27 décembre 2007

CiscoMag
Votre rendez-vous mensuel avec Cisco France
numéro 13

Comment Cisco a mis en place un réseau WAN à haute disponibilité

Résumé

Cette étude de cas décrit comment l'équipe Cisco IT a réussi à mettre en œuvre en 2003 une haute disponibilité du réseau et a réduit en conséquence les coûts opérationnels. Les facteurs clés du succès :

- Conception réseau – conception tournée vers une architecture homogène
- Opérations réseau – des processus homogènes de changement et de mises à jour
- Gestion du réseau – modèles de configuration et gestion proactive des incidents et de la performance
- Support réseau – formation, équipement de rechange et gestion des incidents
- Infrastructures réseau – Standardisation des plateformes

En se concentrant sur ces domaines, l'équipe CAPNet a grandement amélioré la disponibilité à 99.999% tout en réduisant le nombre de personnes affectées à son support, mises sur des projets à plus forte valeur ajoutée.

Note : cet article fait souvent référence à des équipements datant de 2003 donc, pour certains, entrés en phase d'obsolescence à ce jour.

Le réseau CAPNET

Le réseau Cisco 100% paquet (Cisco All-Packet Network ou CAPNet) est un réseau backbone mondial qui dessert des dizaines de milliers d'employés et de sous-traitants de Cisco à 15 endroits sur quatre continents (figure 1).

« CAPNet représente le cœur de l'infrastructure de communication convergente mondiale de Cisco, transportant de la voix, de la vidéo et des données pour les employés Cisco entre des centaines de sites Cisco et de sites partenaires dans le monde entier. La disponibilité de ce réseau est d'une importance capitale pour soutenir l'activité commerciale de Cisco » explique Lance Perry, Vice Président, Infrastructures Mondiales IT.

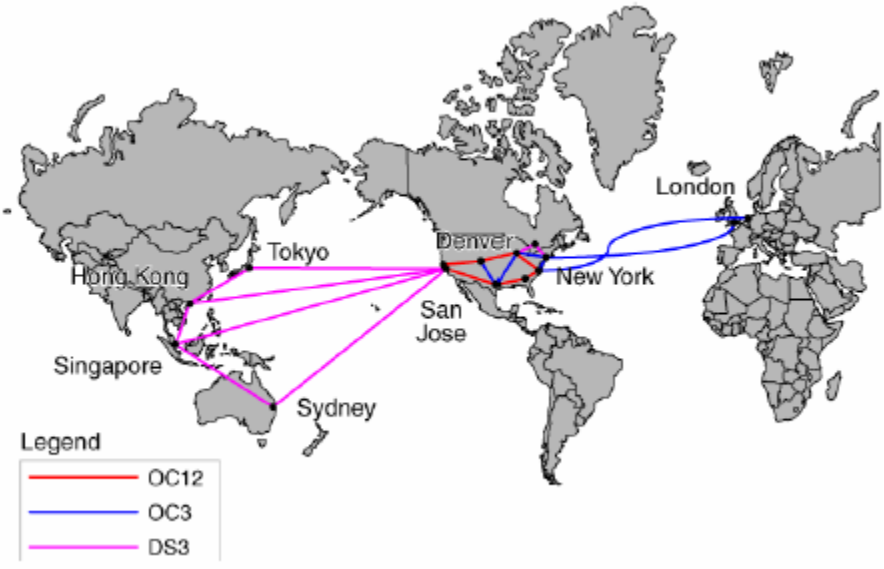

Figure 1. Le réseau CAPNet mondial

Les employés et sous-traitants de Cisco font confiance à CAPNet pour leurs applications métiers critiques quotidiennes, les communications entre bureaux et la connectivité à Internet dans les locaux de Cisco dans le monde entier. Etant donné que CAPNet est le backbone du réseau mondial de Cisco, même une brève interruption peut perturber l'activité de milliers d'employés. Par conséquent une haute disponibilité est une priorité pour l'équipe CAPNet.

Des circuits Gigabit Ethernet, OC12, OC3 et DS3 connectent les sites Cisco dans la plupart des villes en Europe, Amérique du Nord, Asie et Australie. Chaque site dispose d'au moins deux circuits routés différemment sur du matériel redondant pour maximiser la tolérance de panne. La bande passante CAPNet varie de 45 à quelques Gigabits en fonction du lieu.

Comment est exprimée la haute disponibilité ?

La haute disponibilité est traditionnellement exprimée comme le nombre de « neufs » dans le pourcentage de disponibilité temporelle :

- 3 neufs (99.9 %) – 10 minutes d'indisponibilité par semaine
- 4 neufs (99.99 %) – 1 minute d'indisponibilité par semaine
- 5 neufs (99.999 %) – 6 secondes d'indisponibilité par semaine

Les applications métiers Cisco nécessitent un minimum de disponibilité de quatre « neufs » mais l'objectif pour CAPNet est cinq neufs ou mieux. De nombreux réseaux d'entreprise sont capables d'assurer cinq neufs, mais bien peu atteignent cette disponibilité sans une attention particulière à tous les facteurs qui contribuent à l'indisponibilité du réseau. Pour atteindre cinq neufs, les entreprises doivent valider et améliorer l'architecture du réseau, les opérations, le management et le support.

La récompense est immense : un réseau à haute disponibilité qui diminue les coûts opérationnels, améliore la productivité des employés, rationnalise les activités logistiques et fournit l'infrastructure nécessaire pour des applications telles que la visioconférence et les communications IP.

La route vers les cinq neufs

Le WAN Cisco s'est développé progressivement pour accompagner la croissance, les acquisitions et les progrès du réseau. Différents sites utilisaient différents équipements, différentes versions logicielles Cisco IOS et des configurations non standards. Les réseaux des sociétés achetées étaient

fusionnés avec CAPNet sans grande préparation et sans intégration. Les procédures opérationnelles et de support comportaient des lacunes qui augmentaient la durée des incidents. Tout ceci, entre autres, conduisait à des indisponibilités imprévues qui affectaient la disponibilité.

Dans le même temps, Cisco investissait massivement dans les communications sur IP (données, voix et vidéo) car les réseaux de données IP avaient atteint un tel point de maturité qu'ils pouvaient et devaient être aussi fiables que les réseaux téléphoniques. L'équipe CAPNet se rendit compte qu'il était temps de renforcer l'infrastructure sous-jacente pour garantir la qualité des communications IP.

Au début de l'effort pour la haute disponibilité, le niveau de service (SLA) était de 3 neufs (99.975 %) grâce à des technologies robustes telles que des routeurs et circuits redondants déployés dans l'infrastructure réseau. Le temps d'indisponibilité n'était en général pas le fait d'incidents matériels ou provenant des circuits. Des incidents imperceptibles ou intermittents tels que des problèmes de pertes momentanées de routes, des configurations d'équipements instables ou des lacunes dans les procédures de support en étaient en général responsables.

L'équipe CAPNet a mis à mal ces problèmes en plusieurs étapes. Tout d'abord elle établit des mesures fiables de disponibilité afin de pouvoir quantifier les progrès. Ensuite elle identifia l'architecture clé et les lacunes opérationnelles et procéda à des mises à jour de programmes. L'objectif initial était quatre neufs et elle l'atteignit en comblant les principales lacunes. L'objectif final était cinq neuf ou mieux, ce qui nécessita une attention particulière à tous les facteurs qui affectent la disponibilité du réseau.

C'est l'histoire d'un succès qui raconte comment l'équipe CAPNet a atteint des cibles de haute disponibilité et a réduit les coûts opérationnels, le tout dans un environnement réel d'un réseau global. Et l'équipe CAPNet l'a fait sans personnel supplémentaire ; l'équipe en place a planifié et mis en œuvre toutes les améliorations. En fait, comme la disponibilité s'améliorait, le support réseau était moins sollicité et l'équipe a eu plus de temps pour s'occuper d'autres programmes.

Comment mesurer la disponibilité de CAPNet ?

L'équipe CAPNet supervise la disponibilité en utilisant EMAN, un système interne de gestion de réseau. Ce système collecte en continu des données de disponibilité pour des nœuds CAPNet, calcule les pourcentages de disponibilité et présente les résultats.

EMAN affiche les données de disponibilité sous forme d'histogrammes qui montrent la performance de manière temporelle ou par site. Par exemple la figure 2 montre la disponibilité quotidienne de CAPNet pour le mois d'août 2003.

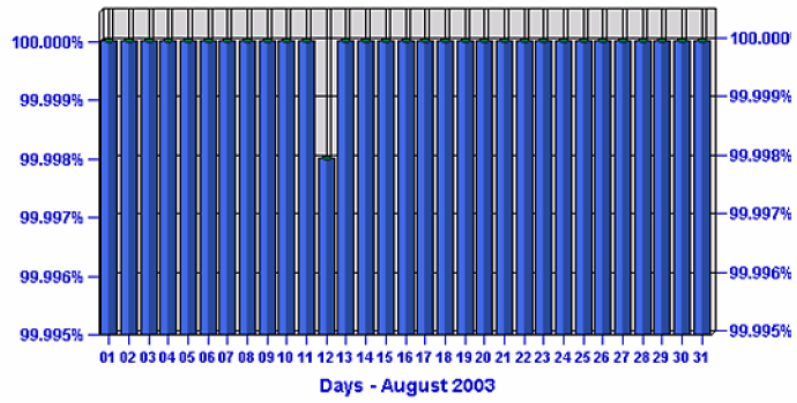

Figure 2 : Graphique de disponibilité pour le mois d'août 2003

Le système EMAN fournit au groupe CAPNet de bonnes mesures de disponibilité depuis le début mais l'équipe a amélioré la précision des mesures au cours du développement du programme. Le changement le plus important en termes de précision était la mesure de la disponibilité de l'hôte composite.

Pourquoi mesurer la disponibilité ?

L'équipe IT de Cisco utilise des mesures de disponibilité pour déterminer comment CAPNet se comporte afin d'aider à identifier les causes d'incidents spécifiques et, encore plus important, afin d'établir les tendances de disponibilité dans le temps. La disponibilité s'améliore-t-elle ? La disponibilité se dégrade-t-elle ? Ceci vous permet de quantifier vos progrès. Des mesures de disponibilité constantes dans le temps aident aussi l'équipe CAPNet à tracer les effets de modifications de matériel, de logiciels, de circuits, de topologie et de pratiques opérationnelles. CAPNet utilise aussi les mesures de disponibilité pour vérifier les niveaux de services pour les utilisateurs du système.

Comment mesure-t-on la disponibilité ?

CAPNet mesure la disponibilité en « pingant » chaque site CAPNet toutes les 15 secondes 24 heures par jour 7 jours par semaine. Si un « host » sur le site répond, le site est considéré comme disponible pour l'intervalle de temps. CAPNet mesure la disponibilité d'un site plutôt que celle d'un équipement individuel ou d'un lien, étant donné que la seule panne d'un équipement ou d'un lien n'isole pas un site. CAPNet supervise la disponibilité d'un équipement ou d'un lien mais ces mesures n'ont pas de conséquences sur les rapports de disponibilité de CAPNet.

Les hôtes composites

CAPNet mesure la disponibilité d'un site en utilisant des hôtes (hosts) composites qui sont une fonctionnalité d'EMAN qui groupe tous les routeurs ONE d'un site en un seul hôte logique. En testant la disponibilité de l'hôte composite, on détermine la disponibilité du site. EMAN considère aussi l'hôte composite comme un sous-groupe de disponibilité de telle sorte que vous puissiez voir les données de disponibilité du réseau par site.

Dans cet exemple, le matériel redondant et les connexions croisées rendent le site résistant à une panne d'un seul équipement ou lien. Etant donné que le trafic se re-route rapidement après une panne, un ou deux hôtes individuel(s) ou circuits WAN peuvent tomber en panne sans avoir de conséquences sur la disponibilité.

Les mesures de disponibilité ne testent pas directement d'autre équipement sur le site tel que des commutateurs régionaux ou des circuits de management hors bande.

Disponibilité agrégée

La disponibilité agrégée d'un réseau est la résultante des mesures de disponibilité pour tous les sites ou de sous-groupes de disponibilité dans le réseau mondial CAPNet. Chaque site a un sous-groupe de disponibilité et ce sous-groupe a un seul hôte composite. CAPNet contient 13 sous-groupes de disponibilité – un pour chaque nœud à l'extérieur de San José. Un collecteur de disponibilité EMAN situé à San José mesure la disponibilité dans le monde entier.

Le tableau 1 donne des exemples de disponibilité pour tous les sites CAPNet (sous-groupes de disponibilité) sur une période de 12 mois.

Sous-groupe de disponibilité	Disponibilité
Atlanta	99.998 %
Chicago	99.999 %

Dallas	99.999 %
Denver	100 %
EMEA	99.91 %
Honk-Kong	100 %
Kanata	99.99 %
New-York	99.999 %
RTP	99.999 %
Redwood city	100 %
Singapour	99.999 %
Sydney	99.998 %
Tokyo	100 %
Réseau entier	**99.9916 %**

Tableau 1 : disponibilité d'avril 2003 à mars 2004

La disponibilité du réseau entier est simplement la moyenne des disponibilités des sous-groupes. Un sous-groupe n'a pas plus d'importance qu'un autre.

Mesures de disponibilité

L'équipe CAPNet collecte des données brutes de disponibilité pour chaque nœud, circuit et équipement.

- Site de concentration

L'hôte composite est considéré comme disponible si au moins un des équipements du composite répond. C'est la mesure qu'utilise l'équipe CAPNet pour déterminer la disponibilité.

Les mesures de disponibilité de l'hôte ne font pas de différence entre les disponibilités brutes et ajustée. Etant donné que CAPNet est un service backbone, l'équipe CAPNet ne planifie jamais d'interruption qui interromprait le service.

- Circuit WAN (brute et ajustée pour maintenance planifiée)

Chaque circuit est supervisé pour connaître sa disponibilité en utilisant ICMP au niveau de l'adresse d'interface IP (hôte virtuel EMAN) à l'extrémité du circuit la plus éloignée du collecteur EMAN à San José. Les données aident à vérifier que les circuits WAN sont conformes à leurs SLAs.

Les circuits WAN sont caractérisés en général par une valeur de disponibilité ajustée, qui soustrait les temps de maintenance planifiée des temps d'indisponibilité. CAPNet minimise le risque d'interruptions mon planifiées en utilisant des équipements de rechange présents sur le site et un support sur site.

- Routeur WAN

Chaque équipement est supervisé pour connaitre sa disponibilité en analysant les enregistrements d'indisponibilité sur le journal par appel (voir section support réseau). Cette activité permet d'identifier les équipements qui sont trop souvent indisponibles.

Tests de disponibilité

Le collecteur EMAN envoie deux « pings » à l'adresse IP adéquate toutes les 15 secondes. Un équipement est considéré comme disponible pour un intervalle de 15 secondes s'il répond à au moins un des deux « pings » pendant l'intervalle. Par conséquent la disponibilité moyenne d'un équipement est égale au nombre d'intervalles correspondant à des « pings » positifs divisés par le nombre d'intervalles possibles de « pings ». Sur une journée de 24 heures, il y a 5760 intervalles de « pings », d'une durée de 15 secondes chacun.

La perte d'un intervalle de « ping » diminue la disponibilité à moins de quatre neufs (99.982 %) pour la journée. Le tableau 2 donne la correspondance entre la perte de « ping » et la disponibilité mensuelle.

Nombre d'intervalles de pings perdus	Indisponibilité mensuelle	Disponibilité
1.728	26.1 secondes	99.999 %
17.28	4.3 minutes	99.990 %
30*	7.5 minutes	99.982 %

Tableau 2 : conséquence de la perte de « ping » sur la disponibilité en 2003
**Un intervalle de « ping » perdu par jour*

L'interruption de service la plus longue théorique qui ne serait pas remarquée est inférieure à 15 secondes (interruption suivant immédiatement un intervalle de « ping » et s'arrêtant juste avant le prochain intervalle). En utilisant un intervalle de 15 secondes, on obtient un équilibre entre une supervision de trafic appropriée et une supervision de trafic intrusive.

Améliorations résultant des mesures de disponibilité

CAPNet s'était engagé à fournir une disponibilité de 99.99%, ce qui laisse une faible marge pour l'erreur. Un changement momentané dans le routage qui ne serait pas remarqué par l'utilisateur moyen peut conduite à une disponibilité non réussie que CAPNet ne peut pas accepter. Un système de mesures de disponibilité robuste est la pierre angulaire pour le programme de haute disponibilité de CAPNet.

En route vers les quatre neufs

Maintenant que l'équipe CAPNet a de bonnes mesures de disponibilité, elle est prête à conduire une évaluation stratégique de l'ensemble du réseau et des infrastructures opérationnelles. Cette évaluation identifie clairement les projets d'amélioration et attribue les priorités pour chacun. Pour cette phase du projet de disponibilité, les sujets suivants d'architecture et de standardisation ont été identifiés comme hautement prioritaires :

- Plan d'adressage IP pour une réduction des routes
- Matériel et logiciel standard
- Processus de gestion de configuration

Problème de réduction des routes

Le réseau WAN Cisco s'est développé progressivement pour accompagner la croissance, les acquisitions et les évolutions du réseau. Par conséquent, les adresses IP n'étaient pas groupées par région, les tables de routage étaient longues et la réduction des routes n'était pas réalisable. Une instabilité du réseau dans une région pouvait se propager sur une large zone ce qui réduisait la disponibilité.

L'équipe IT Cisco a choisi d'implémenter des réductions de routes car elles :

- Réduisent la taille des tables de routage. Par conséquent les ressources en mémoire et en CPU sont préservées
- Renforcent la hiérarchie des routes et limites les instabilités de routage à une zone de faible ampleur. Si une adresse dans une plage réduite change ou si l'état d'un lien change, ce changement n'est pas propagé en dehors de cette zone réduite

Pour implémenter la réduction des routes, l'équipe CAPNet et les groupes régionaux IT ont dû adopter un nouveau plan d'adressage IP pour l'ensemble du réseau. Ce nouveau plan a regroupé les adresses réseau par région de telle sorte qu'elles ont pu être réduites au niveau de l'interface WAN. La figure 4 montre le réseau CAPNet aux USA et les réductions d'adresses pour les zones sélectionnées.

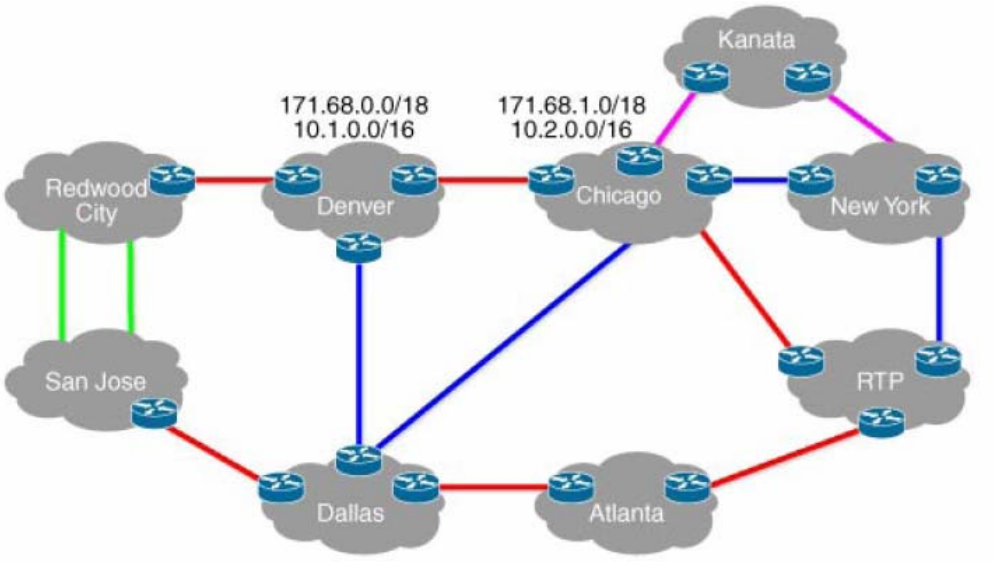

Figure 4.

De nombreux sites propagent uniquement deux adresses : une pour l'administration du site et les téléphones IP et une autre pour le routage Internet. Par exemple, le site de Denver a deux adresses :

- 171.68.0.0/18 – adresses de 171.68.0.0 à 171.68.63.255
- 10.1.0.0/16 – adresses de 10.1.0.0 à 10.1.255.255

Standardisation matérielle

Le projet suivant de l'équipe CAPNet était de choisir et de déployer un matériel standard. Des configurations matérielles homogènes sont un point critique pour faire fonctionner CAPNet à une échelle mondiale tout en maintenant une grande disponibilité. Chaque configuration particulière complique potentiellement le support, prolonge les incidents et augmente le coût total de possession (TCO) pour l'équipe Cisco.

Minimiser le nombre de plateformes matérielles supportées simplifie les opérations et minimise les risques d'incompatibilités de plateformes. La standardisation matérielle comprend le châssis de base, toutes les cartes de ligne et les slots équipés.

CAPNet utilise les plateformes matérielles standards décrites dans le tableau 3.

Routeur	Fonction	Fonctionnalité clé
7206VXR	Routeur backbone	Interface DS3
7603	Routeur backbone	Interface OCx
3640	Routeur hors-bande	Interface frame-relay

Tableau 3 : routeurs standards pour CAPNet en 2003

CAPNet travaille avec des groupes réseau régionaux pour assembler ces éléments standards en

briques de base pour être réutilisées sur chaque site. Ces briques de base ne sont pas uniquement que des éléments matériels standards, elles adoptent aussi une utilisation standard des ports et des conventions de nommage.

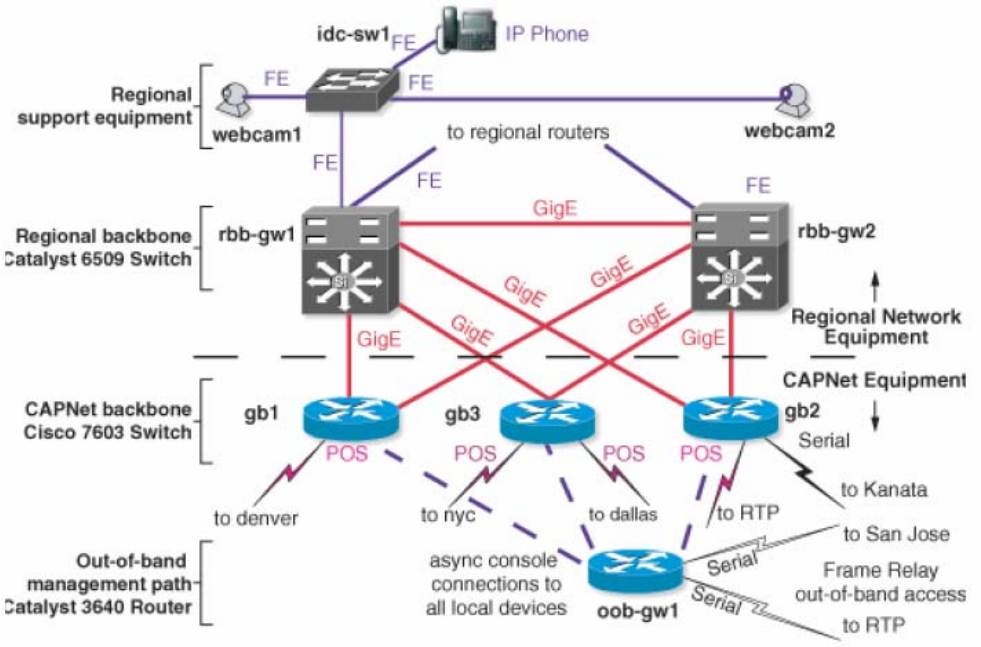

Figure 5. Configuration d'équipements typique sur un site CAPNet

Ces sites utilisent les composants primaires suivants :

- Routeurs Cisco 7603

Ces trois routeurs CAPNet se connectent aux commutateurs régionaux de backbone par des circuits Gigabit Ethernet. Des routeurs et des circuits redondants garantissent la disponibilité du site lors d'incidents sur le routeur ou le circuit. Le nombre de routeurs peut varier d'un site à l'autre, mais tous les sites ont au moins deux routeurs avec des circuits redondants.

- Plateforme multiservice Cisco 3640

Ce routeur permet une gestion hors-bande. On peut alors ouvrir une session console avec un équipement local même en cas de coupure de tous les circuits WAN.

- Commutateurs Cisco Catalyst 6509

Les commutateurs Catalyst 6509 du backbone régional ne font pas partie intégrante de CAPNet, mais sont figurés ici car ils sont importants dans la standardisation des sites. Ces routeurs forment la passerelle régionale vers le réseau backbone CAPNet.

- Commutateur Cisco Catalyst 3550

Ce commutateur accepte un téléphone IP local, un accès local console et des caméras web. Les caméras web sont utiles pour la prise de main à distance pour résoudre des incidents qui nécessitent une présence physique sur site. C'est un équipement régional, mais il facilite la tâche des équipes de support CAPNet.

Standardisation du logiciel Cisco IOS

Après avoir sélectionné et déployé le matériel standard, l'équipe CAPNet a eu à choisir et déployer des versions logicielles standard de l'IOS Cisco.

En collaboration avec « Advanced Services » et d'autres groupes d'architecture et d'opérations, au sein de Cisco, CAPNet a déployé très rapidement un nombre aussi réduit que possible de versions logicielles du Cisco IOS sur plusieurs sites et équipements.

La standardisation des versions logicielles de l'IOS Cisco n'élimine pas complètement les incompatibilités, mais elle minimise les défauts d'interopérabilité entre des équipements CAPNet et ceux d'autres groupes d'opérations.

La standardisation du logiciel Cisco IOS apporte les avantages suivants :

- Utilise l'expérience et des tests d'autres groupes
- Améliore les opérations réseau en réduisant le nombre de bugs que l'équipe doit identifier et tracer
- Garantit que les services critiques tels que le routage, la qualité de service (QoS) et le multicast fonctionnent correctement d'un bout à l'autre

L'équipe CAPNet a choisi les versions logicielles de l'IOS Cisco parmi la liste standard des IOS mondiaux que l'équipe IT Cisco publie. Cette liste définit deux catégories de versions, recommandées et acceptées, et ce par type de plateforme et de fonction.

Les versions logicielles actuelle et précédente de l'IOS Cisco utilisées dans CAPNet sont mises en ligne sur un site web internet Cisco et sont disponibles pour l'équipe réseau.

Les groupes opérationnels au sein de l'équipe IT Cisco, y compris CAPNet sont considérés comme conformes avec les standards logiciels mondiaux de l'IOS Cisco s'ils utilisent les versions recommandées ou acceptées. L'équipe CAPNet ne bascule pas d' « acceptable » à « recommandée » automatiquement ; les mises à jour sont en général réalisées lorsque des utilisateurs réseaux ont besoin de nouvelles fonctionnalités qui sont disponibles uniquement dans les dernières versions.

Configuration des équipements

Maintenant que CAPNet a déployé des matériels et logiciels standards, l'équipe veut s'employer à appliquer et renforcer les configurations standards. CAPNet adopte des configurations standards pour réduire les incompatibilités créées par des configurations inhomogènes ou incorrectes. Des configurations standards pour tout, depuis l'authentification AAA, les listes d'accès pour SNMP, NTP et le login permettent de minimiser les incidents de support et d'interopérabilité tout en maximisant la performance et la fiabilité.

CAPNet utilise l'outil d'auto-configuration EMAN et les modèles de configuration mondiaux pour mettre en œuvre la configuration basique (par exemple, encryption des mots de passe, et horodatage) de l'authentification AAA, du multicast et des configurations SNMP et NTP.

EMAN reproduit quotidiennement la configuration standard sur à chaque équipement, en écrasant (et rapportant) tout changement de configuration adéquate qui aurait été effectué. L'utilisation de l'outil d'auto-configuration a permis d'augmenter l'homogénéité de configuration à un nouveau niveau, qui n'était pas précédemment possible. Avant l'introduction de cet outil au 4ème trimestre de 2002, l'équipe CAPNet s'appuyait sur une installation manuelle et une inspection périodique des configurations pour les converser homogènes. Ceci était chronophage et il était facile de passer à côté des erreurs de configuration.

Avantages des quatre neufs

Le chemin vers les quatre neufs a été construit avec des améliorations de routage, des standardisations matérielles, logicielles et de configuration. Les problèmes dans ces domaines peuvent s'accumuler au cours du temps au fur et à mesure de la croissance du réseau ; en effet les différents sites sont déployés à différents moments avec différents matériels, logiciels et sous-réseaux IP. Résoudre ces problèmes seuls a hissé la disponibilité de CAPNet bien au-delà de quatre

neufs. Conserver quatre neufs et tendre vers cinq neufs, nécessite cependant une attention particulière dans les processus des opérations, de gestion et de support. La section suivante décrit ces efforts.

En route vers les cinq neufs

Les étapes suivies pour atteindre les quatre neufs ont utilisé des occasions faciles d'amélioration. Aller vers les cinq neufs requiert un raffinement dans les procédures opérationnelles et de support.

L'équipe CAPNet a identifié les programmes et priorités suivantes :

- Architecture réseau – planification des locaux et des circuits et adoption de la technologie
- Gestion du réseau – définition des hôtes et gestion hors-bande
- Opérations réseau – meilleures pratiques pour les mises à jour du logiciel Cisco IOS et changements dans le réseau
- Gestion des incidents et support réseau – supervisions, alertes et procédures d'évènement

Architecture réseau

CAPNet est un réseau étendu composé de SONET/SDH, DS3 et de circuits Frame Relay (pour les accès hors bande à des centres de données internet [IDC]) qui sont connectés aux locaux de Cisco en Amérique, EMEA (Europe, Moyen-Orient et Afrique), dans la région Asie-pacifique et au Japon. Les sites CAPNet sont situés dans des locaux possédés ou loués par Cisco et dans des ICD d'opérateurs sur quatre continents.

Une architecture soigneusement planifiée et détaillée et une conception qui incluent la redondance, la tolérance de panne est le socle de ce réseau à haute disponibilité. La performance, la fiabilité et la valeur pour Cisco (coût et valeur de vitrine) sont des facteurs essentiels pris en compte dans la conception.

Conception des locaux

Prenez en considération les points suivants lorsque vous choisissez des locaux physiques :

Site – choisissez un site physique convenant à tous les équipements, tel qu'une salle sécurisée avec des racks pour les équipements et qui possède des contrôles d'environnement
Energie – Une haute disponibilité requiert des sources d'alimentation fiables. Tous les équipements doivent être reliés à des alimentations in-interruptibles (UPS) et les équipements de backbone nécessitent des UPS avec des groupes électrogènes de secours.

Planification du circuit de l'opérateur de télécommunications

Les circuits des réseaux étendus haute disponibilité requièrent des accords de niveau de service englobant multi-hébergement, diversité des circuits, latence faible, protection des circuits et d'autres pratiques de disponibilité. Les concepteurs de CAPNet collaborent avec les fournisseurs de circuits pour obtenir les services nécessaires. Pour diverses raisons, la bande passante, la diversité des circuits ou la latence souhaitée ne sont pas toujours disponibles pour chaque circuit. Parfois les coûts, les chemins disponibles pour la fibre optique, la capacité de l'opérateur de télécommunications ou d'autres facteurs exigent des compromis. Dans de tels cas, le compromis est documenté afin que l'équipe des opérations et l'opérateur de télécommunications en aient connaissance et qu'en cas d'interruption du service, ils puissent engager les actions appropriées pour résoudre rapidement le problème et fournir à nouveau un service normal.

Adoption des technologies à tolérance de panne

Les technologies à tolérance de panne permettent au réseau de tolérer les défaillances matérielles et des circuits. Gardez à l'esprit que la simplicité est fondamentale à l'adoption des technologies à tolérance de panne ; ne choisissez que les technologies dont vous avez besoin pour vos applications.

Hôtes et circuits redondants

Chaque site CAPNet est connecté par au moins deux circuits de matériel redondants routés différemment afin de maximiser la tolérance aux pannes. Grâce à cette configuration, un hôte ou un circuit peut tomber en panne sans que le trafic soit interrompu, car il est réorienté vers des hôtes et des circuits redondants.

IP Event Dampening

CAPNet commence à déployer IP Event Dampening sur les plates-formes Cisco 7200 (exécutant le logiciel Cisco IOS version 12.2T). IP Event Dampening fonctionne de la même manière que BGP Route Dampening. En cas de battement de route (en raison du battement d'un circuit ou pour toute autre raison), la route est supprimée temporairement. Dans un réseau tel que celui de CAPNet, qui présente une excellente redondance au niveau de la couche 3, IP Event Dampening procure une grande stabilité, car il empêche les pertes de trafic lors des battements de route.

L'équipe CAPNet envisage de déployer IP Event Dampening sur ses plates-formes Cisco 7600 dès que cette fonctionnalité sera prise en charge dans une version du logiciel Cisco IOS testée et approuvée par Cisco IT.

Gestion de réseau

La simplicité et la cohérence sont des concepts essentiels pour gérer la haute disponibilité d'un réseau. Assurez-vous que les hôtes sont clairement identifiés et toujours accessibles.

Configuration de l'hôte du système de gestion EMAN

Chaque périphérique CAPNet est saisi dans EMAN Host Management. Cette tâche d'aménagement jette les bases de la surveillance et de l'alerte, abordées à la section Opérations réseau. Il est extrêmement important que les informations d'EMAN Host Management soient précises et cohérentes pour chaque périphérique. Les champs suivants sont standards pour les hôtes CAPNet :
Area (Zone) = En fonction du site
Street (Rue) = En fonction du site
City (Ville) = En fonction du site
Support Group (Groupe d'assistance) =IT
PGM Group (Groupe PGM) = IT
Duty Pager (Téléavertisseur) = capnet-duty
Contact = capnet-core@cisco.com
Collect Syslog Messages (Recueillir les messages Syslog) = Oui
Read-Only Community String (Chaîne de communauté en lecture seule) = Voir config. standard
Rear-Write Community String (Chaîne de communauté en écriture arrière)= Voir config. standard
Collector Name (Nom du collecteur) = IS-HQ (et autres, tel que requis)
Priority Level (Niveau de priorité) = P1/P2 (tel que requis)
Report Type (Type de rapport) = WAN
Alerts Enabled? (Alertes activées ?) = Oui
Download Config? (Télécharger la configuration ?) = Oui
Business Support (Support commercial) = CAPNet
Router Service Type (Type de service du routeur) = Routeur CAPNet
Comments (Commentaires) = Brève description de la fonction du périphérique et de la latence disponible (le cas échéant)

Chemin de gestion hors bande

Le chemin de gestion hors bande garantit que l'équipe de maintenance du réseau peut accéder aux sites de colocation même si tous les circuits du réseau étendu sont arrêtés. Il s'agit-là d'un facteur de disponibilité critique puisque si l'équipe de maintenance ne peut pas accéder au site victime d'une défaillance, cette dernière sera plus longue à résoudre et le service sera d'autant plus long à restaurer.

Chaque site de colocation dispose de circuits permanents virtuels (PVC) de relayage de trames sur une plate-forme multiservice Cisco 3640, laquelle se connecte aux ports de console de chaque périphérique de production au niveau du site.

En utilisant ce chemin, l'équipe de maintenance est en mesure d'ouvrir une session de la console pour chaque périphérique et analyser le problème à distance, sans envoyer de personnel sur place. La figure 6 illustre le réseau de gestion hors bande de CAPNet.

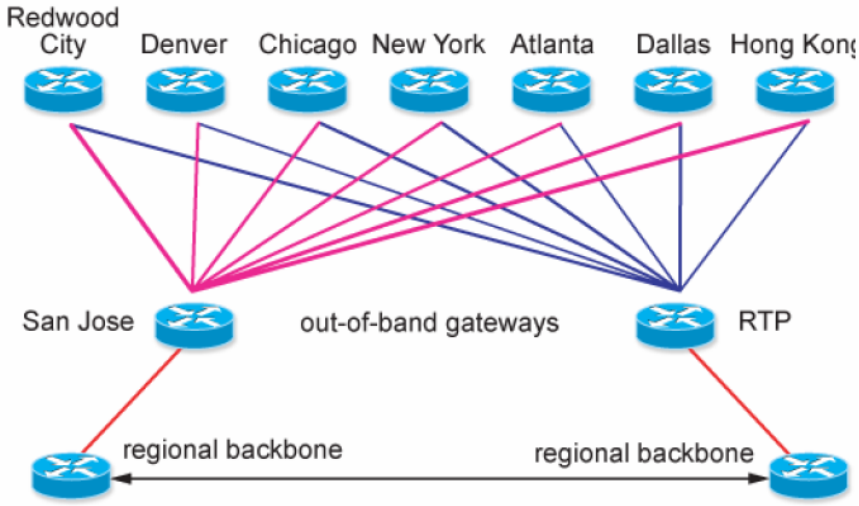

Figure 6. Réseau hors bande

Chaque site est accessible depuis deux chemins hors bande indépendants, le premier depuis San Jose, le deuxième depuis RTP. Par conséquent, chaque site est accessible même si tous les circuits du réseau étendu et l'un des deux circuits hors bande sont défaillants. Si un site est totalement inaccessible, cela est dû à un grave problème du réseau étendu, pas simplement à un problème au niveau du site.

Les circuits à relayage de trames doivent être totalement indépendants des circuits primaires du réseau étendu. Ils utilisent divers circuits à partir de divers emplacements afin que la probabilité qu'ils tombent en panne en même temps que les circuits primaires soit minimale.

Opérations réseau

L'équipe CAPNet a amélioré les opérations réseau en adoptant les meilleures pratiques relatives aux mises à niveau du logiciel Cisco IOS et à la gestion des modifications.

Meilleures pratiques relatives aux mises à niveau du logiciel Cisco IOS

L'équipe de CAPNet n'adopte une nouvelle version du logiciel Cisco IOS que lorsque les utilisateurs ont besoin d'une nouvelle fonctionnalité et seulement après qu'elle a été approuvée pour un déploiement à l'échelle de l'entreprise par l'équipe d'ingénierie et de conception du transport informatique. Lorsque cela s'avère nécessaire, l'équipe de CAPNet sélectionne un candidat à utiliser pour la mise à niveau, puis procède à la mise à niveau du logiciel Cisco IOS (voir figure 7).

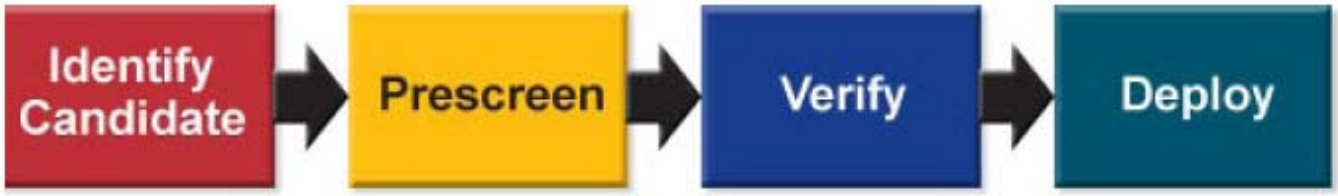

Figure 7. Processus de mise à niveau du logiciel Cisco IOS

Bien que les images répertoriées dans le document sur les normes globales du logiciel Cisco IOS aient été testées et déployées par d'autres groupes de transport chez Cisco, l'équipe des opérations de CAPNet effectue néanmoins un filtrage et une vérification de chaque nouvelle image du logiciel Cisco IOS avant de la déployer.
Le filtrage consiste à :

- Rechercher les bogues via Cisco.com et Advanced Services ;
- Rechercher dans les notes de version du logiciel Cisco IOS les points problématiques.

CAPNet fait ensuite subir au logiciel Cisco IOS candidat une batterie de tests pilotes et de laboratoire. Les tests de laboratoire servent à vérifier les fonctionnalités de base et la compatibilité, tandis que les tests pilotes ont pour but de vérifier le fonctionnement du routeur dans un environnement de production limité. Dès que le candidat passe avec succès tous les tests, il devient la nouvelle norme et son déploiement sur tous les sites de CAPNet est planifié.

Stockage d'image du logiciel Cisco IOS

La mémoire Flash (intégrée ou enfichable) de tous les serveurs de CAPNet est suffisante pour stocker au moins deux images du logiciel Cisco IOS (voir le tableau 5).

	7603	7206VXR	3640
Image primaire	Flash de démarrage du superviseur	Fente 0	Flash de démarrage
Image secondaire	Fente 0	Fente 1	Fente 0

Tableau 5. Emplacement de stockage des images du logiciel Cisco IOS

CAPNet a pour habitude de stocker l'image en cours et l'image précédente du logiciel Cisco IOS sur tous les routeurs. Il est important d'avoir à sa disposition une image prête pour une mise à niveau inférieur ou pour remplacer l'image primaire du logiciel Cisco IOS si cette dernière devient inutilisable. Si une image mise à niveau n'est plus une alternative viable à l'image primaire en cours, stockez deux copies de l'image primaire en cours sur le routeur. Cela permet de garantir qu'une autre image de démarrage est toujours disponible si l'image primaire devient inutilisable.

Mise à niveau des images du logiciel Cisco IOS

La mise à niveau des images du logiciel Cisco IOS à travers l'ensemble de CAPNet s'effectue périodiquement ; elle doit donc être réalisée correctement pour éviter toute interruption de service. Pour que les mises à niveau se passent dans les meilleures conditions, CAPNet publie des procédures de mise à niveau détaillées sur son site Web interne. Ces procédures comprennent :

- Transfert du logiciel Cisco IOS : il s'agit du chargement de la nouvelle image dans l'emplacement de sauvegarde.
- Planification de la mise à niveau du logiciel Cisco IOS : il s'agit de la planification d'une période de maintenance via le système officiel de gestion des modifications Cisco. Ce système est un outil basé sur le Web qui simplifie les processus de création, d'approbation et de suivi des demandes de modification.
- Activation du logiciel Cisco IOS : il s'agit de l'activation des nouvelles images et de la vérification de leur bon fonctionnement. Cette étape inclut la notification de l'équipe d'assistance technique afin qu'elle soit prévenue de l'imminence de changements.

Meilleures pratiques relatives à la gestion des modifications

CAPNet gère de façon similaire les autres modifications du réseau, comme l'ajout de nouveaux circuits ou matériels. La modification est planifiée via le système de gestion des modifications, en tenant compte des périodes de gel des fonctionnalités du réseau Cisco, puis elle est déployée de façon systématique. Cette pratique est typique de Cisco IT, elle n'est pas spécifique à CAPNet.

Gestion des défauts

Même les réseaux hautement disponibles sont susceptibles de connaître des défaillances et des temps d'arrêt. Le matériel tombe en panne, les logiciels ont des bogues, le circuit du réseau étendu s'arrête et le personnel réseau commet des erreurs. La surveillance des performances du réseau et l'alerte de l'équipe d'assistance technique ne réduisent pas le nombre de défaillances mais peut en réduire les effets. Un système fiable de surveillance et d'alerte capable d'identifier rapidement les problèmes et d'avertir l'équipe des opérations permet de minimiser efficacement la durée et les effets d'une quelconque interruption de service.

Surveillance des activités

EMAN Enterprise Monitor est un système de gestion de réseau Cisco IT interne qui fournit un jeu d'outils fiable pour surveiller les activités du réseau et envoyer des alertes en cas de modification significative.
CAPNet utilise EMAN Enterprise Monitor pour capturer les informations suivantes sur le réseau :

- Disponibilité ICMP de l'hôte virtuel et du périphérique
- Déroutement des événements majeurs :
    - État de l'interface
    - Rechargement du routeur
    - Démarrage à froid du routeur
- Surveillance en temps réel de :
    - État de l'interface
    - Niveaux d'utilisation de l'UC du routeur
    - Mémoire du routeur
    - Latence (chaque circuit a une latence définie par contrat)
- Messages Syslog
- EIGRP bloqué sur actif (SIA, Stuck in active)
- Non-concordances des modes duplex
- Autres événements

La surveillance des déroutements de l'interface, la surveillance en temps réel et les hôtes virtuels semblent être des procédures redondantes. Toutefois, dans un environnement constitué de circuits et d'hôtes redondants, un tel degré de surveillance minimise le risque de ne pas détecter un événement. Le redémarrage d'un routeur ou le battement intermittent d'un circuit ne se répercute pas sur la disponibilité mais génère un déroutement. Ce type de défaut invisible peut affecter les performances et la fiabilité d'un réseau. Il vaut donc mieux trop surveiller le réseau que pas assez.
L'équipe de CAPNet a ajouté à EMAN une vue personnalisée pour la surveillance en temps réel. Cette vue donne à l'ingénieur de garde un aperçu de l'état en cours et des exceptions pour tous les événements détectés par la surveillance en temps réel.

Surveillance des hôtes équipés de circuits redondants

La précision des mesures de disponibilité est fonction de l'utilisation correcte de l'interface et de la configuration de l'adresse d'hébergement. Sinon, l'hôte peut sembler arrêté alors qu'il ne l'est pas. Chaque nom d'hôte de CAPNet est hébergé de manière unique à l'adresse de l'interface de boucle 0 et cette adresse de boucle est utilisée pour surveiller chaque périphérique. L'utilisation de l'interface de boucle fournit une interface stable toujours active permettant de surveiller les hôtes et d'effectuer des commandes à distance à partir d'EMAN. Cela permet également de simplifier les opérations de maintenance et d'assistance technique. Les noms d'hôte à hébergement unique sont plus performants que ceux à hébergement multiple pour les DNS circulaires pour la surveillance, car il est possible d'obtenir fréquemment des fausses réponses positives dans EMAN Enterprise Monitor (hôte présenté comme arrêté alors qu'il fonctionne).

La figure 8 illustre comment l'hébergement multiple peut conduire à des données incorrectes sur la disponibilité.

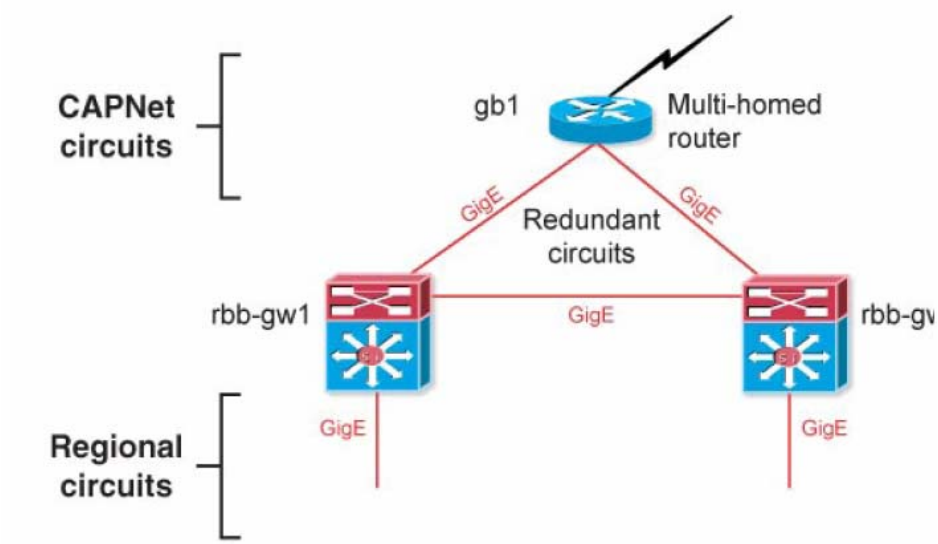

Figure 8. Hôtes à hébergement multiple avec circuits redondants

Si gb1 est surveillé à l'aide de noms d'hôte à hébergement multiple, il apparaîtrait comme arrêté pendant une période de maintenance planifiée d'une heure pour rbb-gw2, car les interfaces reliant gb1 à rbb-gw2 seraient arrêtées, bien que le routeur dispose d'une connectivité redondante à rbb-gw1. Il est possible de contourner ce problème en incluant gb1 à la gestion des modifications pour rbb-gw2, mais cette inclusion cacherait tout problème réel de gb1 qui surviendrait pendant la période de maintenance.

Alertes réseau

EMAN peut être configuré de sorte à envoyer des alertes pour toute donnée surveillée. Elles peuvent être envoyées à un individu ou à un numéro de téléavertisseur. L'équipe de CAPNet utilise des groupes d'alertes pour personnaliser l'avertissement en fonction des parties du réseau et de la priorité de l'alerte (voir tableau 6).

Groupe d'alertes	Action	Exemple
Élevé	Notification immédiate de l'ingénieur de garde 24 h/24, 7 j/7	Panne du circuit
Moyen	Notification de l'ingénieur de garde pendant les heures de travail et envoi d'un e-mail en dehors des heures de travail	Battement de circuit hors bande
Faible	Notification par e-mail uniquement	Non-concordance des modes duplex

Tableau 6. Notification des groupes d'alertes

L’utilisation de plusieurs groupes d'alertes garantit la résolution dans les plus brefs délais (24 h/24, 7 j/7) des problèmes critiques. Les problèmes moins critiques, mais néanmoins importants, sont gérés dans un laps de temps adéquat sans surcharger inutilement l’ingénieur de garde.

Assistance réseau

CAPNet utilise un service d’ingénierie de garde pour l’assistance technique du réseau, avec l’aide de Cisco Advanced Services. L’ingénieur de garde est disponible 24 h/24, 7 j/7, pour résoudre les problèmes de réseau. Il est chargé de consigner les problèmes rencontrés dans un journal et de publier la synthèse des informations dans EMAN.

Service d’ingénierie de garde

L’équipe de service (garde) CAPNet se compose de huit ingénieurs qui effectuent chacun une semaine de garde 24 h/24, 7 j/7, par roulement. Chaque ingénieur a donc une semaine de garde et sept semaines de « relâche ». L’ingénieur de garde est responsable de la gestion des problèmes d'urgence, généralement générés en temps réel par le service d’alerte EMAN sous la forme d’une page de tâches à effectuer. À l’occasion, l’ingénieur de garde peut recevoir une alerte du service des opérations réseau (qui n’est généralement pas liée directement à CAPNet).

CAPNet publie le planning de garde sur le planificateur IT Operations Support Duty Scheduler, avec d’autres groupes d’assistance technique Cisco IT. Ce planificateur est une page Web qui a la forme d’un calendrier dans lequel sont indiqués les ingénieurs titulaires et suppléants de garde pour chaque journée.

Roulement de la garde

Le service de garde de CAPNet change chaque semaine, le changement d’équipe ayant lieu chaque lundi matin à 8 h, heure du Pacifique. À cette heure-là, l’ingénieur de garde transfert le service de garde à l’ingénieur suivant dans le roulement, par téléphone ou messagerie instantanée. L’ingénieur CAPNet de garde est responsable du service de garde jusqu’à ce que son successeur ait confirmé la prise de relai. Les dossiers en cours et les tickets d’incidents au moment de la relève doivent être transmis au nouvel ingénieur CAPNet de garde, sauf si cela s’avère non souhaitable ou peu pratique.

Procédure d’événements

L’ingénieur CAPNet de garde doit suivre une procédure standard d’identification des problèmes, de communication de l’avancée de la résolution du problème et de consignation des résultats (voir la figure 9).

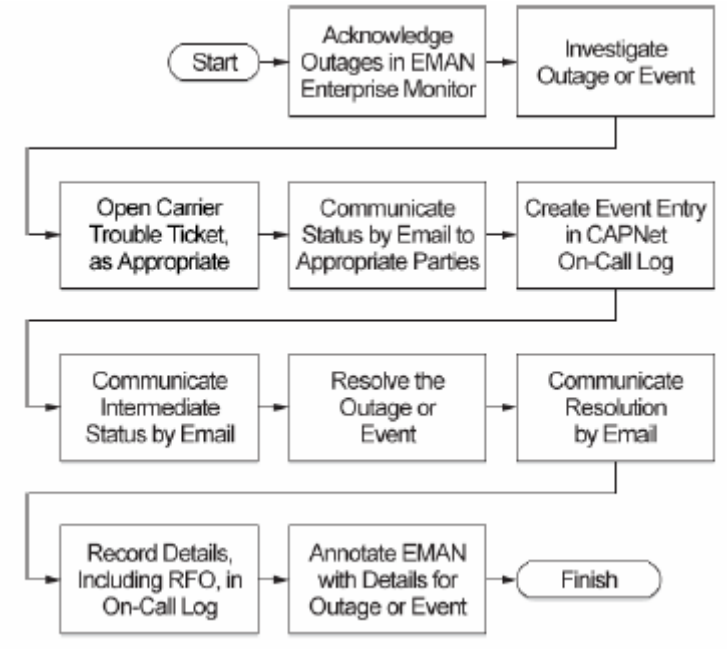

Figure 9. Organigramme de la procédure d'événements

Journal de garde de CAPNet

Chaque incident géré par l'ingénieur de garde est consigné dans un journal de garde récapitulatif. Celui-ci permet de suivre et de calculer les interruptions de service/événements en fonction de la classification et de la sous-classification du problème, des heures de début et de fin, de la durée de l'interruption de service/événement, du temps nécessaire à la résolution de l'incident et de la raison de l'interruption de service (RFO). Le tableau 7 présente la classification et la sous-classification des incidents.

Classification de l'incident	Sous-classification de l'incident
COS-CatOS	COS-Other (COS-Autre)
	COS-Undetermined/intermittent (COS-Indéterminé/intermittent)
	COS-Version Interoperability (Interopérabilité de version)
EV-Environmental (Environnemental)	EV-Power--Equipment (EV-Alimentation--Équipement)
	EV-Power--Room (EV-Alimentation--Salle)
	EV-Power--Site (EV-Alimentation--Site)
HE-Human Error (Erreur humaine)	HE-Misconfiguration (HE-Erreur de configuration)
	HE-No CM Approuved (Aucun CM approuvé)
	HE-Redundancy failure (HE-Problème de redondance)
	…
HF-Hardware Failure (Panne matérielle)	HF-Cabling (HF-Câblage)
	HF-Cisco System Component (HF-Composant Cisco System)
	HF-Non-Cisco Equipement (HF-Équipement non Cisco)
IL-Increased Latency (Augmentation de la latence)	IL-Increased Latency – Carrier Reroute (IL-Augmentation de la latence – Reroutage de l'opérateur de télécommunications)
	IL-Increased Latency – Circuit Congestion (IL-Augmentation de la latence – Congestion des circuits)
IOS-IOS	IOS-CPU Load (IOS-Charge de l'UC)
	IOS-Multicast (IOS-Multidiffusion)
	IOS-Routing (IOS-Routage)
	...
NA-N/A	NA-Engineer Troubleshooting (NA-Dépannage ingénieur)
	NA-Not a Network Related Problem (NA-Incident non lié au réseau)
	NA-P3 Site (NA-Site P3)
	NA-Problem with Monitoring (NA-Problem de surveillance)
TF-Transport Failure (Echec du transport)	TF-LAN
	TF-WAN Circuit down - General Carrier Outage (TF-Panne du circuit du réseau

	étendu – Interruption de service générale de l'opérateur de télécommunications)
	TF-WAN Circuit down – No Backup (TF-Panne du circuit du réseau étendu – Pas de sauvegarde)
	…
UD-Undetermined (Indéterminé)	UD-Undetermined (UD-Indéterminé)

Tableau 7. Classification des incidents

Suivi des incidents

Le suivi temporel des détails des interruptions de service et des événements est critique à la réussite opérationnelle. Avec un système de service de garde par roulement, il n'existe aucune autre méthode fiable pour identifier les tendances ou les problèmes chroniques. Chaque trimestre, CAPNet examine les données de suivi et identifie les améliorations opérationnelles qui peuvent être apportées.

Par exemple, la classification des problèmes dans le journal de garde permet d'identifier facilement les problèmes suivants :

- Problèmes chroniques du matériel ou du logiciel Cisco IOS ;
- problèmes périodiques avec un opérateur de télécommunications ou un circuit individuel ;
- problèmes environnementaux, comme les problèmes d'alimentation, ou de chauffage, ventilation ou climatisation ;
- erreurs humaines, comme les erreurs de configuration.

Les problèmes tels que les pannes de circuit ou matérielles ne peuvent pas être évités, mais le journal de garde facilite l'identification des problèmes facilement résolubles. En bref, il est impossible de réparer un problème sans l'avoir au préalable identifié. Le journal de garde est un outil critique employé par CAPNet pour identifier et résoudre les problèmes chroniques ou en cours et maintenir un niveau opérationnel d'excellence.

Il est également possible de copier et coller tout ou partie du contenu du journal de garde pour annoter les pages d'EMAN, ce qui permet ainsi de fournir des informations sur les interruptions de service et les événements aux membres du personnel ou aux groupes qui n'ont pas facilement accès au journal de garde. Afin que les annotations d'EMAN fournissent des informations cohérentes et complètes, CAPNet utilise un modèle d'annotation incluant les informations suivantes :

- Hôtes et circuits concernés
- Heure de survenue de l'incident
- Heure de reprise
- Description du problème
- Raison de l'interruption de service (RFO)

Gestion proactive des défauts

L'ingénieur CAPNet de garde est chargé de vérifier les mesures de la disponibilité du réseau EMAN et d'annoter les éléments qui n'atteignent pas les objectifs en matière de disponibilité. CAPNet reçoit quotidiennement des rapports détaillant les modifications de configuration, le nombre de routes de la table de routage, l'échec ou la réussite de la configuration automatique et les rapports d'exception de configuration. CAPNet reçoit également des alertes Syslog pour les événements tels que les EIGRP SIA et les non-concordances des modes duplex Ethernet.

L'examen des problèmes de disponibilité, même si les accords de niveau de service pour le site ou l'équipement sont respectés malgré l'occurrence de ces problèmes, est fortement encouragé. L'examen proactif des problèmes mineurs peut permettre de découvrir une faiblesse avant que celle-ci se transforme en interruption de service.

Cisco Advanced Services

CAPNet utilise Cisco Advanced Services comme ressource technique pour :

- La recherche des bogues
- Le développement des produits
- Le matériel et les logiciels
- Les experts du dépannage
- Les concepteurs experts

Composants de rechange

CAPNet possède sur chaque site des composants de rechange. En cas de panne d'un appareil, le personnel sur place peut rapidement échanger le composant matériel et rétablir une exploitation normale avec la redondance complète.

Caméras et manœuvres manuelles à distance

Dans chaque site de colocation CAPNet, des webcams sont installées en face des racks d'équipements. Grâce à celles-ci, l'ingénieur de garde peut voir l'équipement et aider à distance une personne sur place à résoudre le problème. Cisco IT a signé des contrats d'assistance sur site pour tous les sites de colocation ; il est donc facile d'obtenir une assistance technique sur un site quelconque.

Documentation CAPNet

La documentation en ligne, précise et facilement accessible, constitue une aide importante pour l'ingénieur de garde afin qu'il puisse résoudre les problèmes à mesure qu'ils surgissent. La documentation en ligne suivante est conservée par l'équipe de CAPNet :

- CAPNet Duty Procedures (Procédures de service de garde CAPNet)
- CAPNet Carrier Contacts Page (Page des contacts des opérateurs de télécommunications CAPNet)
- CAPNet Network Maps (Cartes du réseau CAPNet)
- CAPNet IOS Standards (Normes IOS CAPNet)
- CAPNet BGP
- CAPNet Dashboard Global Duty Schedules (Planification des tâches globales du tableau de bord CAPNet)
- TAC Case Procedures (Procédures des cas TAC)

Tous ces documents sont accessibles facilement sur le site Web interne de Cisco IT.

Conclusions et recommandations

À bien des égards, la route vers la haute disponibilité est pavée de bonnes pratiques opérationnelles et de bon sens. L'adoption des meilleures pratiques peut souvent augmenter à court terme le temps système opérationnel mais, si elles sont correctement mises en œuvre, celui-ci sera sensiblement réduit à long terme. Concentrez-vous sur les domaines de la conception du réseau, de la configuration, de la surveillance et de l'alerte, des procédures d'assistance par service de garde, et sur la documentation. Si vous ne le faites pas, il est difficile d'atteindre, et a fortiori de conserver, l'excellence en matière opérationnelle.

Lors du démarrage d'un programme haute disponibilité, commencez par chercher les opportunités de mettre en œuvre quelques améliorations simples. Si trop de plates-formes matérielles et de versions du logiciel Cisco IOS sont déployées, essayez de changer les plates-formes matérielles standard et les versions du logiciel. Toutefois, n'oubliez pas que vous n'atteindrez jamais une disponibilité à 99,999 % uniquement par une combinaison de technologie et de normalisation. De

nombreuses défaillances sont dues à de mauvaises procédures d'assistance, de gestion et d'exploitation. Cisco fournit aux entreprises de nombreuses ressources, y compris des livres blancs sur les meilleures pratiques pour les processus importants.

Les avantages de la haute disponibilité dépassent de loin les coûts. Les réseaux hautement disponibles améliorent l'image de l'entreprise, réduisent les frais d'exploitation, améliorent la productivité des fournisseurs et des employés, et prennent en charge les applications modernes de communication IP, comme la vidéoconférence et la voix sur IP.

Pour aller plus loin

Site web « Cisco on Cisco »
http://www.cisco.com/web/about/ciscoitatwork/index.html

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_12/07