

Extension du réseau de niveau 2 entre centres de données : Virtual Switching System et L2VPNNoGRE

Addendum.....	1
Objectifs.....	1
Scope du Document	2
Déploiement géographique de réseau de niveau 2	3
Le niveau 2 étendu entre plusieurs centres de données (quelques raisons).....	3
Extension de niveau 2	3
Les différentes alternatives	3
Virtual Switching System (VSS)	5
EoMPLS et VPLS over GRE (aka AToMoGRE)	9
Protection de boucle de niveau 2.....	10
Conclusion.....	15

Addendum

Cet article apporte des informations supplémentaires au document publié dans le CiscoMag de Septembre 2007 :


http://www.cisco.com/web/FR/documents/pdfs/newsletter/ciscomag/2007/09/dossier_interconnexion_de_reseaux_pour_ha_clusters_etendus.pdf¹

Objectifs

Cet article fournit des informations complémentaires au déploiement complexe d'une architecture géographique de réseaux de niveau 2 étendu. Ces informations doivent permettre à toutes les entreprises de pouvoir déployer des extensions du niveau 2 au-delà du campus en exploitant ces solutions techniques, qui complètent celles décrites dans l'article précédent, sans devoir déployer un réseau MPLS dans le cœur de l'entreprise.

En effet, les technologies décrites précédemment concernent des extensions de réseaux de niveau 2 via un réseau MPLS pour deux scénarios distincts, soit un réseau point à point assuré par Ethernet over MPLS (EoMPLS), soit un réseau multipoint assuré par Virtual Private LAN Services (VPLS) avec ou sans isolation du protocole de Spanning Tree (STP).

La première solution technique que nous abordons dans ce document, est l'utilisation de la

¹ Une version Anglaise est disponible sur [HA Cluster Interconnection using L2VPN](#) 

technologie de « Virtual Switching Systems » qui peut être déployée dans une distance maximale de type « Metro ² » entre les centres de données.

A noter que l'architecture et le fonctionnement du VSS dans un environnement local de centre de données sont traités en détail dans un autre article de ce numéro de CiscoMag (par Irène Golbery). De ce fait, nous nous focaliserons uniquement sur l'architecture globale d'interconnexion de plusieurs sites distants, basée sur la fonction de « Virtual Switching ».

Concernant les 2 solutions techniques décrites dans le CiscoMag précédent, nous avons précisé le besoin de déployer un cœur de réseau MPLS pour supporter ces fonctions EoMPLS ainsi que VPLS. Or, nous constatons que seul un certain nombre de grandes entreprises qui ont déjà déployé ou qui envisagent de déployer un réseau MPLS - pour une segmentation de niveau 3 par exemple - peuvent, de ce fait et de manière assez simple, étendre des réseaux virtuels de niveaux 2 tout en conservant la même flexibilité et robustesse décrites précédemment.

Il est donc important que nous puissions apporter également des réponses tout aussi efficaces à l'ensemble des autres entreprises qui ne peuvent ou ne souhaitent pas mettre en place un réseau de cœur MPLS.

La deuxième solution que nous abordons, reprend les techniques basées sur EoMPLS et VPLS. Maintenant que nous savons que ces fonctions répondent parfaitement à la problématique de l'extension de niveau 2 d'une manière fiable, redondante et rapide tout en pouvant isoler le STP entre les sites distants, nous allons élaborer ces mêmes techniques mais sur un réseau de cœur pur IP, sans la nécessité d'avoir un cœur MPLS pour interconnecter les centres de données.

Scope du Document

Cet article s'adresse aux Managers de Réseaux ainsi qu'aux Managers de centres de données pour les aider à mieux appréhender l'architecture réseau recommandée par Cisco pour étendre du niveau 2 entre plusieurs sites distants, de la manière la plus résistante et redondante possible.

Cet article ne couvre pas les besoins en termes de réseaux pour le SAN.

² Les distances de type « Metro » peuvent dans certains cas atteindre une extension maximale totale proches des 100kms.

Déploiement géographique de réseau de niveau 2

Le niveau 2 étendu entre plusieurs centres de données (quelques raisons)

Cisco recommande de limiter le réseau de niveau 2 à sa plus petite distance, généralement limité à un niveau Tiers – entre le niveau d'accès et le niveau d'agrégation - dans une architecture réseau hiérarchique d'un centre de données. Cette recommandation s'applique seulement lorsqu'il est nécessaire d'utiliser le niveau 2 entre deux ou plusieurs équipements réseaux au sein d'un même centre de données.

Cependant, il existe également un certain nombre de raisons pour lesquelles le niveau 2 doit être déployé au-delà du centre de données, principalement lorsque les applications ou scénarios ont été développés pour un environnement de « Campus » mais exploités dans un environnement de longues distances.

On peut en citer les plus importants :

Cluster HA : La communication entre membres de Cluster à haute disponibilité demande parfois l'utilisation d'un réseau de niveau 2 :

- à la fois pour la communication publique (VIP)
- ainsi que la communication privée (Heartbeat) utilisée pour le maintien et le contrôle de l'état du ou des nœuds actifs du cluster.

Redondance étendue d'un centre de données : Dans le cadre d'un centre de données à haute disponibilité mais étendu entre plusieurs sites éloignés :

- Communication privée entre les éléments de services réseaux redondants - « Load balancers » ou « firewalls » - pour le maintien et le contrôle des différents contextes de services réseaux actifs dispersés.
- Communication pour la redondance pour les interfaces routées (HSRP, VRRP, GSLB)

Migration : Dans le cas d'une procédure de migration physique de serveurs :

- Certaines applications sont difficilement ré-adressables au niveau IP (Mainframe), il est donc nécessaire d'étendre le VLAN en dehors de ces limites recommandées, de manière à conserver la configuration d'origine des serveurs après déplacement des machines.
- Egalement, lors de migration d'une partie uniquement de la ferme de serveurs d'un site à un autre dont le réseau de niveau 2 doit être maintenu entre les machines physiques appartenant à la même ferme de serveurs.
- Toujours dans le domaine de la migration de serveurs, certaines applications³ qui offrent la virtualisation de systèmes d'exploitation peuvent permettre des migrations de systèmes logiques sur des machines physiques séparées par de longues distances. Pour maintenir les états actifs de chaque module software durant la migration, il est impératif de conserver les mêmes réseaux de niveau 2 d'un bout à l'autre.

Extension de niveau 2

Cet addendum concerne uniquement l'extension du LAN entre centres de données distants. Toutes les solutions décrites dans le document précédent et celui-ci respectent à la fois stabilité, redondance, performance et Qualité de Service.

Les différentes alternatives

Pour fournir la haute disponibilité entre les sites de données, les interconnexions physiques doivent être dupliquées. De ce fait, un mécanisme de contrôle de boucle de niveau 2 et de protection contre

³ Attention à bien noter avec les fournisseurs de software les recommandations des distances maximales supportées par l'application de virtualisation.

tout type de problèmes survenant dans ces liens d'interconnexion doit être mis en place. Toutefois il est impératif de limiter la propagation du protocole de Spanning Tree pour le contrôle des boucles de niveau 2 sur l'ensemble des sites distants, au risque de voir l'ensemble du réseau global perturbé par des phénomènes locaux.

Cisco recommande de ne pas étendre le Protocole de Spanning Tree au-delà du campus à cause de sa fragilité native sur de longues distances ainsi que les risques d'interruption de trafic tout du long de son domaine de Spanning Tree.

Actuellement Cisco recommande 3 solutions techniques pour l'extension de niveau 2 entre des sites distants tout en offrant performance (vitesse du câble) et redondance (temps de basculement maximum inférieur à 4 secondes) sans extension du protocole de Spanning Tree.

1. Virtual Switch System (VSS) sur un réseau optique très haut débit DWDM.
2. EoMPLS et VPLS distances non limitées sur cœur de réseau MPLS
3. EoMPLS et VPLS distances non limitées sur cœur de réseau IP

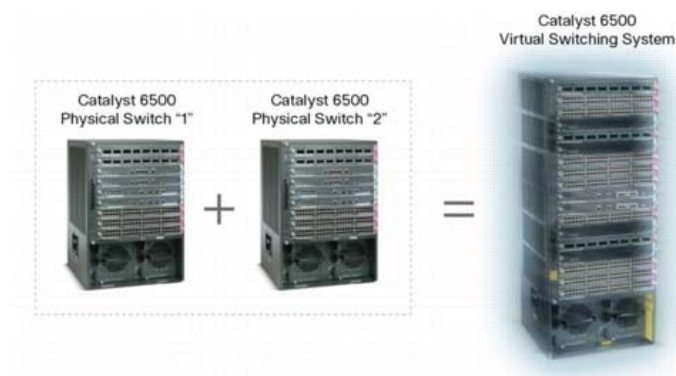
- VSS est la solution la plus simple à déployer. Elle est recommandée par Cisco spécialement pour les distances de type « Metro » et dont l'interconnexion des liens physiques est assurée par de la fibre noire (fibre dédiée). Cette technologie assure une très haute disponibilité avec des liens redondants (Multi-Chassis Etherchannel) sans toutefois devoir faire appel au protocole de Spanning Tree. Elle offre des temps de basculement inférieurs à la seconde, tout en autorisant le trafic à utiliser tous les liens physiques à la vitesse du câble. Elle peut être déployée, à la fois pour des interconnexions en point à point entre deux centres de données à partir des commutateurs d'agrégation, ou également en multipoint lorsque le nombre de centres de données est supérieur à deux.
- EoMPLS est la solution recommandée par Cisco lorsque les liens inter-sites ne sont pas des fibres optiques dédiées ou que les distances sont supérieures à une zone dite « Metro » ou éventuellement que le coût de déploiement d'un réseau de fibres optiques est trop élevé pour l'entreprise. Cette technologie assure une haute disponibilité. Elle est toutefois préférable pour l'interconnexion de 2 centres de données en point à point. EoMPLS peut-être initié aussi bien à partir des commutateurs d'agrégation que des commutateurs de cœur.
- De même, VPLS est la principale solution recommandée pour assurer une haute disponibilité et une haute résistance, pour étirer des liens de niveau 2 redondants entre plusieurs centres de données distants (Multipoints), sans avoir à étendre le protocole de Spanning Tree de bout en bout. Théoriquement un « pseudowire » basé sur EoMPLS nécessite un cœur de réseau MPLS. VPLS sera établi entre les commutateurs de cœur.

EoMPLS et VPLS en mode natif (c'est-à-dire déployés sur un cœur de réseau MPLS) ayant été préalablement décrits dans le CiscoMag de septembre 2007, cet article traite donc spécialement les deux autres options pour l'extension du niveau 2 :

- Virtual Switching System (VSS) pour les réseaux distants de type « Metro ».
- Ainsi que la possibilité d'étendre un réseau virtuel de type EoMPLS et VPLS mais sur un réseau pur IP.

Virtual Switching System (VSS)

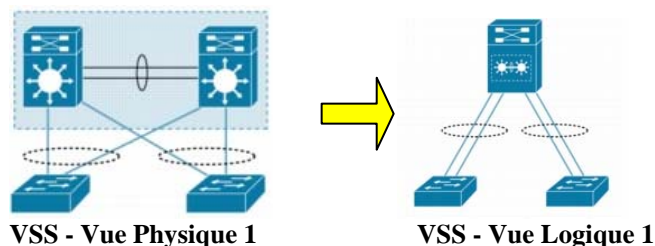
Petit résumé sur la description du VSS. Le VSS est une fonction qui s'active sur le Catalyst 6500 et s'exécute au niveau du hardware. Il n'y a donc aucun impact sur les performances. Bien au contraire, il va permettre de doubler les performances de deux commutateurs physiques connectés entre eux en formant un commutateur virtuel, simplifiant de ce fait la configuration et le management d'un seul commutateur virtuel.



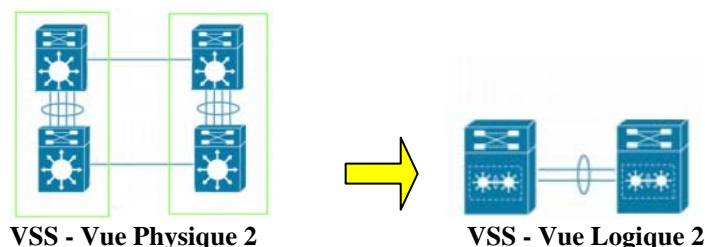
Si le VSS permet d'exécuter les fonctions de Contrôles et de Management de l'ensemble du système sur une machine dite « active », la commutation des données quant à elle, va s'exécuter sur les deux matrices de commutation physiques, en apportant, en plus, des optimisations sur les chemins entre les flux entrants et sortants, en amont (réseau cœur) et en aval (réseau d'accès) des deux commutateurs.

Il y a donc une seule machine à configurer qui intègre à la fois les ressources hardware de celui-ci et également la partie hardware offerte par le second commutateur (interfaces de lignes ainsi que les services réseaux redondants⁴).

Le fait d'avoir les fonctions de Contrôles et de Management sur une seule machine active, VSS va autoriser l'extension de plusieurs liens physiques, à partir des 2 commutateurs physiques tout en appartenant au même commutateur logique. C'est la technologie dite « Multi-Châssis Etherchannel ».



Si nous exploitons cette fonction entre deux paires de VSS, nous obtenons 2 commutateurs logiques formés chacun de 2 commutateurs physiques.



Nous arrivons donc à obtenir une redondance complète avec une totale séparation des équipements de commutation ainsi que des liens physiques, offrant des temps de basculement inférieurs à la seconde (~500ms).

⁴ Les services réseaux de type ACE et FWSM seront supportés avec l'arrivée de Whitney 2. Actuellement seules les cartes de lignes CFC et DFC (C67xx) sont supportées.

Si nous étendons cette logique sur une topologie géographique formée de plusieurs sites, nous pouvons créer une solution d'architecture réseau très flexible, permettant l'évolution de nouveaux centres de données.

Dans l'exemple de la figure 1, ci-dessous, nous avons 4 centres de données distants à interconnecter via un réseau DWDM qui va servir de support physique pour créer les différentes liaisons en point à point à partir des lambdas disponibles de la liaison optique. La distance entre les sites de données est complètement liée au réseau DWDM. Toutefois Cisco recommande de ne pas étendre cet anneau optique sur des distances supérieures à 100kms.

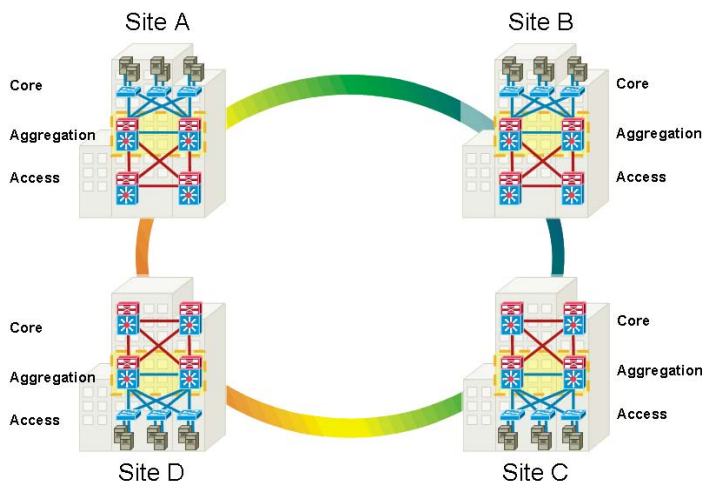


Figure 1 -VSS & Fibres Dédiées

Au niveau de chacun des centres de données, chaque niveau d'agrégation est assuré par un commutateur virtuel (VSS).

Dans la figure 2, en plus de ce niveau d'agrégation intra-DC, nous rajoutons un cœur de VSS pour pouvoir distribuer le trafic entre les différents centres de données.

Les deux commutateurs physiques appartenant au VSS central seront disposés sur deux sites distants de manière à offrir une très haute disponibilité. Les liaisons point à point physiques vont être créées à partir du réseau DWDM. Les liaisons⁵ formant l'interconnexion du VSS, lui-même, doivent être chacune de 10Gig Ethernet.

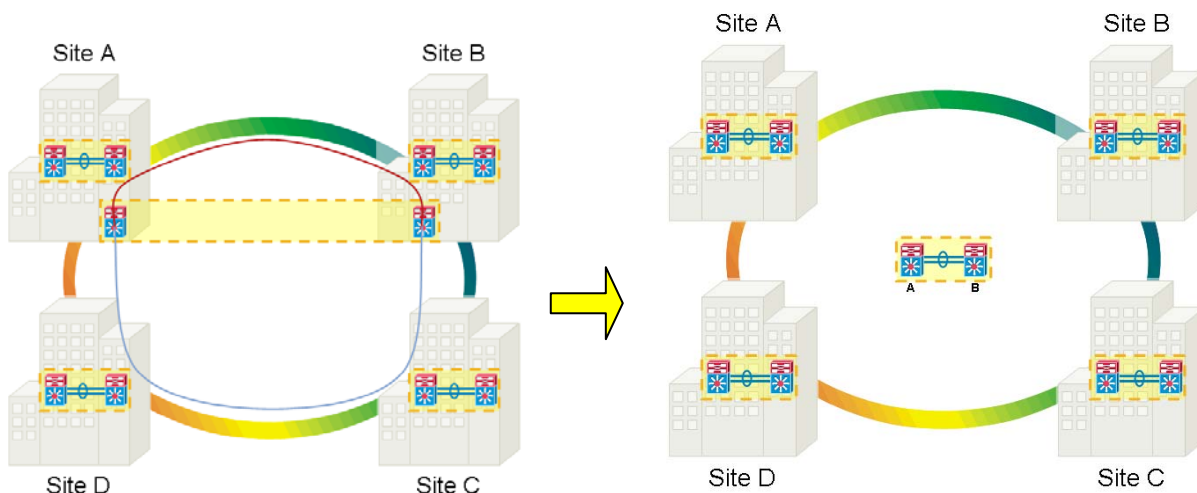


Figure 2 - Niveau Cœur VSS - Vue physique Figure 2(bis) - Niveau Cœur VSS - Vue logique

⁵ La liaison qui interconnecte les deux membres d'un VSS est appelée Virtual Switch Link (VSL). Elle doit être formée, à partir de 2 liaisons à 10GE (Interconnexion entre les 2 Sup720-10GE).

Il nous reste à interconnecter chaque niveau d'agrégation virtuel (VSS) de chaque site au niveau du cœur VSS. Dans cet exemple figure 3, pour l'interconnexion du site A, le commutateur de gauche du cœur VSS, sera physiquement dans le même centre de données du site A. Il utilisera une fibre locale de 10GE. Le commutateur de droite du cœur VSS sera, lui, physiquement dans le site B, et utilisera un lambda de 10GE créé entre les sites A & B. Et ainsi de suite pour les autres Sites B, C, et D.

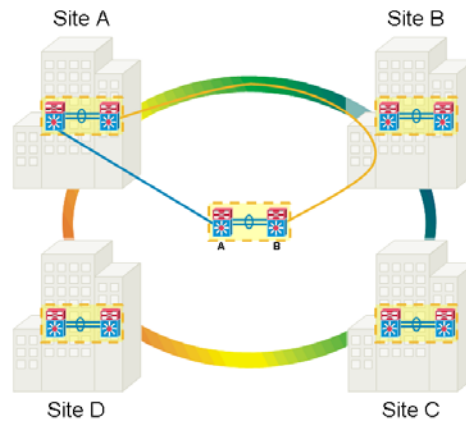


Figure 3 – Interconnexion des Sites sur le VSS central

Si nous appliquons la même logique sur l'ensemble des sites distants, nous obtenons une grande flexibilité, dont la seule limite sera le nombre maximum de liens montants disponibles entre le cœur VSS et les différents centres de données ainsi que les lambdas disponibles sur le réseau DWDM. Dans cet exemple avec 4 sites distants, nous utiliserons 8 liaisons fibres dédiées : 2 pour le VSL du VSS central et 6 pour chaque VSS d'agrégation (Site A et B) supportant chacun, dans cet exemple, un des commutateurs du VSS central.

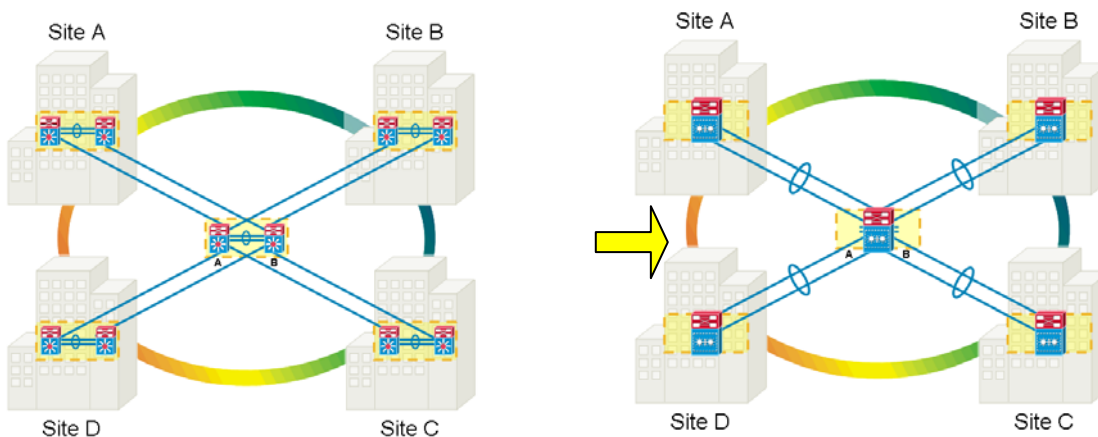


Figure 4 - Vue physique

Figure 4 (bis) - Vue Logique avec MEC

Le niveau d'agrégation dans chaque site étant assuré par une paire de VSS⁶, localement chaque commutateur d'accès peut être « dual-attaché » avec des liens redondants tous actifs assurés par le mécanisme d'Etherchannel. Le fait de pouvoir partager le même Etherchannel entre deux paires de commutateurs, va nous permettre de déployer un réseau de niveau 2 100% redondant et sans besoin activer le Protocole de Spanning Tree pour contrôler d'éventuelles boucles de niveau 2.

⁶ Le Nexus 7000 supportera en 4.1 une fonction pour activer la Virtualisation du Portchannel (VPC) qui pourra être déployé au niveau d'agrégation.

Le Protocole de Spanning Tree sera activé localement dans chaque centre de données. Il sera toutefois possible de conserver le Spanning Tree actif entre les centres de données distants en créant une Région MST pour chaque site. MST permet en effet d'isoler nativement des domaines de Spanning Tree et permet de prévenir des risques de perturbations liés à des problèmes de STP locaux.

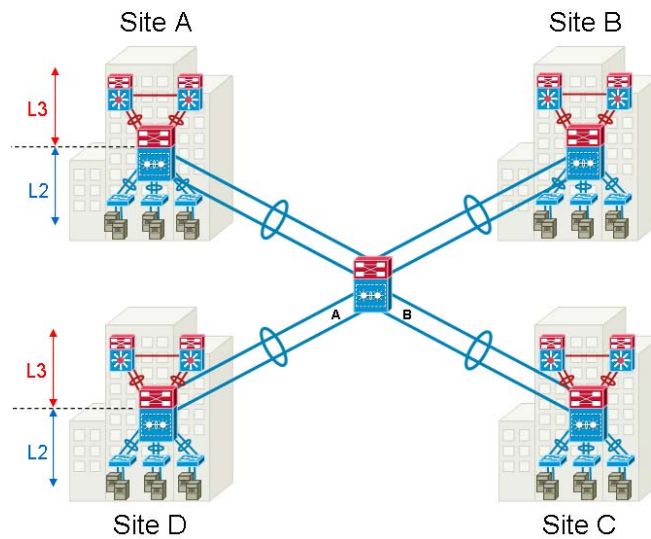


Figure 5 – Multi-châssis Etherchannel sur l'ensemble des centres de données.

EoMPLS et VPLS over GRE (aka AToMoGRE)

Dans l'article de CiscoMag précédent, nous avons traité les possibilités d'utiliser EoMPLS et/ou VPLS sur un réseau de cœur MPLS pour supporter principalement le déploiement de Géo-cluster.

- EoMPLS étant la recommandation pour des liaisons dédiées de niveau 2 en point à point. Ce que nous avons attribué au réseau « Privé » du cluster à haute disponibilité.
- VPLS étant la recommandation pour des liaisons partagées de niveau 2 en multipoint. Ce que nous avons attribué au réseau « Public » du cluster à haute disponibilité.

Que ce soit EoMPLS ou VPLS, ils peuvent être utilisés également pour d'autres types de scénarios auxquels un certain nombre d'entreprises sont confrontées et décrits dans l'introduction de ce document.

Si les solutions EoMPLS et VPLS restent aujourd'hui les solutions qui répondent le mieux à la problématique de l'extension du niveau 2 sur de longues distances, il reste tout de même un point sensible pour un certain nombre d'entreprises qui doit être abordé et auquel Cisco apporte une nouvelle réponse basée sur les capacités hardware.

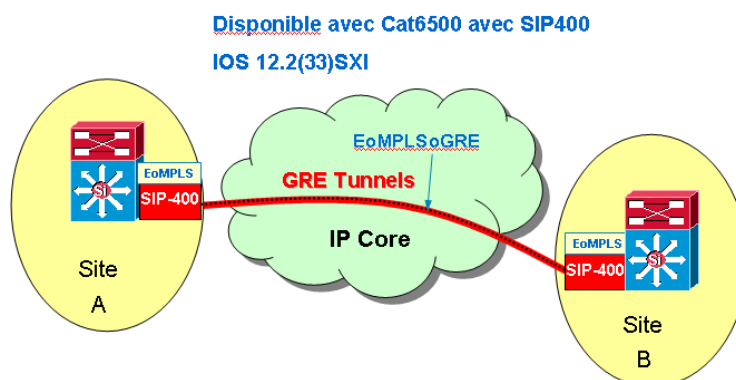
Le fait de devoir faire migrer le cœur du réseau IP vers un réseau parallèle MPLS pour supporter ces technologies de réseaux de niveau 2 virtuel impose une certaine expertise pour son déploiement et la maintenance au cœur de l'entreprise.

Cisco répond à ce besoin spécifique par la possibilité d'étendre un réseau de niveau 2 virtuel sur un tunnel de type GRE tout en conservant exactement les mêmes avantages qu'avec un réseau de cœur MPLS. Cette fonction est appelée AToMoGRE ou L2VPN0GRE.

Cette fonction consiste à créer un tunnel GRE – commuté par le hardware, donc sans aucun impact sur les performances de commutations – et d'y encapsuler des paquets labellisés de type ATOM (Any Transport over MPLS) comme EoMPLS ou VPLS (L2VPN).

Au même titre qu'avec un réseau de cœur MPLS, EoMPLS « port xconnect » au-dessus de GRE sera l'option préférable pour une liaison étendue de type point à point.

Dans la figure 6, un lien GRE est établi entre les 2 commutateurs ⁷ de cœur. Ensuite un tunnel MPLS LSP est établi dans ce tunnel GRE (également appelé MPLSoGRE). Puis la session ATOM est établie dans ce tunnel MPLSoGRE.



Ce qui permet à l'entreprise d'établir à chaque extrémité un tunnel EoMPLS établi lui-même au-dessus d'un tunnel GRE sur un réseau IP sans avoir besoin de déployer un réseau MPLS avec les entités LSP requises dans le cœur du réseau d'entreprise.

De même que le tunnel EoMPLS est établi sur un tunnel GRE pour une liaison de type point à point, si le réseau d'entreprise demande à avoir des interconnexions de niveau 2 entre plus de 2 centres de

⁷ La fonction AToMoGRE est supportée avec la version de code IOS 12.2(33)SXI du Catalyst 6500, disponible courant été 2008. Le Cisco 7600 supporte la fonction de EoMPLSoGRE depuis 12.2.(33)SRB1 (Juin 2007).

données, VPLS peut être utilisé comme le montre la figure 7.

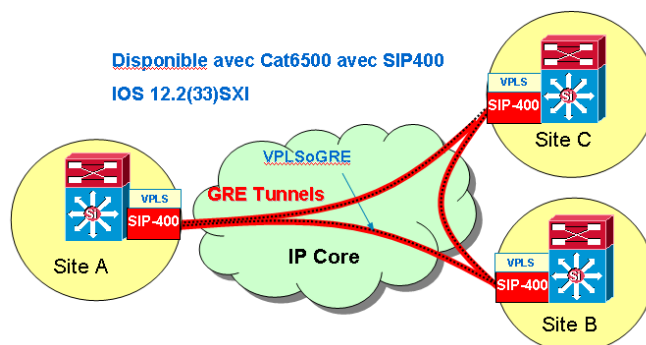


Figure 7 - VPLSoGRE

La force de VPLS est de pouvoir initier une ou plusieurs instances de « commutation » virtuelle (Virtual Forwarding Instance - VFI) complètement maillées entre tous les sites distants sans risque de boucle de niveau 2 à l'intérieur du cœur de réseau IP. Ce comportement d'autoprotection est disponible grâce à sa fonction native dite « split horizon » qui empêche tout paquet reçu sur une interface virtuelle de transmission d'être retransmis à son tour sur le même VFI par lequel il est arrivé.

Son second intérêt est de pouvoir faire évoluer l'architecture globale du réseau d'entreprise de manière très dynamique et très flexible en pouvant rajouter autant de sites distants que souhaités sans perturber le réseau de production.

Protection de boucle de niveau 2

Nous savons que le réseau de niveau 3 est de manière native très stable et intègre des mécanismes de convergence très rapide, ce qui nous permet de transporter de bout en bout des « pseudowires » de niveau 2 très stables. Tout problème survenant sur une liaison physique dans le cœur du réseau IP sera transparent pour le réseau de niveau 2 virtuel (L2VPN).

Nous savons également que dans un réseau maillé de type VPLS, celui-ci fournit des liens redondants (Split-Horizon) sans devoir activer le STP dans le cœur du réseau.

Toutefois, si un des équipements à chaque extrémité du réseau IP qui établit le L2VPN devait être interrompu pour des raisons de maintenance ou de crash, il est impératif de dupliquer cet équipement pour pouvoir offrir une passerelle de sauvegarde en cas de problème.

Il est très important d'assimiler la topologie globale de niveau 2 de bout en bout dès lors que les équipements d'extrémité sont dupliqués. En effet, si on analyse les liaisons de niveau 2 virtuelles nous nous apercevons, que ce soit pour EoMPLS ou VPLS, que ce soit pour un cœur de réseau MPLS ou IP (L2PVNoGRE), qu'une boucle de niveau 2 peut se créer comme le montre la figure 8.

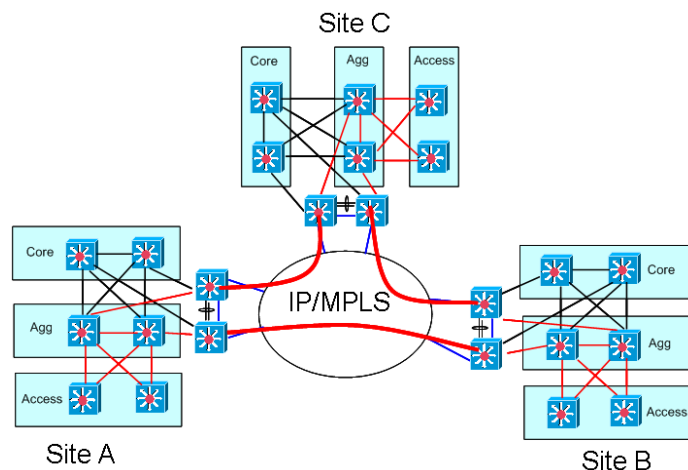


Figure 8 - boucle de niveau 2

Dans cet exemple, chaque « pseudowire » de type EoMPLS est garanti lui-même au cœur du réseau IP/MPLS. Mais l'entité qui établit ce « pseudowire » doit être redondante. Nous avons donc dans chaque centre de données 2 commutateurs qui vont établir chacun un lien virtuel de niveau 2 formant une grande boucle entre tous les sites distants.

Si nous tenons compte du Protocole de Spanning Tree, il existe au moins 3 moyens essentiels de contrôler cette boucle de niveau 2. Toutefois, le STP n'étant pas une solution recommandée pour les longues distances, nous allons expliquer deux autres méthodes :

- MST
- EEM – Embedded Event Manager.

MST dans le N-PE⁸

Deux fonctions très importantes au niveau de MST font que sa fonction principale peut être optimisée pour isoler le protocole de Spanning Tree au niveau de chaque centre de données.

La 1^{ère} est le « mapping » de plusieurs VLAN pour une même instance de Spanning Tree.

Seul un VLAN est actif pour contrôler les boucles de niveau 2.

La 2^{ème} est que vu de l'extérieur de sa région MST, l'ensemble de tous les commutateurs qui constituent cette région est vu comme un « simple » commutateur logique.

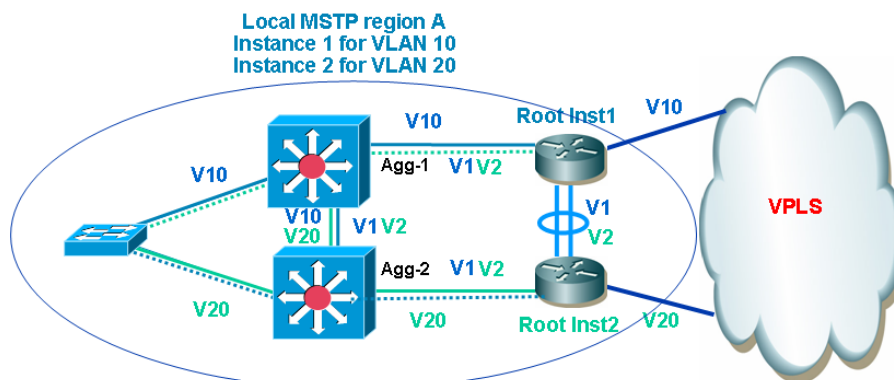


Figure 9 – MST dans tout le centre de données

Dans l'exemple de la figure 9, MST est déployé dans tout le centre de données. Chaque centre de données a sa propre Région MST. Le STP est isolé vers le cœur du réseau IP/MPLS.

Nous allons également profiter de MST et le support de plusieurs instances de STP pour distribuer le trafic sur tous les liens disponibles.

Nous avons établi 2 instances de STP, dans lesquels les VLAN de données sont distribués équitablement. Les 2 NPE sont « root » respectivement de leur instance de STP.

Il est important de noter que les VLAN de données ne sont pas autorisés sur le lien entre les 2 NPE (root 1 et root 2). Basé sur le coût (STP) des l'interfaces, chaque instance de STP verra un de ses

⁸ commutateur de cœur de l'entreprise exécutant les fonctions de virtualisation des lien de niveau 2 (VPLS)

liens vers le niveau d'agrégation en mode d'attente (Alternate).

Ce qui nous permet de contrôler la boucle géante de site à site et de la contrôler de la même manière sur chacun des centres de données.

Dans la figure 10, nous avons souhaité conserver STP ou RSTP dans le centre des données.

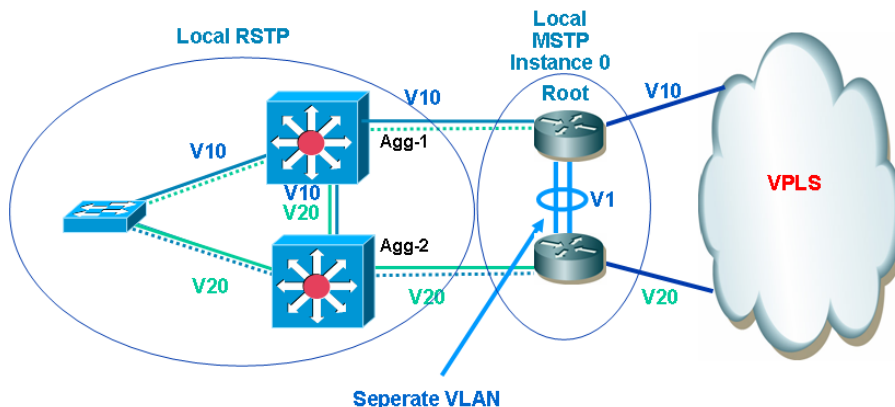


Figure 10 - RSTP dans le centre de données

Vus de l'extérieur, tous les commutateurs qui constituent la région MST, sont vus comme un unique commutateur logique (figure 11)

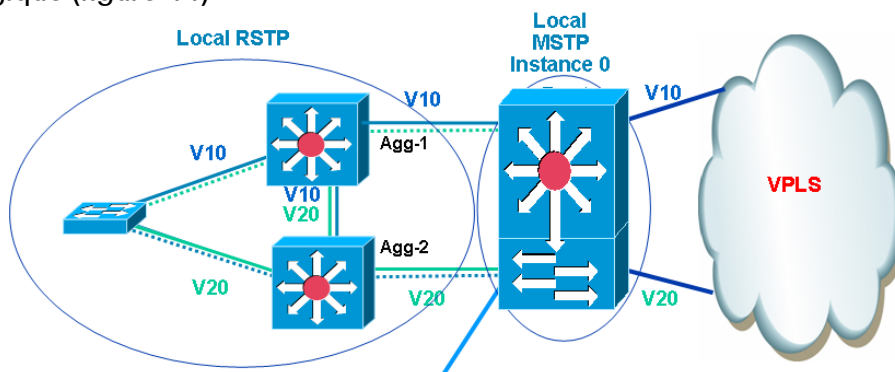


Figure 11 - RSTP dans le centre de données – Vue logique

Par ce biais, chaque commutateur d'agrégation va jouer sur le coût de ses interfaces VLAN pour rendre le lien actif ou en attente. De la même manière que précédemment les VLAN de données ne sont pas transmis sur le lien entre les 2 N-PE (root).

L'état de fonctionnement des interfaces WAN, c'est-à-dire les interfaces qui vont initier les réseaux de niveau 2 virtuels vers les différents sites distants, doit être rigoureusement surveillé de manière à éviter un trou noir.

La méthode utilisée est EEM, Embedded Event Manager. EEM va vérifier l'état et les événements liés à ces interfaces. En cas de problèmes, EEM va ordonner une action immédiate, à savoir, faire tomber toutes les interfaces internes liées à cet événement. Ces actions sont très rapides et efficaces.

EEM dans le N-PE

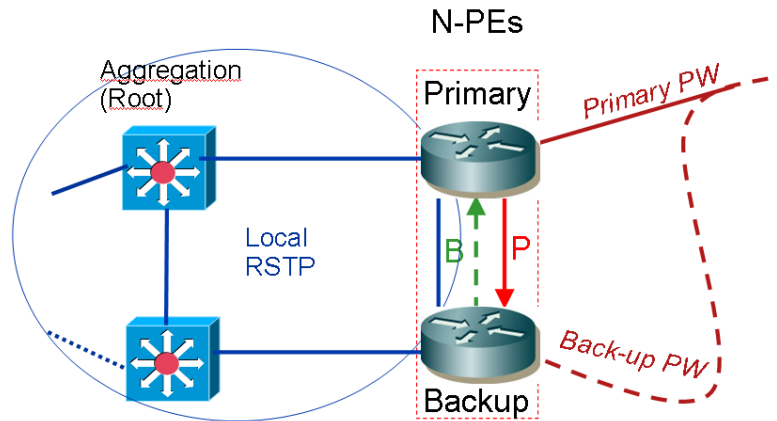


Figure 12 - EEM dans le N-PE 1

Avec EEM, les commutateurs d'agrégation restent Root pour le centre de données, ce qui est un élément très important à prendre en compte. Une autre valeur majeure de EEM est sa possibilité d'extensibilités ainsi que son mariage optimisé avec des commutateurs VSS dans l'agrégation. Le principe de EEM est relativement simple. Un des N-PE est désigné comme « primaire », l'autre étant désigné comme secondaire. Le lien de niveau 2 virtuel (Pseudowire or PW) est dupliqué sur le N-PE secondaire.

A partir du N-PE primaire, un signal P (primary) indique au N-PE secondaire que son état est toujours actif – des sondes d'état analysent sans interruption les conditions de fonctionnement du N-PE. Figure 13, tant que le N-PE secondaire reçoit ce signal P, aucune action n'est mise en route.

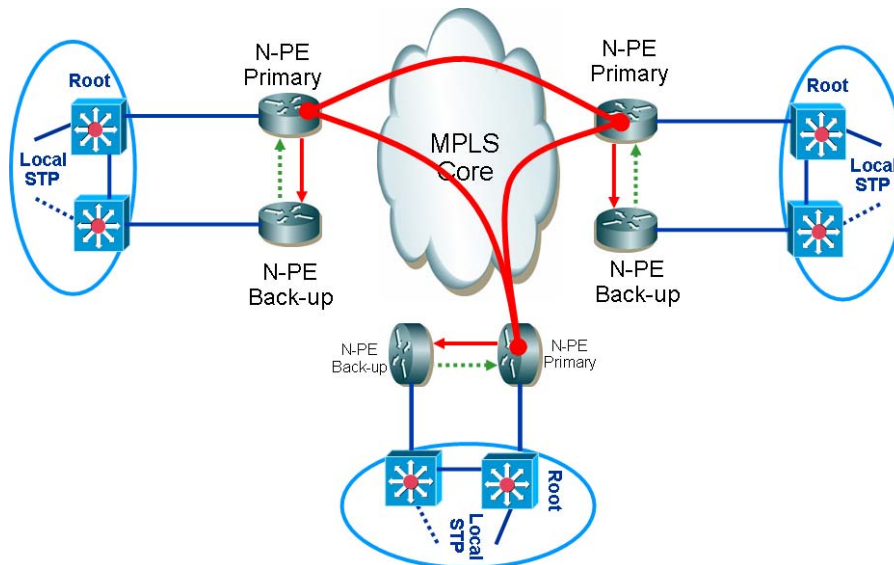


Figure 13 - N-PE primaire est OK

Le signal P « Primary » en rouge est monté, il force le signal B « Backup » en vert à être inactif. Le Signal B « Backup » est descendu, le N-PE Primary peut être actif.

Si ce signal devait disparaître pour quelque raison que ce soit, le N-PE secondaire prendrait le relais immédiatement comme indiqué dans la figure 14.

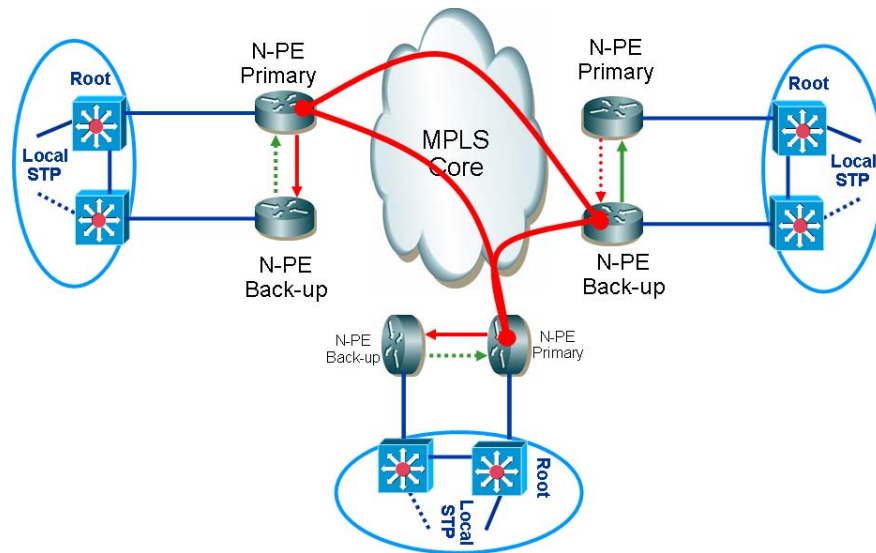


Figure 14 - N-PE primaire est tombé

Le signal P en rouge a été interrompu. Le N-PE de sauvegarde prend immédiatement le relais et envoie le sémaphore B au N-PE « primaire ».

L'étape suivante, le N-PE redevient à nouveau prêt à être actif. Il reçoit le sémaphore B de la part du N-PE de sauvegarde lui indiquant de patienter.

Le N-PE de sauvegarde s'aperçoit par le signal P réémis par le N-PE primaire que celui-ci est de nouveau opérationnel.

Le N-PE de sauvegarde va décrétement un compteur qui permettra, pendant une durée de temps flexible, de surveiller l'état général du N-PE primaire. En cas de problèmes intermittents, celui-ci devra attendre que le réseau primaire se stabilise avant de reprendre le relais.

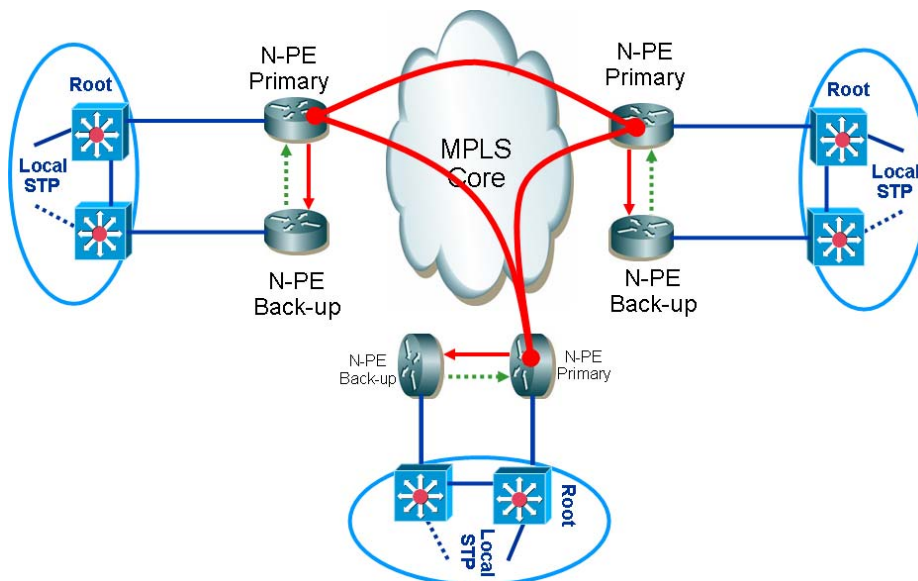


Figure 15 - le N-PE primaire est de nouveau actif

Dans la figure 15, après avoir attendu et s'être assuré que le réseau était de nouveau stable et opérationnel, le N-PE de sauvegarde va autoriser le N-PE primaire à redevenir actif.

En même temps, le N-PE de sauvegarde passera en mode d'attente, tout en continuant à surveiller le sémaphore de PE primaire.

Conclusion

Cisco recommande de limiter au maximum le réseau de niveau 2 dans le centre de données.

Si toutefois, pour des raisons applicatives, il était impératif pour l'entreprise d'étendre le niveau 2 au-delà du centre de données, Cisco recommande alors 3 approches distinctes. Ces approches permettent de garantir un réseau de niveau 2 étendu, performant, basé sur des fonctions hardware totalement, totalement redondant à basculement rapide.

En cas de besoin, l'entreprise peut déployer également différentes classes de service par type d'applications.

Ces trois recommandations répondent aux problématiques induites par l'extension du Protocoles de Spanning Tree en dehors du centre de données en termes de risques d'instabilité partielle ou totale de l'ensemble du domaine de Spanning Tree, ou de dégradation des temps de basculement.

- Virtual Switching System (distance "Metro") sur un réseau optique à très haut débit DWDM..
- EoMPLS et VPLS sur un réseau de cœur MPLS (pas de limite de distance⁹)
- EoMPLS et VPLS sur un réseau de cœur IP (pas de limite de distance)

D'autre part, pour isoler le STP de bout en bout de l'architecture globale, Cisco recommande 2 méthodes distinctes :

- MST dans le N-PE
 - o Avec MST dans le centre de données
 - o Ou avec RSTP dans le centre de données
- EEM dans le N-PE avec les sémaphores pour valider l'état des différents éléments de l'architecture de niveau 2 à des fins d'extensibilité.

⁹ Attention toutefois au temps de latence engendré par les longues distances qui peut avoir un impact sur certaines applications sensibles à la latence. Les distances sans limite entre deux centres de données ne s'appliquent pas pour des Applications qui requièrent de la duplication de données en mode synchrone.



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



Copyright © 2008 Cisco Systems, Inc. Tous droits réservés. CCSP, CCVP, le logo Cisco Square Bridge, Follow Me Browsing et StackWise sont des marques de Cisco Systems, Inc. ; Changing the Way We Work, Live, Play, and Learn, et iQuick Study sont des marques de service de Cisco Systems, Inc. ; et Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, le logo iQ, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, le logo Networkers, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient et TransPath sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web appartiennent à leurs propriétaires respectifs. L'emploi du mot partenaire n'implique pas nécessairement une relation de partenariat entre Cisco et une autre société. (0502R) 205534.E_ETMG_JD_05/08