Janvier 2010

Virtualisation - Principes et fonctionnement Campus

1 INTRODUCTION

Les entreprises implémentent aujourd'hui majoritairement des infrastructures routées, pour des besoins de haute disponibilité, et d'évolutivité.

Le réseau fédère désormais les flux de diverses entités d'une même entreprise, de partenaires ou sous-traitants ainsi que d'invités. Le besoin de segmentation et de virtualisation au sein du réseau de l'entreprise est donc de plus en plus important afin de supporter les nouvelles applications, la sécurité entre les groupes d'utilisateurs ainsi que la nécessaire souplesse d'évolution en fonction des demandes.

Le réseau doit donc être à même de fournir une isolation de couche 2 et de couche 3, renforçant la sécurité pour les abonnés partageant cette même infrastructure. Les entités n'auront aucune possibilité de communiquer les unes avec les autres, sans une définition explicite de ces autorisations.

Pour cela, il est nécessaire de virtualiser les instances de routage, les services des différents équipements constituant cette infrastructure ainsi que les chemins entre les routeurs.

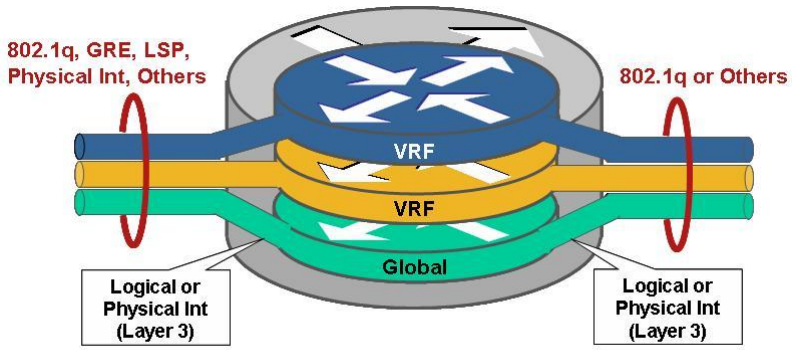
Les routeurs Cisco ainsi que la gamme de commutateurs Catalyst supportent dès à présent la notion de routeurs virtuels (VPN routing and forwarding instances, RFC 2547) qui sont à la base de la technologie plus globale utilisée par les opérateurs MPLS-VPN.

2 PRINCIPE DE LA VIRTUALISATION

La solution de virtualisation d'un réseau comprend :

- la virtualisation des routeurs/catalyst du réseau
- la virtualisation des liens reliant les routeurs pour assurer l'isolation du trafic
- la virtualisation des services tels que firewall, load-balancing etc

La segmentation du réseau est réalisée en séparant les utilisateurs dans des instances de routage et de forwarding différentes appelées VRF pour Virtual Routing and Forwarding.



Les VRFs ainsi utilisées pour assurer le partitionnement de l'infrastructure :

- Permettent la constitution de Virtual Private Network (VPNs)
- Fournissent un moyen sécurisé d'accéder à l'ensemble des machines des centres de production de l'entreprise.
- Permettent également aux différentes entités d'utiliser des réseaux IP en overlapping, ce qui n'est pas supporté avec du routage IP global.

Cette technologie est aujourd'hui déployée dans les réseaux LAN & MAN des entreprises et dérive directement de la notion de Virtual Routing and Forwarding (VRF) implémentée dans les réseaux MPLS-VPN.

L'accès à une VRF pourra se faire statiquement par l'affectation de l'interface VLAN dans une VRF, ou bien dynamiquement en utilisant 802.1x et l'affectation de vlan.

Les méthodes permettant l'isolation du trafic entre les routeurs peuvent se diviser en deux grandes catégories :

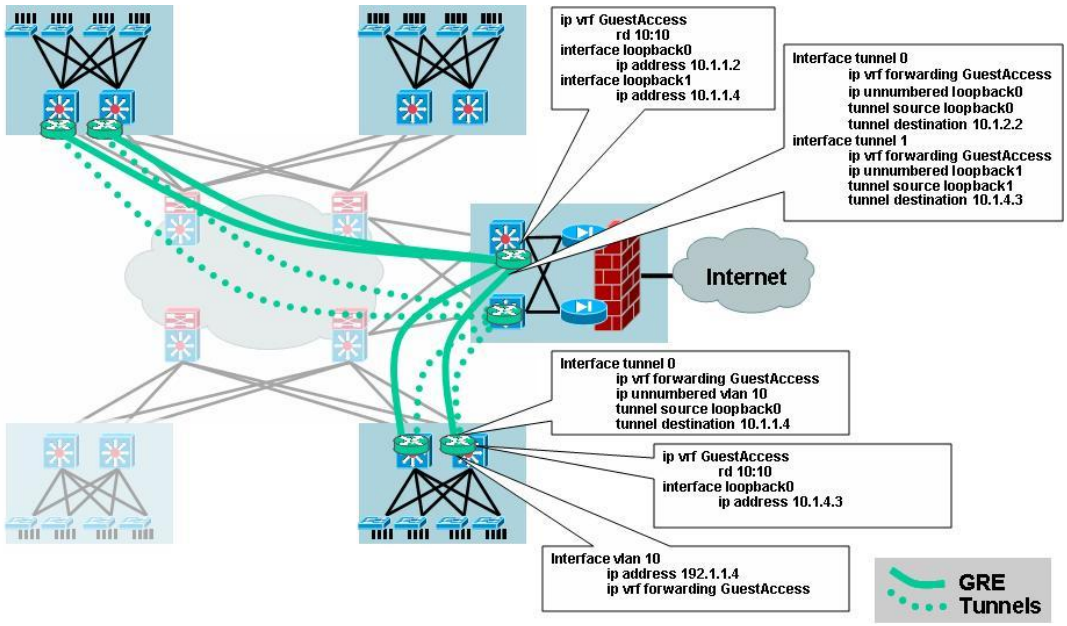
- Single Hop Data Path Virtualisation : on retrouve là les méthodes de tagging de trames telles que 802.1Q, ATM VC, Frame Relay DLCI ou autres qui permettent d'affecter une valeur spécifiques de tag en fonction de la VRF. Dans un environnement campus, on utilisera principalement l'encapsulation

802.1Q bien sûr. La solutiobn VRF-Lite entre dans cette catégorie et est principalement utilisée dans des environnements de campus ou le nombre de routeurs est limité.

- Multi-hop Data Path Virtualisation : on retrouve dans cette catégorie, les méthodes de tunneling permettant de relier une VRFx d'un routeur avec une VRF-x sur un autre routeur au travers d'un réseau IP. On retrouve donc les tunnels GRE, L2TPv3 et bien sûr LSP (MPLS-VPN)

3 UTILISATION DE TUNNELS GRE

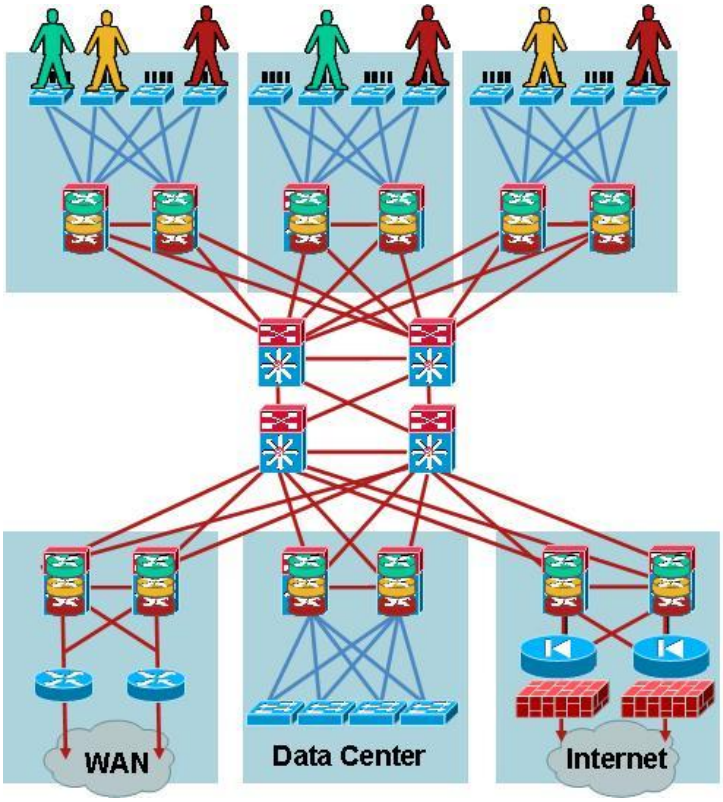
Dans ce cas de figure, on utilise un tunnel GRE pour relier une VRF avec une autre VRF au travers d'un réseau de campus IP.
Typiquement une méthode facile pour implémenter un guest access.
L'encapsulation GRE est supportée en hardware sur les Catalyst 6500 sup720/sup32 et en software sur les Catalyst 4500.



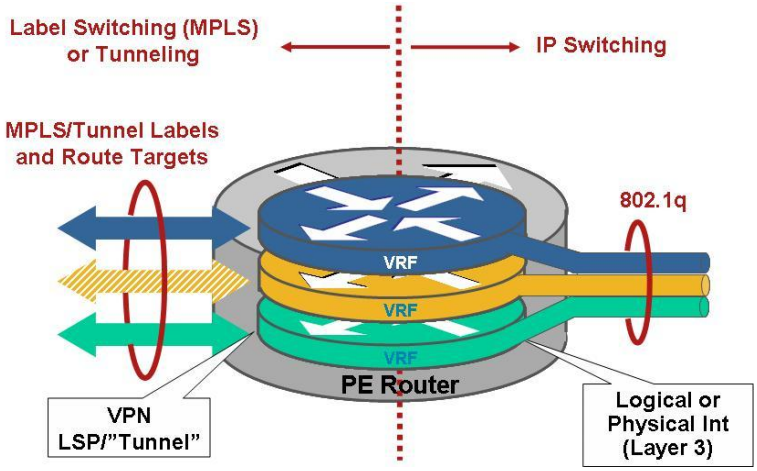
L'avantage est de ne pas toucher au cœur du réseau et de n'implémenter les VRFs que là où il y en a besoin.
L'inconvénient majeur et que cela peut entrainer une complexité importante si on relie en full mesh. Cette méthode est donc plutôt utilisée dans une architecture hub and spoke où tous les tunnels se terminent sur des Catalyst 6500 centraux.

4 UTILISATION DE MPLS-VPN

Il s'agit là de la méthode classique de constitution des VPNs. Cela suppose de mettre en phase la labelisation dans le cœur du réseau, de mettre en place LDP pour la distribution de ces labels ainsi que BGP pour distribuer les routes VPN ainsi que les labels associés.
On trouvera surtout cette méthode employée dans les réseaux métropolitains, WAN mais aussi dans quelques réseaux importants de campus.



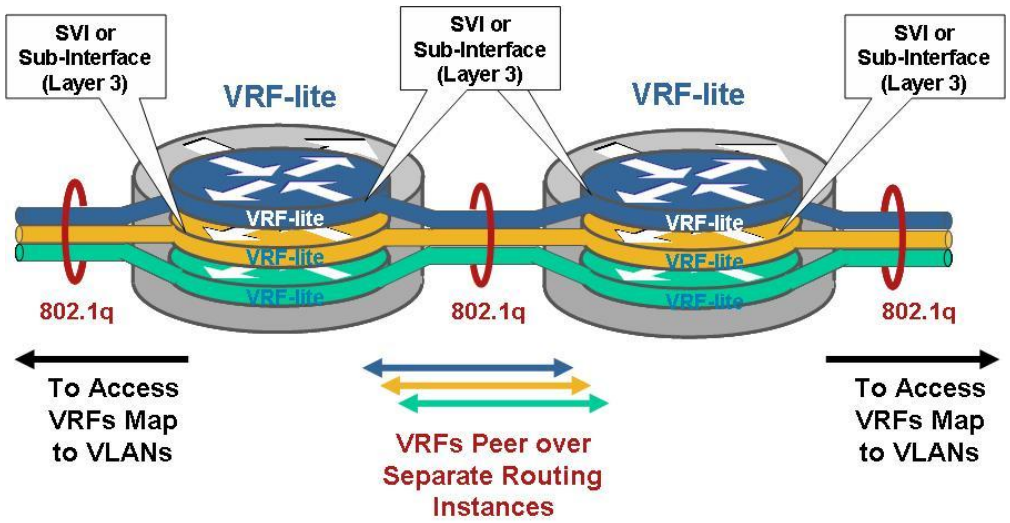
Dans ce cas, les routeurs de distribution faisant l'interconnexion entre le réseau MPLS de cœur et la périphérie peuvent être vus comme ci-dessous, d'un coté avec des interfaces 802.1Q et de l'autre des interfaces labélisées MPLS :



5 UTILISATION DE VRF-LITE

On trouve ce dernier modèle plus récemment mais de plus en plus souvent. L'idée est de conserver les VRFs mais de ne pas implémenter le modèle MPLS. Au lieu de cela, les routeurs seront interconnectés avec des interfaces permettant de relier les VRFs en conservant l'isolation.

Pour se faire, nous établissons un trunk 802.1q entre les 2 équipements à connecter.



Il suffit alors de définir des sub-interfaces sous l'interface physique d'interconnexion, et d'associer ces sub-interfaces aux VRF à router sur le trunk.

La table de forwarding n'autorisant pas la commutation de paquet entre des sub-interfaces associées à des VRF-id différents, aucun paquet ne pourra être commuté entre ces sub-interfaces.

Le réseau est alors dit VRF-lite End-to-End, c'est-à-dire que ce modèle est répercuté et implémenté dans tous les Catalyst/routeurs du réseau de campus :

Les avantages évidents de cette méthode sont dans la facilité d'utilisation puisque cela reste un réseau routé (OSPF ou EIGRP) mais simplement par VRF au lieu d'être global. L'exploitation n'en est que très peu modifiée et il n'y a pas de nouveaux protocoles comme BGP ou LDP à apprendre.

Par contre, cette configuration des sous interfaces entre les routeurs est manuelle.

6 COMMUNICATION INTER-VRF

Les utilisateurs sont donc répartis dans les différents VPN, il reste la nécessité de les interconnecter.

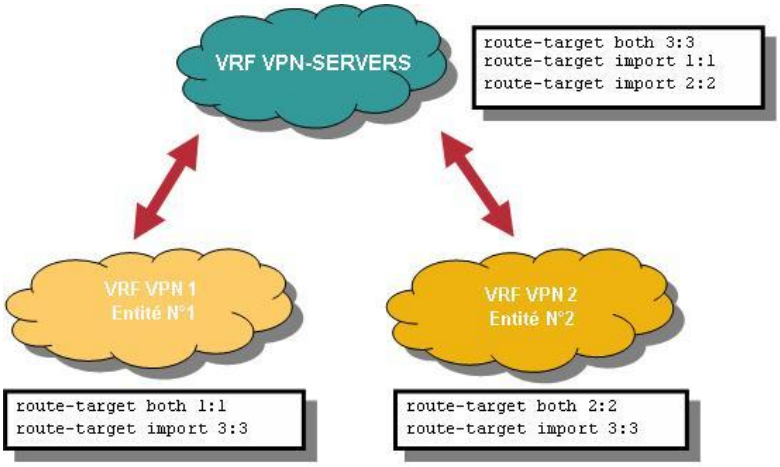
Deux méthodes principales :

- Utiliser un firewall pour le filtrage du trafic entre les différents VPN du réseau. Ce firewall pourra être externe, mais sera de préférence interne en utilisant la carte FWSM du catalyst 6500 qui a elle-même la possibilité d'implémenter des contextes virtuels. L'avantage principal étant bien sur de définir les règles nécessaires pour n'autoriser qu'un certain type de trafic. Tout les flux transitant d'un VPN à un autre VPN traverseront le firewall et seront donc analysés.

- Utiliser un processus mBGP en local sur un Catalyst. On pourra alors redistribuer les routes entre les VPNs en utilisant la notion de route-target, notion qui est à la base de la population des routes dans les VRFs dans des environnements MPLS-VPN. Tous les flux transitant d'un VPN a un autre VPN sont alors commutés localement par le Catalyst 6500. Ce type de solution est utilisée dans les environnements d'entreprises ou plusieurs VPN utilisateurs doit accéder à des ressources communes situées dans un VPN de type serveurs par exemple.

Service d'interconnexion purement réseau (routage uniquement).

Le routage inter-VRF utilise un processus de routage mBGP, permettant un contrôle précis des subnets devant être routés d'une VRF à l'autre.

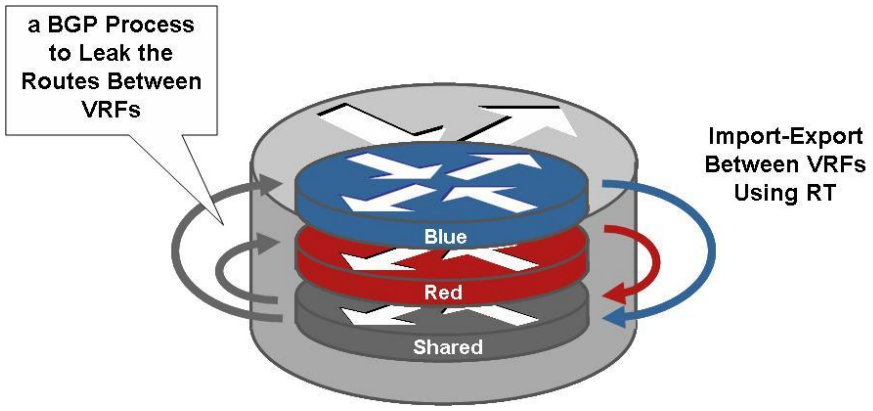


L'exemple ci-dessus montre la configuration des règles d'Import / Export permettant aux VPN1 et VPN2 d'accéder à des ressources mutualisées dans VPN-SERVERS.

Il est important de noter ici, que malgré le fait que VPN1 et VPN2 accèdent au VPN-SERVEURS, VPN1 et VPN2 ne pourront pas communiquer ensemble.

En effet, VPN1 n'important pas VPN2 et VPN2 n'important pas les subnets de VPN1, les 2 tables de routage resteront totalement disjointes.

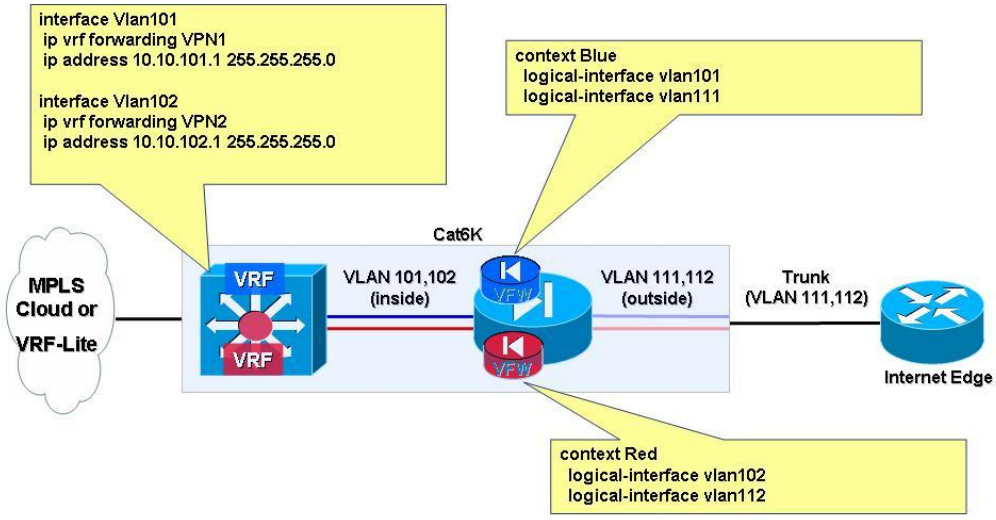
Cette interconnexion de VRF au travers de BGP peut être réalisée en local avec un seul process BGP n'ayant aucun peer défini. Le process BGP n'est alors utilisé que pour réaliser l'interconnexion des VRFs comme illustré ci-dessous :



Service d'interconnexion sécurisé (via Firewall)

L'interconnexion sécurisée des VRF passera par l'utilisation d'un Firewall qui pourra être externe à cette infrastructure, ou bien de façon plus optimisée par une fonction Firewall interne aux équipements et supportant elle aussi la notion de virtualisation.

Comme illustré ci-dessous les contextes virtuels du Firewall seront « mappés » aux VRF définies.



Les Firewalls Cisco permettant d'interconnecter les VRF peuvent être configurés de 2 manières différentes :

- Firewall en mode transparent
- Firewall en mode routé

7 CONCLUSION

Les services de virtualisation et segmentation sur les réseaux permettent d'apporter une très grande souplesse dans la constitution des groupes d'utilisateurs tout en assurant leur sécurisation.
Les solutions actuelles sont très utilisées et Cisco travaille de manière importante sur ce sujet pour continuer à apporter de la valeur ainsi que des fonctionnalités permettant un déploiement plus rapide et une exploitation simplifiée.

Contactez-nous :
www.cisco.fr
0800 907 375

Siège social Mondial
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France
Cisco Systems France
11 rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.fr
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :

www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili Colombie • Corée Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie Mexique • Nouvelle Zélande • Norvège • Pays-Bas • Pérou Philippines • Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine • Russie Singapour • Slovaquie • Slovénie • Suède Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe

205534.E_ETMG_JD_10/09