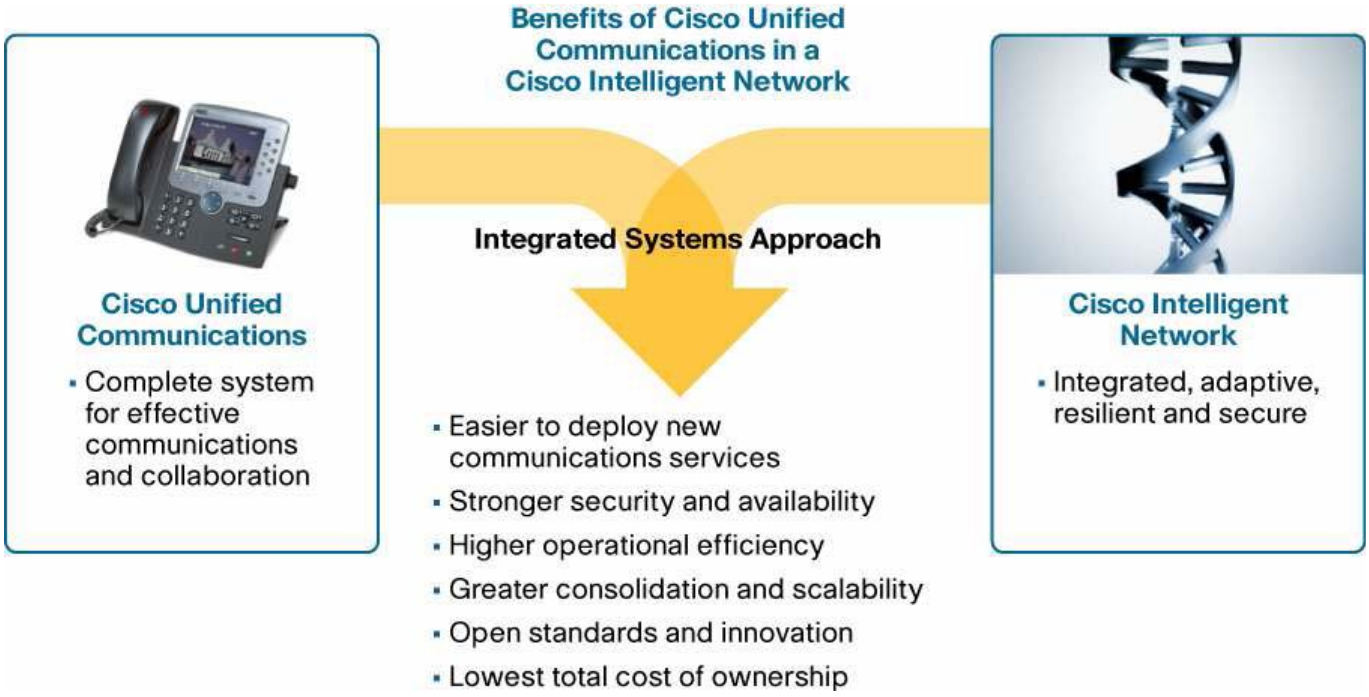
décembre 08

CiscoMag
Votre rendez-vous mensuel avec Cisco France

numéro 22

Le réseau comme plateforme des communications unifiées et de la collaboration

Nous vous proposons dans ce document d'aborder tous les éléments que le réseau Cisco apporte en termes de services d'infrastructure pour déployer des services de communications unifiées et de collaboration en entreprise.



Les services rendus peuvent être résumés suivant ces grandes familles :

- Services de haute disponibilité
- Services de sécurité : authentification, confidentialité, renforcement contre les dénis de service, gestion de l'identité des utilisateurs
- Mutualisation des services sur les équipements d'infrastructure
- Services de virtualisation
- Services de mobilité
- Services d'automatisation et de simplification des déploiements

L'infrastructure

L'infrastructure doit permettre de déployer tous les composants nécessaires aux services de communications unifiées, à savoir :

- Les serveurs de communications
- Les serveurs applicatifs complémentaires
- Les passerelles vers le réseau RTC (voix ou vidéo TDM ou IP)
- Les IP Phones
- Les postes de travail informatiques
- Les terminaux de tous types connectés en WiFi

Les équipements pour une haute disponibilité

La convergence des flux sur le même réseau dit de campus nécessite une disponibilité accrue. Les besoins des flux constituant les communications unifiées et la collaboration nécessitent des temps d'indisponibilité plus faible que pour de simple flux de données.

Les besoins de haute disponibilité sont beaucoup plus forts qu'auparavant :

- Moins d'une seconde pour la voix
- Moins de 200-300 ms pour la vidéo

Il faut également prendre en considération les impacts subjectifs des problèmes réseaux sur les applications voix ou vidéo, à savoir qu'en fonction d'un temps de coupure donné lors d'une communication téléphonique, l'impact pour l'utilisateur peut aller d'une totale transparence à un reset complet du poste téléphonique. Afin d'améliorer l'expérience utilisateur nous cherchons donc a proposer des architectures avec un temps de convergence minimal.

La haute disponibilité du réseau est basée sur les critères suivants, qu'il faut intelligemment conjuguer pour arriver à des taux de disponibilité compatibles avec ces nouveaux usages, à savoir :

- Redondance matérielle intrinsèque aux équipements sur châssis modulaires (série Catalyst 6500, 4500) :
    - redondance des alimentations sur réseau électriques différents et secourus, remplaçables à chaud,
    - redondance des ventilateurs, remplaçables à chaud,
    - Doublement des cartes de supervision avec des mécanismes de basculement transparents,
    - Fond de panier entièrement passif,
    - Horloge redondante,
    - Cartes changeables à chaud.

- Utilisation de technologies de « stacking » (série catalyst 3750)
    - Chaque équipement de la pile possède sa propre alimentation, changeable à chaud,
    - Membres hot swappable,
    - Le contrôle de la pile est réalisé par un des éléments de la pile avec une une redondance du master en 1:N.

- Mécanisme de bascule de la carte de supervision

    - Catalyst 6500 and 4500 stateful switchover (SSO)
        - La carte redondante est en 'hot-standby' et est entièrement synchronisée avec la carte de supervision active,
        - Les informations de tables ou états des ports synchronisés entre les deux cartes de supervision,
        - En cas de basculement :
            - Les ports des téléphones restent actifs,

        - Les états restent inchangés.

    - Catalyst 3750/3750E stackwise Plus :
        - Gestion de la perte du Master,
        - La switching fabric est étendue au travers de l'anneau,
        - Double anneau en redondance.

    - En fonction des plateformes, impact minimal à quasi nul sur les flux voix ou vidéo

- Redondance matérielle entre équipements

    - Utilisation de technologies d'agrégations de liens (multicartes ou multi-switchs sur une technologie de pile)
    - Double attachement des équipements réseaux
    - S'assurer que le matériel remonte la perte d'un lien
    - Utilisation de protocoles de détection rapide de perte de lien (comme BFD : Bidirectional Forwarding Detection)

- Stabilité logicielle :

    - IOS Modulaire : cette nouvelle architecture logicielle permet une réduction ou même suppression des arrêts non planifiés en permettant de mettre à jour un module logiciel dans un commutateur sans toucher aux autres processus ce qui assure un impact minimum sur les flux voix et vidéo.
    - ISSU sur 4500 apporte aujourd'hui la possibilité de mettre à jour l'IOS avec une interruption de service < 50 msec.
    - Gestion de la sauvegarde automatique et régulière des configurations
    - Automated System Configuration Check
    - Control Plane Policing : pour assurer un service performant aux applications voix / vidéo en protégeant la CPU qui est en charge de tout le control plane contre des virus, vers ou dénis de service par des services de limitation de débit « hardware ».

- Détection de problèmes matériels et réactions :

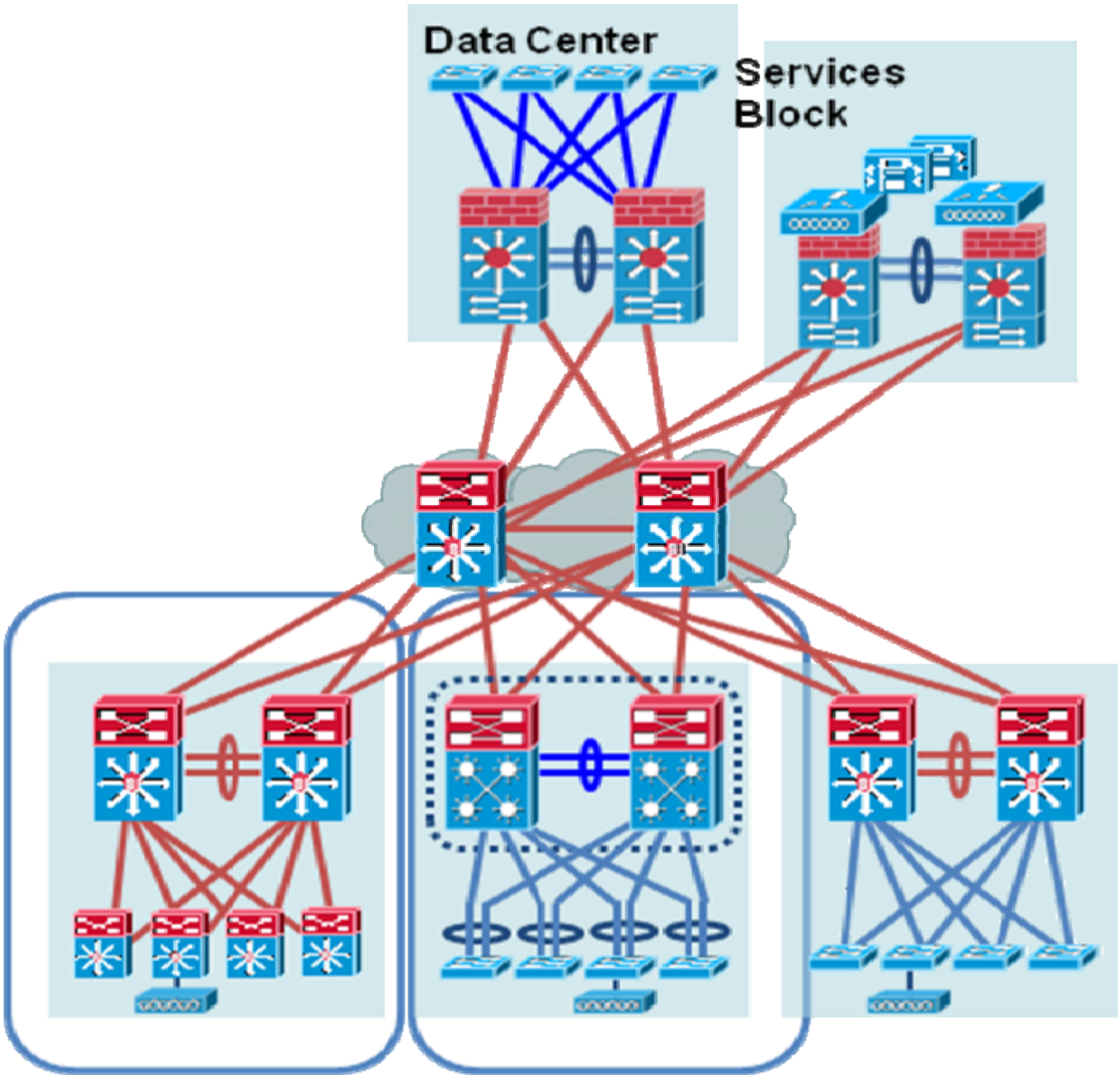
    - Generic On-Line Diagnostics (GOLD)
    - Automated System Health Check

Les architectures pour une haute disponibilité

Le design est réalisé en blocs fonctionnels en faisant appel aux meilleurs protocoles (spanning tree protocol ou protocoles de routages) ainsi qu'à des mécanismes de type NSF/SSO. Non-Stop Forwarding (NSF) est une fonction permettant aux protocoles de routage de redémarrer proprement avec un impact minimal sur les flux en cours, la nouvelle carte active continue de router sur la base des tables synchronisées par SSO (table CEF). Le catalyst est aidé par ses voisins pour reconstruire sa table de routage et les adjacences sont reconstruites sans perte de trafic.

Le design en blocs fonctionnels permet d'assurer une haute disponibilité ainsi qu'une évolutivité de la solution proposée.
Les commutateurs d'accès permettent de connecter tous les équipements utilisateurs ou serveurs sur le réseau. Ces derniers sont connectés sur des commutateurs, généralement par couple, qui agrègent par étage ou par bâtiment les commutateurs d'extrémité.
Différents blocs de distribution existent avec des fonctions généralement dédiées :

- Bloc de distribution « Utilisateurs »
- Bloc de distribution « Serveurs »
- Bloc de distribution « Internet »
- Bloc de distribution « Wan »



Sur le concept des blocs fonctionnels, plusieurs modèles de déploiement existent.

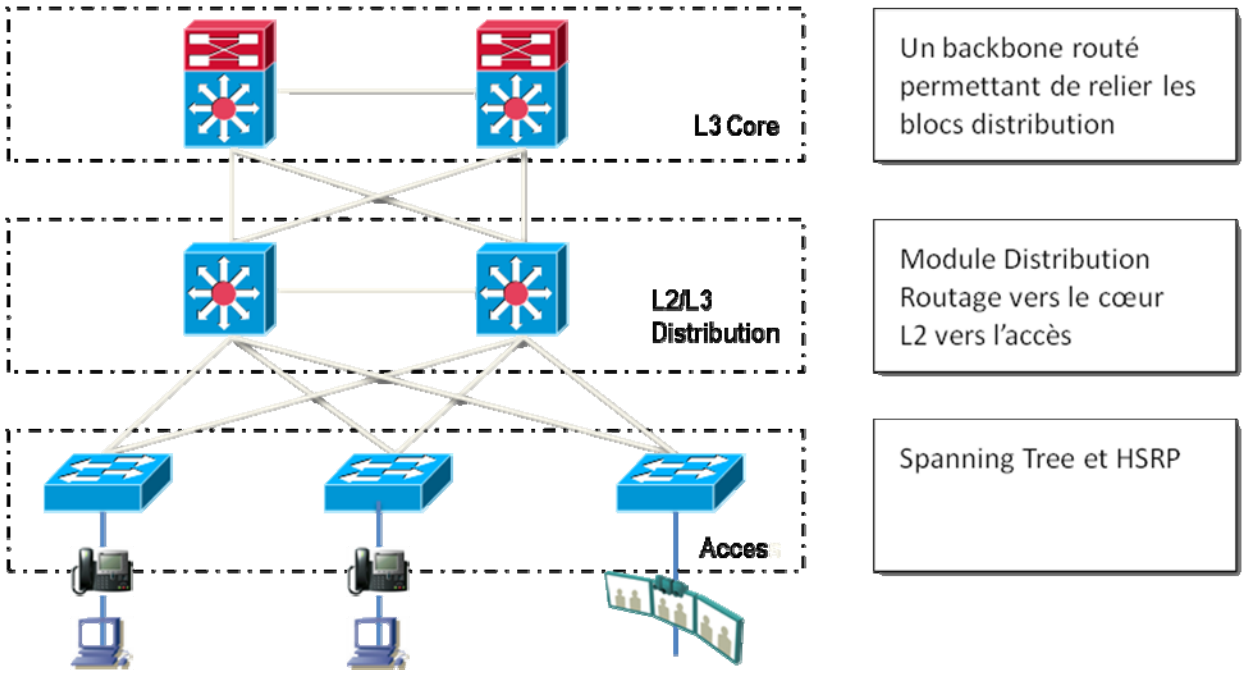
Modèle 1 : Cœur routé/Fonction FHR sur distribution

Dans ce modèle, le bloc de cœur est dit routé (pas d'extension de domaines Ethernet sur ce bloc), et la passerelle par défaut des VLANs Utilisateurs sont sur les blocs de distribution. Les commutateurs des blocs accès « utilisateurs » sont alors des commutateurs utilisés en niveau 2.

Dans ce modèle, le temps de convergence est basé sur le rapid STP (802.1w) pour les domaines Ethernet et sur fast convergence OSPF pour liens routés.
L'utilisation de plusieurs protocoles avec des interactions multiples (HSRP ou VRRP, Rapid STP) sont nécessaires ainsi que l'utilisation de protocoles de routage (OSPF, EIGRP, ...) entre les équipements de distribution et de cœur.
La convergence dépend de plusieurs facteurs, dont le temps de convergence de protocole de FHRP (comme HSRP) de 900 msec à 9 secondes ainsi que le Spanning Tree de 400msec à 50 seconds.
Les domaines Ethernet sont communs à tous les commutateurs derrière un bloc de distribution et pour réduire les risques d'un problème de STP, plusieurs fonctions de protection du STP sont

implémentées notamment BPDU Guard, Root Guard, Loop Guard.

Un design alternatif de ce modèle consiste à dédier les VLANs par commutateur d'accès pour éviter de constituer de trop importantes boucles.

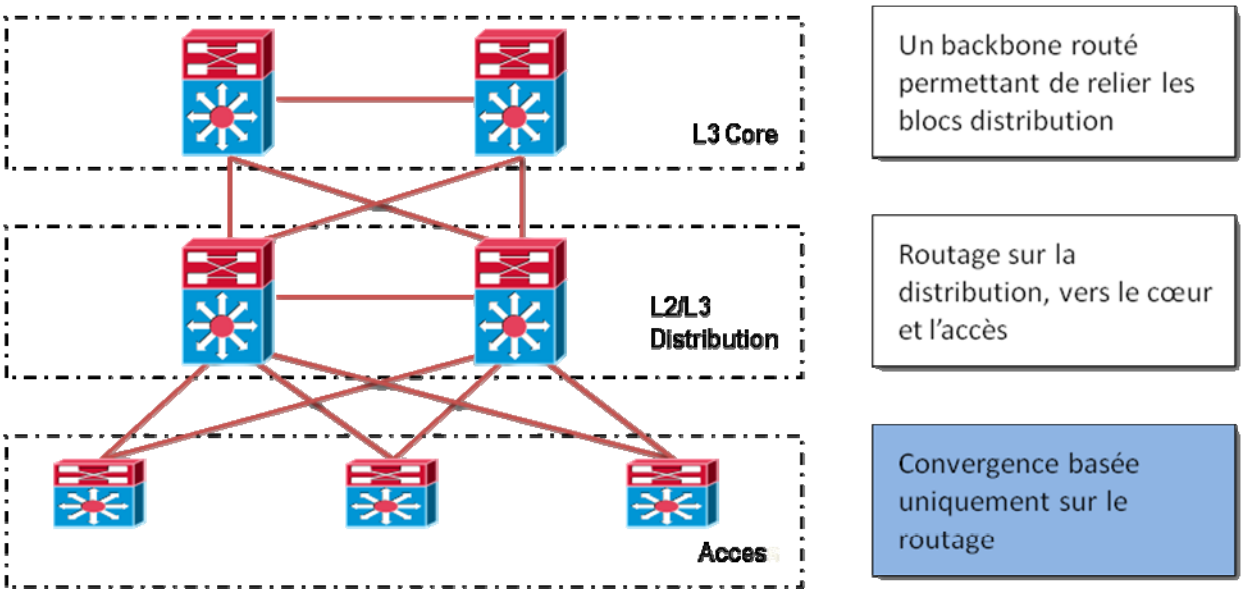


Modèle 2 : FHR effectué en accès

Dans ce modèle le routeur par défaut du VLAN « utilisateur » se situe sur le commutateur d'accès qui est un commutateur niveau 3. Les blocs de distribution et de cœur sont donc complètement routés. Ce modèle offre une isolation plus forte entre les blocs utilisateurs, car le domaine Ethernet est dans ce cas local aux commutateurs. Les algorithmes de type STP ou rapid STP ne sont donc plus utilisés.

Le routage est porté jusqu'à l'accès afin de bénéficier au maximum de la stabilité apportée, de la vitesse de convergence en cas de perte de liens ou de routeurs.
Un seul protocole pour les exploitants est mis en jeu et tout un jeu de commandes et debug sont donc simplifiés.

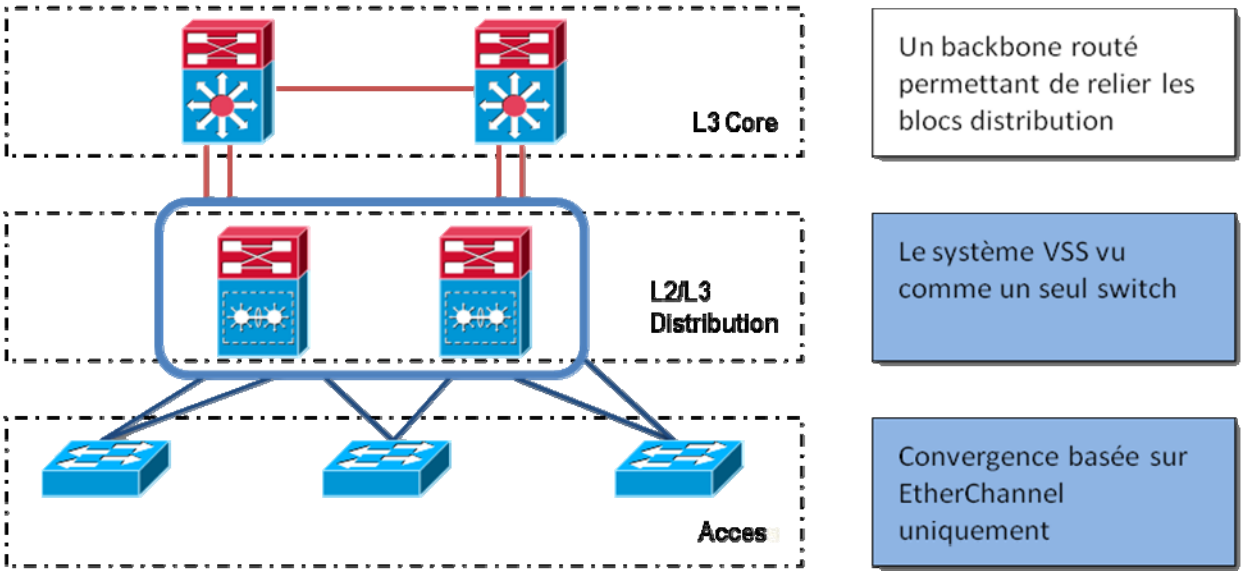
Outre une meilleure stabilité du réseau due à la réduction au minimum des domaines Ethernet et sans aucun risque d'inconsistance entre les topologies niveau 2 et niveau 3, ce modèle offre également une vitesse de convergence plus faible. L'exploitation en est simplifiée grâce au seul besoin de connaissance des protocoles de routage.
OSPF configuré avec les améliorations Cisco (timers sub-second) ou EIGRP peuvent converger en moins de 200 ms dans ce genre d'architecture alors qu'un temps de convergence d'un « Spanning Tree » dépend également de GLBP ou HSRP.



Modèle 3 : VSS

Le modèle 3 apporte une variante en utilisant la fonction VSS disponible sur les châssis Catalyst 6500.

Cette approche permet à deux équipements de n'apparaître comme un seul vu du reste du réseau. Ceci permet d'apporter de la redondance avec deux châssis indépendants sans nécessiter l'activation de protocoles de type STP. La redondance est ici gérée par des agrégats de liens multi châssis.

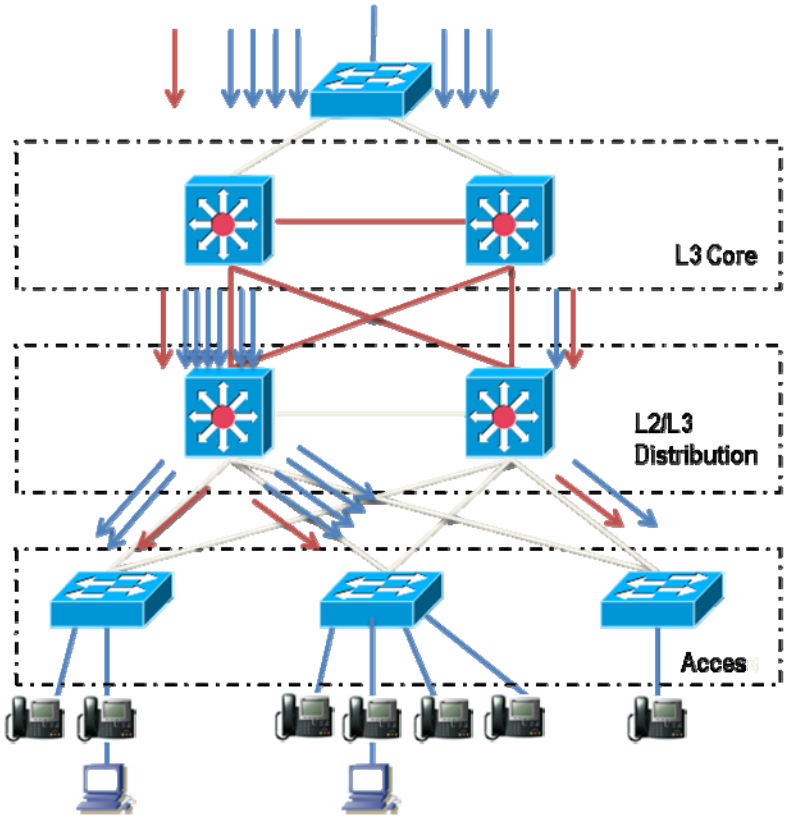


Les architectures traditionnelles L2 restent valides mais les évolutions présentées ci-dessus fournissent :

- Une simplification des plans de contrôle
- Des capacités de commutation accrues
- Une meilleure disponibilité (200 msec)

Les services de multicast

Que ce soit pour des flux de type « musique d'attente pour la téléphonie » ou pour diffuser un contenu voix ou vidéo, le déploiement le plus efficace est d'utiliser les capacités de réplication intelligente du réseau avec le multicast. Ainsi la réplication des données est gérée par ce dernier sans impact en termes de performances sur les serveurs de diffusion.



Diffusion en unicast

Réplication par le serveur
Charge supplémentaire à prendre en compte
Dimensionnement des serveurs ??

Diffusion en multicast

Réplication par le réseau
Charge nulle sur le serveur

PIM Sparse Mode est majoritairement utilisé dans ce cas sur l'infrastructure. Le mécanisme de redondance du « rendez-vous point » basé sur anycast RP apporte une convergence rapide lors de la perte du nœud qui supporte le RP.

Il est également possible, en utilisant PIM-SSM et SSM Mapping, de simplifier et sécuriser le déploiement de multicast et musique d'attente puisque plus aucun RP n'est à définir. Pour éviter de gérer des RPs et les problèmes de redondance, il faut utiliser PIM SSM.
La fonction SSM Mapping sur les Catalyst permet de gérer les clients ne générant pas de requêtes IGMPv3.

L'approche où le réseau est routé à l'accès (sur le commutateur d'accès) simplifie quant à lui grandement la topologie Multicast.

Les services sur le commutateur « accès »

Un certain nombre de fonctions doivent être disponibles sur les commutateurs d'accès pour apporter des services de sécurité, ainsi que d'aisance dans le déploiement des différents terminaux (Téléphones IP, Postes de travail informatique).

Les commutateurs d'extrémités doivent apporter les fonctions nécessaires à une interaction entre réseau et téléphone pour automatiser le déploiement des IP Phones telles que :

- Alimentation
- Définition des « VLANs voix » pour une isolation des flux
- Définition des paramètres de QoS à utiliser

- Définition des domaines de confiance – trust/untrust

Le téléphone contient un commutateur 3 ports configuré dynamiquement par le commutateur et le Call Manager. Il participe dynamiquement à la QoS et à la sécurisation de la solution.

Le téléphone doit pouvoir négocier intelligemment les besoins en alimentation, les VLANs, les droits d'accès au réseau (notamment basés sur 802.1x), la configuration de la QOS.

Renforcement de l'accès au VLAN voix/data

CDP ou LLDP-MED permet de ne donner accès au VLAN voix que si la négociation s'est déroulée correctement. N'importe quel équipement connecté sur le port accès ne peut donc pas pénétrer dans le VLAN voix.

Nous proposons historiquement d'utiliser CDP pour assurer tous ces services entre les commutateurs d'accès et les téléphones. CDP dans sa version 2 offre les services suivants complémentaires nécessaires pour faciliter le déploiement des téléphones :

- Négociation d'alimentation
- Définition de VLAN – en particulier VLAN voix
- Extension de la frontière de confiance sur les téléphones pour le déploiement de la QOS
- Détection de téléphone pour bypasser 802.1x
- OER (Optimized Edge Routing)
- Cisco Emergency Responder (basé sur la MIB CDP)

LLDP-MED permet aujourd'hui de continuer cette approche de négociation par port. LLDP-MED est donc devenu l'implémentation standard de CDPv2 :

- Découverte de l'équipement et de ses capacités du device (routeurs, bridge, téléphones, etc)
- Speed et duplex de l'interface
- Affectation voice VLAN
- Découverte localisation
- Découverte alimentation – combien, priorité, type
- Découverte d'équipements dans un environnement multi-vendeur
- Inventaire réseau
- Détection des configurations erronées (duplex, speed, etc.)

Le commutateur d'accès doit également être capable de respecter le niveau de sécurité choisi par l'entreprise pour l'accès au VLAN data (poste de travail) et au VLAN voix (Téléphone IP). Tous les commutateurs de la gamme Catalyst supportent 802.1x pour le VLAN Voix et pour le VLAN Data avec 2 domaines d'authentifications différents. Il est ainsi possible sur le même port de configurer 2 domaines de sécurité (802.1x dans le VLAN data et CDP/LLDP-MED ou 802.1x dans le VLAN Voix) grâce à une fonction nommée MDA (Multi Domain Authentication).

Les méthodes d'authentification du téléphone peuvent être les suivantes :

- 802.1x dans le téléphone Cisco
- Bypass 802.1x grâce à la détection CDP par le commutateur
- Mac-Authentication-Bypass permettant d'utiliser l'adresse mac des téléphones comme nom d'utilisateur pour l'authentification

NB : lorsque qu'un poste de travail est connecté derrière un téléphone sur l'infrastructure, il est important de notifier le commutateur d'une déconnexion du PC connecté au téléphone pour éviter qu'un autre utilisateur puisse bénéficier des droits du précédent simplement en connectant son PC sur le téléphone. Cisco propose pour ce faire des mécanismes dans les téléphones (notamment l'envoi de trames de type EAP-LOGOFF dans le VLAN data) pour que le commutateur ferme l'accès au VLAN data à la déconnexion du PC.

Une fois l'autorisation donnée de rentrer dans le VLAN, la fonction de « Port Sécurity » permet de limiter le nombre d'adresses mac et donc de terminaux autorisés par port (évite par exemple qu'un terminal connecté derrière un commutateur pirate ne puisse ouvrir la porte en 802.1x autorisant tous les autres terminaux à en bénéficier).
La fonction « BPDU Guard » permet aussi de détecter la connexion d'un commutateur pirate sur un port accès.

Fonctions complémentaires sur le commutateur d'accès par port

Des fonctions apportent un complément en terme de sécurité au sein des VLANs utilisateurs voix et data. Par exemple les fonctions de type : Dynamic Arp Inspection (DAI), IP Source guard, DHCP Snooping, permettent respectivement de se protéger d'attaques de type ARP Spoofing ou IP Spoofing ainsi que de l'insertion volontaire ou non d'un serveur DHCP sur le VLAN utilisateurs.

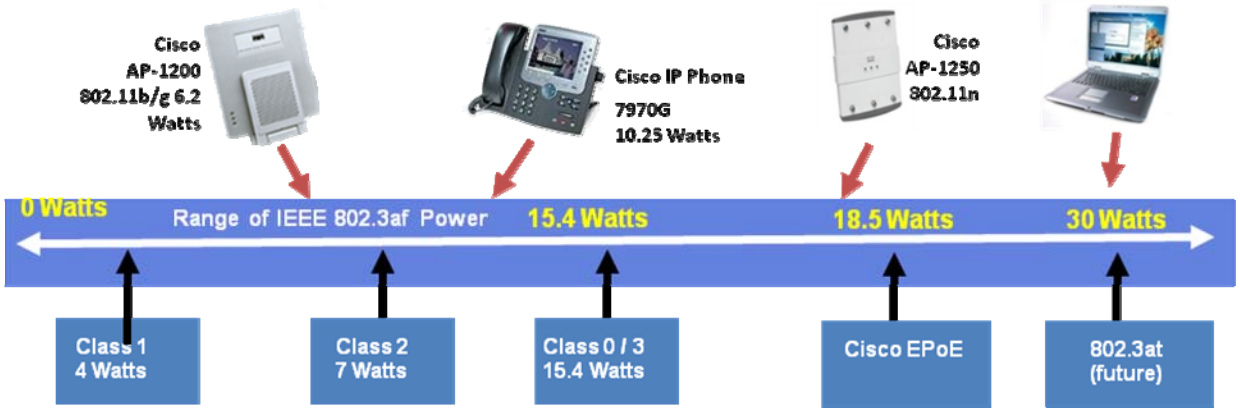
Fonctions complémentaires sur le commutateur d'accès par VLAN :

- VLAN ACL : ACL qui permet de limiter le trafic au sein d'un VLAN. Ceci permet par exemple de n'autoriser que le RTP au sein du VLAN voix. Ainsi, même un équipement non autorisé entré dans ce VLAN ou un comportement anormal d'un téléphone ne pourra pas communiquer avec les autres terminaux de ce VLAN.

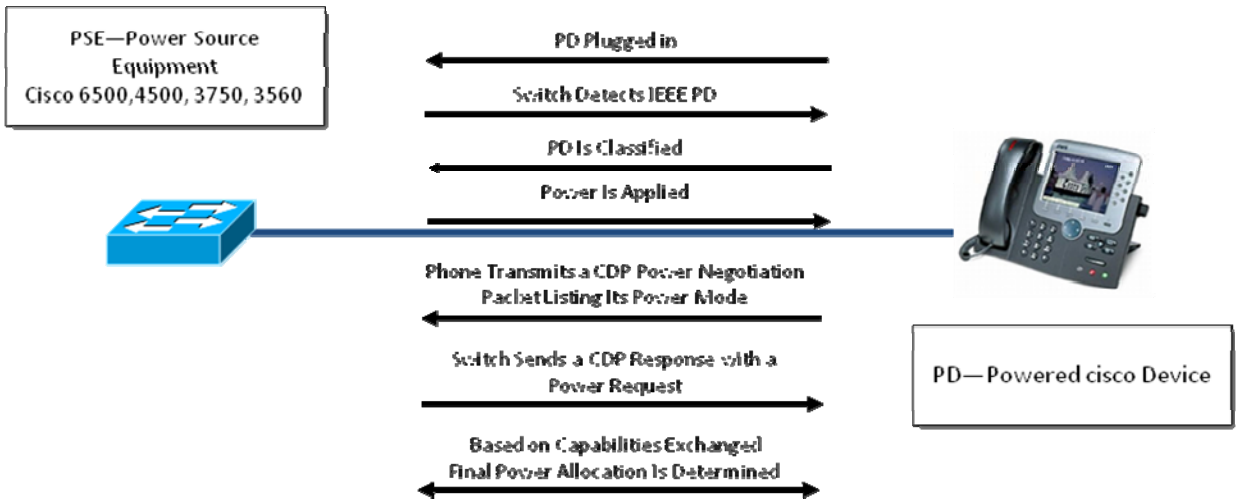
- L'affectation du VLAN voix ne doit pas remettre en cause les autres fonctionnalités, notamment de QoS et de sécurité. Toutes les fonctions doivent pouvoir être activées simultanément.

Négociation intelligente de la puissance délivrée aux téléphones - Cisco Intelligent Power Management (IPM)

Cisco propose aujourd'hui plusieurs possibilités pour fournir l'alimentation aux terminaux. 802.3af ainsi qu'une méthode « Cisco Enhanced PoE » délivrant jusqu'à 18.5w.



En utilisant la négociation bidirectionnelle CDP, le commutateur peut provisionner les besoins réels en terme de puissance électrique (au delà des quelques classes définies par le standard 802.3af)

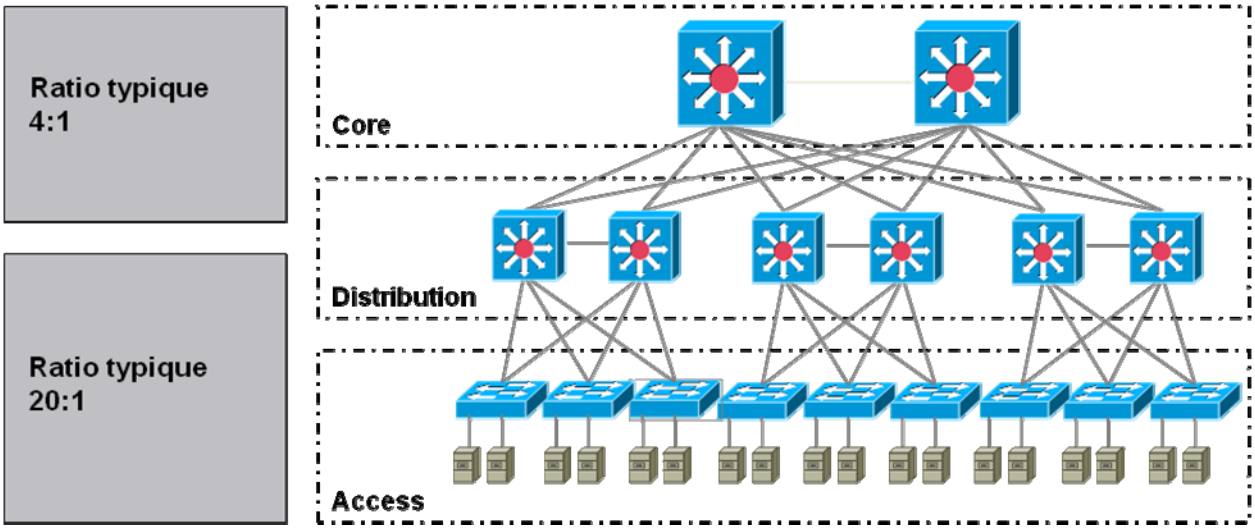


Les besoins et l'approche de la QoS

La qualité de service est nécessaire pour un engagement de qualité lors d'un déploiement de communications unifiées. Que ce soit sur le WAN, où les débits sont généralement plus faibles, ou bien sur le LAN, cette QoS permet de s'assurer, dans le temps, que le niveau de services fournis aux utilisateurs sera toujours le meilleur.

Associé à la gestion de la QoS, l'infrastructure doit être capable de réaliser le CAC (Contrôle d'admission) afin que la politique de QoS soit respectée.

Sur le LAN les points potentiels de congestion sont nombreux sur les liens dits « uplink » entre les commutateurs, et ce d'autant plus qu'un élément réseau ou un lien peut venir à ne plus être disponible et donc mener à un risque de congestion plus fort.

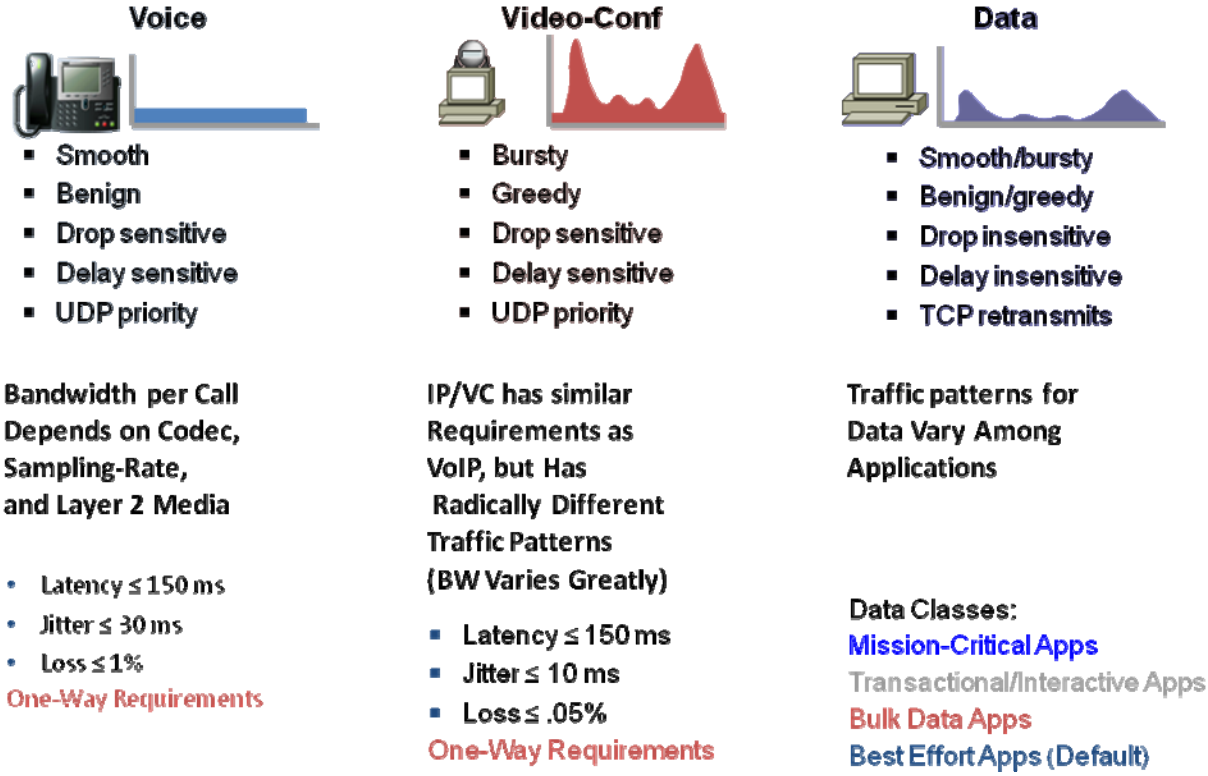


Les étapes principales suivantes sont à prendre en compte lors d'un déploiement de la QoS :

- Définir clairement les objectifs - Quels sont les critères importants ?
  - Protection flux voix? vidéo? data?
  - Protection contre les virus/vers?
  - S'assurer du soutien général dans la démarche avant tout déploiement
- Choisir un nombre restreint d'applications considérées comme "critiques" dont la voix et la vidéo font partie
  - Déterminer avec soin le nombre de classe de service
  - Plus de classes = un service plus granulaire ... mais plus difficile à gérer
- Certaines fonctions sont primordiales à l'accès :

  - Classification des différents flux
  - Mise en file d'attente par fonction de Queueing
- Mais il existe des possibilités d'automatisation : auto-QoS, macros pour simplifier le déploiement :
  - Définition de profils
  - Par défaut les paramètres de QoS sont définis

La gestion des files d'attente doit être mise en œuvre pour les déploiements téléphonie ou vidéo pour assurer un fonctionnement correct en toute circonstance – même en cas de congestion en respectant les besoins des applications tels qu'exprimés ci-dessous :



Sur le LAN :

Trois principaux modèles de déploiement de la QoS sur le commutateur d'accès sont disponibles :

- Modèle 1 : Modèle le plus simple, mais le moins sécurisé :
  - Prise en compte sans contrôle du champ DSCP d'entrée.
  - On peut ajouter un policer pour contrôler ce qui est envoyé dans la classe voix.

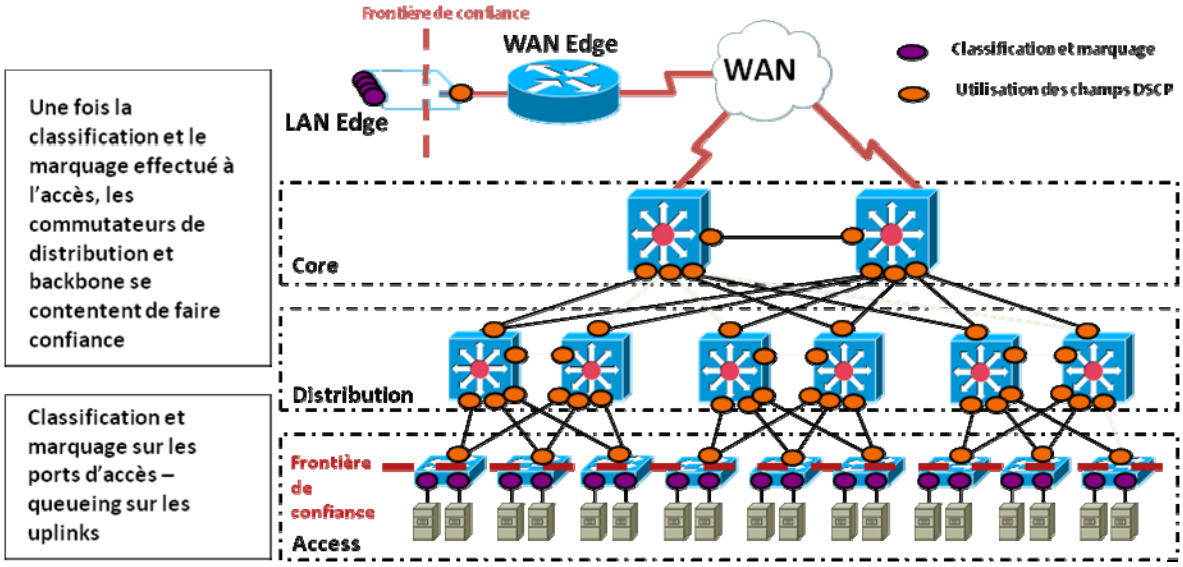
- Modèle 2 : Modèle plus évolué qui prend en compte la détection automatique des téléphones
  - Prise en compte de la CoS d'entrée uniquement s'il y a un téléphone pour les flux voix et la signalisation voix.
  - On peut ajouter un policer pour contrôler ce qui est envoyé dans la classe voix.

- Modèle 3 : Modèle le plus évolué qui peut aussi prendre en compte la détection automatique des téléphones.
  - Prise en compte de la CoS d'entrée pour les flux voix et la signalisation voix.
  - Policer pour contrôler ce qui est envoyé dans la classe voix et dans la classe data pour ne pas saturer les uplinks.

La classification par port ou VLANs en fonction du trafic est également nécessaire pour les applications sur le poste de travail informatique.

De manière générique, il faut reconnaitre puis marquer à l'entrée du réseau (port du commutateur ou

même téléphone qui représente la limite du domaine de confiance en terme de QoS), puis sur le reste du réseau gérer le marquage DSCP pour assurer l'engagement de QoS demandé par l'application.



Un certain nombre de fonctions doivent être disponibles sur le commutateur d'accès afin de gérer correctement la QoS nécessaire pour un flux temps réel :

- File d'attente de type PQ, strictement prioritaire
- Rate limiting : Limitation d'un flux entrant dans une classe (exemple classe VoIP)

Classification : Identification du trafic avec marquage, re-marquage au niveau DSCP/COS en faisant confiance a la QoS du tel et pas à celle du PC.
Le téléphone affecte la CoS du PC à 0.
Le téléphone affecte la CoS 5 pour la VoIP et CoS 3 pour la signalisation.
Le commutateur prend le CoS (niveau 2) entrant et mappe sur DSCP (niveau 3) pour ensuite envoyer vers la file d'attente appropriée.
Il faut également pouvoir reconnaitre le flux applicatif provenant d'un PC sur une application de communications unifiées avec gestion du flux média installée.

Tous les Catalyst gèrent les files d'attente en hardware (pas d'impact sur les performances). Les implémentations peuvent varier entre les modèles.

Chaque port dispose d'une quantité finie de buffers. L'activation de la QoS répartit les buffers entre les files d'attente. Il est donc vital de pouvoir gérer cette répartition en particulier pour les applications critiques qui demandent beaucoup de buffers (NFS sur UDP par exemple).

Sur le WAN :

Le WAN doit également pouvoir garantir les paramètres de QoS demandées en implémentant les mécanismes de mises en file d'attente et de vidage ordonnée.

Gestion du CAC :

Le contrôle d'admission ou CAC visant à limiter le nombre d'appels voix/vidéo pour respecter les règles de QoS afin de garantir la qualité de toutes les communications (et ce pendant toute la durée de la communication établie) peut être réalisé de 2 manières :

- Statique : De manière statique, l'infrastructure (CUCM, Gatekeeper H323, SBC ou passerelle) peut limiter les appels voix et vidéo entre sites.
  Le CUCM offre cette possibilité de manière globale pour tous les appels voix et vidéo sur le

réseau :

- Terminaux enregistrés sur le CUCM
- Terminaux de Visioconférence
- Passerelles Voix ou Vidéo sur IP
- Ressources média localisées sur le réseau

- Dynamique : Le CUCM avec l'aide des routeurs ISR répartis sur les différents sites propose également un mécanisme de CAC dynamique. Dans cette approche le CUCM utilise un agent RSVP embarqué dans le routeur ISR d'un site d'agence qui génère, à sa demande et à l'établissement de l'appel une requête RSVP. L'intérêt d'un tel mécanisme est d'avoir une visibilité en temps réel de la bande passante disponible sur un lien et non une vision statique. Le reste du réseau doit respecter l'engagement « statique » de Qos.

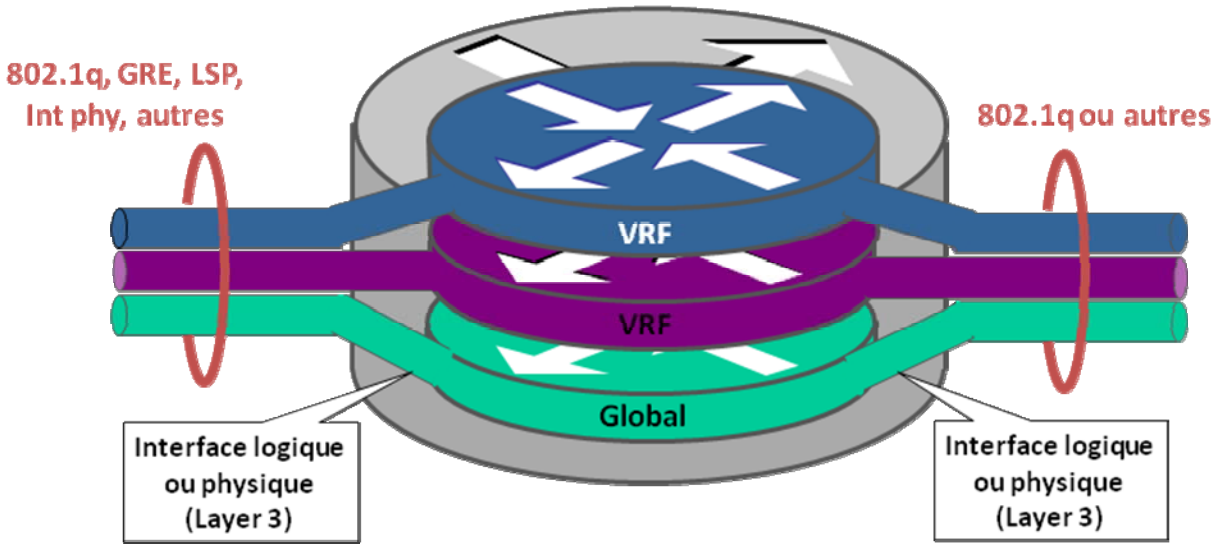
Que ce soit pour une gestion du CAC statique ou dynamique, l'intelligence du CUCM lui permet de choisir un chemin alternatif (comme l'utilisation du réseau RTC) pour assurer l'acheminement de l'appel en cas de congestion sur un lien.

Il est important de vérifier que tous les équipements traversés implémentent la QoS demandée. Il faut par exemple que les pare-feux traversés respectent les engagements demandés en termes de QoS.

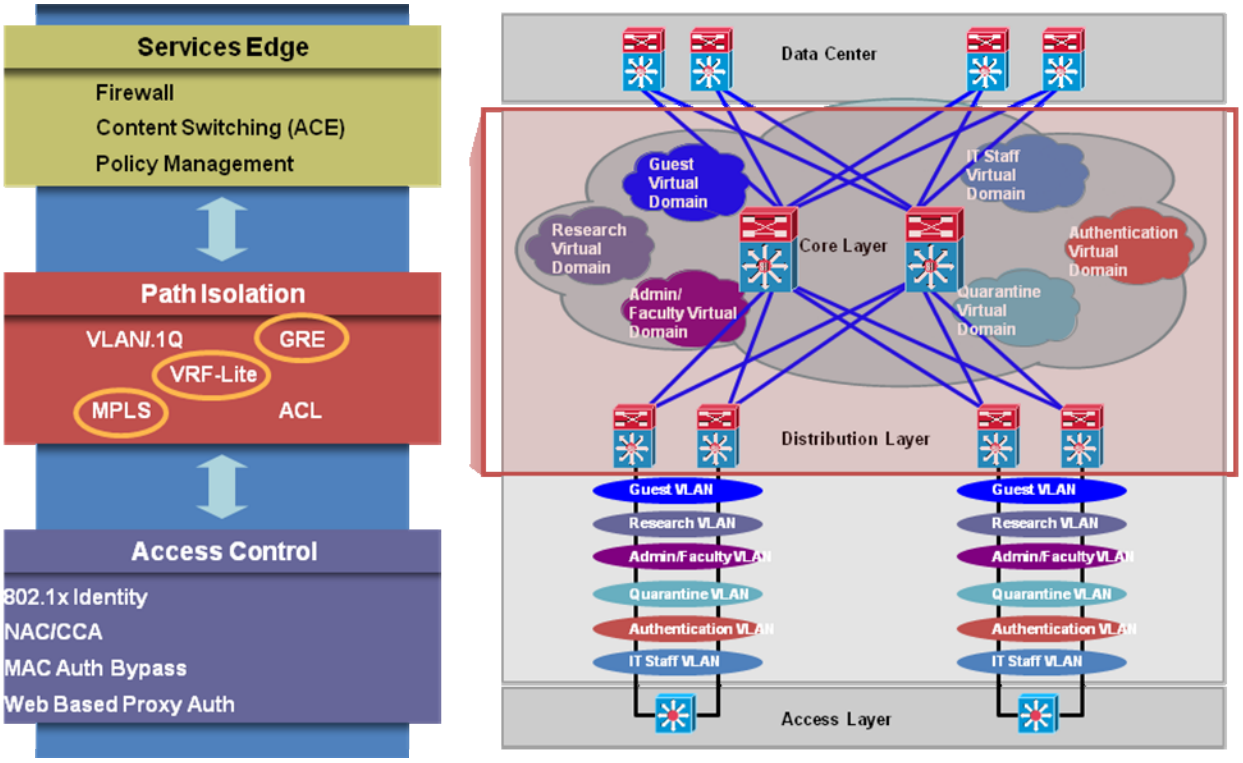
La segmentation et la virtualisation

Le service de segmentation et virtualisation a commencé dés les premiers déploiements de ToIP grâce à la notion de VLAN voix séparé.
Il s'étend aujourd'hui au delà du domaine Ethernet afin de prolonger cette segmentation du réseau dans tout ou partie de l'entreprise.

La notion de VRF présente sur les équipements de type routeur ou commutateur permet de conserver l'étanchéité du flux voix en traversant une infrastructure de niveau 3. Ainsi étendu, le nombre de points de passage entre les domaines voix et data peut être réduit afin notamment de mutualiser les équipements permettant de gérer la sécurité notamment des routeurs filtrants, des pare-feu ou sondes IPS/IDS.

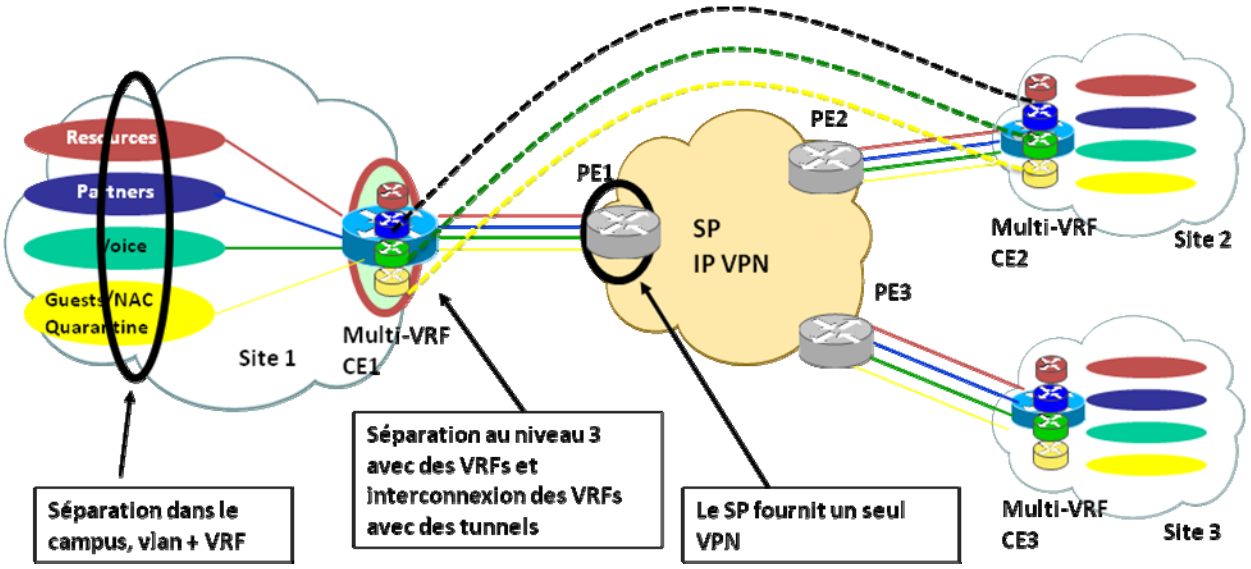


Ainsi une même infrastructure véhicule de manière étanche les flux par profil ou par type dans l'entreprise.



Plusieurs technologies permettent d'étendre cette segmentation au dela du réseau local pour par exemple la conserver entre sites distants et le site principal.

- Utilisation des VRFs de bout en bout par un mécanisme de type VRF-Lite (utilisation d'un VLAN par VRF et par lien routé)
- Aboutement des VRFs sur différents VPN/MPLS privés ou opérateurs
- Aboutement des VRFs sur tunnels GRE ou mGREs

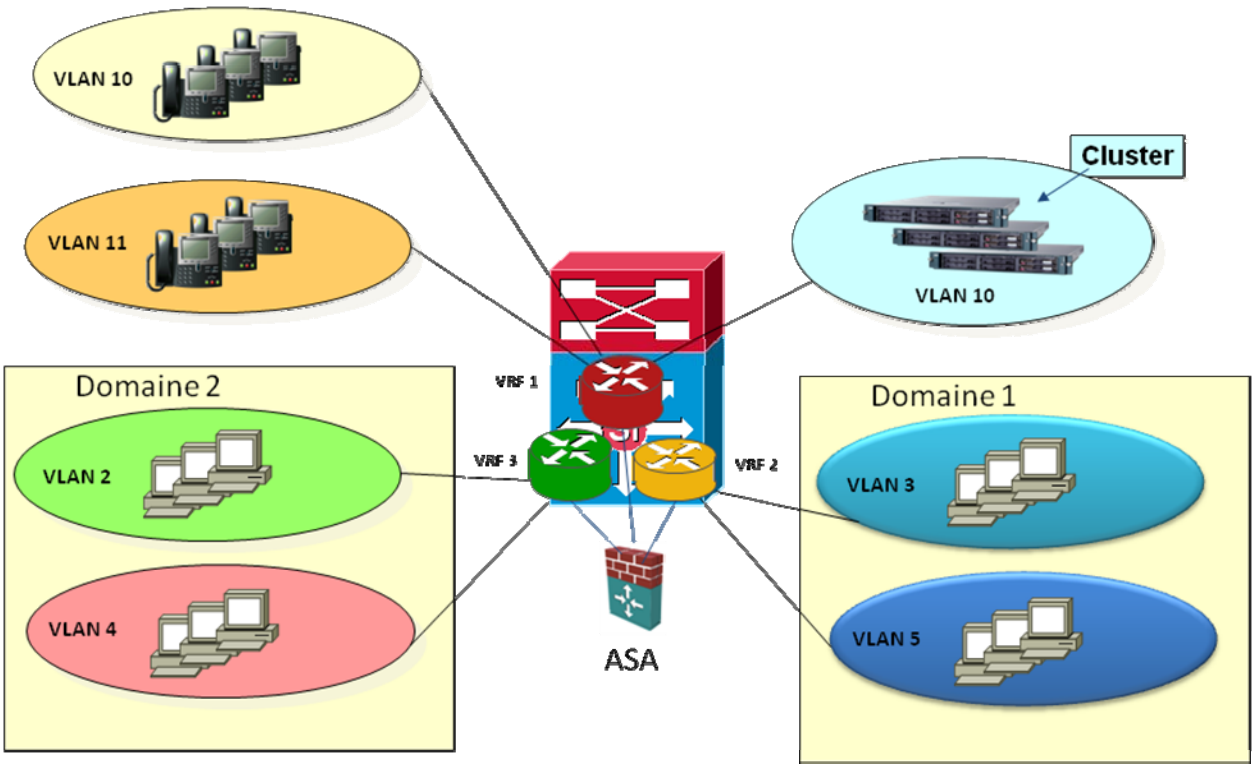


Entre ces différents domaines (sur base de simples VLANs ou de VRFs), plusieurs solutions sont offertes pour assurer la sécurité et gérer les différents flux présents entre les zones fonctionnelles :

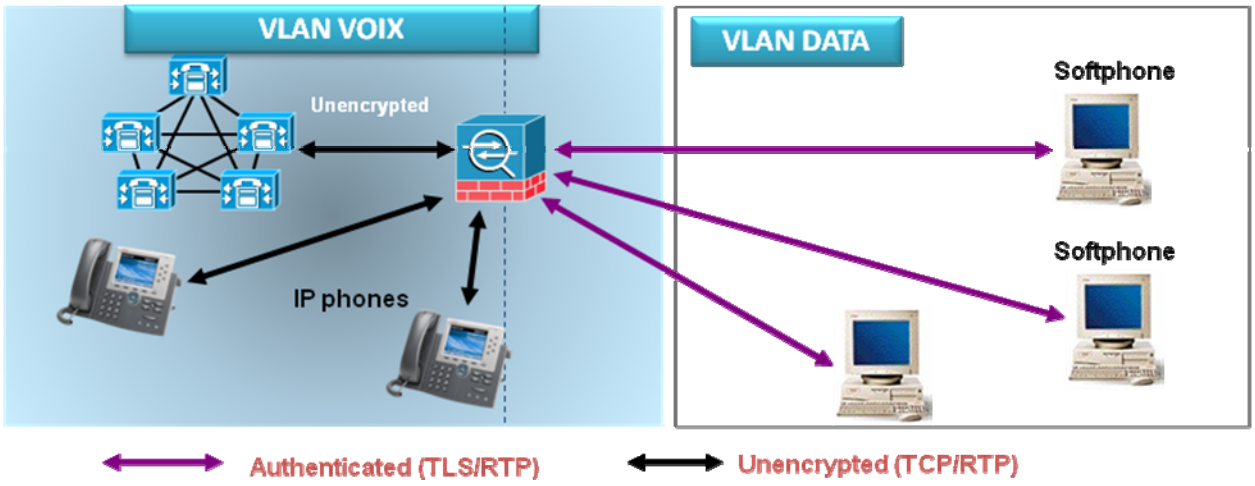
	Services d'appels	Passerelles	Applications tierces	Supervision	Vlans voix	Data users
Services d'appels	Informix (intra-cluster), H323, SIP (inter-clusters)	MGCP, H323	CTI, SIP, SCCP	SNMP, HTTPS, SCP, SFTP, SSH	SCCP, SIP, TFTP	SCCP, SIP, CTI-QBE, JTAPI, etc ….
Passerelles	MGCP, H323	RTP, SRTP, SIP	Dépend des applications	SSH, SCP, HTTPS	RTP, SRTP	
Applications tierces	CTI, SIP, SCCP	Dépend des applications	Dépend des applications	SNMP, HTTPS, SCP, SFTP, SSH	DHCP, HTTP, DNS	Dépend des applications
Supervision	SNMP, HTTPS, SCP, SFTP, SSH	SSH, SCP, HTTPS	SNMP, HTTPS, SCP, SFTP, SSH	X	HTTP, ICMP	X
Vlans voix	SCCP, SIP, TFTP	RTP, SRTP	DHCP, HTTP, DNS	HTTP, ICMP	RTP, SRTP	RTP, SRTP
Data users	SCCP, SIP, CTI-QBE, JTAPI, etc …	RTP, SRTP	Dépend des applications	X	RTP, SRTP	RTP, SRTP

- Routage IP avec fonction de filtrage par ACL sur équipement dédié ou mutualisé. Les ACLs sont traitées en hardware par nos équipements pour ne pas impacter les performances.

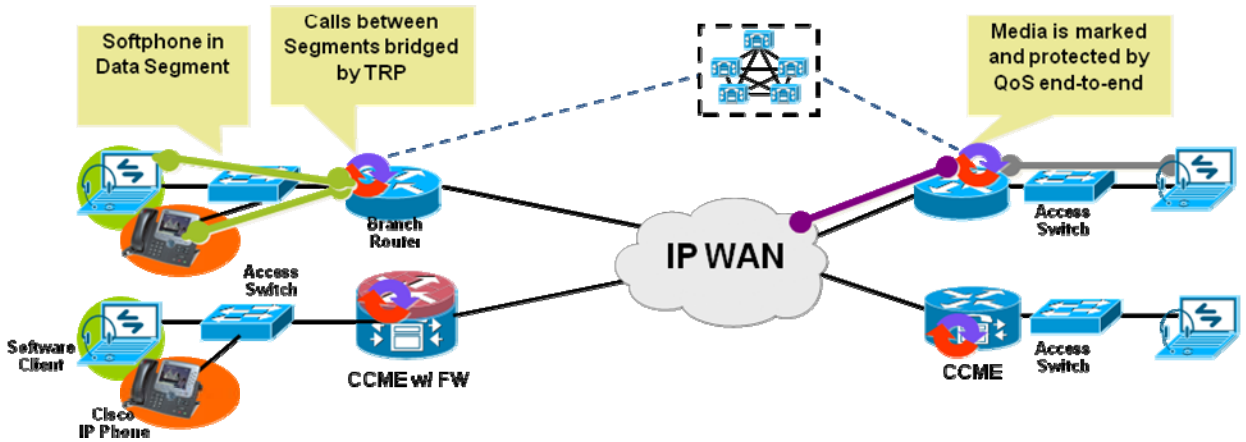
- Fonction de pare-feu avec inspection applicative permettant à la fois une analyse protocolaire fine (signalisation : SIP, H323, SCCP, CTI : CTI QBE, http, etc.) ainsi qu'une ouverture et fermeture dynamique des ports RTP en fonction des communications. Ces fonctions de pare-feu peuvent être présentes dans les commutateurs de type Catalyst 6500 par l'ajout de carte de services (FWSM – Firewall Service Module) ou de manière autonome par un ASA.



- La fonction de Phone Proxy permet d'isoler (sans activer de routage) les segments voix et data dans l'entreprise. Que ce soit pour rebondir d'un VLAN data à un VLAN voix ou bien d'une VRF data à une VRF voix, le module logiciel Phone Proxy dans l'ASA apporte un relai complet des différents flux (configuration, signalisation et média). Pouvant être utilisé entre une zone de défiance (Zone Guest par exemple) ou entre le segment voix et data de l'entreprise, le Phone Proxy apporte outre cette étanchéité complète, l'analyse protocolaire des flux le traversant.



- La fonction d'IOS TRP (Trusted Relay Point) permet au CUCM de terminer les flux Média (voix et vidéo) sur un routeur ISR de manière transparente plutôt que de les faire transiter nativement entre les équipements. Cette fonction permet de grandement simplifier la sécurité entre les segments voix et data sur le réseau puisque seul l'équipement ISR choisi doit être autorisé à transiter entre ces deux segments. L'intelligence du CUCM permet de choisir le meilleur ISR pour réaliser ce service en fonction de la charge, la disponibilité et la localisation des clients.



Les services voix par la mutualisation de l'infrastructure

L'approche Cisco a toujours été de pouvoir mutualiser l'investissement en proposant des plateformes multiservices qui en plus de leurs fonctionnalités « data » apportent leur lot de fonctionnalités « communications unifiées ».

Le principal exemple est la plateforme ISR « Integrated Services Router ».

Les services de l'ISR

Cette plateforme apporte en complément des fonctions de routage multi-protocolaire les services suivants qui sont tous mutualisables sur la même plateforme :

- Adjonction de fonctions de pare-feu basées sur IOS Firewall et fonctions d'IDS/IPS avec une analyse protocolaire des protocoles orientés « Communications unifiées ». Ceci permet par exemple de distribuer les fonctions de pare-feu et IPS sur chaque routeur d'agence pour mieux protéger le réseau ou sur le routeur utilisé comme passerelle voix/vidéo TDM pour renforcer sa propre sécurité.

- Adjonction des modules « cartes voix/vidéo » (analogiques et numériques) permettant d'apporter la fonction de passerelle voix/vidéo TDM au routeur. Les liens T2 peuvent aujourd'hui être mutualisés pour un usage voix/vidéo grâce aux routeurs ISR. Tous les protocoles de signalisation TDM normalisés sont nativement supportés notamment Q931, QSIG, etc.

- Ajout de DSP répartis sur l'infrastructure qui permettent dans tous les codecs supportés par l'infrastructure Cisco :

    - De terminer les flux voix/vidéo TDM,
    - D'apporter des ressources de conférence voix,
    - D'apporter des ressources de transcoding (changement de codec audio à la volée) ou d'adaptation du média (Adaptation DTMF notamment).

- Fonctions de SBC (Session Border Controler) SIP et H323 en « Back to Back User Agent » pour relier l'infrastructure à une offre de type Trunk SIP opérateur (pour réaliser de la collecte IP opérateur) ou pour réaliser une interconnexion B-to-B voix/vidéo avec des partenaires de l'entreprise.

Les modules applicatifs dans l'ISR

Ou encore par l'ajout de modules applicatifs :

- Le module CUE (Cisco Unity Express) permet d'apporter des fonctions de messagerie vocale et intégrée de manière répartie. En réseau, ces messageries peuvent offrir une alternative à une centralisation complète.
- Le module UMG (Cisco Unified Messaging Gateway) permet d'interconnecter plusieurs systèmes de messagerie entre eux pour les mettre en réseau grâce au protocole VPIM.
- Le module CUSP (Cisco Unified SIP Proxy) permet d'offrir une fonction de proxy SIP entre composants SIP pour assurer un routage intelligent ou des fonctions de haute disponibilité et de répartition de charge.
- Le module AXP permet de faire bénéficier de l'infrastructure à des applications de l'écosystème. Sous la forme d'une carte de services embarquée dans les ISR, cela permet à moindre cout de déployer de manière distribuée des services d'infrastructure. Les premiers services disponibles aujourd'hui sont :
    - Reconnaissance/synthèse vocale
    - Serveur d'enregistrement
    - Serveur de fax

- D'autres modules sont également disponibles notamment « controler WiFi », module d'optimisation applicative Waas, de diffusion de contenu ACNS, etc. Ceux-ci apportent des services permettant de simplifier le déploiement ou de libérer de la bande passante de type data pour le projet de communications unifiées.

Les services intelligents dans l'ISR

Enfin, des services vocaux peuvent être rendus localement par les ISRs.

- Les fonctions de terminaison de flux vocaux et d'exécution de scripts permettent de gérer une partie des appels entrants en terminant l'appel dans la passerelle. Ainsi le flux RTP n'est pas véhiculé sur un serveur central. Ce script peut être développé en TCL et donc local à l'équipement ou bien être exécuté sur ordres reçus d'un serveur vocal interactif en Voice XML.
- Des services de type « Self-Care », pré-décroché, accueil automatique peuvent être réalisés par ce biais.
- Un service de traitement des appels est également disponible dans les ISRs. Soit dans un mode autonome nommé CUCME (Cisco Unified Communication Manager Express) soit dans un mode de secours nommé SRST (Survivable Remote Site Telephony), l'ISR permet en fonction des architectures de proposer une solution offrant des fonctionnalités téléphoniques et de la haute disponibilité rendant transparent la perte du WAN. Par exemple, une communication téléphonique en cours vers le RTC ne sera pas coupée lors de la perte du WAN.
- L'ISR apporte également des fonctions de MoH Multicast localement si le WAN ne permet pas de véhiculer les flux de MoH depuis les serveurs CUCM (Cisco Unified Communication Managers).

Le routeur ISR est en relation avec les serveurs CUCM (Cisco Unified Communication Managers) qui permet de coupler des fonctions locales avec l'intelligence centralisée de ce dernier.
L'alliance des deux permet notamment de gérer un plan de numérotation centralisée et un routage d'appels intelligents avec sorties locales possibles, tout en gérant la haute disponibilité de la solution.
Le CUCM permet également, en relation avec les ISRs, de localiser les meilleures ressources pour les utilisateurs (conférence, transcoding, etc.).

Les plateformes ISR peuvent recevoir une alimentation secourue et sont connectables au réseau en double attachement.

Leur aspect multiservices permet une flexibilité dans leur utilisation et dans l'évolution de leur utilisation. Il est en effet possible de mutualiser les services rendus sur le même équipement mais aussi de migrer une passerelle VoIP TDM en la transformant en SBC (Session Border Controller) SIP pour accompagner l'évolution des choix télécoms des clients.

L'infrastructure Wireless Lan pour la mobilité des UC

Architectures et infrastructure

L'architecture WiFi doit fournir un certain nombre de services afin de pouvoir véhiculer des flux voix et vidéo sur le réseau de communications unifiées.

Basé sur 802.11e, la qualité de service ainsi que le contrôle d'admission est disponible. WMM et ses 4 files d'attentes sont disponibles dans les AP et un mécanisme de contrôle d'admission permet de limiter le nombre d'appels par AP pour en assurer la qualité (TSPEC). Cette qualité de services vient prolonger celles du LAN et du WAN abordés auparavant.
De plus la fonction « Auto Power Save Delivery » permet notamment de réduire la consommation électrique des clients et donc de maximiser les temps en veille et en communication.

Nous apportons également une solution de « Fast Secure Roaming » en attendant l'intégration de 802.11r Fast Secure Roaming à une norme dite « voice enterprise » de la WiFi Alliance.

L'infrastructure WiFi Cisco propose également une approche centralisée basée sur des contrôleurs facilitant le déploiement et l'administration d'une telle solution pour des sites locaux et distants.

A cette approche centralisée vient s'ajouter la possibilité d'utiliser H-Reap qui apporte notamment la possibilité de sortir localement pour certains WLANs tels que ceux utilisés par les téléphones pour éviter que les flux de VoIP locaux à un site ne remontent jusqu'aux contrôleurs quelques fois centralisés.
Cette souplesse d'architecture permet également un secours local des services de téléphonie par le service SRST du routeur ISR lorsque le WAN est indisponible.

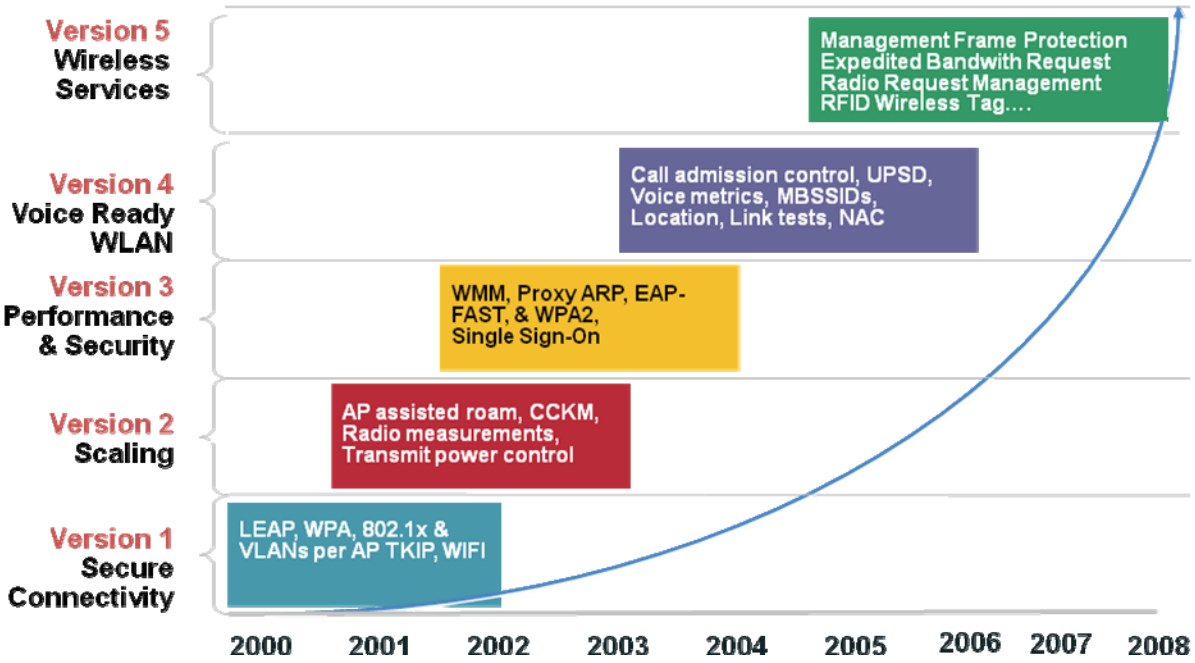
L'infrastructure Wireless LAN Cisco propose maintenant le support de la VoIP sur réseau WiFi Mesh Indoor. Ceci permet de bénéficier d'une infrastructure WiFi Mesh dans un bâtiment (hangar ou grands hall d'accueil notamment sans Ethernet Filaire), de pouvoir utiliser le même réseau mutualisé pour apporter des services de communications unifiées en complément des services natifs de type : accès invités, WLAN Data, et services métiers.

Enfin la qualité de la radio Cisco et notamment la mise à disposition du 802.11n (grâce à MIMO) permet d'améliorer la couverture radio. L'intégration des radios 2.4Ghz et 5Ghz permet aux terminaux de choisir la meilleure bande de fréquence.

Cisco met à disposition gratuitement un guide de design et de déploiement de Voix sur WiFi permettant de simplifier l'implémentation d'un tel réseau.

Terminaux

Cisco propose une classification des terminaux nommée CCX (Cisco Compatible Extention) permettant de lister les pré-requis (notamment dans ses versions 4 et 5) que les terminaux doivent respecter afin d'offrir un service de qualité pour les communications unifiées ainsi qu'une meilleure prédictibilité du déploiement d'un tel service.



Administration

WCS (Wireless Control System) est l'outil de gestion des services de mobilité d'entreprise.

Sa fonction « Planning Tools » permet de déterminer un positionnement théorique des points d'accès pour un service de type VoIP en fonction du site, des points d'accès choisis.

« Voice Readiness », quand à lui, a pour objectif de vérifier sur réseau existant, le déploiement d'un

service de voix sur WiFi au niveau radio.

« VoWLAN Configuration Audit » a pour objectif de vérifier la conformité de configuration des contrôleurs et points d'accès au déploiement d'un service voix (802.11e, 802.11i, CCKM, etc.).

De plus, afin d'assurer une meilleure couverture radio, les services de Radio Ressource Management vérifient en temps réel l'environnement radio. Ainsi sur disparition, ajout d'un AP ou évolution de l'environnement physique, les radios (fréquence, puissance, etc.) des APs seront automatiquement ajustées. Toute impossibilité de fournir un service sans « zone noire », sera immédiatement remontée à l'administrateur.

Voice Reports et Voice Metrics permettent aux terminaux CCX de remonter des informations à WCS afin de compléter la vue de l'infrastructure par des données clients (puissance du signal, rapport signal sur bruit, utilisation du canal, etc.).

La fonction de « Client Troubleshooting » permet à distance à l'administrateur de pouvoir analyser les causes d'une défaillance pour un terminal (problème radio, d'association, d'authentification, de DHCP) afin de réduire le délai d'indisponibilité de l'accès au service. Cette fonctionnalité est très appréciée couplée au service de géo-localisation des terminaux.

Services

Le WCS permet de localiser en « temps réel » les terminaux au sein des contrôleurs et d'en publier la localisation sur une cartographie à des fins d'administration.

Couplée à la MSE (Mobility Service Engine), le réseau WiFi devient partie intégrante du métier du client afin de fournir aux travers de ces APIs une géo-localisation et un historique complet des positions afin de déclencher ces évènements sur entrée dans une zone, sortie de zone. En complément cette information peut être exploitée au travers d'un serveur vocale interactif ou d'une application métier afin de trouver rapidement l'équipement ou la personne associée.

La MSE grace au module MIR (Mobile Intelligent Roaming) fournit également un service qui permet aux terminaux de prendre des décisions de roaming d'un appel voix sur WiFi vers GSM sur sortie de zone (passage par l'accueil de l'entreprise).

L'intégralité de ces services permet aujourd'hui de réels déploiements sur une infrastructure convergente pour des services de WLANs data, voix sur WiFi, diffusion vidéo et d'accès invités.

La sécurité

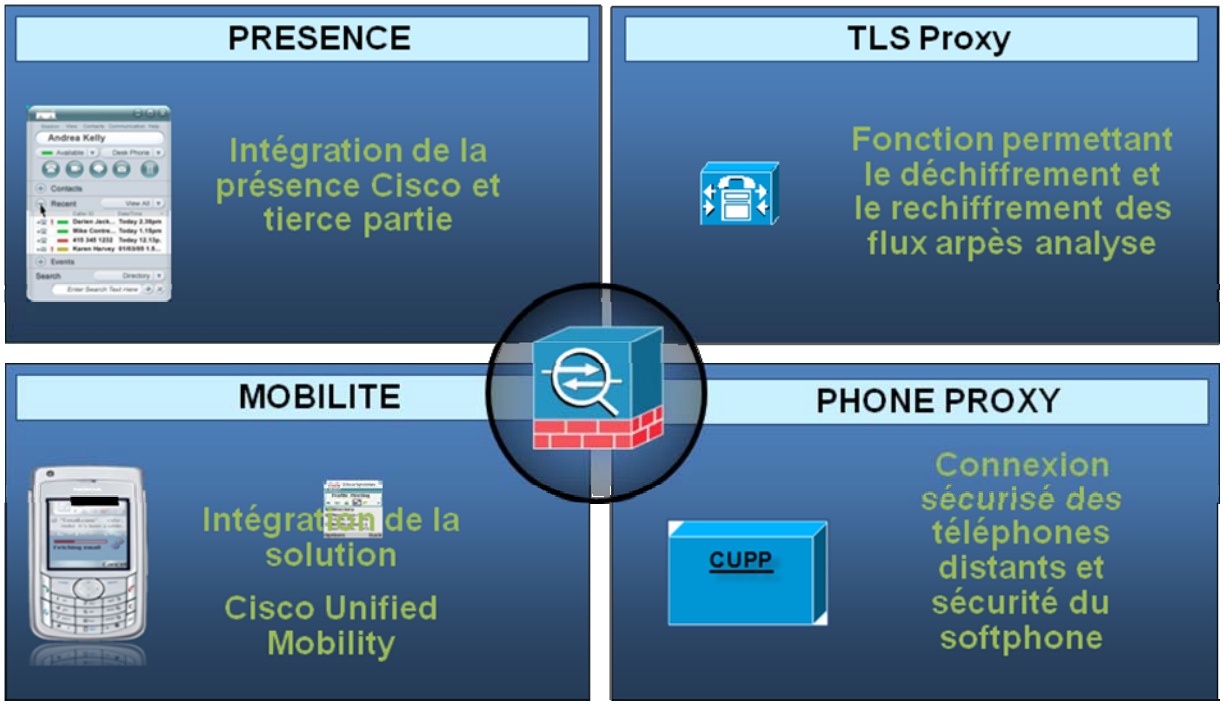
L'approche de la sécurité Cisco pour les communications unifiées est globale.
Dans les terminaux, les serveurs de communication, les serveurs applicatifs, ainsi que les éléments d'infrastructure.
Nous traiterons ici uniquement les services offerts par l'infrastructure. La vision globale de cette sécurité est traitée dans divers précédents articles de Ciscomag.

Nous y avons expliqué l'usage :

- Des fonctions de sécurité dans les commutateurs d'accès à savoir : RACL, VCAL, PACL, CoPP, URPF, Port Security, IP Source Guard, Rate Limiting, etc.
- Des fonctions de segmentation par VLAN, VRF avec point de passage entre segments. Les services ici rendus (Filtrage, IPS, peuvent être apportés par les Cisco ASA, cartes FWSM dans Catalyst 6500 ou IOS TRP dans ISR,
- Des fonctions dans les routeurs ISR permettant d'assurer des services de pare-feu et d'IPS quelque soit les fonctions implémentées dans le routeur.

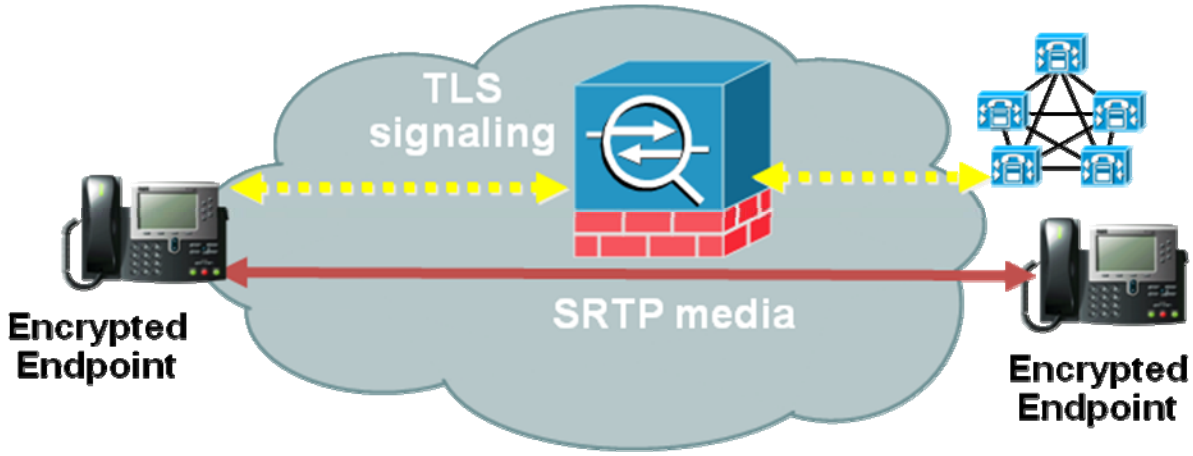
Les services complémentaires de l'ASA

Nous proposons ici 4 services de type proxy sur l'ASA



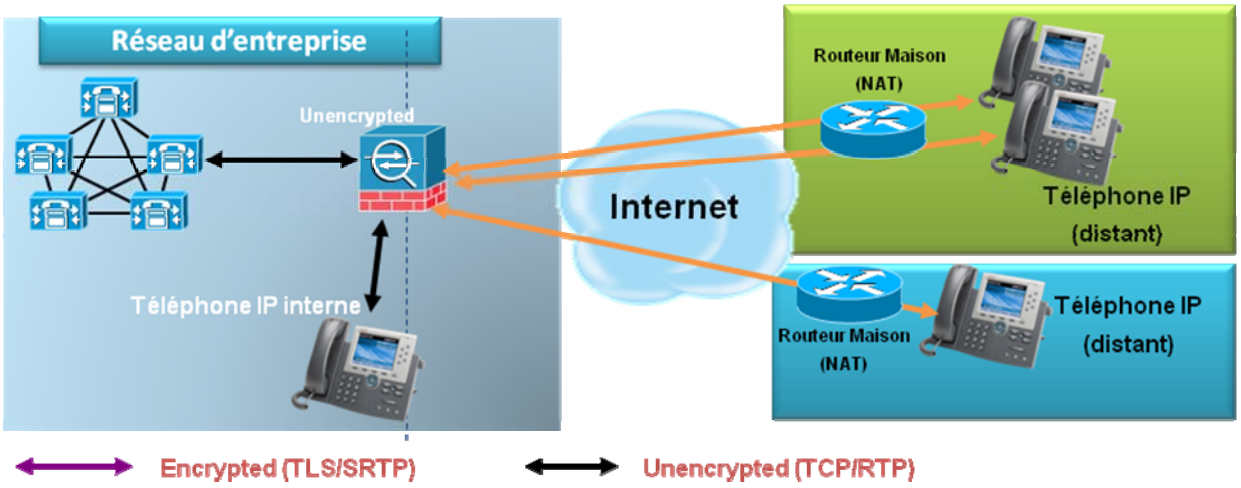
La plateforme multiservices de sécurité de Cisco nommée ASA offre, outre les fonctions historiques d'inspection applicative de tous les flux de communications unifiées (de signalisation à savoir SIP, H323, SCCP, - d'intégration applicative à savoir TAPI ou JTAPI – et de flux média RTP) 4 services modules Proxy dédiés aux communications unifiées Cisco. L'ASA conserve bien sûr toutes les offres fonctions qu'on lui connait.

- TLS Proxy : Lorsque la sécurité par le chiffrement et l'authentification de la signalisation a été activée sur l'infrastructure, cette fonction permet de la déchiffrer et de la chiffrer de nouveau à la volée et ce de manière transparente pour les utilisateurs. Ceci permet de continuer l'inspection applicative de conformité des protocoles et de pouvoir ouvrir dynamiquement les ports RTP ou SRTP. Grace à cette intégration avec le CUCM, la mise en place du chiffrement n'impacte pas la politique de sécurité de l'entreprise.

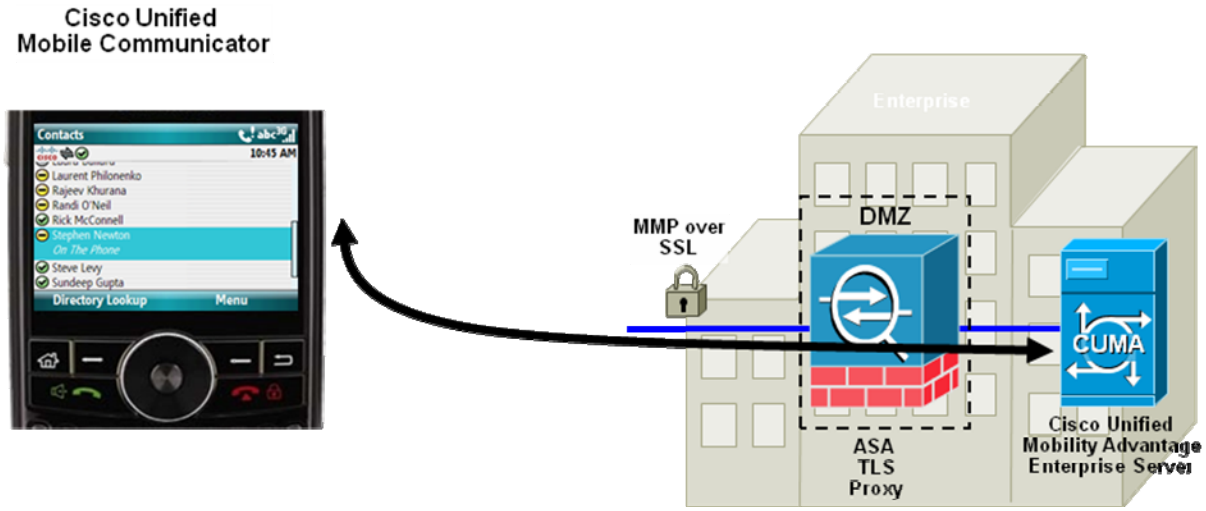


- Phone Proxy : Le module Phone proxy permet de déployer des téléphones IP ou téléphones logiciels dans un zone non sécurisée comme Internet ou une zone de défiance dans l'entreprise (VLAN Guest par exemple). Tous les flux de signalisation, média et de services

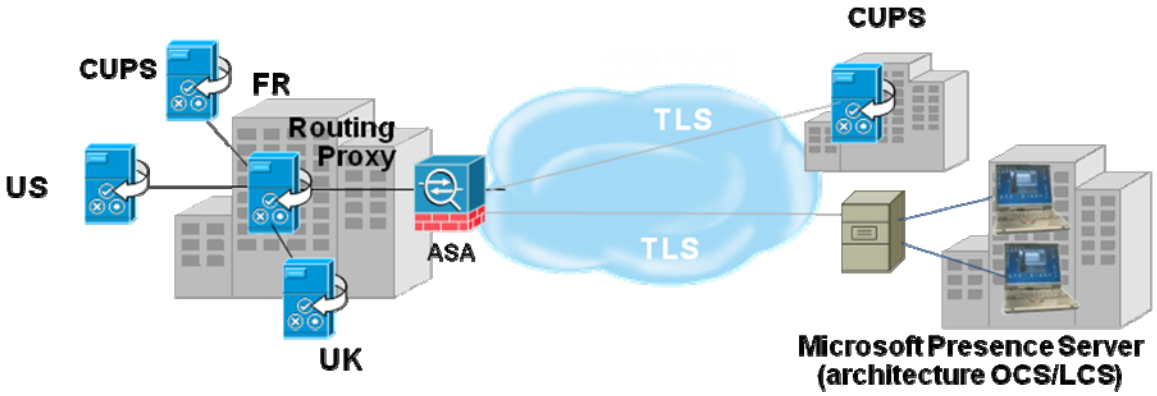
XML sont interceptés par l'ASA qui les analyse et les relaie de manière sécurisée. Il est à noter que cette implémentation peut être réalisée sur un cluster de CUCM sur lequel le chiffrement n'est pas activé.



- Mobility Proxy : Les flux des terminaux mobiles utilisant le CUMC (Cisco Unified Mobile Communicator) se terminent sur l'ASA en DMZ avant d'être relayés sur le serveur applicatif CUMA (Cisco Unified Mobility Advantage). Les flux sont déchiffrés par l'ASA, une inspection applicative des différents messages XML est réalisée puis les flux sont de nouveaux chiffrés pour être transférés au serveur CUMA.



- Presence Federation Proxy : La fédération de présence (présence et messagerie instantanée) entre entreprises se développe. Les flux SIP/SIMPLE du CUP (Cisco Unified Presence Server) sont agrégés sur l'ASA en périphérie de l'entreprise (DMZ) pour être déchiffrés et analysés avant d'être de nouveau chiffrés et routés vers un système de collaboration distant.



Les outils de gestion

Les outils d'administration proposés par Cisco tirent partie de la connaissance de l'infrastructure et des applications ainsi que d'un certain nombre de fonctions disponibles dans les différents équipements de l'infrastructure.

Les routeurs ou commutateurs Cisco proposent, de manière embarquée, la fonction « IP SLA » très facilement activable permettant de générer du flux synthétique de différents types afin de collecter des informations sur la qualité du réseau (temps de transit, gigue, perte de paquets, ...) et temps de réponse applicative. Ces flux peuvent par exemple être de type : RTP voix ou vidéo, session TCP, requête DNS, requête http, ...

Les fonctions de type « duplication de trafic » plus connus sous les noms de SPAN/RSPAN/ERSPAN sur les commutateurs permettent de recopier le trafic intelligemment:

- Sur un même port d'un commutateur (fonction SPAN)
- Sur un VLAN à destination d'un autre commutateur du même domaine Ethernet (fonction RSPAN)
- Sur un tunnel à destination d'un commutateur distant au travers d'un réseau IP routé (particulièrement utile dans le cas d'un WAN).

Ces fonctions permettent par exemple de dupliquer un flux audio pour analyse qualitative, enregistrement ou écoute.

Les fonctions de type « NetFlow » présentes en standard dans nos équipements ou l'adjonction de cartes de type « NAM » ou encore de sondes externes vont permettre de suivre l'évolution du trafic sur le réseau et ainsi d'assurer une prédictibilité dans le niveau de services rendu.

Les authentifications ainsi que les modifications de configuration sont centralisées sur une plateforme de type serveur Radius/Tacas de type Cisco ACS couplée à l'annuaire d'entreprise. Ce même serveur ACS est utilisé pour gérer de manière globale l'identité (administrateur, utilisateurs, terminaux et posture des postes de travail informatique).

CDP ou LLDP-MED est également disponible pour assurer un service de localisation physique des téléphones filaires dans l'infrastructure à des fins d'inventaire ou de maintenance ou à des fins de sécurité. Ceci en complément de la géo-localisation WiFi.

EEM « Embedded Event Manager » présent sur la plupart de nos plateformes peut être utilisé pour faciliter l'administration d'un réseau supportant des flux de communications unifiées.
Il va permettre par exemple :

- réagir à des évènements particuliers de type (connexion/déconnexion d'un Téléphone) pour alerter l'administrateur ou exécuter une série de commandes sur l'équipement.
- être utilisé comme automate de configuration ou reconfiguration de l'équipement à heure définie. Il est par exemple possible de couper l'alimentation 802.3af des téléphones la nuit de manière automatique par EEM.
- superviser l'équipement et d'alerter l'administrateur en cas de changement (défaillance matérielle ou logicielle, événement externe, ...).

Des fonctions de « macro » et d'automatisation de certaines fonctions dans les équipements de type « Auto QoS » permettent de simplifier le déploiement et permettent à l'équipement d'appliquer dynamiquement une configuration prédéfinie par port à la connexion d'un téléphone.

Des fonctions de type « Automated System Configuration Check » permettent de vérifier la conformité des configurations dans les équipements et ainsi de détecter des problèmes impactant la disponibilité ou la sécurité de la solution.

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_12/08