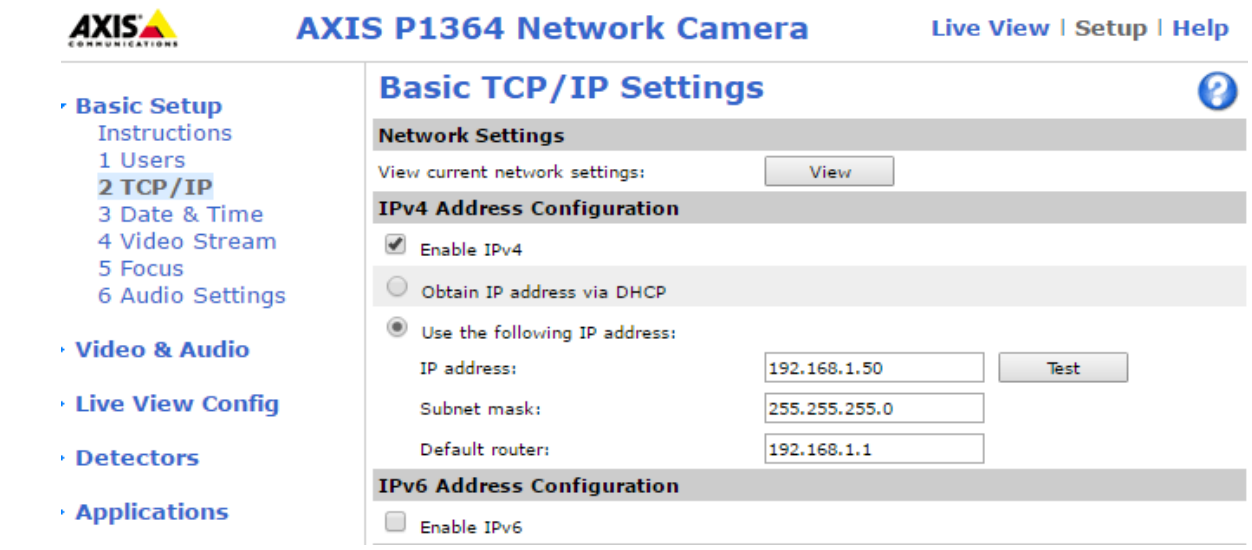
ANNEXE 4 : Switching

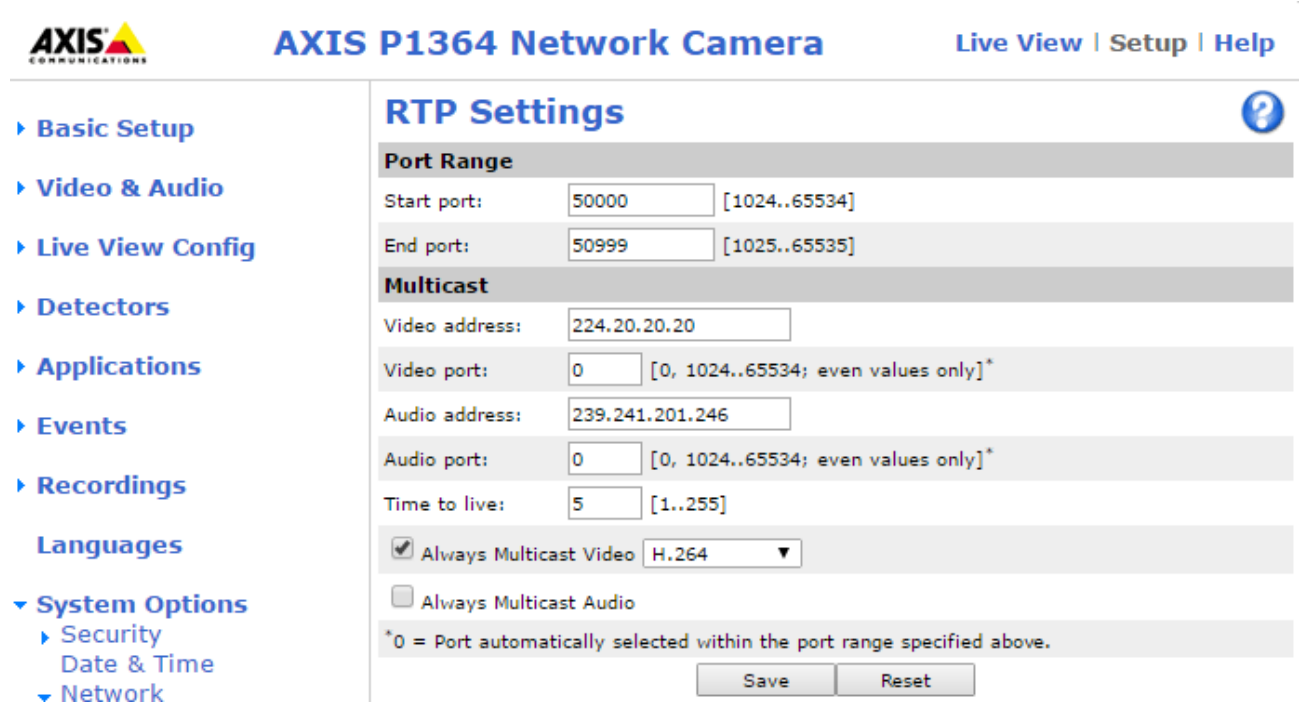
Pour garantir une meilleure stabilité et sécurité, plusieurs paramètres de sécurité sont mis en place :
- **Port-Security** : cette fonctionnalité permet de restreindre le nombre d'adresses MAC sur un port donné du commutateur :
Switch (config-if-range) #**switchport port-security**
Switch (config-if-range) #**switchport port-security maximum <1-…>**
Switch (config-if-range) #**switchport port-security aging time <1-…>**
Switch (config-if-range) #**switchport port-security violation restrict**
Switch (config-if-range) #**switchport port-security aging type inactivity**
Remarque : En cas de dépassement du seuil, une alarme est remontée au niveau des logs (en local et syslog) et un trap SNMP est envoyé vers le serveur de supervision.

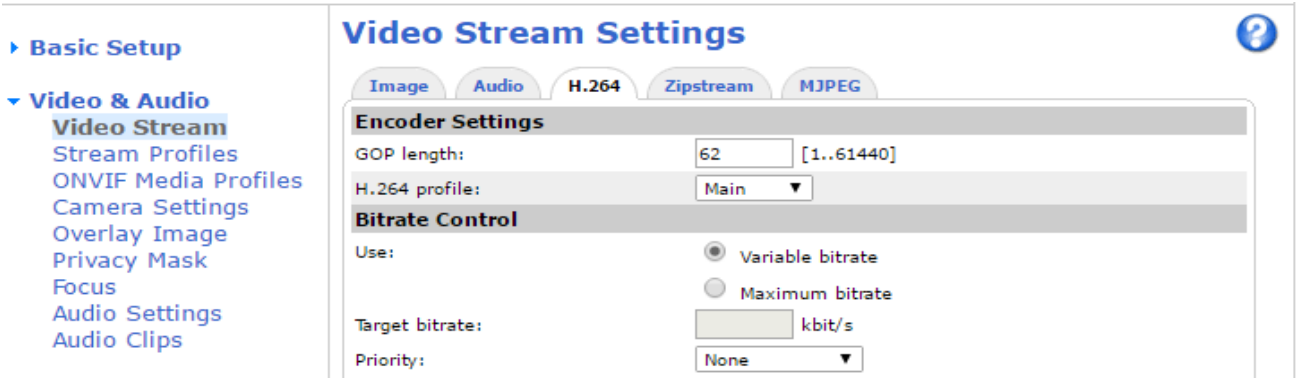
- Le « **Storm-Control** » permet au commutateur de s'auto-défendre en cas de tempête de broadcast. Il sera limité à **1%** de la bande passante.
Switch (config-if-range) #**storm-control broadcast level <1.00> <0.50>**
Switch (config-if-range) #**storm-control action trap**
Remarque : En cas de tempête de broadcast, une alarme est remontée au niveau des logs (local et syslog) et untrap SNMP est envoyé vers le serveur de supervision.

- Le spanning-tree doit être désactivé sur les ports d'accès. Cependant, en cas de réception d'un «BPDU» sur le port, il est désactivé pendant 5 min (fonctionnalités portfast et bpduguard).
Switch (config-if-range) #**spanning-tree portfast**
Switch (config-if-range) #**spanning-tree bpduguard enable**

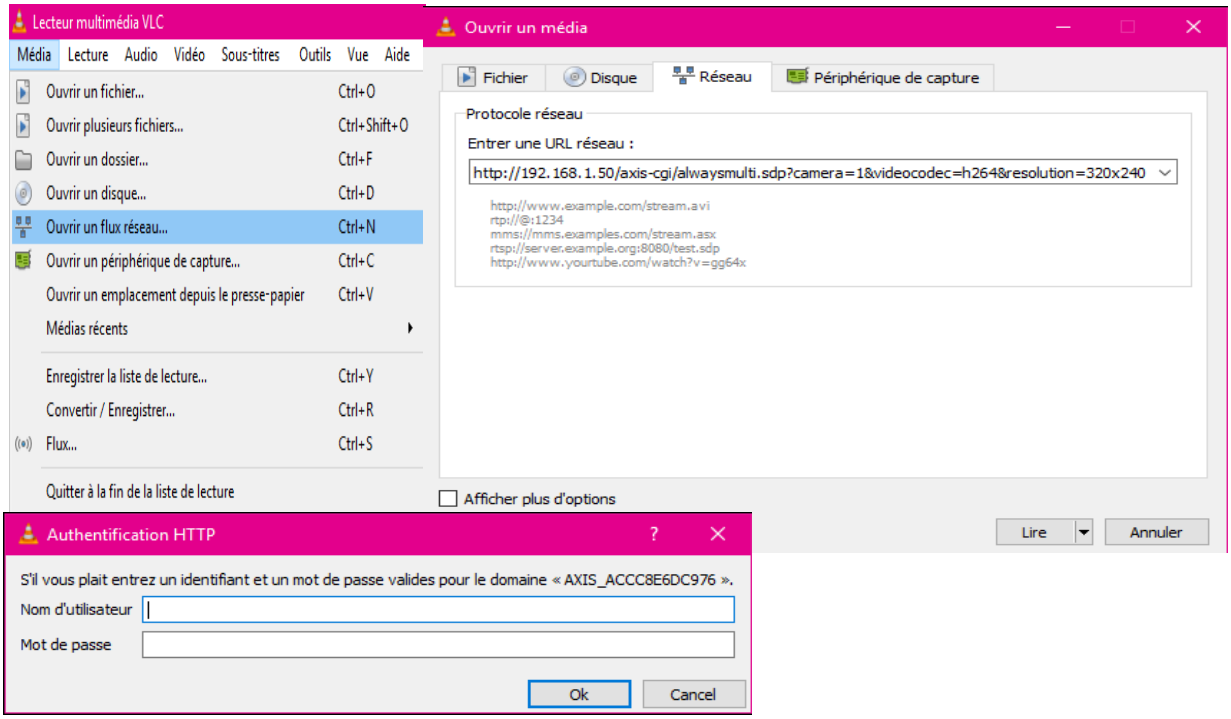
ANNEXE 5: Configuration caméra IP AXIS



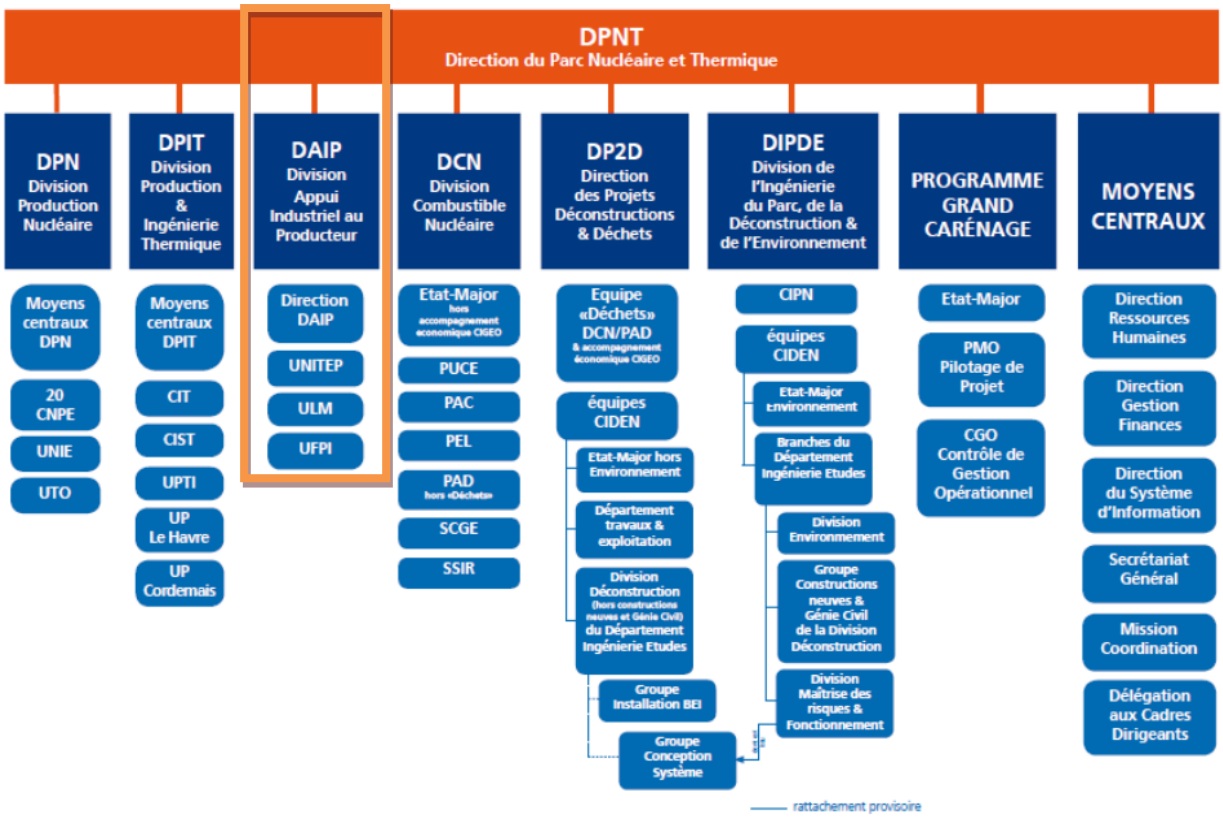


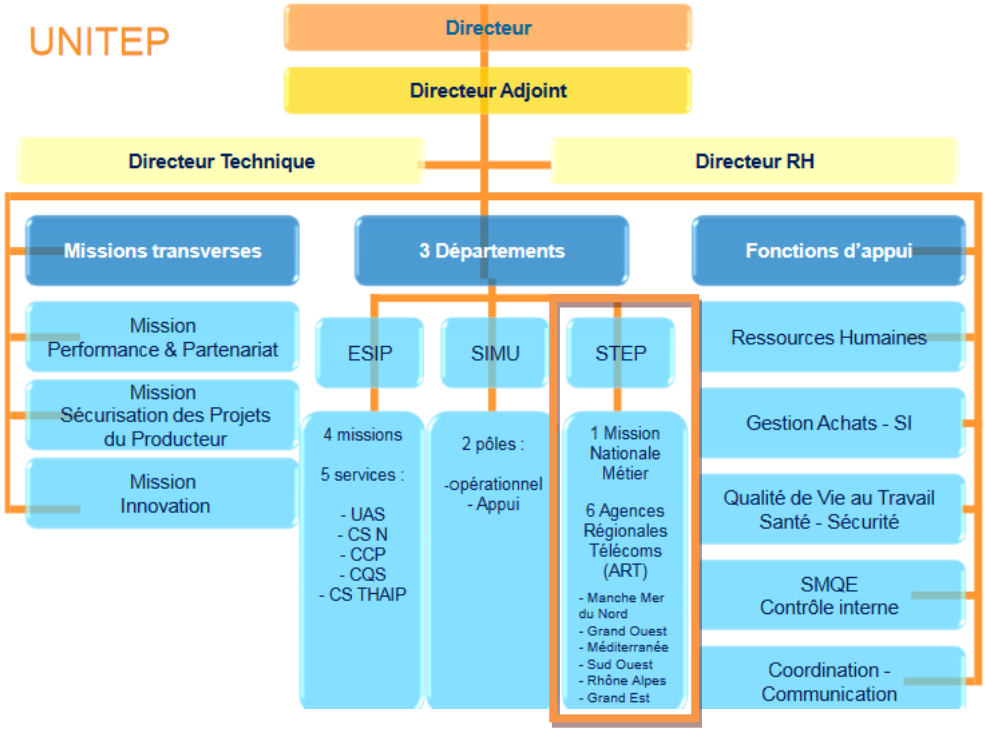


ANNEXE 6 : Configuration poste de visionnage avec VLC



ANNEXE 7 : Organigrammes du groupe EDF





ANNEXE 8 : Fichier de configuration xml pour le poste de visualisation

```
<?xml version="1.0"?>
<!-- Logiciel réalisé par Websenso.com en 2014 sous licence EDF -->
<!-- Le mode 3G permet de remplacer les vidéos par des photos en journée et de ne rien rafraichir dans la période de nuit. Mode nuit inactif si mode3G=0 -->
<config animationBackground="0" modeNuitMessage="Mode nuit activé - Pas de rafraichissement" modeNuitFin="7" modeNuitDebut="18" mode3G="0" dureeParCamera="7" name="AMENAGEMENTS GH">
        <!-- debitReserve=1 permet d'afficher les photos sur la partie gauche de l'écran -->
        <!-- Si l'image ne peut pa s'afficher, elle sera remplacée par l'icone sur fond blanc. Si hs=1, la caméra est retirée de l'animation. -->
        <!-- overlay indique le nom de l'image à superposer sur la caméra. Placer le fichier dans \ConfigBorneEDF\Overlays. L'image doit être en 800x600 et avoir un fond transparent. -->
  - <amenagement name="L'Argentière" abreviation="LA" color="0x1e7fcb">
      - <site name="Prise d'eau de Vallouise">
            <webcam name="Aval RD" compression="0" fps="30" resolution="CIF" hs="0" overlay="" debitReserve="0" pass=[redacted]" user=[redacted]" port="80" host="[redacted]"/>
            <webcam name="Amont RG" compression="0" fps="30" resolution="CIF" hs="0" overlay="" debitReserve="0" pass=[redacted]" user=[redacted]" port="80" host="[redacted]"/>
            <webcam name="Local prise d'eau" compression="0" fps="30" resolution="CIF" hs="0" overlay="" debitReserve="0" pass=[redacted]" user=[redacted] port="80" host="[redacted]/>
            <webcam name="Local prise d'eau2" compression="0" fps="30" resolution="CIF" hs="0" overlay="" debitReserve="0" pass=[redacted]" user=[redacted] port="80" host="[redacted]/>
            <webcam name="Débit réservé" compression="0" fps="30" resolution="320x240" hs="0" overlay="" debitReserve="1" pass=[redacted]" user=[redacted] port="80" host=[redacted]"/>
        </site>
      - <site name="Station de pompage">
            <webcam name="Amont barrage" compression="0" fps="30" resolution="CIF" hs="0" overlay="" debitReserve="0" pass=[redacted]" user=[redacted] port="80" host=[redacted]"/>
            <webcam name="Débit réservé" compression="0" fps="30" resolution="320x240" hs="0" overlay="" debitReserve="1" pass=[redacted]" user=[redacted] port="80" host="[redacted]/>
        </site>
```

10 Glossaire

Item	Description
EDF	**Electricité de France**
RP	**Rendez-vous point**
DAIP	**Division Appui Industriel à la Production**
UNITEP	**Unité Nationale systèmes d'Information et Télécoms d'Exploitation du Producteur**
COPAT	**Equipement électrique des salles de pilotage d'arrêt de tranche, comprenant le réseau informatique, les vidéo-projecteurs (…)**
STEP	**Service Télécoms d'Exploitation du Producteur**
IGMP	**Interne Group Management Protocol**
DR	**Designated Router**
PIM	**Protocole Independent Multicast**
OSPF	**Open Shortest Path First**

11 Bibliographie

Informations sur l'entrreprise . myelectricnetwork.fr*(EDF)* .

Configuring IGMP Snooping. (July 17, 2015). *LAN Switching (Cisco Networking Academy Program)* .

Multicast Quick-Start Configuration Guide. (August 30, 2005). *PIM routing (Cisco Networking Academy Program)* .

FortiGate Multicast Version 4.0 Technical note. (-). *Configuration note (Fortinet)*

Configuration SNMP: http://www.acipia.fr/support/faq/protocole-snmp-switch-cisco/

VLC documentation. https://wiki.videolan.org/Documentation:Documentation