Accéder à son réseau local depuis un réseau sans fil de 400 bornes

Sébastien Boggia
Centre Réseau Communication (CRC), Université Louis Pasteur
7, rue René Descartes, 67084 Strasbourg
Sebastien.Boggia@crc.u-strasbg.fr

Résumé

Depuis 2002, le Centre Réseau Communication est impliqué dans le déploiement à grande échelle du réseau sans fil Osiris. Mis en exploitation en avril 2005, celui-ci est en expansion constante. Il compte à ce jour plus de 400 points d'accès répartis sur l'ensemble des campus strasbourgeois.

Le CRC propose deux méthodes d'accès complémentaires dans deux réseaux mutualisés : un accès rapide basé sur un portail d'authentification web et un accès sécurisé 802.1X.

Suite à des demandes récurrentes, nous avons décidé de faire évoluer l'infrastructure 802.1X en permettant aux utilisateurs de se retrouver dans le réseau de leur composante (établissement, laboratoire, service) quel que soit le lieu de connexion sur le réseau sans fil Osiris.

Cet article décrit la solution que nous avons conçue, basée sur un développement noyau dans un équipement dédié embarquant une fonction d'aiguillage de trafic. Nous aborderons également les choix que nous avons faits pour l'intégrer dans l'infrastructure sans fil existante constituée de points d'accès standards et nous conclurons sur quelques perspectives d'évolution.

Mots clefs

Wi-Fi, Mobilité, 802.1X

1 Introduction

En 2002, le CRC (Centre Réseau Communication), opérateur du réseau métropolitain Osiris a été impliqué pour soutenir un projet de recherche sur la mobilité IPv6 dans les réseaux sans fil. Ce projet a entraîné une première phase de déploiement. Par la suite, le souhait des utilisateurs et des directions des établissements, soutenu par l'appel d'offres MIPE, a permis de généraliser le déploiement à très grande échelle. Le réseau sans fil devait répondre aux besoins de mobilité des utilisateurs tout en assurant la sécurité des communications et une bonne qualité de service. Pour satisfaire l'ensemble de ces critères, il est rapidement apparu qu'un déploiement anarchique devait être évité. C'est pourquoi les établissements du réseau Osiris ont décidé de confier le déploiement et l'exploitation du réseau sans fil au CRC.

À ce jour, le réseau sans fil est en expansion constante ; il compte actuellement 405 points d'accès répartis dans 50 bâtiments. Depuis la mise en exploitation généralisée en avril 2005, le service a été adopté par 13 500 utilisateurs différents.

Afin d'offrir le maximum de flexibilité aux utilisateurs, deux méthodes d'accès aux réseaux au sans fil ont été définies : un accès « rapide » par l'intermédiaire d'un portail captif Web et un accès sécurisé par l'intermédiaire d'un client IEEE 802.1X. Pour accroître la mobilité des utilisateurs, le service « Eduroam » a été déployé sur l'accès sécurisé depuis début 2007.

Suite à l'adoption massive du service et pour tenir compte des demandes récurrentes des utilisateurs, nous avons fait évoluer la connectivité pour offrir une mobilité optimale. Notre implémentation permet désormais aux utilisateurs du réseau sans fil de se retrouver dans le réseau de leur composante quel que soit leur lieu de connexion et de profiter de leur politique de sécurité interne, et ce en toute transparence.

Nous allons décrire ici la solution que nous avons conçue, les développements que nous avons mis en œuvre puis nous terminerons par les perspectives d'évolution.

2 Le contexte du réseau sans fil Osiris

Le réseau sans fil Osiris conçu dans le but d'apporter un maximum de sécurité et de flexibilité pour répondre à l'ensemble des besoins, nous a conduit à déployer deux méthodes d'accès :

- **l'accès sécurisé**. Ce mode d'accès est basé sur une authentification IEEE 802.1X [1] supportant l'ensemble des protocoles de chiffrement (WEP, WPA, WPA2, TKIP, AES-CCMP). L'authentification 802.1X a été choisie pour plusieurs raisons : elle permet une authentification EAP/TTLS totalement sécurisée et une gestion automatique des clefs. Elle donne aussi un accès au réseau au niveau 2, ce qui a pour avantage de permettre le fonctionnement de tous les protocoles de niveau supérieur (IPv6, Multicast...). Son adoption massive fait que cette méthode d'authentification est maintenant nativement intégrée dans la majorité des systèmes d'exploitation.
- **l'accès rapide**. Ce mode d'accès développé comme une solution complémentaire à l'authentification 802.1X fonctionne à l'aide d'un portail captif couplé à une authentification Web HTTPS. Il a le mérite d'être

particulièrement simple d'utilisation puisqu'il ne nécessite aucune installation et configuration d'un client 802.1X sur le poste client. Il se montre adapté aux utilisateurs occasionnels comme les invités ou les conférenciers car il répond à 90% des besoins en permettant l'utilisation du Web et des protocoles sécurisés de la messagerie.

Les accès rapides (portail captif) et sécurisés (802.1X) sont déclinés sous la forme de deux SSID : « **osiris** » pour l'accès rapide et « **osiris-sec** » pour l'accès sécurisé. Ils connectent les utilisateurs dans deux réseaux IP propagés sur l'ensemble des équipements sans fil.

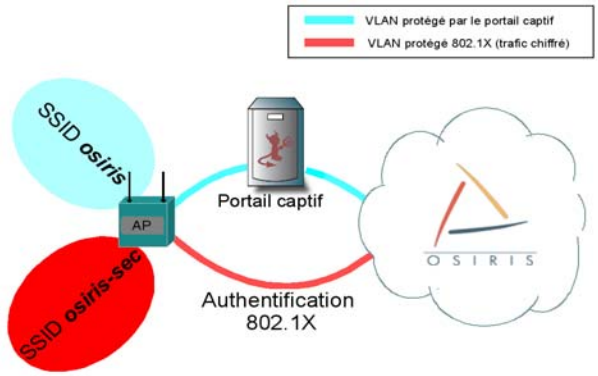

Figure 1: modes d'accès

Avec le recul, ces deux méthodes cumulent des temps de connexion sensiblement identiques. Comme l'ensemble des services authentifiés Osiris, l'accès au réseau sans fil repose sur le service d'authentification centralisé Osiris [2] lui même basé sur les annuaires d'établissement et les protocoles Radius et LDAP.

3 Les objectifs

Le développement d'un nouveau service pour donner accès aux utilisateurs du réseau sans fil à leur propre réseau de composante doit tenir compte d'un certain nombre de critères.

Pour commencer, le nouveau service doit s'intégrer parfaitement à l'infrastructure existante. À ce jour plus de 400 points d'accès ont été déployés et les 500 devraient être atteints d'ici la fin de l'année 2007. Il faut donc adapter le nouveau service en fonction du parc existant.

Le réseau sans fil Osiris a été pensé pour n'utiliser que des solutions et protocoles standards. L'évolution des matériels d'un constructeur n'étant pas prévisible, le matériel déployé a été sélectionné de manière à ne pas nous lier à un constructeur d'équipements actifs ou à une technologie propriétaire. Nous avons donc exclu les solutions propriétaires qui peuvent se montrer d'ailleurs très onéreuses en particulier en raison de la taille de notre réseau.

Pour ne pas nuire à la mobilité, critère très important dès l'origine des études du réseau sans fil, nous devons permettre à l'utilisateur de se connecter à son réseau de composante où qu'il se trouve. C'est à dire y compris lors de ses déplacements sur l'ensemble des campus Osiris. Ceci exclut la mise en place d'un SSID spécifique à une composante dans ses propres locaux.

Pour des raisons de convivialité, la méthode d'authentification pour l'accès au nouveau service doit rester identique aux méthodes d'authentification du réseau sans fil Osiris. L'utilisateur ne doit pas être rebuté par une nouvelle méthode supplémentaire pas forcément évidente à configurer.

Enfin, être connecté depuis le réseau sans fil directement dans son propre réseau de composante, c'est un peu comme prolonger le réseau en question jusqu'au point d'accès : cela nécessite un niveau de sécurité très élevé.

À ce jour le service VPN Osiris [3] peut répondre à une partie de nos besoins. Le VPN, grâce aux offres « VPN-lab » et « VPN-lab+ », peut faire arriver un utilisateur via un tunnel IPSec directement dans son réseau de composante. Utilisé sur le réseau sans fil, il permet de répondre à nos besoins de sécurité et d'accès dans le réseau de composante. Nous devons par contre tenir compte de certaines limitations. Le VPN ne répond pas à nos critères de convivialité puisque l'utilisateur doit s'authentifier en premier lieu pour accéder au réseau sans fil puis installer et lancer un client VPN ; des utilisateurs nous ont fait part de leur souhait de se connecter à leur composante de manière plus transparente. De plus, il arrive souvent que le tunnel VPN soit rompu en cas de roaming. Enfin, le VPN Osiris n'a pas vocation à servir de contrôleur d'accès pour le réseau sans fil. Il a été étudié avant tout pour donner accès aux ressources internes des utilisateurs connectés hors du réseau Osiris. Un aussi grand nombre d'utilisateurs du réseau sans fil pourrait influer sur les performances du serveur VPN.

Pour répondre à nos besoins de sécurité et aussi de convivialité, nous nous sommes donc tournés vers un accès 802.1X. L'authentification 802.1X nous apporte beaucoup d'avantages. Elle est déjà utilisée pour l'accès sécurisé de notre réseau sans fil avec un système d'authentification robuste et de très bons systèmes de chiffrement des données. Elle donne également un accès direct au niveau Ethernet ce qui permet en plus d'IPv4, d'utiliser IPv6 ou le Multicast. Enfin, l'accès direct au réseau de la composante n'implique aucune modification par l'utilisateur de l'accès sécurisé de la configuration de son client 802.1X.

Ce protocole fournit des fonctionnalités d'affectation dynamique de Vlan selon le profil de l'utilisateur. Cependant en raison du nombre important de composantes existantes sur le réseau Osiris (environ 150) nous nous heurtons aux limitations de nos points d'accès en nombre de Vlans. À ce jour, nous n'avons pas pu tester de point d'accès supportant autant de Vlans et répondant à tous les prérequis du réseau sans fil Osiris. Nous devons aussi tenir compte du parc existant sur lequel nous rencontrons un problème qui rend la fonctionnalité d'affectation dynamique de Vlan inopérante dans le cadre du réseau sans fil Osiris.

En prenant en compte l'ensemble de ces critères, nous avons donc décidé de développer une nouvelle solution innovante que nous avons appelée le « Vlaniseur ».

4 Le Vlaniseur

4.1 Principe de fonctionnement

Le Vlaniseur est un dispositif pour aiguiller le trafic depuis un réseau d'accès sans fil vers des Vlans spécifiques de chaque entité. Il se trouve en coupure sur le réseau entre les points d'accès sans fil et les différents réseaux de composantes.

Ainsi, nous avons créé sur chaque point d'accès du réseau sans fil Osiris un nouveau SSID « **osiris-lab** » qui indique clairement à l'utilisateur qu'en s'y connectant, avec les configurations 802.1X du mode sécurisé, il accède dans son réseau de composante.

Les utilisateurs associés au SSID « **osiris-lab** » se trouvent connectés dans un unique Vlan d'accès directement déployé sur le point d'accès. Le terme « Vlan d'accès » est important, il reviendra à plusieurs reprises dans ce document.

Le Vlaniseur intervient ensuite pour aiguiller le trafic de chaque utilisateur vers son réseau de composante.

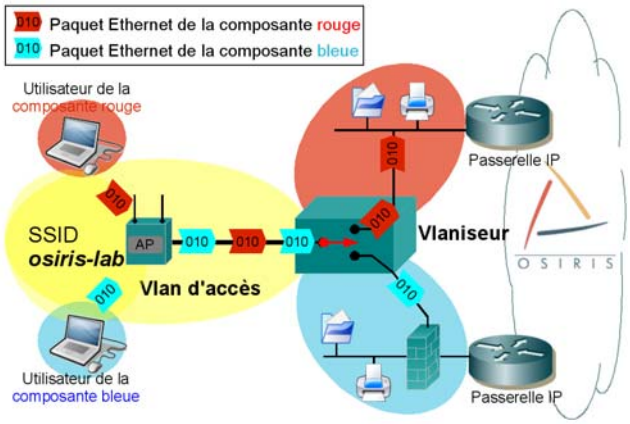

Figure 2: principe du Vlaniseur

La figure 2 illustre le principe : on peut voir que l'ordinateur de l'utilisateur appartenant à la composante rouge est authentifié et identifié comme devant accéder à la composante rouge. Le trafic Ethernet est aiguillé par le Vlaniseur directement vers le Vlan de la composante rouge et inversement.

Le Vlaniseur n'intervient qu'au niveau de la couche 2 (Ethernet), ce qui laisse une grande flexibilité aux entités pour la gestion des couches supérieures. L'utilisateur peut ainsi profiter du plan d'adressage IPv4 et IPv6 de sa composante ou de sa politique de sécurité. Il peut aussi, selon la politique appliquée par l'administrateur, avoir accès à l'ensemble des ressources de son réseau local comme les serveurs de fichiers, les imprimantes, etc.

L'administrateur de la composante peut décider de faire arriver le trafic sortant du Vlaniseur sur une interface spécifique de son garde-barrière ou même de bridger cette interface directement avec son réseau local.

4.2 Commutateur ou gare de triage ?

Le Vlaniseur fonctionne comme un commutateur au niveau de la couche « liaison » du modèle OSI (Ethernet). Cependant, la différence avec un commutateur est la présence d'une fonction d'aiguillage, basée sur une table d'association < adresse MAC de l'utilisateur authentifié, numéro du Vlan de composante, numéro du Vlan d'accès > qui est fournie après chaque authentification 802.1X. Il n'y a aucune fonction d'apprentissage automatique comme sur un commutateur.

Ce mode de fonctionnement est relativement simple et nécessite peu de données.

Lorsqu'un utilisateur se connecte au réseau sans fil en 802.1X le Vlaniseur récupère 3 paramètres essentiels :

- l'adresse MAC du poste client. Celle-ci est connue par le serveur RADIUS lors de l'authentification.
- le Vlan d'accès du point d'accès sans fil. Celui-ci est connu grâce à l'adresse IP du point d'accès obtenue lors de l'authentification 802.1X.
- le Vlan de composante de l'utilisateur. Cette donnée est récupérée dans l'annuaire LDAP Osiris.

Avec ces paramètres, le Vlaniseur peut rediriger le trafic d'un utilisateur connecté à un point d'accès vers son réseau de composante.

Pour illustrer le fonctionnement du Vlaniseur sur un exemple, basons-nous sur la table d'association suivante contenue en mémoire dans le Vlaniseur.

Adresse MAC du client	*Vlan d'accès*	*Vlan de composante*
A	11	101
B	12	102
C	12	101

Après authentification, les adresses MAC de trois machines sont inscrites dans le Vlaniseur : les adresses MAC A, B et C.

Sur la figure 3, A envoie une trame Ethernet avec une adresse de destination quelconque (adresses Unicast ou Multicast). Le Vlaniseur sait, par l'adresse source, que A appartient au Vlan de composante 101. Le Vlaniseur redirige simplement la trame vers l'interface correspondant au Vlan 101.

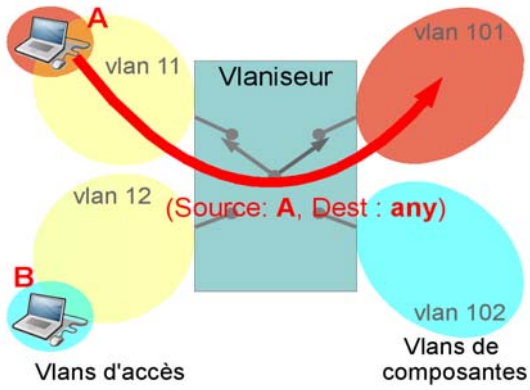

Figure 3: trame Vlan d'accès vers Vlan de composante

Sur la figure 4, une machine du Vlan de composante 101 envoie une trame à destination de l'adresse MAC A. Le Vlaniseur redirige cette trame vers le Vlan 11, car A est dûment enregistrée dans la composante 101.

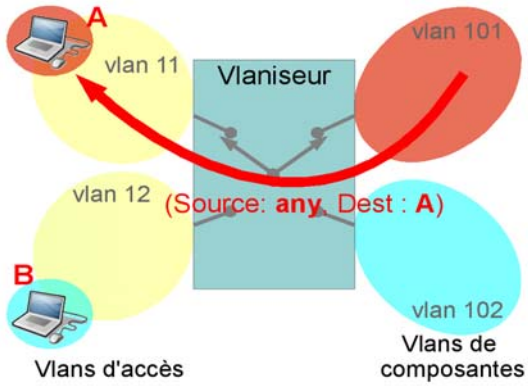

Figure 4: trame Vlan de composante vers Vlan d'accès

4.3 Le traitement du trafic de diffusion

Comme nous l'avons vu, les utilisateurs de composantes différentes peuvent se trouver connectés dans un même Vlan d'accès. Pour assurer un bon fonctionnent au niveau du réseau mais aussi pour des raisons évidentes de sécurité, les trames à destination d'adresses Ethernet de broadcast ou multicast ne doivent être diffusées qu'aux membres de la composante.

La figure 5 illustre donc une spécificité du Vlaniseur : le traitement des trames Ethernet à destination d'adresses de diffusion vers les Vlans d'accès.

Lorsque le Vlaniseur reçoit telle trame de diffusion depuis un Vlan de composante, il doit la transmettre à tous les utilisateurs de la composante connectés dans des Vlan d'accès.

Le Vlaniseur transforme donc une trame Ethernet de diffusion en n trames Ethernet unicast. Dans cet exemple on duplique la trame et on envoie une copie avec pour adresse de destination A et une autre avec pour adresse de destination C.

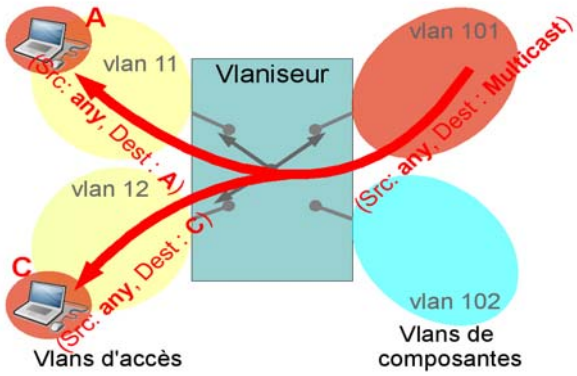

Figure 5: trafic de diffusion vers Vlans d'accès

Ce procédé obligatoire, dans le cas du fonctionnement du Vlaniseur, peut demander des ressources importantes selon le nombre d'inscrits dans un Vlan de composante et occasionner beaucoup de bruit sur le réseau. C'est en partie pour cette raison que nous utilisons plusieurs Vlans d'accès sur un Vlaniseur.

Nous verrons ultérieurement les autres solutions à adopter pour limiter le bruit engendré par cette duplication de trafic.

5 L'implémentation du Vlaniseur

5.1 Introduction

Le développement du Vlaniseur a été réalisé sous la forme d'un module noyau pour le système FreeBSD.

Après un premier développement en mode utilisateur, nous nous sommes dirigés vers le développement actuel en mode noyau, malgré la difficulté que cela représente, afin d'obtenir de bonnes performances et une bonne intégration du dispositif.

Nous utilisons l'infrastructure « Netgraph » qui facilite considérablement l'écriture de code réseau dans le noyau.

5.2 L'infrastructure Netgraph

Netgraph [4] est un sous-système réseau fonctionnant au niveau du noyau FreeBSD. Il permet de recréer des fonctionnalités réseau complexes en combinant entre elles différentes briques effectuant des tâches bien spécifiques. Cet outil a été développé dans le but de bénéficier de bonnes performances tout en maintenant une grande souplesse d'utilisation.

Les briques réseau sont appelées des nœuds (nodes) et peuvent êtres combinées entre elles par des liens (hooks) pour former un graphe réseau.

Un graphe réseau permet à une machine de réaliser des tâches spécifiques comme, par exemple, de la commutation de niveau 2 sur Ethernet ou bien du routage IP encapsulé dans des trames HDLC sur des interfaces Séries.

Lorsqu'un nœud reçoit une trame, il réalise certaines actions (ajout / suppression d'en-tête, aiguillage...) puis

transmet la trame traitée à un autre nœud par l'intermédiaire d'un lien.

L'utilitaire « ngctl » apporte les outils pour contrôler les nœuds. Il permet de les interconnecter facilement entre eux, de les paramétrer ou d'afficher les configurations et des statistiques.

5.3 Un module Netgraph pour le Vlaniseur

Développer du code noyau est une activité particulièrement exigeante : il n'y a pas de place pour l'erreur. Toute erreur dans le code peut bloquer instantanément le système. Pour faciliter le développement du Vlaniseur et visualiser rapidement les messages de debug suite à une panique du système, nous avons créé un environnement de développement constitué de plusieurs machines virtuelles sous VMware.

En général à une fonctionnalité réseau de Netgraph, correspond un module noyau. Nous avons donc écrit un nouveau module Netgraph dans lequel sont implémentées les fonctionnalités du Vlaniseur. Ce module porte le nom de « ng_e2v ».

Pour faire fonctionner le Vlaniseur, nous utilisons aussi deux autres modules existants :

– le module ng_ether qui permet de lire et décrire directement les trames Ethernet sur la carte réseau ;

– le module ng_vlan qui permet d'insérer ou de retirer le tag 802.1Q dans la trame Ethernet.

Voici la liste des modules Netgraph du Vlaniseur :

```
majax# kldstat
Id Refs Address    Size     Name
 1    9 0xc0400000 63070c   kernel
 ...
 4    1 0xc1f5c000 3000     ng_ether.ko
 5    4 0xc1f5f000 a000     netgraph.ko
 6    1 0xc1f6d000 3000     ng_vlan.ko
 7    1 0xc1f70000 4000     ng_e2v.ko
 8    1 0xc1f7a000 4000     ng_socket.ko
```

La figure 6 donne une représentation de l'infrastructure Netgraph dans la machine faisant office de Vlaniseur.

– Les nœuds sont représentés par des carrés scindés en deux. La partie supérieure indique le nom du nœud (et donc le module utilisé, ajouter le préfixe ng_), la partie inférieure son type.

– Les liens sont représentés par des ovales avec des noms indiquant leurs fonctionnalités.

Les nœuds ont été connectés entre eux par l'intermédiaire de leurs liens grâce à la commande « ngctl » en quelques lignes de commandes. Si l'on prend l'exemple de l'ajout d'un nouveau Vlan, le graphe peut être très rapidement modifié sans interruption du service.

On peut voir sur la figure 6 que le Vlaniseur possède deux interfaces physiques : la première sur laquelle arrivent les

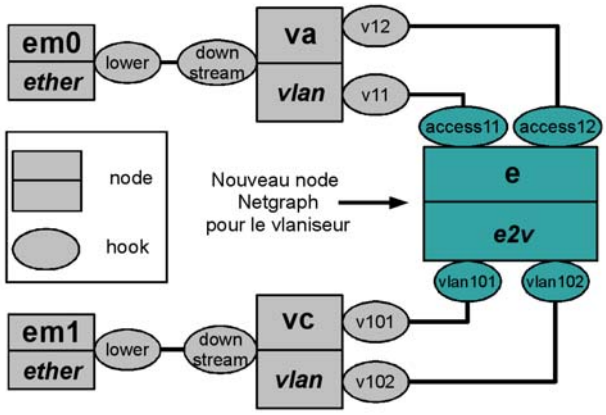

Figure 6: infrastructure Netgraph du Vlaniseur

Vlans d'accès (interface em0) et la seconde pour les Vlans de composantes (interface em1).

Les nœuds que l'on a nommés em0 et em1 ont la fonction de lecture et d'écriture des trames sur les cartes réseau. Lorsqu'une trame arrive par l'interface des Vlans d'accès (em0), elle est transmise par le lien « lower » au lien « downstream » du nœud « va ».

Comme la trame provient du lien « downstream », le nœud « va » sait qu'il s'agit d'une trame Ethernet 802.1Q, qu'il faut retirer le tag et le transmettre au lien approprié au bon Vlan.

Si la trame provient du Vlan 12, elle sera transmise sur le lien « v12 » qui la transmettra à son tour au lien « access12 » du nœud « e » de type « e2v », le cœur du Vlaniseur.

En fonction du Vlan de composante à laquelle est associée l'adresse Ethernet source de la trame, le trame sera transmise sur le lien qui indique le Vlan de la composante. Le tag 802.1Q sera inséré par le nœud « vc » et enfin la trame sera transmise sur l'interface « em1 ».

L'infrastructure Netgraph et les outils qu'elle apporte nous a permis d'écrire le module pour le Vlaniseur en 1500 lignes de code sans apporter aucune modification au code existant.

6 La sécurisation des échanges

Les utilisateurs du Vlaniseur qui se connectent sur un point d'accès accèdent dans un unique Vlan d'accès qui peut être partagé entre plusieurs équipements de l'infrastructure sans fil. Comme les utilisateurs appartiennent à différentes entités, dans un même Vlan d'accès, ils doivent donc être totalement cloisonnés. L'absence de cloisonnement des différents réseaux provoquerait de graves problèmes de sécurité et des dysfonctionnements importants.

Plusieurs dispositifs ont donc été imaginés pour éviter ces problèmes.

Comme nous l'avons vu dans le principe de fonctionnement du Vlaniseur, celui-ci n'envoie aucune trame Ethernet de diffusion en direction des Vlans d'accès. Toutes les trames

de diffusion sont « multi-unicastées » vers tous les membres d'un même Vlan de composante. Ceci élimine totalement l'utilisation par un point d'accès de clefs de chiffrement communes à tous les associés pour le trafic de diffusion.

Ainsi, grâce aux solides algorithmes de chiffrement utilisés par la norme 802.11i liés à l'authentification 802.1X, le trafic depuis un réseau de composante (en passant par le Vlaniseur) à destination d'un ordinateur connecté sur le réseau sans fil ne peut pas être intercepté par un tiers.

Les communications directes entre les composantes et un ordinateur du réseau sans fil étant sûres, il faut aussi éviter que les machines connectées dans un même Vlan d'accès puissent s'entendre par l'intermédiaire de leur trafic multicast lorsqu'elles n'appartiennent pas au même réseau de composante.

Nous avons donc interdit dans la configuration de nos points d'accès et de nos commutateurs du réseau sans fil la communication entre tous les membres d'un même Vlan d'accès.

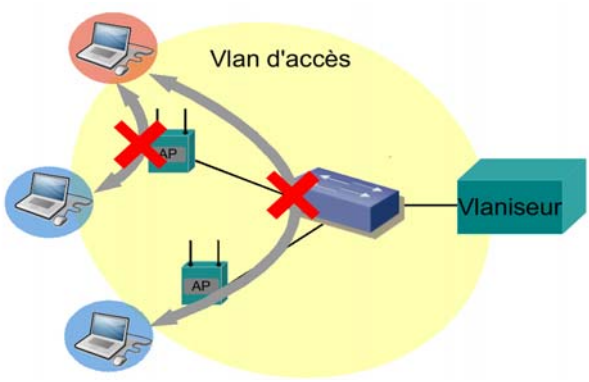

Figure 7: le cloisonnement des utilisateurs

Ce dispositif a l'avantage de parfaitement s'intégrer à notre réseau, puisqu'il est déjà activé pour les Vlans de l'accès rapide et de l'accès sécurisé. Nous l'avons fait pour des raisons de sécurité car nous évitons ainsi la transmission directe de virus d'une machine à l'autre, les désagréments provoqués par la mise en place de serveurs DHCP ou d'autoconfigurations IPv6 pirates et bien d'autres...

Dans le cadre du nouveau service fourni par le Vlaniseur, ce type de protection entre les différentes machines peut se montrer gênant pour les composantes. Nous avons donc implémenté plusieurs fonctionnalités dans le but d'établir ou non la communication entre les membres d'un même Vlan de composante connectés en sans fil.

Par défaut, le Vlaniseur est configuré en mode « No Communication » pour l'ensemble des Vlans de composantes.

Les figures 8 et 9 illustrent ces modes. On peut voir plusieurs utilisateurs appartenant à un même réseau de composante. Deux machines sont connectées dans le Vlan d'accès 1. Une autre dans le Vlan d'accès 2.

La figure 8 présente le mode « no communication ». Les trois machines ne peuvent absolument pas communiquer entre elles au niveau Ethernet. Le Vlaniseur ne relaye que le trafic entre les Vlans d'accès et les Vlans de composantes.

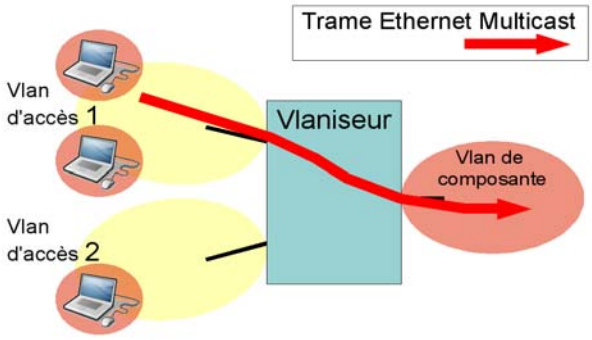

Figure 8: Vlaniseur : mode No Communication

Dans la figure 9 le Vlaniseur est en mode « protected port » pour le Vlan de composante représenté. Comme les points d'accès et les commutateurs du Vlans d'accès ont été passés en mode « protected port », c'est le Vlaniseur qui permet de rétablir la connexion entre plusieurs ordinateurs appartenant à une même composante.

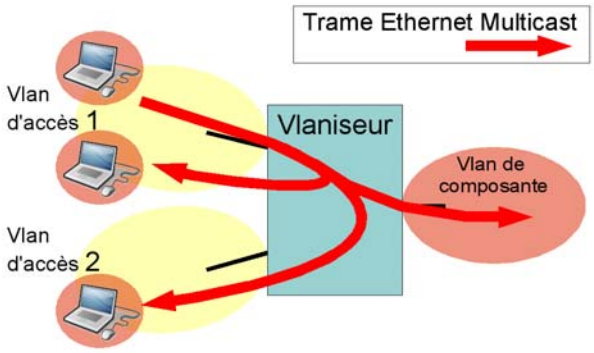

Figure 9: Vlaniseur : mode Port Protected

Cette solution est intéressante mais plus consommatrice de ressources pour le Vlaniseur. Elle n'est pas utilisée par défaut, mais peut l'être suite à une demande expresse d'un administrateur du réseau d'une composante.

7 L'interface avec l'infrastructure d'authentification Osiris

7.1 Les attributs Radius et l'annuaire LDAP

Le Vlaniseur doit connaître le numéro du Vlan d'appartenance d'un utilisateur pour y affecter sa machine. Cette information est stockée dans l'annuaire LDAP du réseau Osiris [2].

Dans l'enregistrement de chaque utilisateur, un attribut associe celui-ci à un profil WiFi.

Deux types de profils ont été définis :

– un profil « wifi-default » qui associe l'utilisateur au réseau WiFi par défaut. Celui-ci ne permet pas à l'utilisateur d'accéder aux services du Vlaniseur.

– un profil qui associe l'utilisateur à un réseau de composante du réseau sans fil. Par exemple pour le réseau interne du CRC : « wifi-crc ».

Lorsque l'utilisateur s'authentifie, le serveur Radius récupère son profil WiFi et en déduit le numéro du Vlan de composante par l'intermédiaire de dictionnaires d'attributs.

Grâce à l'application de gestion des comptes utilisateurs « Authiris » [2], chaque administrateur de composante peut modifier très facilement le profil WiFi de l'un de ces utilisateur pour l'associer à son réseau de composante. L'adoption massive du service proposé par le Vlaniseur en est grandement facilité.

7.2 Le service d'état global et les mécanismes d'enregistrement

Une des difficultés lors du développement du service a été d'interfacer l'authentification Radius avec le Vlaniseur.

Lorsqu'il authentifie un utilisateur, le serveur Radius ne maintient pas de session. Il se contente simplement d'indiquer si l'authentification a réussi ou non.

Au niveau du Vlaniseur, il faut maintenir des sessions pour chaque utilisateur. Dès qu'un utilisateur quitte le réseau sans fil, l'enregistrement de son ordinateur doit être supprimé.

Dans le but d'avoir les meilleures performances possibles, nous n'avons pas placé la gestion des sessions dans le Vlaniseur. Nous avons confié cette mission à un service d'état global.

La figure 10 représente le mécanisme d'authentification.

Les flux 1, 2 et 3 sont directement liés à l'authentification 802.1X EAP/TTLS. La machine M fait une demande d'authentification (1). Le serveur Radius contrôle la validité de l'utilisateur dans l'annuaire LDAP (2). Si l'utilisateur est bien authentifié, l'annuaire LDAP renvoie l'attribut Radius correspondant au Vlan de composante (3).

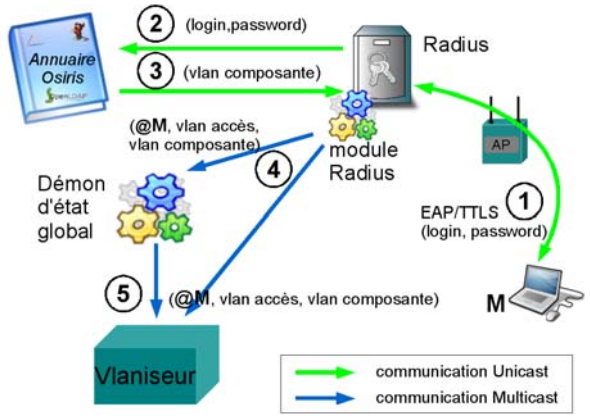

Figure 10: Enregistrement des utilisateurs

Pour communiquer avec le service d'état global et le Vlaniseur, nous avons écrit un module Radius qui envoie après chaque authentification réussie, le triplet <adresse MAC de la machine, Vlan de composante, Vlan d'accès>. Les communications se font en IP multicast. Cela a pour avantage, comme on est en mode non connecté, de ne pas bloquer de ressources du serveur Radius, mais aussi de pouvoir communiquer simultanément avec le service d'état global et le Vlaniseur. Le module Radius envoie également les dé-associations sur les points d'accès à partir de l'accounting.

Le service d'état global récupère les triplets de connexion et maintient des sessions pour chaque machine. Pour fermer les connexions des utilisateurs, il se base sur deux sources d'informations :

– tout d'abord, les données d'accouting Radius envoyées par le serveur Radius mais elles ne peuvent pas être considérées comme fiables puisqu'un accounting de dé-association peut très bien ne pas arriver jusqu'au serveur Radius.

– la liste des associés au réseau sans fil collectée par le serveur de métrologie Osiris qui interroge périodiquement en SNMP l'ensemble du parc WiFi.

8 Les perspectives d'évolution

8.1 La mise en place de plusieurs Vlaniseurs

Pour faire face à la montée en charge prévisible sur le Vlaniseur, il sera assez aisé d'en ajouter un ou plusieurs autres (cf. figure 11).

Les Vlaniseurs auront accès à tous les Vlans de composante mais les différents Vlans d'accès seront répartis. Ceci permettra de distribuer au plus juste la charge selon la fréquentation des points d'accès.

Grâce à la souplesse d'utilisation de Netgraph avec la commande « ngctl », il sera très facile de déplacer un Vlan d'accès d'un Vlaniseur à l'autre sans avoir à les redémarrer.

De plus, avec cette architecture, les communications Ethernet entre 2 machines connectées à 2 Vlaniseurs différents seront possibles.

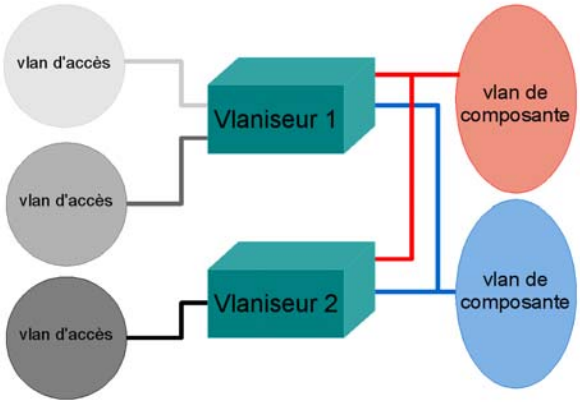

Figure 11: Répartition de la charge

Il n'y aura pas de modification spécifique à apporter au mécanisme d'enregistrement d'un utilisateur dans un Vlaniseur, puisque les communications entre le service d'état global vers le ou les Vlaniseur(s) se font en multicast.

Les Vlaniseurs seront inscrits dans le même groupe et enregistreront les nouvelles machines que s'ils sont concernés par le numéro du Vlan d'accès.

8.2 La redondance des Vlaniseurs

Pour répondre aux objectifs de disponibilité qui ont été fixés pour le réseau Osiris, le CRC a mis en place des systèmes de redondance sur l'ensemble des services. Nous souhaitons également appliquer cette règle au niveau du Vlaniseur.

Sur la plupart des services mis en place par le CRC, nous utilisons le système de redondance CARP [5]. Nos serveurs sont organisés en couple avec l'un d'eux positionné en secours. Celui-ci doit être capable de reprendre instantanément la main en cas de défaillance du maître.

Nous souhaitons appliquer le même schéma avec les Vlaniseurs, à la différence qu'un seul d'entre eux servira de backup pour tous les autres. Tous les Vlans de composantes, mais aussi tous les Vlans d'accès devront donc être connectés au Vlaniseur de backup. Bien sûr, nous tablons sur le fait que tous les Vlaniseurs ne tombent pas en panne en même temps.

8.3 La diminution du trafic de diffusion

L'optimisation du traitement du trafic de diffusion entre un Vlan de composante et un Vlan d'accès reste un point très important à régler dans le mécanisme du Vlaniseur.

Le directeur du CRC a confié une étude à un étudiant de Master 2 de recherche sur l'optimisation du trafic de diffusion dans les réseaux IP sur Ethernet. Cette étude [6] se base notamment sur des analyses de captures du trafic sur le réseau sans fil sécurisé.

Les conclusions de cette étude nous montrent qu'il faut que nous implémentions en priorité trois nouvelles fonctionnalités sur le Vlaniseur :

- un cache dans le but de ne pas diffuser les requêtes ARP sur les Vlans d'accès ou bien seulement à la machine susceptible d'être concernée. Ceci implique de découvrir les adresses IPv4 (et ultérieurement IPv6) des machines enregistrées dans le Vlaniseur.
- un cache ARP négatif. L'étude a montré que la plupart des requêtes ARP se font vers des adresses IP non utilisées. Cela provient la plupart du temps de scans ou de logiciels P2P mal écrits. L'idéal serait de ne pas transmettre les requêtes ARP pour les adresses IP non utilisées.
- l'implémentation de la fonctionnalité d'IGMP snooping. Pour l'instant, la diffusion de flux multicast est possible à travers le Vlaniseur, mais elle est très gourmande en ressources car chaque trame est transmise à l'ensemble des inscrits dans un Vlan de composante. L'IGMP snooping permettrait de connaître les machines inscrites à un groupe multicast et donc de limiter la diffusion de ces flux.

Ces nouvelles fonctionnalités peuvent être implémentées mais elles apporteront davantage de complexité dans le traitement des trames qui traverseront le Vlaniseur. L'impact sur la charge reste à définir.

9 Conclusion

Après une année d'exploitation du Vlaniseur au CRC nous avons ouvert le service aux utilisateurs des composantes du réseau Osiris. Les premiers résultats sont très encourageants. Le Vlaniseur se montre fiable et performant. Il nous permet d'offrir un véritable service de mobilité, transparent pour l'utilisateur, qui s'intègre parfaitement à l'infrastructure sans fil existante et à l'ensemble du réseau Osiris.

Les adaptations que nous avons apportées à l'infrastructure d'authentification sont mineures et offrent à l'administrateur de composante une gestion totalement autonome de ses utilisateurs. Le service du Vlaniseur fournit un port Ethernet sur lequel sont branchés les utilisateurs de la composante et laisse à celle-ci une totale liberté dans la mise à disposition des ressources et dans la politique de sécurité.

Le projet n'est pas considéré comme achevé. Il reste des évolutions à mettre en place en commençant par l'implémentation des solutions visant à réduire le trafic de diffusion et la mise en place d'autres Vlaniseurs en fonction de l'augmentation de la charge.

Bibliographie

[1] Christophe Saillard, 802.1X : Solution d'authentification sécurisée pour le futur réseau sans fil de l'université Louis Pasteur. Dans *Actes du congrès JRES2003*, Lille, décembre 2003.

[2] Alain Zamboni, Pierre David, Jean Benoit, Des services authentifiés pour une communauté de 50000 utilisateurs. *JRES2005*, Marseille, décembre 2005.

[3] Laurence Moindrot, Jean Benoit, Mutualisation d'un service d'accès à distance sécurisé VPN. *JRES2007*, novembre 2007.

[4] Archie Cobbs, All about Netgraph, http://ezine.daemonnews.org/200003/netgraph.html

[5] Haute-disponibilité des pare-feu avec CARP et pfsync, http://openbsd.org/faq/pf/fr/carp.html

[6] Mehdi Amini, Réduction de broadcast dans les réseaux IP sur Ethernet. *Mémoire de Master 2 de recherche*, septembre 2007.