

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

Table des matières

Préface.....	3
Mesure de la disponibilité brute	4
Mesure de la disponibilité ajustée	8
Disponibilité de Cisco IT-LAN-SJ-Production en 2002	10
Les étapes Cisco pour une disponibilité de 99,9 %	14
Etape 1 : Mesure de la disponibilité	14
Etape 2 : Alertes d'interruption de service	17
Etape 3 : Hiérarchie physique	17
Etape 4 : Hiérarchie logique	20
Etape 5 : Analyse des causes fondamentales des interruptions de service	26
Etape 6 : Des onduleurs pour les unités critiques.....	30
Etape 7. Gestion de la redondance	30
Etape 8 : Gestion des changements	31
Etape 9 : Pièces de rechange en cas d'urgence.....	31
Etape 10 : Gestion hors bande	31
Les étapes Cisco pour une disponibilité de 99,99 %	33
Etape 1 : Le contrôle proactif de la redondance	33
Etape 2 : Des onduleurs pour toutes les unités	35
Etape 3 : Des générateurs pour les unités critiques	35
Etape 4 : Des audits automatisés sur la configuration des routeurs.....	35
Etape 5 : Intégration de la gestion des changements avec la surveillance de la disponibilité.....	36
Etape 6 : Normalisation des versions de code	36
Etape 7 : Formation au dépannage	44
Etape 8 : Séparation de la gestion des incidents et de la résolution des problèmes	44
Les étapes Cisco pour une disponibilité de 99 999 %	46
Etape 1 : Toutes les unités doivent être sur générateur de secours.....	46
Etape 2 : Contrôle automatique de la configuration des commutateurs	46
Etape 3 : Audit manuel semi-annuel	46
Les tactiques spécifiques de Cisco pour améliorer la disponibilité du réseau Production	47
Séparation des réseaux Production et Alpha	47
Le centre d'assistance technique	47
Adoption des recommandations précédentes par l'équipe du Cisco IT-LAN-SJ.....	49

Préface

Le réseau est le principal facteur de productivité de l'entreprise du 21^{ème} siècle. Vos clients l'utilisent pour acheter vos produits. Il contrôle votre chaîne d'approvisionnement, simplifie le travail des ressources humaines, facilite la gestion de la paie, des avantages sociaux et de la formation. Grâce à la téléphonie IP, les appels téléphoniques partagent l'infrastructure du réseau de données.

Dans un tel environnement, Cisco Systems® serait dans l'incapacité de travailler sans un réseau opérationnel à haute disponibilité. Pour mesurer cette disponibilité, l'entreprise compte généralement le nombre de minutes d'interruption de service ou d'indisponibilité du réseau :

- trois 9 (99,9 %) = 10 minutes de temps d'arrêt chaque semaine ;
- quatre 9 (99,99 %) = 1 minute de temps d'arrêt chaque semaine ;
- cinq 9 (99,99 %) = 6 secondes de temps d'arrêt chaque semaine ;

Pour Cisco, une disponibilité « trois 9 » ne suffit plus. Nous devons atteindre au moins « quatre 9 » pour travailler de manière efficace, mais toute entreprise soucieuse de sa productivité aspire à une disponibilité de 99,999 %. Bien que les grandes compagnies possèdent le plus souvent des réseaux et des équipements conçus pour le niveau « cinq 9 », très peu d'entre elles font état d'une telle disponibilité dans un environnement productif à grande échelle.

Réparti sur 50 bâtiments dans toute la ville de San Jose en Californie, où il connecte des ordinateurs de bureau, des centres de calcul, des laboratoires et des unités de fabrication, le réseau local informatique Cisco de San Jose (Cisco IT-LAN-SJ) compte 900 commutateurs, 200 routeurs, 250 serveurs consoles, 800 points d'accès Cisco® Aironet® et toute une batterie d'appareils de commutation de contenus protégés par le pare-feu Cisco. Malgré sa taille et sa complexité, le réseau de San Jose a frôlé les 99,999 % de disponibilité en 2002. Au cours du second trimestre 2003, dans les zones où le réseau est soutenu par des onduleurs et des générateurs à 100 % non interruptibles, le réseau Cisco IT-LAN-SJ a atteint une disponibilité de 99,99853 %.

Dans cet article, nous vous donnons les raisons de cette réussite Cisco : comment nous nous sommes doté d'un réseau à haute disponibilité sur le campus de San Jose, comment nous avons mesuré cette disponibilité, et quelles ont été les étapes mises en oeuvre sur le réseau Cisco IT-LAN-SJ pour atteindre une disponibilité « cinq 9 ». Nous terminons par une discussion sur la manière dont le réseau Cisco IT-LAN-SJ s'est adapté à ces mesures et sur l'importance de la planification pour élaborer la démarche la plus économique d'atteindre la haute disponibilité.

LES INFORMATIONS PRESENTEES ICI SONT FOURNIES « TELLES QUELLES », SANS AUCUNE GARANTIE OU DECLARATION EXPRESSE, IMPLICITE OU STATUTAIRE, ET NOTAMMENT SANS LIMITATION OU GARANTIE DE NON CONTREFACON, DE QUALITE BONNE ET MARCHANDE OU D'ADAPTATION A UNE UTILISATION QUELCONQUE

Mesure de la disponibilité brute

Depuis le lancement de Six Sigma, les entreprises ont mesuré la qualité en définissant des éléments de référence, en fixant des objectifs et en améliorant leurs processus. Aujourd'hui, la réussite d'une société dépend souvent de manière directe de sa capacité à garantir l'optimisation, le bon fonctionnement et la haute disponibilité de son réseau. Cependant, les plans destinés à atteindre cette haute disponibilité doivent être réalistes et ne tenir compte que des unités qui ont une incidence directe sur la satisfaction des utilisateurs.

Les mesures de disponibilité ont ainsi deux principaux objectifs :

- l'évaluation du service fourni aux utilisateurs du réseau ;
- la mise en place d'outils destinés à améliorer le service fourni à ces mêmes utilisateurs.

Les mesures de disponibilité ne se limitent pas à celles du service : elles constituent également un outil stratégique pour l'améliorer. En ce qui concerne les connexions réseaux, la meilleure estimation du niveau de service fourni aux utilisateurs du réseau est la disponibilité des commutateurs de couche d'accès. Ces commutateurs connectent les ordinateurs portables des utilisateurs au moyen d'un câble de catégorie 5, le plus souvent sur un câblage structuré qui relie l'espace de travail ou le bureau, à la plus proche des armoires réseaux. Si la disponibilité des commutateurs de couche d'accès touche directement les utilisateurs finaux, la disponibilité des unités de distribution et de cœur de réseau est moins importante pour l'évaluation du service. Les réseaux redondants sont conçus pour permettre à chaque unité du cœur de réseau de tomber en panne sans que cela affecte les utilisateurs. En revanche, tout dysfonctionnement d'un commutateur de couche d'accès a systématiquement des conséquences sur ce service car l'utilisateur final connecte généralement son ordinateur à un unique commutateur. Pour ces raisons, le département informatique de Cisco évalue le niveau de service fourni aux utilisateurs en mesurant la disponibilité de ce type de commutateurs. Les défaillances de redondance au niveau du cœur de réseau sont toujours prises en compte dans ces mesures car toute panne du cœur fait transiter les sollicitations (pings) jusqu'aux commutateurs de couche d'accès.

Bien que la surveillance des commutateurs de couche d'accès demeure la meilleure manière d'évaluer le niveau de service fournis au client, le suivi de la disponibilité vers les unités de cœur de réseau possède malgré tout une valeur opérationnelle. Lorsque vous ne disposez que des données de disponibilité des commutateurs de couche d'accès, il devient difficile d'identifier le lien de cœur de réseau qui rejette les paquets. A l'inverse, si l'opérateur peut connaître les données de disponibilité de chaque unité réseau, il lui est bien plus aisé d'identifier l'endroit où les paquets disparaissent. Ainsi, la disponibilité de toutes les unités réseaux doit être mesurée car l'équipe réseau s'appuie sur ces rapports de disponibilité pour identifier les problèmes. En revanche, les valeurs de la disponibilité du cœur de réseau ne traduisent pas le niveau de service fourni aux utilisateurs, et le département informatique de Cisco ne les intègre pas dans les valeurs transmises à la direction.

Connexions sans fil

Pour le département informatique de Cisco, la connectivité de réseau filaire est un service classé Priorité 1 (P1) : les interruptions de service qui touchent la connectivité de réseau filaire sont immédiatement identifiées et réparées, 24 heures par jour, tous les jours. S'il le faut, un ingénieur réseau est prévenu par radio-messagerie, même en dehors des heures d'ouverture (le lecteur trouvera un descriptif des niveaux de priorité page 21).

A l'inverse, la connectivité sans fil est un service de Priorité 4 (P4). Les interruptions de service du réseau sans fil ne sont réparées que pendant les heures d'ouverture car elles n'empêchent pas les utilisateurs de travailler – il leur suffit de se connecter à un port physique si nécessaire. Les chiffres montrent que le réseau sans fil est essentiellement utilisé au cours des réunions qui se tiennent pendant

les heures de travail, et l'incidence d'une interruption prolongée du service en dehors de ces heures est minimale.

Par ailleurs, le nombre de « pings » adressés aux points d'accès sans fil n'est pas un indicateur fiable de la disponibilité du service sans fil. La sollicitation d'un point d'accès ne signifie pas, en effet, que les utilisateurs puissent s'associer au réseau sans fil, et ce pour de nombreuses raisons : interférences radio, défaillance de la radio du point d'accès, problèmes avec les pilotes logiciels ou le serveur d'authentification, etc.

Ainsi, les points d'accès gérés par le département informatique de Cisco ne sont pas intégrés au groupe de disponibilité Production du réseau Cisco IT-LAN-SJ. Ils sont en revanche inclus dans le groupe de disponibilité Test (voir « Groupes et sous-groupes », ci-dessous). Bien que Cisco continue d'étudier le moyen d'évaluer de manière précise la disponibilité du service sans fil, ce sujet ne sera pas davantage abordé dans le présent article.

Mesure de la disponibilité brute d'une unité donnée

La disponibilité du réseau Cisco IT-LAN-SJ est mesurée dans un centre de calcul à San Jose à partir des serveurs de gestion. Deux pings sont générés toutes les 15 à 20 secondes en direction de chaque unité gérée. Si le serveur de gestion reçoit au moins une réponse, il considère l'unité comme fonctionnelle, autrement dit, disponible, sur cette période. On détermine ainsi la disponibilité brute quotidienne de l'unité concernée.

Groupes et sous-groupes

Deux groupes de disponibilité : Cisco IT-LAN-SJ-Production et Cisco IT-LAN-SJ-Test

Cisco assure la surveillance et l'évaluation de toutes les unités associées à la connectivité de réseau. Toutefois, afin de différencier les interruptions de service qui affectent directement les utilisateurs de celles qui n'ont pas d'incidence sur eux, Cisco IT-LAN-SJ a créé deux groupes de disponibilité appelés Cisco IT-LAN-SJ-Production et Cisco IT-LAN-SJ-Test.

Cisco IT-LAN-SJ-Production – le groupe Cisco IT-LAN-SJ-Production mesure le service fourni aux clients en sollicitant par des pings les commutateurs de la couche d'accès directement connectés aux clients. La seule exception est le réseau du laboratoire où le point de démarcation entre le service informatique de Cisco IT et le laboratoire est un routeur d'accès. Dans le cas du laboratoire, on surveille les adresses de bouclage des routeurs d'accès.

Le groupe Production se compose de deux sous-groupes organisés selon leur fonction et leur localisation :

- le centre de calcul Production ou PDC1 (Production Data Center 1)
- le PDC2
- le centre de calcul développement ou DDC1 (Development Data Center 1)
- le DDC2
- le DDC3
- le DDC4
- le DDC5 (fermé en novembre 2002)
- les laboratoires
- les ordinateurs de bureau du réseau MAN (Metropolitan Area Network) de San Jose
- les ordinateurs de bureau des sites 1 à 3 de San Jose
- les ordinateurs de bureau du site 4 de San Jose
- les ordinateurs de bureau du site 5 de San Jose
- le réseau CallManager de San Jose

Les centres de calcul Production supportent les fonctions métiers de Cisco business (site Web, commandes, fabrication et progiciel de gestion intégré [PGI]). Les centres de calcul de développement supportent le développement matériel et logiciel Cisco. Cette distinction permet de déterminer la

disponibilité de manière exploitable. En plus de la disponibilité globale du réseau Cisco IT- LAN-SJ dans son ensemble, cette répartition par sous-groupes permet à la direction de comprendre si un problème de disponibilité a touché les laboratoires – ce qui peut être gênant – ou un centre de calcul de production, ce qui peut faire baisser nos revenus.

La création et la modification des groupes et des sous-groupes de disponibilité Production sont soigneusement contrôlées, et les grandes mises à jour ne sont effectuées que par la direction technique une fois le projet longuement mûri. De plus, et comme toute mise à jour réalisée à la fin d'un trimestre fiscal peut introduire un biais dans les statistiques de ce trimestre, les grandes mises à jour comme la création ou la suppression d'un sous-groupe, n'interviennent qu'au début de chaque trimestre fiscal.

Cisco IT-LAN-SJ-Test – Le groupe de disponibilité Cisco IT-LAN-SJ-Test se compose de toutes les autres unités de réseau gérées par Cisco IT-LAN-SJ : routeurs, commutateurs autres que ceux de la couche d'accès, serveurs de sécurité Cisco PIX®, serveurs LocalDirectors, commutateurs de services de contenus, unités de gestion hors bande et points d'accès sans fil. Comme toutes ces unités de réseau appartiennent à un même groupe de disponibilité, l'équipe Cisco IT-LAN reçoit des rapports de disponibilité automatisés ce qui leur permet d'identifier les problèmes de connectivité et de mener leur enquête, quelle que soit l'incidence de ces problèmes sur les clients. Le groupe de disponibilité Cisco IT-LAN-SJ-Test est également appelé le groupe de disponibilité « Test ».

Les ingénieurs réseaux de Cisco n'utilisent le groupe de disponibilité Cisco IT-LAN-SJ-Test que pour des fonctions de diagnostic et ne transmettent pas ses résultats à la direction. Le groupe de disponibilité Test se répartit en plusieurs sous-groupes définis de manière informelle et n'importe quel ingénieur réseau de l'équipe peut créer un sous-groupe de test lorsqu'il en a besoin. Voici une liste des sous-groupes qui composent actuellement Cisco IT-LAN-SJ-Test :

- Cisco Lightweight Extensible Authentication Protocol (Cisco LEAP) – Assure la surveillance de l'application d'authentification utilisée pour la connectivité sans fil, afin de mesurer la disponibilité du service sans fil ;
- IPv6 – Assure l'évaluation des unités du déploiement IPv6 qui n'ont pas encore été définies en tant que service P1 ;
- tous les routeurs du réseau IT-LAN-SJ ;
- l'infrastructure du Site 5 – Ce sous-groupe a été créé par l'ingénieur réseau responsable du site pour son propre usage ;
- WAN-SJ-Reliability – Assure l'évaluation des temps de fonctionnement des circuits de réseau WAN et MAN dans la zone ;
- WAN-SJ-Availability – Mesure le pourcentage du temps de fonctionnement d'au moins un circuit de réseau WAN ou MAN vers chaque site distant ;
- tous les points d'accès du réseau IT-LAN-SJ.

Calcul de la disponibilité brute des groupes et des sous-groupes

La disponibilité brute d'un sous-groupe est la moyenne des disponibilités brutes de toutes les unités de ce sous-groupe. La disponibilité brute d'un groupe est la moyenne des disponibilités brutes de toutes les unités de ce groupe, y compris des unités de ses sous-groupes.

Note : La disponibilité brute d'un groupe n'est pas la moyenne des disponibilités brutes de ses sous-groupes. Une telle définition donnerait un poids considérable aux petits sous-groupes, comme le sous-groupe IT-LAN-SJ- Production/DDC4 avec ses cinq commutateurs de couche d'accès. Le sous-groupe Cisco IT-LAN-SJ-Production/Ordinateurs de bureau du Site 4 a un poids plus important car il dispose de 374 commutateurs de couche d'accès. Les unités du groupe interviennent chacune de manière égale dans les calculs de disponibilité, ce qui n'est pas le cas des divers sous-groupes.

Calculs quotidiens, mensuels, trimestriels et annuels

La disponibilité de chaque unité, groupe et sous-groupe est calculée tous les jours selon les statistiques de sollicitation (pings) à partir d'un « jour de disponibilité » qui va de 16h00 à 16h00 Heure du Pacifique (de minuit à minuit GMT). Les statistiques mensuelles de chaque groupe et sous-groupe sont la moyenne des statistiques quotidiennes du mois correspondant. Bien que cette définition entraîne une erreur d'arrondi, elle évite de prendre en compte la mise en service ou le retrait des unités dans les sous-groupes au cours du mois.

Des statistiques sont également générées chaque trimestre fiscal. Pour Cisco, ces trimestres fiscaux étaient définis de la manière suivante pour 2003 :

- premier trimestre de l'exercice 2003 : du 28 juillet 2002 au 26 octobre 2002 ;
- deuxième trimestre de l'exercice 2003 : du 27 octobre 2002 au 25 janvier 2003 ;
- troisième trimestre de l'exercice 2003 : du 26 janvier 2003 au 26 avril 2003 ;
- dernier trimestre de l'exercice 2003 : du 27 avril 2003 au 26 juillet 2003.

Les trimestres fiscaux ne correspondant pas à ceux du calendrier, les statistiques trimestrielles sont définies comme la moyenne des 91 jours qui constituent le trimestre. Les statistiques trimestrielles du groupe et des sous-groupes Production sont transmises selon la voie hiérarchique à la direction, tandis que les statistiques mensuelles sont utilisées au sein de l'équipe pour suivre plus précisément la disponibilité.

Mesure de la disponibilité ajustée

L'objectif d'une évaluation de la disponibilité est de mesurer le niveau de service fourni aux clients. Les interruptions qui ont une incidence sur les utilisateurs doivent être mesurées mais les interruptions planifiées qui n'ont pas d'incidence doivent être évaluées de manière différente et ajustées afin de calculer le véritable niveau de service fourni aux utilisateurs du réseau.

Envisageons les circonstances d'une interruption de service A :

- le réseau des ordinateurs de bureau du bâtiment 11 est en panne de 21h00 à minuit le mardi soir ;
- l'interruption de service correspond à une mise à jour planifiée du réseau ;
- dans ce bâtiment, les utilisateurs ont été prévenus à l'avance.

Dans ce bâtiment, les utilisateurs n'ont été que très faiblement affectés. Bien qu'ils n'aient pas pu travailler après 21h00 ce soir là, ils ont été notifiés longtemps à l'avance : s'ils avaient eu à effectuer des travaux essentiels dans ce bâtiment – comme un transfert sur bande – ils auraient pu demander le report de la mise à jour. Compte tenu des conséquences minimales de cette interruption, la mesure de la disponibilité doit être ajustée afin de ne pas en tenir compte.

Considérons maintenant l'interruption de service B :

- le réseau PDC1 est indisponible de 21h00 à minuit le mardi soir ;
- l'interruption de service correspond à une mise à jour planifiée du réseau ;
- les utilisateurs de ce centre de calcul ont été prévenus à l'avance.

Les utilisateurs du centre de données ont été affectés. Bien que la notification préalable et l'intervention tardive réduisent quelque peu les conséquences de cette interruption, le centre de calcul effectue des fonctions métiers critiques 24 heures par jour, tous les jours de la semaine. Dans ce cas, la disponibilité brute est la meilleure mesure de l'incidence sur les utilisateurs du réseau.

Considérons enfin l'interruption de service C :

- le réseau des ordinateurs de bureau du bâtiment 11 tombe en panne de 14h00 à 17h00 le mardi après-midi ;
- l'interruption de service n'était pas prévue.

Les utilisateurs dans ce bâtiment ont été affectés : plusieurs centaines d'employés de Cisco ont peut-être été empêchés de travailler pendant la quasi-totalité de la demi-journée. Dans ce cas, la disponibilité brute doit être mesurée en raison des conséquences négatives de l'interruption sur les utilisateurs du réseau.

En raison de la diversité des circonstances, le département informatique de Cisco IT mesure à la fois la disponibilité brute et la disponibilité ajustée, en excluant de la disponibilité ajustée les interruptions de service planifiées. Pour les réseaux de bureau et les laboratoires, la disponibilité ajustée est la plus pertinente mais pour les centres de calcul, ainsi que pour le sous-groupe Cisco CallManager, les deux valeurs de la disponibilité – brute et ajustée – sont soigneusement calculées.

Cette évaluation permet d'inciter les ingénieurs réseaux à adopter une attitude optimale : le simple rechargement d'un commutateur, par exemple, permet d'effectuer des mises à jour du code dans les réseaux d'ordinateurs de bureau. Ce processus est le plus économique en termes de main d'œuvre et n'a pas d'incidence sur la disponibilité ajustée qui est la plus pertinente pour ce type de réseaux. Les mises à niveau de code dans les réseaux des centres de calcul passent par des procédures de haute disponibilité afin de minimiser leur impact sur la disponibilité brute, qui est la plus pertinente pour les centres de calcul, mais entraînent un plus gros investissement en termes de main d'œuvre.

Processus de gestion des changements

Le plus difficile et en même temps le plus important dans cette stratégie est de déterminer les interruptions de service prévues. Si le processus était manuel, il permettrait les tricheries. Pour éliminer cette possibilité, Cisco a intégré son processus de gestion des changements aux mesures de la disponibilité.

Les règles fondamentales du processus de gestion des changements sur le réseau Cisco IT-LAN-SJ sont les suivantes :

- les demandes de gestion des changements doivent être soumises avant le début des interruptions de service correspondantes ;
- ces demandes doivent préciser le moment où ces changements interviendront ainsi que toutes les unités qui seront affectées ;
- les demandes doivent être systématiquement approuvées par la direction ;
- les utilisateurs doivent être avertis en conséquence ;
- tous les changements dans l'urgence pour lesquels il est impossible de prévenir les utilisateurs suffisamment à l'avance doivent être approuvés par le responsable opérationnel compétent.

La plupart des changements s'effectue en dehors des heures normales de travail et les approbations sont le plus souvent accordées au cours de la réunion quotidienne spécifique qui se tient en général à 08h00, heure du Pacifique. Les changements qui ont une incidence lourde – comme une interruption de service dans les centres de calcul – sont refusés lorsqu'ils ne sont pas prévus suffisamment à l'avance.

Note : Pour le calcul de la disponibilité ajustée, toute unité considérée comme « touchée » par une décision de gestion du changement est considérée comme pleinement opérationnelle pendant la durée d'intervention.

Interruptions de service évitables et inévitables

La disponibilité ajustée mesure le niveau de service fourni aux utilisateurs. Parallèlement à cette disponibilité, Cisco IT-LAN-SJ classe les interruptions de services en deux catégories : évitables et inévitables. Voici quelques exemples d'interruptions inévitables :

- les pannes de courant,
- les catastrophes naturelles (dans la zone touchée).

Par défaut, toutes les interruptions de service sont considérées comme évitables. Voici quelques exemples d'interruptions de services évitables :

- les pannes matérielles,
- les pannes logicielles,
- les erreurs humaines,
- les défaillances de processus,
- les attaques par saturation,
- les interruptions de service d'origine inconnue,
- les catastrophes naturelles (en aval de la catastrophe, là où une redondance aurait dû être fournie).

Le classement d'une interruption de service dans l'une de ces catégories permet d'identifier les problèmes qui peuvent être prévenus à l'avenir et donne à la direction un meilleur point de vue pour l'examen des principales interruptions. Évitable ou non, lorsqu'une interruption n'a pas été planifiée, elle affecte aussi bien la disponibilité brute qu'ajustée en raison de son incidence sur le service.

Disponibilité de Cisco IT-LAN-SJ- Production en 2002

Les résultats suivants montrent les différences entre les disponibilités ajustées et brutes dans chaque sous-groupe.

Résultats 2002 par sous-groupe

Sous-groupe	Ajustée	Brute
Générale	99,992 %	99,964 %
DDC4	99,998 %	99,964 %
Réseau CallManager	99,998 %	99,967 %
PDC1	99,997 %	99,995 %
DDC5	99,997 %	99,997 %
PDC2	99,996 %	99,991 %
Ordinateurs du site 5	99,995 %	99,992 %
DDC1	99,995 %	99,878 %
Ordinateurs des sites 1 à 3	99,993 %	99,966 %
DDC3	99,992 %	99,909 %
Ordinateurs du réseau MAN	99,991 %	99,969 %
DDC2	99,991 %	99,912 %
Ordinateurs du site 4	99,991 %	99,947 %
Grappe laboratoire	99,973 %	99,943 %

Résultats globaux mois par mois

Mois	Ajustée	Brute
Janvier	99,998 %	99,991 %
Février	99,985 %	99,950 %
Mars	99,994 %	99,989 %
Avril	99,992 %	99,992 %
Mai	99,994 %	99,991 %
Juin	99,987 %	99,978 %
Juillet	99,999 %	99,880 %
Août	99,999 %	99,984 %
Septembre	99,998 %	99,984 %
Octobre	99,995 %	99,994 %
Novembre	99,997 %	99,948 %

Décembre	99,970 %	99,892 %
----------	----------	----------

Les cinq principales interruptions de service non planifiées

Date	Disponibilité ajustée quotidienne	Description de l'interruption
19 décembre 2002	99,618 %	Panne de courant imprévue sur les sites 3 et 4
20 décembre 2002	99,644 %	Panne de courant importante dans le bâtiment 13
21 février 2002	99,747 %	Interruption dans DDC2 et DDC3 en raison d'une panne matérielle
28 juin 2002	99,764 %	Mises à niveau simultanées ayant entraîné une instabilité de routage
23 avril 2003	99,880 %	Panne de courant à Senter Road

Analyse des cinq principales interruptions de service non planifiées

19 décembre 2002, panne de courant imprévue sur les sites 3 et 4 – San Jose a connu une panne d'alimentation électrique de grande ampleur qui a touché près de 25 bâtiments Cisco pendant près de 3 heures. Bien que les centres de calcul de Cisco soient tous équipés d'onduleurs et de générateurs de secours, les équipements des réseaux d'ordinateurs de bureau sont assez souvent alimentés par le secteur, sans onduleur ou avec onduleur seul. Cette panne d'électricité, principal incident de disponibilité pour 2002, a été considérée comme inévitable par Cisco IT- LAN-SJ. Malgré ce classement, elle a été comptabilisée dans les statistiques de disponibilité ajustée en raison de son incidence sur le niveau de service fourni à nos utilisateurs.

20 décembre 2002, panne de courant importante dans le bâtiment 13 – au début de la matinée, une surtension brève mais importante sur le site 4 de San Jose a entraîné une défaillance des équipements électriques du bâtiment 13, privant d'électricité l'ensemble du bâtiment pendant presque toute la journée. Bien que cette interruption ait été inévitable du point de vue du service informatique, elle a été comptabilisée dans les statistiques de disponibilité ajustée, en raison de son incidence sur le niveau de service fourni à nos utilisateurs.

21 février 2002, interruption dans DDC2 et DDC3 en raison d'une défaillance matérielle – un routeur du centre de calcul Développement 3 est tombé en panne sans que l'unité redondante puisse prendre le relais en raison d'une erreur de conception des deux centres de calculs qui étaient tous deux liés dans une configuration hiérarchique incompatible à ce moment. L'interruption de service a été classée comme évitable. La séparation physique et logique des centres de calculs et la refonte des réseaux correspondants conformément à la nouvelle architecture normalisée Cisco pour centres de calcul ont permis de corriger l'erreur de conception.

28 juin 2002, des mises à niveau simultanées ont entraîné une instabilité de routage – une erreur de processus est à l'origine de cette interruption de service évitable : deux ingénieurs du réseau Cisco IT-LAN-SJ ont simultanément effectué des demandes de changement pour la mise à niveau d'unités sur deux couches différentes de la hiérarchie de réseau. Bien que les deux demandes de changement ait été accompagnées de notification par courrier électronique à l'équipe, personne ne s'est aperçu que les deux modifications seraient réalisées en même temps. La mise à niveau simultanée a entraîné une

instabilité du réseau. L'incident a été considéré comme évitable parce qu'il a été causé par une erreur de processus.

23 avril 2002, panne de courant à Senter Road – cette interruption de service inévitable a été occasionnée par une panne de courant sur le site de Senter Road qui abrite le réseau métropolitain (MAN) de San Jose.

Les cinq principales interruptions de services planifiées

Date	Disponibilité brute quotidienne	Description des changements
13 juillet 2002	96,497 %	Travaux électriques et refonte de l'architecture réseau
7 décembre 2002	97,850 %	Travaux électriques dans trois bâtiments
2 novembre 2002	99,167 %	Coupure d'électricité planifiée dans le bâtiment 8
16 février 2002	99,460 %	Coupure d'électricité planifiée à Silvercreek
16 novembre 2002	99,507 %	Coupure d'électricité planifiée dans le bâtiment 2

Analyse des cinq principales interruptions de service planifiées

13 juillet 2002, travaux électriques et refonte de l'architecture réseau – L'équipe locale avait besoin de couper le courant pendant une durée prolongée dans le DDC1 afin d'accroître la capacité électrique de l'installation. L'équipe réseau a profité de cette coupure pour rebâtir le réseau du centre de calcul et le mettre en conformité avec notre architecture standard de centre de calcul.

7 décembre 2002, travaux électriques dans trois bâtiments – L'équipe locale avait besoin de couper le courant dans trois bâtiments. L'équipe réseau a profité de cette coupure pour rebâtir les réseaux des centres de calcul Développement de ces bâtiments et de les mettre en conformité avec notre architecture standard de centre de calcul. Cette interruption a notamment permis de résoudre « à long terme » le problème à l'origine de la panne de réseau imprévue du 21 février dans les centres DDC2 et DDC3.

2 novembre 2002, Coupure de courant planifiée dans le bâtiment 8 – L'équipe locale avait besoin de couper le courant dans l'ensemble du bâtiment 8.

samedi 16 février 2002, Coupure de courant planifiée à Silvercreek – L'équipe locale avait besoin de couper le courant sur l'ensemble du site du réseau métropolitain de Silvercreek.

samedi 16 novembre 2002, Coupure de courant planifiée dans le bâtiment 2 – L'équipe locale avait besoin de couper le courant dans l'ensemble du bâtiment 2.

En résumé

Dans l'ensemble, Cisco a atteint une disponibilité ajustée de 99,992 % sur le réseau local de San Jose en 2002, bien que trois des cinq interruptions les plus graves aient été provoquées par des coupures de courant incontrôlables. Par ailleurs, les réseaux des centres DDC 1 à 3 et des laboratoires ont été considérablement améliorés au cours de l'année ce qui devrait se traduire par une nette progression de la disponibilité en 2003.

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

Dans la suite de cet article, nous présentons des recommandations qui, sur la base de l'expérience du réseau Cisco IT-LAN-SJ, permettent d'atteindre une disponibilité de 99,9 %, de 99,99 % et de 99,999 %. Bien que les résultats puissent varier, le réseau Cisco IT-LAN-SJ a constaté l'efficacité des étapes suivantes sur l'amélioration de la disponibilité.

Cisco IT a mis en œuvre la plupart de ces recommandations, mais leur implantation systématique dans tous les secteurs ne se justifie pas toujours d'un point de vue économique. Il est essentiel de déterminer les parties du réseau qui sont les plus critiques et pour lesquelles la haute disponibilité est indispensable.

Pour atteindre une disponibilité de 99,999 %, par exemple, toutes les unités doivent être protégées par des onduleurs et des générateurs de secours. Devant le coût d'un tel projet, le département informatique de Cisco a choisi de réserver ces équipements à ses centres de calcul. Les réseaux des ordinateurs de bureau et des laboratoires n'en sont pas dotés.

Le lecteur trouvera à la fin de ce document la liste des recommandations adoptées par Cisco sur chacune des sections de son réseau de San Jose.

Les étapes Cisco pour une disponibilité de 99,9 %

Etape 1 : Mesure de la disponibilité

La première étape à suivre pour réaliser des temps de fonctionnement optimaux consiste à surveiller et à mesurer la disponibilité en continu. La mesure de la disponibilité ne doit pas être perçue comme un outil statistique occasionnel pour la gestion, mais plutôt comme un moyen d'améliorer la fourniture de service. Ces mesures peuvent être utilisées pour identifier et corriger, de manière stratégique, les causes des interruptions de service majeures, et de manière tactique, celles des petites interruptions localisées.

Utilisation stratégique des mesures de disponibilité

Les rapports de disponibilité mensuelle, trimestrielle et annuelle sont générés par un ingénieur réseau principal. Ils permettent d'attirer notre attention sur la disponibilité du service et de mettre en évidence les réussites comme les secteurs qui doivent être tous les deux améliorés. Voici le rapport de disponibilité de novembre 2002 :

Date : Lun 2 déc. 2002 15:53:23 US/Pacific

Objet : Rapport de disponibilité de novembre 2002 pour le réseau IT-LAN-SJ

Rapport de disponibilité de novembre 2002 pour le réseau IT-LAN-SJ

Disponibilité ajustée : 99,997 %

Disponibilité brute : 99,948 %

<i>Sous-groupe</i>	<i>Ajustée</i>	<i>Brute</i>
DDC1	99,984 %	99,984 %
Réseau MAN	99,988 %	99,988 %
Site 4	99,998 %	99,887 %
CM	99,998 %	99,886 %
Sites 1 à 3	99,999 %	99,999 %
Site 5	99,999 %	99,999 %
Labos	99,999 %	99,963 %
DDC4	100,000 %	99,599 %
DDC2	100,000 %	100,000 %
DDC5	100,000 %	100,000 %
DDC3	100,000 %	100,000 %
PDC2	100,000 %	100,000 %
PDC1	100,000 %	99,994 %

Principales interruptions de services non planifiées :

23 nov. :	99,949 %	Panne de courant DDC1 / défaillance onduleur
9 nov. :	99,981 %	Panne de courant à Scotts Valley
24 nov. :	99,988 %	Panne de courant sur les sites 1 à 4
28 nov. :	99,997 %	Problème mineur d'origine inconnue

Principales interruptions de services planifiées :

2 nov. :	99,167 %	Coupage d'électricité planifiée dans le bâtiment 8
16 nov. :	99,507 %	Coupage d'électricité planifiée dans le bâtiment 2

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

24 nov. :	99,902 %	Coupure d'électricité planifiée dans le bâtiment 5
21 nov. :	99,922 %	Refonte de l'architecture de DDC4 et du laboratoire du bâtiment 12

COMMENTAIRE : Sauf en ce qui concerne la panne d'origine inconnue du 28 novembre, qui a ramené la disponibilité à 99,997 %, toutes les interruptions de service ont été identifiées, expliquées et considérées comme incontrôlables par l'équipe du réseau IT-LAN-SJ. En l'absence de ces interruptions incontrôlables, la disponibilité aurait été de 100,000 %. Par ailleurs, la haute disponibilité de la grappe du laboratoire découle directement de la refonte de l'architecture de son réseau. Il est à noter que, grâce au travail de l'équipe de déploiement dans ce secteur, la grappe du laboratoire atteint une disponibilité de 99,999 % et dépasse la disponibilité du réseau de production.

Rapport

Ce rapport présente les résultats d'ensemble du groupe de disponibilité Cisco IT- LAN-SJ-Production. Les rapports trimestriels sont transmis à la direction générale pour lui permettre de déterminer les secteurs qui respectent les accords de niveau de service et ceux qui ont des difficultés.

Ces rapports se composent de plusieurs sections comme le montre l'exemple ci-dessous :

Récapitulatif d'ensemble

Rapport de disponibilité de novembre 2002 pour le réseau IT-LAN-SJ

Disponibilité ajustée : 99,997 %

Disponibilité brute : 99,948 %

Récapitulatif par sous-groupe

Sous-groupe	Ajustée	Brute
DDC1	99,984 %	99,984 %
Réseau MAN	99,988 %	99,988 %
Site 4	99,998 %	99,887 %
CM	99,998 %	99,886 %
Sites 1 à 3	99,999 %	99,999 %
Site 5	99,999 %	99,999 %
Labos	99,999 %	99,963 %
DDC4	100,000 %	99,599 %
DDC2	100,000 %	100,000 %
DDC5	100,000 %	100,000 %
DDC3	100,000 %	100,000 %
PDC2	100,000 %	100,000 %
PDC1	100,000 %	99,994 %

Principales interruptions de service non planifiées

23 nov. :	99,949 %	Panne de courant DDC1 / défaillance onduleur
9 nov. :	99,981 %	Panne de courant à Scotts Valley
24 nov. :	99,988 %	Panne de courant sur les sites 1 à 4
28 nov. :	99,997 %	Problème mineur d'origine inconnue

Cette section présente les interruptions de service non planifiées qui, sur le mois écoulé, ont eu la plus forte incidence sur la disponibilité ajustée. Pour montrer clairement l'incidence de chaque interruption, il présente également la disponibilité ajustée du jour en question pour le groupe Cisco IT-LAN-SJ-Production. La disponibilité de 99,949 % du 23 novembre correspond à une indisponibilité de 0,051 %. La disponibilité de 99,997 % du 28 novembre correspond à une indisponibilité de 0,003 %. Dans ce cas, la panne de courant du 23 novembre dans le centre DDC1 a eu un effet 17 fois plus

important sur les utilisateurs du réseau que le « problème mineur d'origine inconnue » du 28 novembre.

Principales interruptions de services planifiées

2 nov. :	99,167 %	Coupure d'électricité planifiée dans le bâtiment 8
16 nov. :	99,507 %	Coupure d'électricité planifiée dans le bâtiment 2
24 nov. :	99,902 %	Coupure d'électricité planifiée dans le bâtiment 5
21 nov. :	99,922 %	Refonte de l'architecture de DDC4 et du laboratoire du bâtiment 12

Cette section présente la liste des demandes de changement approuvées qui ont eu la plus forte incidence sur la disponibilité brute. Pour mettre les chiffres en perspective, le rapport donne également les statistiques de disponibilité brute du réseau Cisco IT- LAN-SJ-Production pour le jour concerné. Ici, les trois plus importantes interruptions de service planifiées étaient dues aux travaux électriques dans trois bâtiments. De plus, la refonte de l'architecture du centre DDC4 et celle du réseau du laboratoire du bâtiment 12 le 21 novembre correspondent à deux changements distincts.

COMMENTAIRE : Sauf en ce qui concerne la panne d'origine inconnue du 28 novembre, qui a ramené la disponibilité à 99,997 %, toutes les interruptions de service ont été identifiées, expliquées et considérées comme incontrôlables par l'équipe du réseau IT-LAN-SJ. En l'absence de ces interruptions incontrôlables, la disponibilité aurait été de 100,000 %. Par ailleurs, la haute disponibilité de la grappe du laboratoire découle directement de la refonte de l'architecture de son réseau. Il est à noter que, grâce au travail de l'équipe de déploiement dans ce secteur, la grappe du laboratoire atteint une disponibilité de 99,999 % et dépasse la disponibilité du réseau de production.

La section « commentaires » indique si l'équipe réseau aurait été en mesure d'éviter les interruptions non planifiées. Toute interruption est considérée comme évitable lorsque son origine est inconnue, comme le problème du 28 novembre. Ces commentaires sont également l'occasion de présenter les réussites de l'équipe. Dans le cas présent, la refonte récente de l'architecture du réseau du laboratoire a directement permis d'atteindre une disponibilité de 99,999 % pour ce sous-groupe. En mettant en évidence ces réussites dans un rapport à haute visibilité destiné à la direction, on appuie de manière forte les actions qui améliorent la disponibilité.

Utilisation tactique des mesures de disponibilité

En plus d'établir la mesure stratégique du niveau de service, les statistiques de disponibilité sont également un outil pour l'amélioration du service fourni aux clients. Les atteintes à la disponibilité des unités individuelles doivent être identifiées et analysées. Pour cela, l'équipe du réseau Cisco IT- LAN-SJ reçoit par courrier électronique une liste quotidienne de toutes les unités qui n'ont pas atteint une disponibilité ajustée de 100 % au cours de la semaine écoulée. Voici un extrait d'un tel rapport :

Groupe ou sous-groupe : IT-LAN-SJ-Production / DDC4

Objectif de disponibilité : 99,985, Objectif analytique de disponibilité : 99,999

Ressource	Date UTC analytique	Disponibilité ajustée	Disponibilité brute	Secteur	Indisponibilité (en minutes)
ddc4-row3-sw1.cisco.com	27-MAR-2003	99,973	99,973	IS-HQ HQ	0
ddc4-row3-sw1.cisco.com	29-MAR-2003	99,975	99,975	IS-HQ HQ	0
ddc4-row5-sw1.cisco.com	29-MAR-2003	99,975	99,975	IS-HQ HQ	0
ddc4-row1-sw1.cisco.com	30-MAR-2003	99,975	99,975	IS-HQ HQ	0
ddc4-row11-sw1.cisco.com	30-MAR-2003	99,977	99,977	IS-HQ HQ	0
ddc4-row2-sw1.cisco.com	30-MAR-2003	99,977	99,977	IS-HQ HQ	0
ddc4-row3-sw1.cisco.com	30-MAR-2003	99,975	99,975	IS-HQ HQ	0

ddc4-row5-sw1.cisco.com	30-MAR-2003	99,975	99,975	IS-HQ HQ	0
ddc4-row11-sw1.cisco.com	31-MAR-2003	99,977	99,977	IS-HQ HQ	0

Ce rapport indique quelles sont les unités qui n'ont pas atteint l'« objectif analytique de disponibilité » à la date en question. Pour éviter d'obtenir des rapports trop longs et donc inexploitable, Cisco IT-LAN-SJ a commencé à donner une valeur faible – 99 %, en l'occurrence – à cet « objectif analytique de disponibilité ». A mesure que les problèmes trouvaient des solutions, l'objectif analytique de disponibilité a été progressivement relevé. Sur la base d'une sollicitation toutes les 15 à 20 secondes, les chiffres de ce rapport de disponibilité – qui vont de 99,973 à 99,977 % – représentent un échec de tentative sur chacune des unités de la liste.

Etape 2 : Alertes d'interruption de service

La communication est un facteur critique de la haute disponibilité et les interruptions de service doivent être signalées en temps réel à l'équipe d'assistance technique. Pour que celle-ci puisse réagir de manière appropriée, un niveau de priorité a été attribué à chaque unité du réseau Cisco IT-LAN-SJ. En voici la liste :

- Priorité 1 : les grands commutateurs de couche d'accès lorsqu'il n'existe pas de possibilité de redondance car les clients se connectent directement au commutateur ou à la passerelle du laboratoire qui ne sont pas doublés.
- Priorité 2 : les routeurs avec redondance et les petits commutateurs de couche d'accès.
- Priorité 3 : les réseaux de gestion hors bande et les autres réseaux d'assistance.
- Priorité 4 : les points d'accès sans fil.

Toutes les unités du groupe de disponibilité Production sont de type (P1) ou (P2). Le centre de commande opérationnel ou OCC (Operations Command Center) surveille les unités P1 24 heures par jour, tous les jours et les unités P2 pendant les heures d'ouverture. Dès qu'une unité est hors service pendant plus de 2 minutes, l'alerte d'interruption est déclenchée. Sur les horaires définis ci-dessus, les problèmes sont gérés par l'OCC qui avertit par messagerie le personnel de service et transmet l'information à la direction.

Les pannes sur les unités de Priorité 1 à 3 sont signalées au personnel de service 24 heures par jour, tous les jours, bien que celui-ci puisse décider de ne pas intervenir immédiatement sur les unités de type P3.

Les problèmes des unités de Priorité 4 sont signalés au personnel de service pendant les heures de d'ouverture.

L'OCC détecte les interruptions du service réseau qui touchent le système de surveillance et d'alerte. Dans ces circonstances, le système de téléphonie IP, protégé par la téléphonie SRST (Survivable Remote Site Telephony), permet à l'OCC de prévenir manuellement le personnel compétent.

Etape 3 : Hiérarchie physique

Pour atteindre une disponibilité de 99,9 %, Cisco avait besoin d'un réseau fondamentalement stable, ce qui sous-entend une double hiérarchie physique et logique.

Agencement physique d'un bâtiment du campus de San Jose

Les réseaux des bâtiments de Cisco sont constitués de répartiteurs IDF, LDF, SDF et BDF et d'un centre NOC (voir les définitions ci-dessous). Les paragraphes suivants décrivent l'agencement physique des bâtiments du campus de San Jose afin de présenter clairement la mise en œuvre de cette hiérarchie physique.

Intermediary Distribution Frame (IDF) – Les bâtiments du campus de San Jose ont généralement entre deux et cinq étages. Chaque étage comprend deux répartiteurs intermédiaires ou IDF avec des câbles de catégorie 5 (Cat5) reliant chaque plaque murale à l'un des répartiteurs. Un petit nombre de

pièces, notamment les plaques murales des téléphones dans les espaces publics, sont équipées de câbles de catégorie 3 (Cat3). L'installation de deux IDF permet de limiter à moins de 100 mètres la longueur du câblage et de respecter ainsi les spécifications Cat5. Sur la base de deux répartiteurs intermédiaires par étage, chaque bâtiment contient ainsi de quatre à dix IDF. Les câbles qui relient chacun d'eux au répartiteur de bâtiment ou BDF (Building Distribution Frame) présentent les caractéristiques suivantes :

- câble en cuivre Cat5 (essentiellement utilisé pour les consoles) ;
- fibre multimode ;
- fibre monomode.

Certains bâtiments plus anciens sont encore équipés de câblage de type Télécom mais celui-ci n'est plus utilisé depuis que Cisco a achevé la migration complète vers la téléphonie IP. Les bâtiments les plus récents du campus de San Jose ont été construits sans ce type de câblage.

Lab Distribution Frame (LDF) – le câblage structuré du BDF vers le laboratoire aboutit à un répartiteur de laboratoire ou LDF. Les câbles qui relient ces LDF au répartiteur de bâtiment présentent les caractéristiques suivantes :

- câblage cuivre Cat5 (sur une distance qui peut parfois dépasser 100 mètres) ;
- fibre multimode.

Certains laboratoires peuvent également être équipés de fibre monomode. Comme les IDF, tous les LDF doivent disposer d'un câblage structuré en direction du BDF pour appliquer la hiérarchie physique.

Building Distribution Frame (BDF) – Le répartiteur de bâtiment ou BDF est le point d'agrégation de tous les réseaux d'un bâtiment, à l'exception du répartiteur SDF. A San Jose, la plupart des BDF sont installés au deuxième étage, et au premier dans certains bâtiments anciens. Le câblage structuré de tous les répartiteurs IDF et LDF de chaque bâtiment aboutit au BDF. Par ailleurs, le BDF est relié aux centres d'exploitation de réseaux ou NOC (Network Operations Center) du campus par le câblage structuré suivant :

- fibre multimode ;
- fibre monomode.

Si un NOC est installé dans le même bâtiment qu'un BDF, tout le câblage structuré est dirigé vers ce NOC avec, si nécessaire, un maillage vers d'autres NOC. Si le NOC n'est pas installé dans le bâtiment du BDF, le câblage structuré est directement dirigé du BDF vers deux NOC distincts du campus. La seule exception à cette règle est lorsque le campus ne possède qu'un seul NOC.

Armoire de zone pour centre de calcul – Les centres de calcul Cisco contiennent des serveurs de calcul généralement organisés en rangées de racks. La plupart des centres de calcul Cisco sont équipés d'une armoire de zone à l'extrémité de chaque rangée ; cette armoire contient un commutateur de couche d'accès et un serveur console. Le câblage structuré entre chaque rack de serveur et l'armoire de zone est composé de câbles Cat5 et de fibres multimodes. Le câblage structuré entre l'armoire de zone et le répartiteur SDF (Server Distribution Frame) est également composé de câbles Cat5 et de fibres multimodes.

Server Distribution Frame (SDF) – Les bâtiments qui hébergent des centres de calcul sont desservis par un répartiteur de serveurs ou SDF. Chaque SDF est installé dans un bâtiment contenant un NOC. Le câblage structuré qui sort des armoires de zone des centres de calcul aboutit sur le répartiteur SDF. Le répartiteur SDF est relié au NOC du bâtiment par un câblage structuré et à un autre NOC par des fibres individuelles, pour des raisons de redondance. Le répartiteur SDF héberge le plus souvent des passerelles de centres de calcul, des serveurs consoles et des unités de commutation de contenus.

Network Operations Center (NOC) – Le centre d'exploitation de réseaux ou NOC est un point d'agrégation physique des équipements de réseau et du câblage structuré. Pour les besoins de l'agrégation de réseau, le réseau LAN du campus de San Jose est subdivisé en plusieurs sites dont voici la liste :

- Sites 1 à 3 (bâtiments A à P) ;
- Site 4 (bâtiments 1 à 19) ;
- Site 5 (bâtiments 20 à 25).

Les sites 1 à 3 disposent de quatre NOC. Le site 4 possède également quatre NOC. Conformément aux recommandations de l'analyse coûts – risques – bénéfices réalisée au moment de sa construction, le site 5 dispose d'un seul NOC.

Note : Cisco envisage de ne poser que des fibres monomodes pour ses nouvelles installations. Le principal obstacle est représenté par les hôtes des centres de calcul équipés de cartes NIC (Network Interface Card) qui nécessitent des fibres multimodes.

La hiérarchie physique du câblage structuré de San Jose

Le câblage structuré du campus de Cisco à San Jose suit un modèle hiérarchique du type cœur de réseau / distribution / accès. Le cœur du réseau est constitué d'un ensemble de neuf NOC. Les répartiteurs de bâtiments (BDF) et de serveurs (SDF) forment la couche de distribution de la hiérarchie physique du réseau, tandis que les répartiteurs intermédiaires (IDF) et de laboratoires (LDF) ainsi que les armoires de zone des centres de calcul réalisent la couche d'accès.

Cisco conçoit et implante ses réseaux selon une hiérarchie physique. Cette stratégie incite nos ingénieurs à déployer des réseaux hiérarchiques en les rendant plus faciles à réaliser.

Par ailleurs, un réseau hiérarchique développé sur une disposition hiérarchique de câblage structuré simplifie le raccordement des fibres en limitant le nombre de liaisons entre les unités de réseau, ce qui améliore la fiabilité et facilite la résolution des problèmes.

La hiérarchie physique du réseau de San Jose

Les niveaux hiérarchiques qui constituent le réseau de San Jose sont une approximation du modèle cœur de réseau / distribution / accès classique. Ils sont présentés ici depuis la périphérie vers le cœur de réseau :

- **les commutateurs de couche d'accès** – Les utilisateurs connectent leurs postes de travail directement aux commutateurs de couche d'accès. Le département informatique de Cisco IT utilise principalement des commutateurs de la gamme Cisco 6500 qui exécutent le système d'exploitation Cisco Catalyst OS. Ils sont remplacés par des commutateurs Cisco Catalyst® 3550-24 PWR dans certains secteurs à faible densité de ports. Les déploiements les plus anciens sont équipés de commutateurs Cisco Catalyst 3524 XL ;

- **les passerelles de couche d'accès** – Chaque commutateur de couche d'accès se connecte directement à une paire de passerelles de couche d'accès. Celles-ci consistent généralement en des commutateurs de la gamme Cisco 6500 ou des routeurs de la gamme 7600 qui exécutent la plateforme logicielle native Cisco IOS®. Chaque bâtiment contient une paire de passerelles de couche d'accès au réseau des ordinateurs de bureau, qui sont également appelées passerelles BDF. De plus, certains bâtiments disposent de paires supplémentaires de ces passerelles qui gèrent des fonctions spécialisées. Dans les bâtiments des centres de calcul, par exemple, le répartiteur SDF est doté d'une paire distincte de passerelles pour centre de calculs ;

- **les passerelles de groupe** – Chaque groupement de 6 à 12 paires de passerelles de couche d'accès est agrégé en amont sur une paire de passerelles de groupe. Celles-ci sont séparées par fonction : les passerelles de couche d'accès des ordinateurs de bureau sont agrégées sur une passerelle de groupe, et les passerelles de centres de calcul sont agrégées sur l'autre passerelle de groupe. Ces passerelles de

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

groupes sont le plus souvent des commutateurs de la gamme Cisco 6500 ou des routeurs de la gamme 7600 qui exécutent la plate-forme logicielle native Cisco IOS® ;

• **le réseau fédérateur de site** – Du point de vue de la topologie de réseau, le campus de San Jose se compose de quatre sites :

- les Sites 1 à 3 (un seul site du point de vue de la topologie de réseau) ;
- le Site 4 ;
- le Site 5 ;
- le réseau MAN.

Chaque site dispose d'une paire de routeurs dorsaux qui sont le plus souvent des commutateurs de la gamme Cisco 6500 ou des routeurs de la gamme 7600 qui exécutent la plate-forme logicielle native Cisco IOS®. L'essentiel de la connectivité des routeurs dorsaux du réseau MAN repose sur des modules FlexWAN et non Gigabit Ethernet ;

• **le réseau fédérateur régional** – Le campus de San Jose utilise six routeurs de la gamme Cisco 6500 qui exécutent la plate-forme logicielle native Cisco IOS pour constituer un réseau fédérateur régional. Les quatre fédérateurs de sites se connectent au réseau fédérateur régional. Ce réseau régional se connecte à son tour aux pare-feu d'entreprise qui mènent à la zone démilitarisée (DMZ) ainsi qu'au réseau WAN de Cisco.

Résumé de la hiérarchie physique

Pour atteindre une disponibilité égale ou supérieure à 99,9 %, le réseau doit être fondamentalement stable avec une hiérarchie physique bien définie. Ceci évite que les extensions de réseau finissent par engendrer une topologie chaotique avec une redondance excessive en certains endroits – qui accroît la complexité du routage – et insuffisante dans d'autres. Une hiérarchie physique bien définie permet d'ajuster au plus près les besoins de redondance et garantit la stabilité fondamentale du réseau.

De plus, la hiérarchie physique est un pré-requis de la hiérarchie logique, laquelle est absolument vitale au maintien de la stabilité du routage.

Etape 4 : Hiérarchie logique

Parallèlement à la hiérarchie physique, la hiérarchie logique pose les fondations d'un réseau fondamentalement stable. La base de données de gestion des adresses du réseau mondial de Cisco recense plus de 23 000 sous-réseaux. Bien que le protocole BGP (Border Gateway Protocol) puisse gérer sans difficulté une table de routage aussi volumineuse, ce n'est pas le cas des protocoles IGP qui favorisent la rapidité de la convergence au détriment de l'évolutivité. La gestion d'une table de routage de 23 000 entrées entraînerait l'instabilité du réseau quels que soient les protocoles IGP (EIGRP, OSPF ou IS-IS).

Une hiérarchie logique permet de réduire la taille de la table de routage. Cette hiérarchie s'appuie sur trois composantes :

1. une hiérarchie physique (voir ci-dessus) ;
2. l'assignation hiérarchique de l'espace d'adressage pour qu'il s'aligne sur la hiérarchie physique ;
3. les résumés de routes qui permettent de profiter de l'allocation hiérarchique de l'espace d'adressage.

Adresses routables Internet et adresses RFC1918

La nécessité de disposer de deux types distincts d'espaces d'adresses accroît encore la complexité de la hiérarchie de l'espace d'adressage. L'espace des adresses routables par Internet est utilisé par les postes de travail des utilisateurs car ceux-ci accèdent à Internet dans le cadre normal de leurs activités professionnelles. En raison de la pénurie globale d'adresses IP avec le protocole IPv4, il est nécessaire d'utiliser l'espace d'adressage RFC1918 chaque fois que possible. Cisco utilise l'espace d'adressage RFC1918 pour la téléphonie IP, la gestion hors bande et la plupart de ses réseaux de laboratoire.

Exemple de hiérarchie d'adressage pour le Site 4

Espace d'adressage RFC1918 pour la téléphonie IP du site

10.16.0.0/17	Téléphonie IP – Site 4
– 10.16.0.0/19	Site 4, Groupe d'ordinateurs de bureau A, Téléphonie IP (Bâtiments 1 à 7)
– 10.16.32.0/19	Site 4, Groupe d'ordinateurs de bureau B, Téléphonie IP (Bâtiments 8 à 12)
– 10.16.64.0/19	Site 4, Groupe d'ordinateurs de bureau C, Téléphonie IP (Bâtiments 13 à 19)
– 10.16.96.0/21	Site 4, Groupe d'ordinateurs de bureau A, Téléphonie IP (Bâtiments 1 à 7)
– 10.16.104.0/22	Site 4, Groupe d'ordinateurs de bureau B, Téléphonie IP (Bâtiments 8 à 12)
– 10.16.108.0/22	Site 4, Groupe d'ordinateurs de bureau C, Téléphonie IP (Bâtiments 13 à 19)
– 10.16.112.0/20	Site 4, Groupe d'ordinateurs de bureau C, Téléphonie IP (Bâtiments 13 à 19)

Les allocations d'adresses ci-dessus sont bonnes mais laissent à désirer. Bien que l'intégralité de l'espace d'adressage pour la téléphonie IP puisse se résumer à une unique notification de routage depuis le fédérateur du site 4 vers le fédérateur régional, la réduction d'adresses à l'intérieur du site 4 est imparfaite. Par exemple, l'espace d'adressage pour la téléphonie IP du Groupe d'ordinateurs de bureau A peut être réduite à deux notifications de routage : 10.16.0.0/19 et 10.16.96.0/21. Ceci est très bien, mais une notification unique serait mieux.

Au sein de chaque groupe d'ordinateurs de bureau, l'espace d'adressage peut être attribuée de manière hiérarchique jusqu'au niveau du bâtiment :

10.16.0.0/19	Site 4, Phase A, Téléphonie IP (Bâtiments 1 à 7)
– 10.16.0.0/22	SJC01 Téléphonie IP (Etages 2 et 3)
– 10.16.4.0/24	SJC01 Téléphonie IP (Etage 1)
– 10.16.5.0/24	SJC02 Téléphonie IP (Etage 1)
– 10.16.6.0/23	SJC02 Téléphonie IP (Etage 2)
– 10.16.8.0/23	SJC02 Téléphonie IP (Etage 3)
– 10.16.10.0/23	SJC03 Téléphonie IP (Etage 2)
– 10.16.12.0/22	SJC03 Téléphonie IP (Etages 3 et 4)
– 10.16.16.0/24	SJC03 Téléphonie IP (Etage 1)
– 10.16.17.0/24	SJC04 Téléphonie IP (Etage 1)
– 10.16.18.0/23	SJC04 Téléphonie IP (Etage 2)
– 10.16.20.0/23	SJC04 Téléphonie IP (Etage 3)
– 10.16.22.0/23	SJC05 Téléphonie IP (Etage 2)
– 10.16.24.0/23	SJC05 Téléphonie IP (Etage 3)

– 10.16.26.0/24	SJC05 Téléphonie IP (Etage 1)
– 10.16.27.0/24	SJC06 Téléphonie IP (Etage 1)
– 10.16.28.0/22	SJC06 Téléphonie IP (Etages 2 et 3)

Cette allocation d'adresses n'est toujours pas parfaite mais elle permet la réduction d'un grand nombre de notifications de routes au niveau du bâtiment. L'équipe topologique du département informatique Cisco a choisi de réduire les adresses au niveau des couches de groupe et de fédérateurs de site de la hiérarchie physique plutôt qu'à celui des passerelles de couche d'accès car chaque réduction accroît la complexité.

Une telle réduction est suffisante pour garantir une excellente stabilité de routage. L'allocation de blocs d'adresses pour la réduction au niveau de chaque bâtiment permet en revanche de prévoir les adressages futurs.

Espace des adresses routables pour le Site

171.71.0.0/16	(Site 4 : Bâtiments 1 à 19)
– 171.71.0.0/24	Liens de réseau WAN point à point pour l'ingénierie (Site 4)
– 171.71.1.0/24	Réseau du site 4
– 171.71.2.0/24	Réservé pour l'expansion du réseau de San Jose
– 171.71.3.0/24	Campus de San Jose, Site 4, Divers groupes
– 171.71.4.0/22	Site 4, Groupe des ordinateurs de bureau Phase A (Bâtiment 1)
– 171.71.8.0/21	Site 4, Groupe des ordinateurs de bureau Phase A (Bâtiments 1 et 2)
– 171.71.16.0/21	Site 4, Réseaux de laboratoire (non RFC1918)
– 171.71.24.0/21	Site 4, Groupe des ordinateurs de bureau Phase A (Bâtiment 3)
– 171.71.32.0/19	Site 4, Groupe des ordinateurs de bureau Phase A (Bâtiments 4 à 7) (Sans fil 1 à 4)
– 171.71.64.0/20	Sites de réseau MAN de San Jose
– 171.71.80.0/20	Site 4, Groupe des ordinateurs de bureau Phase B (Bâtiments 8, 9 et 12)
– 171.71.96.0/20	Site 4, Groupe des ordinateurs de bureau Phase B (Bâtiments 9, 10 et 11)
– 171.71.112.0/22	Site 4, Groupe des ordinateurs de bureau Phase B (Bâtiment 11)
– 171.71.116.0/22	Site 4, Groupe des ordinateurs de bureau Phase C (Bâtiment 13)
– 171.71.120.0/21	Site 4, Groupe des ordinateurs de bureau Phase C (Bâtiments 13 et 14)
– 171.71.128.0/20	Site 4, Groupe des ordinateurs de bureau Phase C (Bâtiments 14 à 16)

– 171.71.144.0/21	Site 4, Groupe des ordinateurs de bureau Phase C (Bâtiments 16 et 17)
– 171.71.152.0/22	Réseau du site 4
– 171.71.156.0/22	-(Bloc non alloué)
– 171.71.160.0/20	Réseau du site 4
– 171.71.176.0/21	Réseau du site 4
– 171.71.184.0/21	Site 4, Réseau sans fil, Bâtiments 5 à 8
– 171.71.192.0/21	Site 4, Réseau sans fil, Bâtiments 9 à 12
– 171.71.200.0/21	Site 4, Réseau sans fil, Bâtiments 13 à 16
– 171.71.208.0/21	Site 4, Réseau sans fil, Bâtiments 17 à 19
– 171.71.216.0/21	Site 4, Groupe des ordinateurs de bureau Phase C (Bâtiments 17 et 18)
– 171.71.224.0/21	Site 4, Groupe des ordinateurs de bureau Phase C (Bâtiments 18 et 19)
– 171.71.232.0/22	Site 4, Groupe des ordinateurs de bureau Phase C (Bâtiment 19)
– 171.71.236.0/27	Réseau du serveur NTG
– 171.71.236.32/27	-(Bloc non alloué)
– 171.71.236.64/26	-(Bloc non alloué)
– 171.71.236.128/25	-(Bloc non alloué)
– 171.71.237.0/24	-(Bloc non alloué)
– 171.71.238.0/23	-(Bloc non alloué)
– 171.71.240.0/22	SJC RBB et liens BB du Site 4
– 171.71.244.0/22	-(Bloc non alloué)
– 171.71.248.0/21	-(Bloc non alloué)

Une fois encore, dans l'exemple ci-dessus, l'allocation de l'espace d'adressage s'effectue de manière hiérarchique. L'espace d'adressage de chaque groupe d'ordinateurs de bureau peut être réduit à une poignée de notifications de routage. L'intégralité du bloc d'adresses 171.71.0.0/16 peut être réduit à une unique notification de route du fédérateur du Site 4 au fédérateur régional. De plus, le bloc d'adresses 171.71.64.0/20 est réduit pour le passage du fédérateur de site MAN au fédérateur régional. Ceci donne deux entrées de route dans la table de routage du cœur de réseau.

Conséquences de l'absence de hiérarchie

172.24.0.0/16	Espace d'adressage RFC1918 du réseau Cisco IT-LAN (Ingénierie)
– 172.24.0.0/19	Campus de San Jose
– 172.24.32.0/20	Sites distants (Régions Ouest et Centre)
– 172.24.48.0/21	Campus de San Jose : Site 4 (réseau IT-LAN Ingénierie)

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

– 172.24.56.0/21	-(Bloc non alloué)
– 172.24.64.0/22	-(Bloc non alloué)
– 172.24.68.0/22	Center for Network Application (CNAP ou POC) Bâtiment 13
– 172.24.72.0/21	-(Bloc non alloué)
– 172.24.80.0/20	-(Bloc non alloué)
– 172.24.96.0/21	Sites distants (toutes régions)
– 172.24.104.0/24	Réseau des Sites 1 à 3
– 172.24.105.0/24	Réseau du site 4
– 172.24.106.0/23	Réseau de laboratoire de St. Paul, Minn (Ieng)
– 172.24.108.0/26	Réseau console d’Ann Arbor, MI
– 172.24.108.64/26	-(Bloc non alloué)
– 172.24.108.128/25	-(Bloc non alloué)
– 172.24.109.0/24	Fédérateur du laboratoire du Site 4
– 172.24.110.0/24	Center for Network Application (CNAP ou POC) Bâtiment 13
– 172.24.111.0/24	Fédérateur du laboratoire du Site 4
– 172.24.112.0/23	Fédérateur du laboratoire des Sites 1 à 3
– 172.24.114.0/24	Fédérateur du laboratoire du Site 4
– 172.24.115.0/24	Fédérateur du Site 5 et du du laboratoire McCarthy
– 172.24.116.0/22	Console Franklin, Mass (Altiga), laboratoire
– 172.24.120.0/22	Réseau d’ordinateurs de bureau Franklin
– 172.24.124.0/22	Espace d’adressage RFC1918 pour l’Inde
– 172.24.128.0/21	Réservé au campus de San Jose
– 172.24.136.0/21	Sites distants
– 172.24.144.0/21	Réservé au campus de San Jose
– 172.24.152.0/30	Réseau du site 4
– 172.24.152.4/30	-(Bloc non alloué)
– 172.24.152.8/29	-(Bloc non alloué)
– 172.24.152.16/28	-(Bloc non alloué)
– 172.24.152.32/27	-(Bloc non alloué)
– 172.24.152.64/26	-(Bloc non alloué)
– 172.24.152.128/25	MSSBU – Espace laboratoire dans le bâtiment 1
– 172.24.153.0/24	-(Bloc non alloué)
– 172.24.154.0/24	Réseau de laboratoire pour le laboratoire sjc1-grs
– 172.24.155.0/24	Expansion du laboratoire, Saint Paul, MN
– 172.24.156.0/23	Réseau de laboratoire de Salem, NH

– 172.24.158.0/24	Essais en mode bouclé Eng net, TBR
– 172.24.159.0/24	RTP Comvault
– 172.24.160.0/19	-(Bloc non alloué)
– 172.24.192.0/18	Site distant

A l'époque, l'équipe Cisco IT avait alloué aux laboratoires le bloc 172.24.0.0/16 sur une base fonctionnelle et non géographique ou hiérarchique. C'était une erreur.

Dans le descriptif ci-dessus, 172.24.155.0/24 correspond au Minnesota. L'espace adjacent, 172.24.156.0/23, se trouve au New Hampshire. Ces blocs d'adresses géographiquement distincts ne peuvent pas être réduits. Conséquence de cette allocation mal pensée, le bloc d'adresses 172.24.0.0/16 génère 26 routes dans la table de routage de cœur de réseau Cisco. D'un autre côté, le bloc d'adresses 171.71.0.0/16 (Site 4 de San Jose et réseau MAN de San Jose) ne donne lieu qu'à deux routes dans la table de routage. La raison de cette différence tient au fait que ce bloc d'adresses a été alloué de manière hiérarchique.

La gestion d'une hiérarchie logique

Pour Cisco, l'espace d'adressage est une ressource stratégique. S'il n'était pas efficacement alloué, Cisco serait dans l'impossibilité de justifier davantage d'espace d'adressage dans les registres Internet pour permettre le développement de l'entreprise. Pour garantir une allocation efficace et hiérarchique de toutes les adresses allocations, l'équipe topologique du département informatique Cisco a mis en œuvre les quatre mécanismes suivants :

1. Toutes les allocations d'adresses sont enregistrées de manière centralisée – Il est essentiel de comprendre et de documenter toutes les allocations actuelles afin d'administrer la hiérarchie logique. Toutes les allocations d'adresses et de sous-réseaux doivent être enregistrées dans un même fichier maître. Celui-ci peut se présenter sous n'importe quelle forme, depuis un fichier texte sous contrôle RCS (Revision Control System) jusqu'à une base de données disposant de fonctions intégrées de calcul d'adresses de sous-réseau. L'essentiel est de disposer d'un fichier maître regroupant toutes les allocations d'adresses au sein de la société, ainsi que tous les espaces d'adressage résultant des acquisitions d'entreprises ;

2. Une équipe d'administrateurs de blocs de routage inter-domaine sans classe ou CIDR (Classless Interdomain Routing) attribue de larges blocs de manière stratégique dans toute la société – Cisco gère quatre grandes installations, dont San Jose : Amériques, Europe, Moyen Orient – Afrique et Asie Pacifique. Une équipe d'architecture mondiale supporte l'ensemble de ces installations. Deux personnes de chaque installation et deux personnes de l'équipe d'architecture du réseau mondial jouent le rôle d'administrateurs de blocs CIDR. Ce comité de dix personnes gère l'intégralité des allocations stratégiques d'espace d'adressage pour Cisco. Les administrateurs de blocs CIDR possèdent une grande expérience dans la gestion des hiérarchies, des réductions, des notifications de routes BGP auprès des fournisseurs d'accès Internet et de la conservation de l'espace d'adressage. Ils peuvent éventuellement consulter l'Internet Registry si nécessaire ;

3. Dans chaque équipe réseau, une personne est spécifiquement chargée des allocations tactiques – Les administrateurs de blocs CIDR allouent de larges blocs d'espace d'adressage à chaque équipe réseau. Au sein d'une équipe, une personne est chargée de gérer l'allocation de l'espace d'adressage local. Consciente des besoins de hiérarchisation, de réduction et de conservation de l'espace d'adressage, cette personne met en place une stratégie centralisée de gestion de l'espace d'adressage ;

4. Les ajouts et les suppressions de routes dans la table de routage de cœur de réseau sont surveillées – Dans un réseau mondial, certaines erreurs de manipulation peuvent entraîner l'allocation

incorrecte de l'espace adressage, la suppression accidentelle des déclarations de réduction pendant les changements de réseau, l'oubli de réductions, etc. Pour déceler ces erreurs, Cisco envoie tous les jours à une équipe d'ingénieurs réseaux un récapitulatif des modifications apportées à la table de routage de cœur de réseau. Voici un exemple de ce courrier électronique qui est généré automatiquement :

Date : Jeu 3 avril 2003 07:30:04 US/Pacifique

Objet : Route Diff

Comparaison des routes du fédérateur régional de San Jose

Du : Mer 2 avril 07:30:01 US/Pacifique 2003

Au : Jeu 3 avril 07:30:00 US/Pacifique 2003

Suppression : 10.96.224.0/24 - Téléphonie IP Buenos Aires

Suppression : 10.96.225.0/24 - Téléphonie IP Rio (DHCP)

Suppression : 10.96.255.216/30 - Liaison WAN Lima <-> San Jose/RWC

Suppression : 10.96.255.220/30 - Liaison WAN Santiago <-> San Jose/RWC

Suppression : 64.100.181.192/26 - Ordinateurs de bureau Brasilia, Brésil

Ajout : 10.96.248.0/31 - Hôte virtuel pour Se1/0 sur mxc-wan-gw1

Ajout : 10.96.248.2/31 - Hôte virtuel pour Se2/0 sur mxc-wan-gw1

Ajout : 172.30.54.0/25 -

Ajout : 172.30.54.128/25 -

Ajout : 64.100.176.0/20 -

Les ingénieurs réseaux parcourent le courrier pour déterminer si des routes « incorrectes » ont été ajoutées ou supprimées, soit en raison d'un résumé manquant, soit à cause d'une simple erreur de frappe. Si une entrée leur semble anormale, ils en recherchent la cause.

L'outil qui examine la table de routage a accès au fichier maître des allocations d'adresses : si la notification de route correspond à une allocation de l'espace d'adressage, la description qui figure dans la base de données est ajoutée à la ligne correspondante. Ceci améliore considérablement la lisibilité du rapport.

Résumé de la hiérarchie

La hiérarchie physique est un pré-requis de toute hiérarchie logique. L'allocation de l'espace d'adressage dans une hiérarchie logique permet la réduction. Cette hiérarchie et cette réduction sont indispensables à la réalisation d'un réseau fondamentalement stable.

Etape 5 : Analyse des causes fondamentales des interruptions de service

Pour l'équipe de topologie de réseau de Cisco, une même interruption évitable ne doit pas se reproduire une seconde fois. Cet objectif important donne lieu à une procédure simple :

1. identifier la cause de l'interruption de service ;
2. éliminer la cause de l'interruption dans le bâtiment concerné ;
3. déterminer si d'autres bâtiments sont vulnérables ;
4. si c'est le cas, modifier le réseau pour éviter la même interruption dans ces autres bâtiments ;
5. mettre à jour la documentation architecturale pour limiter la vulnérabilité des déploiements ultérieurs.

En raison de leur charge de travail, les ingénieurs réseaux ont tendance à s'occuper des causes fondamentales dans le bâtiment touché, puis à passer à leurs autres tâches. La direction doit se charger du suivi pour éviter l'apparition d'interruptions identiques dans les autres bâtiments et vérifier la mise à jour de la documentation architecturale.

Visibilité de gestion

L'OCC de Cisco, opérationnel tous les jours 24 heures sur 24, assure les fonctions suivantes :

- il identifie les interruptions de service en cours lorsqu'elles ont un impact sur l'activité, soit grâce à un logiciel de surveillance, soit sur rapport téléphonique ;
- il classe l'interruption de service en fonction de sa gravité ;
- il notifie le personnel de service pour qu'il résolve le problème technique ;
- en fonction de la gravité et de la durée de l'interruption, il fait remonter l'information à la direction.

Lorsqu'une réparation provisoire a été mise en place, le personnel de l'OCC :

- assure un suivi régulier avec la personne qui a résolu le problème pour s'assurer que la cause fondamentale a été identifiée ;
- assure un suivi régulier avec la personne qui a résolu le problème pour s'assurer qu'une solution à long terme a été trouvée, si nécessaire ;
- envoie, deux fois par jour, un courrier électronique de synthèse sur toutes les interruptions de service P1 qui ont une incidence sur l'activité. Ce courrier électronique est envoyé à l'alias de messagerie de récapitulation P1 auquel tous les employés de Cisco peuvent s'abonner. Les responsables du département informatique de Cisco qui supervisent le personnel de service sont fortement invités à s'abonner à cet alias de messagerie P1.

Définitions des priorités et de la gravité des interruptions de service

Le suivi des unités prioritaires permet d'obtenir à l'avance une estimation de la gravité potentielle d'une interruption. Les unités, les applications et les bases de données de type P1 et P2 sont surveillées car leur défaillance peut avoir des conséquences graves sur l'activité de Cisco. Les incidents de type P1 et P2 nécessitent ainsi une intervention immédiate du service technique lorsqu'il est contacté par les responsables incidents. En théorie, les incidents P1 doivent être résolus en 2 heures maximum, et les incidents P2 en moins de 4 heures.

Priorité 1 : réponse immédiate et résolution en moins de deux heures. Les applications P1 sont nécessaires au traitement des revenus et utilisées par plus de 60 personnes ou par le personnel de direction. Ces applications doivent bénéficier d'une assistance technique sur simple appel 24 heures sur 24. En cas de panne, elles donnent lieu à l'ouverture d'un ticket P1 et à l'envoi de pages de notification. Les équipements de réseau P1 sont ceux qui supportent plus de 100 personnes ou un site partenaire pendant les heures d'ouverture, ou qui accèdent à n'importe quel serveur ou application P1. Un ticket P1 peut être ouvert lorsque le service de réseau est interrompu et si plusieurs unités assimilables à la catégorie P2 sont affectées.

Priorité 2 : réponse dans les deux heures et résolution en moins de 4 heures. Les applications P2 sont utilisées par un plus petit nombre de clients et peuvent, par définition, demeurer en panne plus longtemps sans affecter la capacité de traitement des revenus de Cisco. Les équipements de réseau P2 supportent moins de 100 personnes ou permettent l'accès à des applications et des serveurs de catégorie P2.

Priorité 3 : réponse en moins d'une journée. Les applications P3 sont utilisées par un groupe spécifique de clients : en cas de défaillance, elles ne doivent pas empêcher ces clients de poursuivre leurs activités ou peuvent être aisément contournées. Ces applications peuvent rester en panne pendant une durée prolongée sans incidence sur la productivité. Parmi les équipements de réseau P3 figurent les connectivités RNIS et Frame Relay locales ainsi que les réseaux de serveurs consoles.

Priorité 4 : réponse en moins de deux jours. Les applications P4 sont généralement en cours de développement ou très rarement utilisées et n'ont aucune incidence sur les revenus.

Définition de la gravité d'une interruption

La gravité est une mesure de l'incidence réelle sur l'activité. Les incidents qui entraînent l'indisponibilité des ressources surveillées de type P1 ou P2 n'ont pas systématiquement d'incidence grave sur l'activité. La gravité permet de différencier, en fonction de la priorité, les réponses attendues au problème à partir de l'incidence (la gravité de l'impact sur l'activité) constatée par Cisco. La gravité d'un cas est déterminée au moment de l'incident et sur la base des circonstances réelles. Pour tous les incidents P1 et P2 gérés par les responsables incidents, elle est évaluée selon la grille ci-dessous :

	Définition	Exemples
Gravité 1	<ul style="list-style-type: none"> Incidence immédiate et importante sur l'activité 	<ul style="list-style-type: none"> Coupure de courant dans un centre de calcul
	<ul style="list-style-type: none"> Aucun contournement possible 	<ul style="list-style-type: none"> Panne complète du réseau sur tout le campus
Gravité 2	<ul style="list-style-type: none"> Incidence négative sur l'activité 	<ul style="list-style-type: none"> Dégradation d'un système critique
	<ul style="list-style-type: none"> Aucun contournement possible 	<ul style="list-style-type: none"> Incidence sur la fabrication au niveau mondial
		<ul style="list-style-type: none"> Indisponibilité de nombreuses applications sur Cisco.com
Gravité 3	<ul style="list-style-type: none"> Faible incidence sur l'activité 	<ul style="list-style-type: none"> Indisponibilité d'un contenu de production ou d'un déploiement de code
	<ul style="list-style-type: none"> Contournement possible avec baisse des performances 	<ul style="list-style-type: none"> Effet localisé
Gravité 4	<ul style="list-style-type: none"> Incidence faible ou nulle sur l'activité 	<ul style="list-style-type: none"> Equilibrage de charge des applications
	<ul style="list-style-type: none"> Contournement possible 	<ul style="list-style-type: none"> Service de réseau redondant
		<ul style="list-style-type: none"> Interruption des services de bureau en dehors des heures d'ouverture

La plupart des incidents P1 sont de gravité 3 ou 4. Les incidents de gravité 1 ou 2 sont très rares et sont immédiatement portés à la connaissance des niveaux supérieurs de la direction.

Exemple de courrier électronique récapitulatif P1 :

Date : Lun 7 avril 2003 05:43:55 US/Pacifique

Objet : Récap. P1 pour la matinée du lundi 7 avril

Aujourd'hui, nous avons eu 5 nouveaux P1, 2 mises à jour P1, aucune exception P1 et 13 P2

P1 en bref :

Nombreux fichiers écrits sur l'hôte drno ECS infecté par le virus Lovegate à partir de 01:00 PT (10:00 CET), prochaine mise à jour 07 avr. 08:00 PT

App Eworklli en panne sur l'hôte ework depuis 19:38 PT, prochaine mise à jour 07 avr. 12:00 PT

La tâche de traitement par lots fin_box_ai_daily n'a pas atteint son ANS de 21:00 PT et s'est achevée à 21:10 PT

Le serveur de visualisation ECS smbview2 est tombé en panne de 00:43 PT à 01:10 PT

L'application Universe sur l'hôte jane est tombée en panne de 19:15 PT à 19:29 PT

Mises à jour P1 en bref :

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

Les liaisons WAN avec Johannesburg, Afrique du Sud, étaient indisponibles du 06 avr. 03:26 PT au 07 avr. 02:14 PT, le serveur de courrier POP n'est toujours pas accessible depuis le 06 avr. 03:36 PT.

Progeon, Inde, a connu des problèmes intermittents dans l'utilisation de l'application SOLCAT depuis 23:00 PT le 25 mars. Prochaine mise à jour à 10:00 le 7 avril.

P1 en détail :

GRAVITE 4, dossier no. 817113. Nombreux fichiers écrits sur l'hôte drno ECS infecté par le virus Lovegate à partir de 01:00 PT. L'impact est minimal car les clients peuvent accéder actuellement au serveur. L'assistance technique est en train de supprimer les fichiers infectés. Prochaine mise à jour le 07 avr. A 08:00 PT. Le dossier reste ouvert.

GRAVITE 4, dossier no. 816732. Panne de l'application Eworklli sur l'hôte ework. L'impact est minimal car seul la fonction de recherche de l'outil de collaboration en ligne est en panne ; la fonction principale de chargement et de téléchargement de documents est opérationnelle. L'assistance technique mène l'enquête, la stabilité de l'application est sous surveillance. Prochaine mise à jour le 07 avr. à 12:00 PT. Le dossier reste ouvert.

GRAVITE 3, dossier no. 816587. La tâche de traitement par lots fin_box_ai_daily n'a pas atteint son accord de niveau de service (ANS) de 21:00 PT SLA and et s'est achevée à 21:10 PT. Elle porte sur l'impression de factures clients et le rapport Rapid Revenue. L'assistance technique a suivi la tâche jusqu'à sa finalisation. Ce dossier est considéré comme résolu.

GRAVITE 4, dossier no. 816969. Le serveur de visualisation ECS smbview2 a été indisponible de 00:43 PT à 01:10 PT. En raison de l'heure, l'incident n'a eu qu'un impact minimal sur la capacité des ingénieurs à compiler les développements logiciels et matériels. L'assistance technique a rebooté le serveur pour restaurer les services. Ce dossier est considéré comme résolu.

GRAVITE 4, dossier no. 816494. L'application Universe sur l'hôte jane est tombée en panne de 19:15 PT à 19:29 PT. L'impact sur les tâches de traitement par lots a été minimal en raison de la courte durée de l'indisponibilité. Cette application est revenue à son niveau normal sans intervention de l'assistance technique. Ce dossier est considéré comme résolu.

Mises à jour P1 en détail :

GRAVITE 4, dossier no. 816124. Les liaisons WAN avec Johannesburg, Afrique du Sud, étaient indisponibles du 06 avr. 03:26 PT au 07 avr. 02:14 PT. Les clients disposent de nouveau d'une connectivité de réseau après la fin de la panne de courant. Le serveur de courrier électronique POP n'est toujours pas accessible. L'enquête est menée par EMEA Transport and Sysadmins. Le dossier reste ouvert.

GRAVITE 4, dossier no. 707465. Progeon, Inde, a connu des problèmes intermittents dans l'utilisation de l'application SOLCAT depuis 23:00 PT le 25 mars. Aucune incidence sur la capacité des clients à mener des transactions sur les commandes clients sur un site en Inde car un contournement a été mis en place. L'assistance technique réalise des tests supplémentaires sur le site et étudie la latence du réseau WAN. Prochaine mise à jour à 10:00 PT le 7 avril. Le dossier reste ouvert.

Responsabilité de la direction

Les responsables informatiques de Cisco exposent les informations essentielles à leurs supérieurs au cours d'une revue opérationnelle trimestrielle. Chaque niveau de la gestion informatique de Cisco présente ce type d'analyse, la remontée culminant par une analyse trimestrielle présentée au Directeur général. Ces analyses périodiques de la disponibilité et des évaluations P1 à tous les niveaux de la chaîne de direction donnent la priorité à la résolution des causes fondamentales des interruptions de service.

Les informations clés présentées au cours de ces revues opérationnelles sont notamment :

- les mesures de disponibilité du réseau ou des applications,
- les chiffres des interruptions de service de type P1 (y compris leur nombre et leur gravité),
- des informations détaillées sur les éventuelles interruptions de gravité 1 et 2.

Exemple d'analyse des causes fondamentales

L'analyse des causes fondamentales demande aux ingénieurs réseaux d'identifier le problème, d'en déterminer la cause, puis de prendre les mesures nécessaires pour régler le problème et veiller à ce qu'il ne se reproduise plus. L'exemple suivant présente les différentes étapes de l'analyse des causes fondamentales à partir d'un cas réel.

- **Analyse du rapport relatif au problème** – Au quatrième étage du bâtiment 12, les utilisateurs qui ont connecté leurs ordinateurs portables au réseau Ethernet n'ont pas réussi à se connecter au réseau. Les autres étages de ce même bâtiment n'ont connu aucun problème. Les téléphones IP n'ont pas été affectés, le réseau sans fil non plus, pas plus que les utilisateurs déjà connectés au réseau et ceux qui

disposaient d'adresses IP statiques. Aucun dysfonctionnement des équipements de réseau n'a été signalé.

- **Identification de la cause de l'interruption** – Le problème a été causé par un poste de travail du réseau qui était configuré de manière erronée en tant que serveur DHCP (Dynamic Host Configuration Protocol). Les ordinateurs qui se connectaient au réseau ne pouvaient plus recevoir d'adresse DHCP valide car le serveur DHCP mal configuré répondait aux demandes DHCP par des informations incorrectes.

- **Résolution de la cause de l'interruption dans le bâtiment concerné** – Le serveur DHCP non autorisé a été retiré du réseau et le service est revenu à la normale dans le bâtiment.

- **Evaluation de la vulnérabilité des autres bâtiments** – Les autres bâtiments sont vulnérables à ce type de problème car il est facile de mal configurer un poste de travail en tant que serveur DHCP. Ce type de problème est particulièrement insidieux parce qu'il n'est pas automatiquement détectable par notre système de gestion de réseau.

- **Mesures pour éviter l'interruption dans d'autres bâtiments** – Cisco a déployé des listes de contrôles d'accès au VLAN (VACL) sur tous les commutateurs de couche d'accès afin de bloquer les réponses DHCP (port UDP [User Datagram Protocol] 68) provenant de tous les serveurs autres que les serveurs DHCP autorisés et les routeurs IT exécutant des fonctions d'aide IP. Cette solution a pu être réalisée car les commutateurs de couche d'accès Cisco sont généralement des Cisco Catalyst 6500 équipés de cartes d'application de politique.

- **Mise à jour de la documentation architecturale pour éviter le problème sur les déploiements ultérieurs** – le département informatique de Cisco a mis à jour la documentation du réseau Production des ordinateurs de bureau afin d'inclure que les VACL soient intégrées en configuration standard. Ceci a rendu tous les nouveaux déploiements de réseau d'ordinateurs de bureau invulnérables au problème du « serveur DHCP non autorisé ».

Etape 6 : Des onduleurs pour les unités critiques

Une disponibilité de 99,9 % correspond à 8,766 heures de temps d'arrêt par an. Les coupures de courant imprévues sont à l'origine d'une partie de ces temps d'arrêt, mais comme le réseau électrique de San Jose est raisonnablement stable, il n'est pas nécessaire que toutes les unités soient sur alimentation non interruptible pour atteindre une disponibilité de 99,9 %. Il est toutefois recommandé de mettre sur onduleur les unités critiques, et notamment les routeurs de cœur de réseau, pour :

- éviter que les coupures de courant localisées dans les bâtiments qui hébergent des routeurs de cœur de réseau se transforment en panne de réseau élargie, et
- protéger les unités critiques contre les surtensions qui peuvent générer des défaillances matérielles.

Etape 7. Gestion de la redondance

La redondance est un facteur essentiel pour atteindre une disponibilité de 99,9 %. Pour chaque commutateur de couche 2, Cisco prévoit deux chemins distincts en direction de passerelles de couche 3 indépendantes. L'architecture du réseau est prévue pour empêcher qu'une défaillance unique provoque la segmentation des domaines de couche 2. Chaque passerelle de couche 3 est également dotée de deux chemins distincts vers le cœur de réseau redondant.

La construction des bâtiments prévoit généralement la connexion de chaque répartiteur BDF à deux NOC distincts en utilisant des chemins différents lorsque cela est possible. Les NOC sont interconnectés à l'aide de chemins de fibres distincts et étiquetés « Diverse Path A » ou « Diverse Path B ».

Pour la réalisation de sites de réseau WAN et MAN, la connectivité est assurée par lignes louées avec des chemins différents lorsque cette solution est économiquement acceptable. Chaque passerelle redondante de réseau WAN ou MAN est liée au fédérateur par l'intermédiaire d'une des lignes louées.

Etape 8 : Gestion des changements

La gestion des changements fournit un mécanisme nécessaire de communication qui :

- évite que des changements non planifiés superposent des interruptions de service sur des systèmes liés ;
- crée un enregistrement des changements afin que les ingénieurs d'assistance puissent savoir si une interruption de service est la conséquence d'un changement récent.

Pour mettre en œuvre son processus de gestion des changements, l'équipe Cisco a créé un alias de messagerie que les membres de l'équipe réseau peuvent renseigner à l'aide d'informations du type « qui, quoi, où, quand, pourquoi » lorsqu'ils prévoient un changement. Toute personne qui réalise une opération de changement doit s'abonner à cet alias pour éviter les conflits de changements. Elle doit également lire les messages qui proviennent de l'alias, même lorsque ceux-ci sont filtrés. Le département informatique de Cisco copie tous les changements réseaux dans l'alias de messagerie Cisco IT-LAN- CM auquel sont abonnés tous les membres de l'équipe réseau, ainsi que les principaux contacts extérieurs à l'activité topologique. Un outil permet également d'effectuer des recherches dans les précédentes activités de gestion des changements.

Etape 9 : Pièces de rechange en cas d'urgence

L'équipe du réseau LAN de Cisco à San Jose conserve au moins une pièce de rechange pour chaque pièce déployée sur le réseau de production. Installés de la périphérie jusqu'au cœur du réseau, les commutateurs de la gamme Cisco Catalyst 6500 permettent de limiter considérablement le nombre de pièces détachées qui doivent rester immédiatement disponibles. Les pièces de rechange d'urgence font l'objet d'une gestion distincte de l'inventaire général. Elles sont clairement étiquetées et permettent une intervention en cas d'interruption de service sans attendre la délivrance d'un numéro d'autorisation de retour de matériel ou RMA (Return Materials Authorization). Un ingénieur réseau subalterne est responsable de l'inspection régulière du stock des pièces de rechange.

Etape 10 : Gestion hors bande

Pour limiter les interruptions de service réseau, il est nécessaire de réaliser un réseau distinct de gestion hors bande. Le réseau hors bande du Cisco IT-LAN-SJ présente les caractéristiques suivantes :

- c'est un réseau plat et non redondant ;
- il utilise un routage statique pour la connexion au réseau de production ;
- il possède son propre serveur DNS ;
- chaque console d'unité de réseau de production est connectée à un serveur console sur le réseau hors bande.

Un tel réseau hors bande réduit considérablement la durée des interruptions planifiées et non planifiées car il permet de résoudre de nombreux problèmes à distance.

En résumé : Comment atteindre une disponibilité de 99,9 %

Il n'est pas difficile d'atteindre de tels temps de fonctionnement à la condition de disposer d'un réseau fondamentalement stable. Pour garantir ce niveau de disponibilité, l'équipe du réseau Cisco IT-LAN-SJ a suivi les étapes suivantes :

- mesurer la disponibilité et exploiter activement les rapports de manière tactique et stratégique ;
- construire un réseau doté d'une hiérarchie physique ;
- construire un réseau doté d'une hiérarchie logique ;
- assurer le suivi de l'analyse et de la remédiation des causes fondamentales ;

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

- protéger les unités critiques par des onduleurs ;
- construire un réseau redondant ;
- communiquer et enregistrer les changements à l'aide d'un système simple de gestion des changements ;
- prévoir des pièces de rechange pour les cas d'urgence ;
- réaliser un réseau de gestion hors bande.

La plupart de ces étapes sont relativement simples à mettre en place. La réalisation d'un réseau redondant doté d'une hiérarchie physique et logique peut exiger des travaux d'envergure ; sans ces caractéristiques, toutefois, il est impossible d'atteindre des niveaux élevés de disponibilité sur les réseaux de grande taille.

Les étapes Cisco pour une disponibilité de 99,99 %

Alors qu'une disponibilité de 99,9 % représente 8,766 heures de temps d'arrêt par an, il faut descendre en dessous de 53 minutes d'interruption par an et par appareil pour atteindre une disponibilité de 99,99 % : une seule interruption globale de 15 minutes, et vous dépassez vos objectifs trimestriels ! Un réseau fondamentalement stable permet d'obtenir une disponibilité de 99,9 %, mais le niveau supérieur exige un réseau plus robuste encore.

En plus des étapes décrites ci-dessus (voir la section 99,9 %), l'équipe de réseau Cisco IT-LAN-SJ a constaté que les étapes suivantes étaient nécessaires pour atteindre ce niveau de disponibilité :

- le contrôle proactif de la redondance ;
- des onduleurs pour toutes les unités ;
- l'alimentation par générateur des unités critiques ;
- des audits automatisés sur la configuration des routeurs ;
- l'intégration de la gestion des changements avec la surveillance de la disponibilité ;
- des versions de code normalisées
- la formation au dépannage ;
- la séparation de la gestion des incidents et de la résolution des problèmes

Etape 1 : Le contrôle proactif de la redondance

Dans l'objectif d'une disponibilité de 99,9 %, la construction du réseau de Cisco San Jose avait déjà intégré la redondance. Toutefois, avec le temps, certaines de ces liaisons redondantes peuvent tomber en panne ou être accidentellement mal configurées. Si ces défaillances ne sont pas détectées et réparées, la seconde liaison risque à tout moment de provoquer une interruption importante. Imaginez que vous deviez remettre une analyse de causes fondamentales comportant le message suivant : « Il y a deux mois, notre liaison redondante est tombée en panne. La panne n'a pas été détectée. Hier, la liaison principale est tombée en panne provoquant une interruption de service. »

De telles interruptions sont acceptables lorsque vous disposez d'une marge de manœuvre de 8,7 heures, mais vous ne pouvez pas les laisser se produire si vous n'avez droit qu'à 53 minutes de temps d'arrêt par an.

Cisco exécute chaque semaine un script Perl pour vérifier que chaque commutateur de couche 2 dispose bien de deux chemins différents vers des routeurs distincts, et que chaque routeur de couche 3 est relié de deux manières différentes au cœur de réseau.

Bien que la procédure ne soit pas parfaite – dans notre architecture de réseau, la plupart des commutateurs de couche 2 sont connectés directement aux passerelles de couche 3 – presque toutes les interruptions dues à une « perte non décelée de redondance » ont été éliminées. Ce script peut également distinguer les « unités connues comme non redondantes ». Pour plus de clarté, le rapport de redondance donne la liste de ces « unités connues comme non-redondantes » dans une section distincte. Voici un exemple de ce rapport transmis par courrier électronique :

Date : Mar 1 avril 2003 02:21:36 US/Pacifique

Objet : Rapport de redondance

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

Rapport de redondance

Unités du réseau EMAN associées au contact de radio-messagerie it-lan-sj-duty et de priorité 2 ou plus et qui ne disposent pas de redondance de couche 2 vers d'autres unités associées au même contact de radio-messagerie. Connectivité appuyée sur les données CDP.

Les serveurs de terminaux, les commutateurs directeurs distribués, les RSM et les MSFC hybrides sont exclus de ce rapport.

2 pls1-00lab-sw1 commutateur lan
2 sjcc-12mc-sw1 commutateur lan
1 sjcm-21-sw2 commutateur lan

Unités connues comme non redondantes :

1 pmr-00-sw1 commutateur lan
2 sjc1-00cn-sw1 commutateur lan
2 sjc10-00cn-sw1 commutateur lan
2 sjc11-00cn-sw1 commutateur lan
2 sjc12-00cn-sw1 commutateur lan
2 sjc12-42cn-sw1 commutateur lan
2 sjc13-00cn-sw1 commutateur lan
2 sjc14-00cn-sw1 commutateur lan
2 sjc15-00cn-sw1 commutateur lan
2 sjc16-00cn-sw1 commutateur lan
2 sjc17-00cn-sw1 commutateur lan
2 sjc18-00cn-sw1 commutateur lan
2 sjc19-00cn-sw1 commutateur lan
2 sjc20-00cn-sw1 commutateur lan
2 sjc21-00cn-sw1 commutateur lan
2 sjc22-00cn-sw1 commutateur lan
2 sjc23-00cn-sw1 commutateur lan
2 sjc24-00cn-sw1 commutateur lan
2 sjc3-00cn-sw1 commutateur lan
2 sjc4-00cn-sw1 commutateur lan
2 sjc5-00cn-sw1 commutateur lan
2 sjc6-00cn-sw1 commutateur lan
2 sjc7-00cn-sw1 commutateur lan
2 sjc8-00cn-sw1 commutateur lan
2 sjc9-00cn-sw1 commutateur lan
2 sjca-00cn-sw1 commutateur lan
2 sjcb-00cn-sw1 commutateur lan
2 sjcc-00cn-sw1 commutateur lan
2 sjcd-00cn-sw1 commutateur lan
2 sjce-00cn-sw1 commutateur lan
2 sjcf-00cn-sw1 commutateur lan
2 sjcg-00cn-sw1 commutateur lan
2 sjch-00cn-sw1 commutateur lan
2 sjci-00cn-sw1 commutateur lan
2 sjcj-00cn-sw1 commutateur lan
2 sjcj-trailer-sw1 commutateur lan
2 sjck-00cn-sw1 commutateur lan
2 sjcl-00cn-sw1 commutateur lan
2 sjcm-00cn-sw1 commutateur lan
2 sjcn-00cn-sw1 commutateur lan
2 sjco-00cn-sw1 commutateur lan
2 sjcp-00cn-sw1 commutateur lan

Rapport généré le Mar 1 avril 02:21:36 US/Pacifique 2003

Etape 2 : Des onduleurs pour toutes les unités

Avec une tolérance d'interruption de service inférieure à 53 minutes par an, toutes les unités de réseau doivent être sur onduleurs. Cisco impose une réserve de 2 heures d'alimentation sur onduleur pour chacune des unités réseaux. Cette spécification est d'autant plus importante que les téléphones IP Cisco permettent de contacter le 911, qui est le service des appels d'urgence aux Etats-Unis. La politique de Cisco exige l'évacuation d'un bâtiment en cas de défaillance des systèmes d'alimentation non interruptibles car il devient impossible de composer le 911 dans de telles circonstances.

Etape 3 : Des générateurs pour les unités critiques

Pour éviter qu'une panne de courant prolongée dans un bâtiment de cœur de réseau puisse provoquer une interruption de grande envergure, les unités de cœur de réseau du Cisco IT-LAN-SJ sont alimentées par des générateurs.

Etape 4 : Des audits automatisés sur la configuration des routeurs

Pour faire appliquer ses configurations normalisées, Cisco utilise l'outil RAT (Router Audit Tool) de www.cisecurity.org. Cette politique présente deux grands avantages :

- nous disposons d'une configuration normalisée et documentée ;
- nos routeurs sont conformes à cette configuration normalisée et documentée.

L'équipe de réseau trouve des avantages dans une telle rigueur. Lorsque l'analyse des causes fondamentales suggère des modifications de configuration, cette procédure normalisée à audit automatique renforce la conformité de ces changements.

Chaque semaine, un rapport nommé le « Bottom 10 », donne la liste des dix routeurs les moins conformes aux normes en fonctions des rapports RAT, ainsi que les 10 règles de configuration les plus fréquemment enfreintes. Voici un exemple de ce rapport « Bottom 10 » :

Date : Mar 8 avril 2003 06:15:29 US/Pacifique

Objet : RAT_Bottom_10_Report_For_it-lan-sj-duty

Rapport « Bottom 10 » des fichiers de configuration personnalisés de it-lan-sj-duty

Nom de l'hôte	Score	Propriétaire	Nombre de semaines sur la liste Bottom 10
softoken-test.cisco.com	75	[supprimé]	23
pmr-gw1.cisco.com	85	[supprimé]	8
sjcd-00-cs1.cisco.com	85	[supprimé]	6
wlshb-gw1.cisco.com	85	[supprimé]	8
sjc12-00-gw2.cisco.com	86	[supprimé]	7
sjca-12-cs1.cisco.com	86	[supprimé]	7
wlshd-gw1.cisco.com	87	[supprimé]	7
sjce-00-gw1.cisco.com	89	[supprimé]	4
sjc16-00-gw2.cisco.com	89	[supprimé]	3
sjc15-00-gw2.cisco.com	89	[supprimé]	1

Règles les plus fréquemment enfreintes dans les fichiers de configuration personnalisés de it-lan-sj-duty

133	tacacs-server timeout 3
40	udld enable
33	ip igmp snooping
27	no class-map match-any http-hacks
22	exec-timeout 300 0 (line vty)
22	ip ssh time-out 30
21	ip name-server 171.68.226.120
21	logging source-interface loopback0

```
19    no ip source-route
18    snmp-server community xxxxxx ro 90
```

Etape 5 : Intégration de la gestion des changements avec la surveillance de la disponibilité

Si vous acceptez jusqu'à 8,7 heures d'interruption par an, il n'est pas nécessaire de différencier les interruptions planifiées des interruptions non planifiées. Vous disposez d'une marge suffisante pour absorber les interruptions planifiées et atteindre malgré cela les 99,9 % de disponibilité. Pour le niveau supérieur de 99,99 %, il devient nécessaire de distinguer les deux types d'interruption. Pour cela, le système de gestion des changements de Cisco exige des ingénieurs réseaux qu'ils fournissent les informations suivantes lorsqu'ils planifient une interruption :

- la période à laquelle s'effectuera le changement planifié ;
- les unités affectées par ce changement.

Si le calcul de la disponibilité brute est réalisé de manière normale, celui de la disponibilité ajustée impose que les unités désignées par la demande de changement soient considérées comme opérationnelles à 100 % pendant la fenêtre d'intervention considérée. Ce système, qui fournit des données précises sur la disponibilité brute et ajustée, présente l'avantage supplémentaire d'imposer la plus grande rigueur aux ingénieurs réseaux lorsqu'ils planifient une interruption. La moindre omission peut entraîner un signalement d'indisponibilité et générer l'ouverture d'un ticket P1 par l'OCC.

L'adoption d'une convention standard de dénomination est extrêmement utile à la planification des changements. Le nom de chaque unité de réseau Cisco commence par un identifiant de bâtiment. Par exemple, sjc12-31-sw2 désigne, à San Jose : bâtiment n° 12, 3^{ème} étage, séparateur IDF n°1, le deuxième commutateur de la pièce. Imaginons une coupure de courant planifiée dans le bâtiment 12. L'ingénieur réseau devra s'assurer que toutes les unités dont le nom commence par « sjc12- » sont incluses dans la demande de changement.

Ceci réduit considérablement la possibilité d'oublier une unité pendant la préparation. Si une unité est oubliée, elle subira une « interruption non planifiée » au cours de l'intervention. Une convention de dénomination bien conçue permet de réduire fortement ce type d'erreur.

L'intégration de la gestion des changements et des calculs de disponibilité permet d'avoir des mesures précises de la disponibilité brute et ajustée qui caractérisent les temps d'arrêts planifiés et non planifiés. Cette double mesure invite l'équipe réseau à la rigueur dans la planification des changements sur le réseau. Elle l'incite également à minimiser les interruptions planifiées dans les environnements de centres de calcul car celles-ci sont portées à la connaissance de la direction. La convention standard de dénomination facilite considérablement l'identification des unités touchées par le changement.

Etape 6 : Normalisation des versions de code

Sur le réseau Cisco IT-LAN-SJ, il est possible d'atteindre une disponibilité de 99,9 % avec des versions « prises au hasard » de la plate-forme logicielle Cisco IOS : le risque de ne pas choisir systématiquement des versions rigoureusement testées ne dépasse pas en effet quelques interruptions de services non planifiées supplémentaires. On peut ainsi demeurer en dessous du seuil acceptable de 8,7 heures de temps d'arrêt, et donc au-dessus des 99,9 % de disponibilité, sans le surcroît de travail que représente le choix et la mise à niveau de versions particulières de Cisco IOS.

En revanche, une disponibilité de 99,99 % exige la sélection de versions précises de Cisco IOS et de Cisco Catalyst OS. Les règles générales consistent à :

- sélectionner une version disposant des fonctionnalités requises ;
- sélectionner une version particulière bénéficiant du plus grand nombre possible de correctifs depuis la dernière intégration de fonctionnalités ;
- éviter les images « reportées » (sur www.cisco.com, la liste des images reportées fait l'objet d'une section distincte de la page Web de planification des mises à niveau de la plate-forme logicielle Cisco IOS) ;
- éviter les images avec « avis logiciel » (un avertissement s'affiche sur www.cisco.com avant de vous permettre de télécharger une image contenant un avis logiciel).

Nous donnons ci-après les « tactiques » utilisées par l'équipe de Cisco IT-LAN-SJ dans le choix des versions spécifiques de la plate-forme logicielle Cisco IOS :

Tactiques pour le train de versions 12.2T de la plate-forme logicielle Cisco IOS – A la date d'avril 2003, le train de technologie le plus récent, contenant les dernières fonctionnalités de la plate-forme logicielle Cisco IOS, était la version 12.2T. De nombreuses fonctionnalités ont été récemment introduites et ce train de technologie dispose d'un niveau plus faible de maturité. Lorsque l'équipe informatique de Cisco n'a pas besoin des fonctionnalités du train de technologie, elle choisit un autre train Cisco IOS, comme la version 12.2M (Mainline).

Prenons l'exemple d'un routeur multiservice Cisco 2621XM qui doit disposer des fonctionnalités IPv6 de base. La compatibilité IPv6 exige l'exécution du train Cisco IOS 12.2T. A la date d'avril 2003, les versions 12.2T suivantes étaient disponibles :

Version	Description
12.2(15)T	Première version des nouvelles fonctionnalités de 12.2(15)T
12.2(13)T3	Troisième refonte des fonctionnalités de 12.2(13)T
12.2(13)T1	Première refonte des fonctionnalités de 12.2(13)T
12.2(13)T	Première version des nouvelles fonctionnalités de 12.2(13)T
12.2(11)T6	Sixième refonte des nouvelles fonctionnalités de 12.2(11)T
12.2(11)T5	Cinquième refonte des nouvelles fonctionnalités de 12.2(11)T
12.2(11)T3	Troisième refonte des nouvelles fonctionnalités de 12.2(11)T
12.2(11)T2	Deuxième refonte des nouvelles fonctionnalités de 12.2(11)T
12.2(11)T1	Première refonte des nouvelles fonctionnalités de 12.2(11)T
12.2(11)T	Première version des nouvelles fonctionnalités de 12.2(11)T
12.2(8)T8	Huitième refonte des nouvelles fonctionnalités de 12.2(8)T
12.2(8)T5	Cinquième refonte des nouvelles fonctionnalités de 12.2(8)T
12.2(8)T4	Quatrième refonte des nouvelles fonctionnalités de 12.2(8)T
12.2(8)T3	Troisième refonte des nouvelles fonctionnalités de 12.2(8)T
12.2(8)T2	Deuxième refonte des nouvelles fonctionnalités de 12.2(8)T
12.2(8)T1	Première refonte des nouvelles fonctionnalités de 12.2(8)T
12.2(8)T	Première version des nouvelles fonctionnalités de 12.2(8)T
12.2(4)T5	Cinquième refonte des nouvelles fonctionnalités de 12.2(4)T
12.2(4)T3	Troisième refonte des nouvelles fonctionnalités de 12.2(4)T
12.2(4)T1	Première refonte des nouvelles fonctionnalités de 12.2(4)T
12.2(2)T4	Quatrième refonte des nouvelles fonctionnalités de 12.2(2)T
12.2(2)T	Première version des fonctionnalités de 12.2(2)T

Note : Le lecteur aura remarqué l'absence de certaines versions et refontes. La raison en est double :

- certaines refontes remédient à des problèmes spécifiques pour des plates-formes spécifiques. Si une refonte concerne un problème particulier sur le Cisco 364, elle ne sera pas compilée pour le Cisco 2621 ;
- Cisco supprime périodiquement les images anciennes de Cisco.com – le plus souvent lorsqu'elles sont vieilles de 6 à 9 mois et qu'une refonte plus récente est disponible.

Chaque refonte remédie à des problèmes donnés, mais ne contient pas de nouvelles fonctionnalités. La première décision tactique consiste donc à ne tenir compte que des refontes les plus récentes. La liste des versions utilisables est donc réduite à celle-ci :

Version	Description
12.2(15)T	Première version des fonctionnalités de 12.2(15)T
12.2(13)T3	Troisième refonte des fonctionnalités de 12.2(13)T
12.2(11)T6	Sixième refonte des fonctionnalités de 12.2(11)T
12.2(8)T8	Huitième refonte des fonctionnalités de 12.2(8)T
12.2(4)T5	Cinquième refonte des fonctionnalités de 12.2(4)T
12.2(2)T4	Quatrième refonte des fonctionnalités de 12.2(2)T

Aucune de ces versions ne fait l'objet d'un report ou d'un avis logiciel. Sachant que toutes ces versions disposent des fonctionnalités nécessaires, les versions dont le numéro de refonte est le plus élevé seront certainement préférables, par exemple 12.2(8)T8 ou 12.2(11)T6.

Tactiques pour la version 12.2M de la plate-forme logicielle Cisco IOS – Le train de version 12.2M (Mainline) de Cisco IOS a pour objectif principal la stabilité. La quasi-totalité des changements de code de cette version portent sur des correctifs logiciels, sans pratiquement aucun ajout de nouvelle fonctionnalité.

Prenons l'exemple d'un routeur Cisco 2621XM qui ne nécessite pas d'autres des fonctionnalités que celles comprises dans le train de versions 12.2M de Cisco IOS.

A la date d'avril 2003, les versions suivantes étaient disponibles (seules les refontes les plus récentes sont mentionnées) :

Version	Description
12.2(16)	Première version des fonctionnalités de 12.2(16)
12.2(13b)	Deuxième refonte de 12.2(13)
12.2(12c)	Troisième refonte de 12.2(12)
12.2(10b)	Deuxième refonte de 12.2(10)
12.2(7c)	Troisième refonte de 12.2(7)
12.2(6i)	Neuvième refonte de 12.2(6)
12.2(5d)	Quatrième refonte de 12.2(5)
12.2(3d)	Quatrième refonte de 12.2(3)
12.2(1d)	Quatrième refonte de 12.2(1)

Comme dans le cas du train de version 12.2T de Cisco IOS, les refontes ne portent que sur des correctifs. Toutefois, les versions sont radicalement différentes de celles de Cisco IOS 12.2T. Les trains « Mainline » comme Cisco IOS 12.2M, n'intègrent que rarement de nouvelles fonctionnalités.

Version ou Refonte, que choisir ? : Une version contient généralement un plus grand nombre de correctifs et subit des tests de régression complets. Une refonte ne concerne qu'un ensemble sélectionné de correctifs complémentaires. Pour accélérer la diffusion des correctifs, les refontes ne passent pas les tests de régression complets.

Une bonne règle empirique pour les versions « Mainline » consiste à utiliser l'une des deux dernières versions, ce qui, en l'occurrence, nous amène à :

Version	Description
12.2(16)	Première version des fonctionnalités de 12.2(16)
12.2(13b)	Deuxième refonte de 12.2(13)

L'avantage de la version 12.2(16) de Cisco IOS est qu'elle intègre la totalité des correctifs les plus récents et qu'elle a subi des tests de régression complets. L'avantage de la version 12.2(13b) de Cisco est que la version 12.2(13) a passé les tests de régression complets et que seuls quelques correctifs choisis y ont été intégrés depuis.

Tactiques pour le train de versions 12.1T de la plate-forme logicielle Cisco IOS – La version 12.1T de Cisco IOS est le « vieux » train de technologie utilisé pour la conception du code Mainline de la version 12.2. Les fonctionnalités de la version 12.1T sont intégrées dans la version 12.2M en bénéficiant d'une meilleure maturité car, sur une longue période, seuls des correctifs ont été apportés à la version 12.2M. Comme les fonctionnalités de Cisco IOS 12.1T sont disponibles dans la version 12.2M plus élaborée, il n'est pas recommandé d'utiliser cette version 12.1T.

Tactiques pour le train de versions 12.1M de la plate-forme logicielle Cisco IOS – Pour une meilleure qualité, Cisco conseille le « vieux » train Mainline car aucune nouvelle fonctionnalité importante n'a été intégrée à cette base de code depuis plusieurs années. Depuis la version 12.1(13), ce code a obtenu le label GD (General Deployment) ce qui signifie qu'il est considéré comme offrant le plus haut niveau de fiabilité.

Lorsqu'un code obtient le label GD, chacune de ses versions subit des tests complets de régression. C'est pour cette raison que depuis la version 12.1(13), il n'existe plus de refonte et donc plus de version du type 12.1(13a). Dans la série 12.1, la version la plus récente porte le numéro 12.1(19) (à la date d'avril 2003).

Tactiques pour le train de versions 12.1E de la plate-forme logicielle Cisco IOS (Version 12.1(14)E et précédentes) – La version 12.1E (Enterprise) de Cisco IOS est également appelée « train d'entreprise » parce que ce train de versions de Cisco IOS a été optimisé pour l'entreprise. Bien que ce code présente certaines nouvelles fonctionnalités nécessaires aux entreprises, leur nombre est limité afin d'optimiser la qualité. A la date d'avril 2003, Cisco IOS 12.1E était le principal train capable de supporter la carte MSFC (Multilayer Switch Feature Card) sur le Cisco Catalyst 6500. Il était en cela indispensable au réseau Cisco IT-LAN-SJ qui utilise des Cisco Catalyst 6500 en périphérie de la plate-forme de cœur de réseau.

A cette même date, les versions suivantes de Cisco IOS 12.1E étaient disponibles sur Cisco.com (pour plus de clarté, seules les refontes les plus récentes de chaque version sont mentionnées) :

Version	Description	Appuyée sur la version Mainline
12.1(13)E5	Cinquième refonte de la version 12.1(13)E	12.1(13)
12.1(12c)E5	Cinquième refonte de la version 12.1(12c)	12,1(12c)

12.1(11b)E7	Septième refonte de la version 12.1(11b)	12.1(11b)
12.1(11b)EX1	Première refonte de la version 12.1(11b)EX	12.1(11b)
12.1(8b)E13	Treizième refonte de la version 12.1(8b)E	12.1(8b)
12.1(8b)EX5	Cinquième refonte de la version 12.1(8b)EX	12.1(8b)
12.1(8a)E5	Cinquième refonte de la version 12.1(8a)E	12.1(8a)
12.1(5c)EX3	Troisième refonte de la version 12.1(5c)EX	12.1(5c)

Note 1 : L'intégration d'un correctif dans un train de versions Cisco IOS 12.1E peut s'effectuer de deux manières :

- il peut être directement incorporé à une version ou une refonte de Cisco IOS 12.1E, ou
- il peut être intégré à la version Mainline de Cisco IOS 12.1. Chacune des versions de Cisco IOS 12.1E s'appuie sur une version Mainline.

Par exemple, un correctif intégré à la version Mainline Cisco IOS 12.1(11b) le sera également à la version Cisco IOS 12.1(11b)E. Toutefois, un correctif intégré à Cisco IOS 12.1(11b)E2 ne sera pas nécessairement intégré aux versions Mainline de Cisco IOS 12.1, ce qui est normal lorsque l'erreur est spécifique à une fonctionnalité de 12.1E.

Note 2 : Il existe deux trains de versions distinctes – le train d'entreprise Cisco IOS 12.1E, et le train Cisco IOS 12.1EX qui se compose de variantes provisoires des versions Cisco IOS 12.1E afin d'y introduire des fonctionnalités nouvelles et importantes. Une copie de Cisco IOS 12.1(8b)E a par exemple servi à créer Cisco IOS 12.1(8b)EX. Le support du module d'analyse de réseau NAM (Network Analysis Module) a été ajouté dans un premier temps à 12.1(8b)EX. Ce support a ensuite été réintégré au train d'entreprise dans la version 12.1(11b)E.

Ce mécanisme de création provisoire de nouveaux trains permet aux nouvelles fonctionnalités importantes de subir des tests rigoureux avant leur introduction dans le train d'entreprise principal. Parallèlement, les nouvelles fonctionnalités moins importantes sont directement ajoutées au train d'entreprise.

Les règles utilisées pour choisir une version particulière à déployer sont semblables à celles qui régissent le train de technologie :

- éviter les versions reportées ou faisant l'objet d'un avis logiciel ;
- éviter les versions EX à moins d'avoir spécifiquement besoin des fonctionnalités propres à cette version ;
- prendre uniquement en compte les refontes les plus récentes de la version concernée.

La liste des versions utilisables est donc réduite à celle-ci :

Version	Description	Appuyée sur la version Mainline
12.1(13)E5	Cinquième refonte de la version 12.1(13)E	12.1(13)
12.1(12c)E5	Cinquième refonte de la version 12.1(12c)	12.1(12c)
12.1(11b)E7	Septième refonte de la version 12.1(11b)	12.1(11b)
12.1(8b)E13	Treizième refonte de la version 12.1(8b)E	12.1(8b)
12.1(8a)E5	Cinquième refonte de la version 12.1(8a)E	12.1(8a)

Pour un train de technologie, la version 12.1(8b)E13 de Cisco IOS serait le choix évident en termes de stabilité, compte tenu du nombre de refontes. Toutefois, pour des raisons de qualité, le train d'entreprise limite le nombre de fonctionnalités nouvelles. Cela signifie que toutes ces versions sont probablement robustes, mais il est généralement plus sage d'éviter les premières refontes d'une nouvelle version lorsque cela est possible.

Tactiques pour le train de version 12.1E de la plate-forme logicielle Cisco IOS (versions 12.1(19)E et ultérieures) – A partir de la version 12.1(19)E, le train de versions Cisco IOS 12.1E n'intégrera plus de nouvelles fonctionnalités et deviendra un train de « correctifs seuls », à la manière d'un train Mainline. Les règles à appliquer sont celles des versions Mainline de Cisco IOS 12.1 et de Cisco IOS 12.2, la dernière version étant probablement la meilleure.

Tactiques pour Cisco Catalyst OS

La numérotation des versions de Cisco Catalyst OS respecte le format suivant : Cisco Catalyst OS 1.2(3). Ici, le train de versions porte le numéro « 1 », la version de ce train porte le numéro « 2 » et la version corrective le numéro « 3 ». Chaque fois qu'une nouvelle fonctionnalité est ajoutée, le numéro de version est augmenté d'une unité.

Cisco Catalyst OS 5.X – A la date d'avril 2003, la dernière version 5.X de Cisco Catalyst OS portait le numéro 5.5(19). Aucune nouvelle fonctionnalité n'a été intégrée depuis la version 5.5(1) de Cisco Catalyst OS. Depuis la version Cisco Catalyst OS 5.5(7), le code est considéré comme GD (General Deployment), ce qui garantit la grande maturité du code et l'efficacité de la version la plus récente. Le seul problème est que vous aurez très certainement besoin des nouvelles fonctionnalités d'un nouveau train.

Cisco Catalyst OS 6.X – A la date d'avril 2003, la dernière version 6.X de Cisco Catalyst OS portait le numéro 6.4(2). Bien qu'il s'agisse du premier correctif de la version Cisco Catalyst OS 6.4(1), seules deux nouvelles fonctionnalités mineures ont été intégrées à Cisco Catalyst OS 6.4(1). Cela signifie que la toute dernière version du code Cisco Catalyst OS 6.4 offre une grande maturité. Cisco à l'intention de fermer Cisco Catalyst OS 6.X aux nouvelles fonctionnalités et de faire avancer le train vers le statut GD.

Cisco Catalyst OS 7.X – Cisco Catalyst OS 7.X est le train de version actuellement utilisé pour l'intégration de nouvelles fonctionnalités. Ceci explique pourquoi le nombre des correctifs est relativement faible entre les différentes versions. A la date d'avril 2003, les correctifs les plus récents des différentes versions étaient les suivantes :

Version	Description	Date de sortie
7.5(1)	Première version des fonctionnalités de 7.5(1)	31 décembre 2002
7.4(3)	Second correctif des fonctionnalités de 7.4(1)	6 décembre 2002
7.3(2)	Premier correctif des fonctionnalités de 7.3(1)	2 août 2002
7.2(2)	Premier correctif des fonctionnalités de 7.2(2)	mardi 4 juin 2002
7.1(2)	Premier correctif des	9 février 2002

	fonctionnalités de 7.1(1)	
--	---------------------------	--

Si vous avez besoin des fonctionnalités du train Cisco Catalyst OS 7.X, il est plus prudent de le considérer comme un train de technologie. Adoptez la version dont le numéro de correctif est le plus élevé et évitez les versions les plus anciennes. Par exemple, la sortie de Cisco Catalyst OS 7.3(2) remonte au 2 août 2002, ce qui signifie que cette version n'est pas activement gérée. Les erreurs identifiées dans Cisco Catalyst OS 7.3(2) seront probablement corrigées dans une version plus récente, comme Cisco Catalyst OS 7.5.X.

A cet égard, pour un commutateur qui exige des fonctionnalités Cisco Catalyst OS 7.x, la version Cisco Catalyst OS 7.4(3) sera certainement le meilleur choix.

Catégories des versions de la plate-forme logicielle Cisco IOS

• **Versions ED (Early Deployment)** – Les versions de déploiement anticipé ou ED de la plate-forme logicielle Cisco IOS apportent de nouveaux développements sur le marché. Chaque révision de maintenance d'une version ED comprend non seulement des correctifs mais également de nouveaux ensembles de fonctionnalités, de nouveaux supports de plate-formes et des améliorations d'ordre général aux protocoles et à l'infrastructure de la plate-forme logicielle Cisco IOS. Tous les ans ou tous les deux ans, les fonctionnalités et les plates-formes des versions ED sont transposées sur la version Mainline suivante de Cisco IOS.

• **Versions LD (Limited Deployment)** – Ceci est la phase de maturité de la plate-forme logicielle Cisco IOS située entre la première livraison client ou FCS (First Customer Shipment) et le déploiement général des principales versions.

• **Versions GD (General Deployment)** – Au cours du cycle de vie de la version, Cisco décide qu'une version majeure est prête pour la certification GD ou Déploiement général. Seule une version majeure peut atteindre le statut GD : elle y parvient lorsque Cisco estime avoir satisfait aux critères suivants :

- la version a fait ses preuves après une large diffusion sur le marché et sa mise en œuvre dans de nombreux réseaux ;
- elle répond aux critères d'évaluation de stabilité et d'erreurs ;
- les enquêtes de satisfaction clientèle sont positives ; et
- elle offre une diminution de la tendance normalisée relative aux erreurs constatées par le client par rapport aux quatre précédentes versions de maintenance.

Une équipe inter-fonctionnelle de défense client pour la certification GD est constituée afin d'évaluer chaque défaut important de la version. Cette équipe réunit des ingénieurs du centre d'assistance technique Cisco TAC (Technical Assistance Center), des services AES (Advanced Engineering Services), des tests STE (System Test Engineering) et du développement de Cisco IOS. L'équipe délivre l'approbation finale pour la certification GD. Une fois qu'une version a atteint le statut GD, toutes ses révisions ultérieures possèdent le même statut.

Cela signifie que dès qu'une version est reconnue comme GD, elle entre automatiquement dans la phase de maintenance restreinte. Dans cette phase, les modifications d'ingénierie du code, y compris les correctifs exigeant une révision lourde du code, sont strictement limitées et placées sous la supervision d'un gestionnaire de programmes. On garantit ainsi qu'aucune erreur grave ne sera introduite dans une version certifiée GD de la plate-forme logicielle Cisco IOS. Le statut GD est accordé à une version de maintenance particulière.

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

Les mises à jour de maintenance ultérieures de cette version bénéficient à leur tour du statut GD. La plate-forme Cisco IOS 12.0, par exemple, a reçu la certification GD pour la version 12.0(8). Ainsi, les versions Cisco IOS 12.0(9), 12.0(10), etc. sont également des versions GD.

Pour plus d'informations sur le cycle de vie de la plate-forme logicielle Cisco IOS, visitez : <http://www.cisco.com/go/IOS>

Cisco IOS Safe Harbor

L'objectif de Cisco IOS Safe Harbor est l'amélioration de la stabilité, de la fiabilité et des performances de réseau du point de vue de la plate-forme logicielle Cisco IOS. Safe Harbor comprend la réalisation de tests sur les ensembles de fonctionnalités et les protocoles d'une image donnée de Cisco IOS Software version 12.1 E sur la plate-forme Cisco Catalyst 6500, afin de fournir un code de haute qualité pour les entreprises de services financiers. Cette combinaison de fonctionnalités, de matériels et d'image est testée dans un environnement de laboratoire qui simule le réseau d'une entreprise de services financiers en reprenant des topologies régulièrement mises à jour et des configurations fournies par le client. Pour des détails complémentaires sur le programme Cisco Safe Harbor, visitez : <http://www.cisco.com/univercd/cc/td/doc/solution/systest/safehbr/>.

Résumé des catégories de version de la plate-forme logicielle Cisco IOS

Lorsque vous devez choisir des versions stables de la plate-forme logicielle Cisco IOS, les versions GD (General Deployment) et LD (Limited Deployment) sont préférables. Certaines versions Cisco Cat6K IOS subissent des tests supplémentaires dans le cadre du programme Safe Harbor.

« Version recommandée » ou « Version acceptable » ?

Cisco IT-LAN-SJ reconnaît le concept de version recommandée ainsi qu'une liste de versions acceptables. Nos ingénieurs réseaux utilisent la version recommandée s'ils doivent déployer une nouvelle unité. Les versions acceptables sont différentes des versions recommandées mais ne nécessitent pas de mise à niveau immédiate. Si une erreur critique est découverte dans une version acceptable, celle-ci est retirée de la liste des acceptables : cela signifie que toutes les unités qui exécutent cette version doivent être rapidement mises à niveau.

Révision périodique des versions de code

Cisco IT-LAN-SJ opte pour de nouvelles versions recommandées dans deux cas :

1. lorsqu'une erreur critique est découverte dans la version recommandée en cours – dans ce cas, la version recommandée précédente devient inacceptable et les unités qui les exécutent doivent être rapidement mises à niveau ;
2. tous les 3 à 6 mois, les versions recommandées sont révisées et mises à jour. Dans ce cas, la précédente version recommandée est généralement rétrogradée dans la liste des versions acceptables.

Les projets de mise à niveau d'urgence – la mise à niveau dans un court délai d'un grand nombre d'unités – sont démoralisants. Ils surviennent lorsque la version recommandée passe directement au statut « inacceptable » après la découverte d'une erreur critique. Il convient de minimiser ces mises à niveau d'urgence en disposant de deux ou trois versions acceptables et en effectuant progressivement les mises à niveau à la version recommandée, de préférence pendant d'autres interventions indispensables.

Les exceptions qui exigent des versions différentes

Unifier les versions logicielles de Cisco IOS lorsqu'un petit nombre d'unités exigent les fonctionnalités d'un nouveau train de technologie est une lutte de tous les instants. Faut-il unifier ces versions en dotant tous les routeurs d'un même train de technologie, ou est-il préférable que 90 % des routeurs utilisent le train Mainline tandis que les exceptions exécuteront le train de technologie ? Imaginons que vous disposiez de 100 routeurs dont 10 exigent les fonctionnalités du train 12.2T.

Deux possibilités s'offrent à vous :

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

1. vous installez Cisco IOS 12.2T sur 100 routeurs ;
2. vous installez Cisco IOS 12.2M sur 90 routeurs et Cisco IOS 12.2T sur 10 routeurs ;

S'il est nécessaire de mettre à niveau les routeurs équipés de Cisco IOS 12.2T tous les trimestres, la première solution se traduit par 100 mises à niveau tous les trois mois. Mais si les routeurs équipés de Cisco IOS 12.2M n'ont besoin d'une mise à niveau que tous les trois trimestres, la deuxième solution se traduit par 40 mises à niveau tous les trois mois. En acceptant le surcoût d'une double norme, vous réduisez de 60 % le temps consacré aux mises à niveau de la plate-forme logicielle Cisco IOS. Bien que le fait d'avoir deux versions augmente les frais d'assistance, ce surcoût est relativement minime. C'est pour cela que Cisco IT-LAN-SJ utilise du code Mainline chaque fois que cela est possible. Seuls quelques routeurs qui nécessitent des fonctionnalités particulières exécutent le train Cisco IOS 12.2T.

Etape 7 : Formation au dépannage

Ironiquement, lorsque vous atteignez une disponibilité de 99,99 %, l'absence d'interruptions finit par émousser vos compétences de dépannage. Lorsque la disponibilité est faible, vous n'avez pas vraiment besoin de formation particulière, mais dès qu'elle touche les 99,99 %, il devient nécessaire d'organiser des exercices réguliers de dépannage. L'équipe du réseau Cisco IT-LAN-SJ tient chaque semaine des réunions administratives et techniques distinctes. Régulièrement, ces réunions techniques amènent des ingénieurs à réparer un réseau de laboratoire qui a été délibérément mis en panne. Bien qu'imparfaite, cette formation au dépannage permet de ne pas perdre la main malgré le « problème » que représente la pénurie de défaillances réseau.

Etape 8 : Séparation de la gestion des incidents et de la résolution des problèmes

En cas d'interruption du service réseau, l'équipe informatique de Cisco IT remplit deux fonctions :

- elle résout le problème ;
- elle gère les communications et la remontée des informations concernant l'incident.

Le département informatique de Cisco sépare ces fonctions en deux groupes distincts. L'équipe de Cisco IT-LAN-SJ est responsable de la résolution des interruptions de service réseau tandis que le personnel de l'OCC gère les incidents.

L'OCC fonctionne 24 heures sur 24, tous les jours de l'année, avec une équipe dont la principale mission est de détecter les interruptions de service P1 et P2 (soit grâce à notre système de gestion de réseau ou sur rapport de problème client). Le personnel de l'OCC ne cherche pas à résoudre le problème mais contacte les équipes d'assistance concernées. Un problème sur le réseau LAN de San Jose sera ainsi transmis au responsable de service du réseau Cisco IT-LAN-SJ.

L'OCC ouvre ensuite un pont de conférence pour réunir les personnes concernées. Si nécessaire, le personnel de l'OCC contacte le service d'assistance constructeur (y compris Cisco TAC) et le connecte sur le pont de conférence. Il détermine la gravité du problème et envoie des notifications à la direction. Il continue d'informer la direction à intervalles déterminés en fonction de la gravité de l'incident. Celle-ci déterminera s'il est nécessaire d'affecter du personnel technique supplémentaire à la résolution de l'incident.

Après un incident, le personnel de l'OCC assure un suivi pour vérifier que les causes fondamentales ont été identifiées et, si nécessaire, qu'une solution à long terme a été trouvée pour éviter que le problème se reproduise.

En remettant à l'OCC le travail de notification et de transmission de l'information, les ingénieurs réseaux sont libres de se concentrer sur la résolution du problème technique. Ceci garantit également la cohérence des notifications et des remontées de l'information. L'OCC simplifie également la prévention des interruptions en assurant le suivi des activités d'analyse des causes fondamentales et de correctifs à long terme. Cette séparation des fonctions de gestion des incidents et de résolution des problèmes améliore la qualité du service et réduit la durée des interruptions.

Les étapes Cisco pour une disponibilité de 99 999 %

- Pour atteindre une disponibilité de 99,9 % (8,7 heures d'interruptions de service par an), vous devez disposer d'un réseau stable et bien conçu.
- Pour atteindre une disponibilité de 99,99 % (53 heures d'interruptions de service par an), vous devez disposer d'un réseau encore plus robuste.
- Pour atteindre une disponibilité de 99,999 % (315 secondes d'interruption de service par an, soit moins d'une seconde par jour), votre réseau doit être presque parfait en tout point.

Pour le département informatique de Cisco, qui détermine la disponibilité de chaque unité toutes les 15 à 20 secondes, chaque appareil n'a pas le droit d'échouer à plus d'une mesure de disponibilité toutes les trois semaines. Un tel niveau de disponibilité est extrêmement difficile à obtenir.

Pour y parvenir sur un réseau LAN, le département informatique de Cisco recommande d'adopter toutes les étapes nécessaires aux niveaux 99,9 % et 99,99 %, plus les trois étapes suivantes :

Etape 1 : Toutes les unités doivent être sur générateur de secours

Il est impossible d'atteindre moins d'une seconde de temps d'arrêt par jour sur chaque unité et de subir une coupure électrique imprévue. Dans les secteurs où le réseau Cisco IT-LAN-SJ doit atteindre une disponibilité de 99,999 %, Cisco place chaque unité sur onduleur et générateur de secours pour éviter les conséquences d'une panne d'électricité.

Etape 2 : Contrôle automatique de la configuration des commutateurs

Pour atteindre une disponibilité de 99,99 %, l'équipe du réseau Cisco IT-LAN-SJ a développé une configuration standard des routeurs et un contrôle automatisé de cette configuration appuyé sur le système RAT de www.cisecurity.org.

Une disponibilité de 99,999 % exige l'audit proactif de la configuration standard des commutateurs, de préférence de manière automatisée. L'équipe du Cisco IT-LAN-SJ utilise également le système RAT avec un fichier de configuration modifié pour auditer les fichiers de configuration de ses commutateurs.

Etape 3 : Audit manuel semi-annuel

Même les plus intelligents des outils automatisés d'audit de la redondance et des configurations ne peuvent pas faire face à tout. Pour atteindre une disponibilité de 99,999 %, l'équipe du Cisco IT-LAN-SJ a commencé à vérifier manuellement, au moins tous les six mois, l'ensemble des connectivités, de la topologie, des plans de réseaux et des configurations. Plus particulièrement, il est essentiel de vérifier la bonne tenue de la hiérarchie logique et physique déployée pour atteindre une disponibilité de 99,99 %.

Les tactiques spécifiques de Cisco pour améliorer la disponibilité du réseau Production

En plus des étapes décrites dans les sections précédentes sur la disponibilité, la séparation des réseaux Production et Alpha, ainsi que l'utilisation de l'organisation interne d'assistance technique contribuent à améliorer la disponibilité du réseau Production.

Séparation des réseaux Production et Alpha

Nous sommes une entreprise de création de réseau, ce qui impose les objectifs suivants à l'équipe informatique Cisco chargée de la topologie :

1. fournir un réseau fiable pour l'entreprise ;
2. créer un réseau de référence pour nos clients ;
3. devenir le premier, le meilleur et le plus exigeant de nos clients.

Le premier objectif, l'assurance d'un réseau fiable, nous demande de n'exécuter que du code et des plates-formes testées dans nos efforts pour atteindre la haute disponibilité. Toutefois, le troisième de nos objectifs, devenir le premier, le meilleur et le plus exigeant de nos clients, nous impose d'exécuter du code non encore commercialisé sur du matériel d'avant-garde afin d'améliorer encore les produits Cisco pour nos clients. A première vue, ces deux objectifs sont incompatibles.

La solution consiste à gérer deux réseaux en parallèle – le réseau Production et le réseau Alpha. Le réseau Production est accessible par deux jacks de réseau dans chaque bureau ou espace de travail. Le réseau Alpha n'est accessible que par un seul jack de réseau, généralement de couleur orange, sur environ 40 % du campus de San Jose. Cisco cherche à placer les développeurs sur le réseau Alpha lorsqu'ils travaillent sur leurs produits. Les ingénieurs sont encouragés à se connecter au réseau Alpha, jack orange, par des audits automatisés périodiques dont les résultats sont transmis à la direction.

Les réseaux Production et Alpha sont tous deux connectés par routage statique à un point de démarcation. Alors que les procédures de gestion des changements sont très rigoureuses sur le réseau Production, celles du réseau Alpha sont minimales – et permettent même des changements pendant les heures de travail, si cela est nécessaire au développement. La seule exigence est l'envoi d'un courrier électronique au bâtiment concerné afin d'avertir les employés de se rebrancher sur le réseau Production pendant quelques heures.

La séparation entre les réseaux Production et Alpha permet au premier d'atteindre d'excellents résultats en termes de disponibilité et à Cisco de tester ses produits en interne avant de les publier.

Le centre d'assistance technique

Nous voulons être notre premier client. Le département informatique de Cisco utilise pour cela les mêmes mécanismes d'assistance que ceux de nos clients, y compris les achats d'équipements en interne par l'intermédiaire de www.cisco.com et le recours au centre Cisco TAC (Technical Assistance Center) pour corriger les incidents. Cette politique présente le double avantage d'être à la fois

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

économique et tactique car les compétences du centre TAC et de l'équipe du Cisco IT-LAN se complètent. Les ingénieurs de Cisco TAC sont des « dépanneurs » professionnels, formés à la résolution de problèmes sur n'importe quel réseau. L'équipe du Cisco IT-LAN est formée à la construction de réseaux spécifiques fiables en cherchant à tout prix à éviter les problèmes. L'équipe du Cisco IT-LAN fait également appels aux ingénieurs du Cisco Advanced Services (voir http://www.cisco.com/en/US/products/svcs/ps11/serv_category_home.html) qui l'aident à concevoir le réseau et à choisir les versions de la plate-forme logicielle Cisco IOS.

Adoption des recommandations précédentes par l'équipe du Cisco IT-LAN-SJ

Les étapes nécessaires pour atteindre une disponibilité de 99,999 % peuvent engendrer des coûts prohibitifs si elles sont adoptées sans planification au préalable. Le département informatique de Cisco a mis en œuvre un grand nombre des étapes précédentes, mais pas toutes, ni dans tous les secteurs pour des raisons de coûts - bénéfiques. En effet, certains secteurs de notre réseau, comme les réseaux de laboratoire, sont considérés comme moins importants que d'autres, notamment les centres de calcul.

L'analyse coûts – bénéfiques de la haute disponibilité donne des résultats différents suivant les parties du réseau. Nous donnons ci-dessous un résumé des étapes adoptées par l'équipe du réseau Cisco IT-LAN-SJ dans les différents secteurs. A titre de référence, nous rappelons également les disponibilités ajustées atteintes dans chacun de ces secteurs.

Le tableau co-joint récapitule les résultats de la disponibilité ajustée en 2002 pour chacun des sous-groupes gérés par l'équipe du réseau Cisco IT-LAN-SJ, ainsi que les étapes déployées dans chacun des sous-groupes pour atteindre la haute disponibilité.

Disponibilité ajustée pour l'année 2002

Sous-groupe	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Réseau Call Manager	Ordinateurs des sites 1 à 3	Ordinateurs du site 4	Ordinateurs du site 5	Ordinateurs du réseau MAN	Labo
Disponibilité ajustée 2002 (%)	99,997	99,996	99,995	99,991	99,992	99,998	99,997	99,998	99,993	99,991	99,995	99,991	99,973

Etapes pour une disponibilité de 99,9 %

Mesure de la disponibilité	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Alertes d'interruption de service	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Hiérarchie physique	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Hiérarchie logique	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Analyse des causes fondamentales	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Onduleurs pour les unités critiques	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Gestion de la redondance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non
Gestion des changements	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Pièces de rechange en cas d'urgence	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Gestion hors bande	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Etapes pour une disponibilité de 99,99 %

Sous-groupe	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Réseau Call	Ordinateurs	Ordinateurs du	Ordinateurs du	Ordinateurs du	Labo
-------------	------	------	------	------	------	------	------	-------------	-------------	----------------	----------------	----------------	------

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

								Man- ger	des sites 1 à 3	site 4	site 5	réseau MAN	
Contrôle proactif de la redondance	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Onduleurs pour toutes les unités	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Oui
Générateurs pour les unités critiques	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Audits automatisés sur la configuration des routeurs	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Intégration de la gestion des changements avec la surveillance de la disponibilité	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Normalisation des versions de code	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Formation au dépannage	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Gestion distincte des incidents	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Etapes pour une disponibilité de 99 999 %

Générateurs pour toutes les unités	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non	Non
Audits automatisés de la configuration des commutateurs	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Audit manuel semi-annuel	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non	Non

La disponibilité s'est améliorée dans l'ensemble pour atteindre 99,995 %. Voici les moyennes obtenues sur 12 mois d'affilée (de juillet 2002 à juin 2003) :

Sous-groupe	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Réseau Call Man- ger	Ordina- teurs des sites 1 à 3	Ordina- teurs du site 4	Ordina- teurs du site 5	Ordina- teurs du réseau MAN	Labo
Disponibilité ajustée de juillet 2002 à juin 2003 (%)	99,999	99,997	99,997	99,998	99,999	99,998	99,998	100,000	99,996	99,994	99,998	99,996	99,987

Nombre d'unités par sous-groupe en juin 2003 (novembre 2002 pour le DDC5)

Sous-groupe	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Réseau Call Man- ger	Ordina- teurs des sites 1 à 3	Ordina- teurs du site 4	Ordina- teurs du site 5	Ordina- teurs du réseau MAN	Labo
Nombre d'unités	26	10	72	11	10	5	23	17	166	374	78	39	39

Statistiques mensuelles de disponibilité ajustée de janvier 2002 à juin 2003

Sous-groupe	Général e	PDC1	PDC2	DDC1	DDC2	DDC3	DDC4	DDC5	Réseau CM	Ordina- teurs des sites 1 à 3	Ordina- teurs du site 4	Ordina- teurs du site 5	Ordina- teurs du réseau MAN	Labo
Jan. 2002	99,998	100,000	99,999	99,996	99,999	99,997	99,999	99,998	99,999	99,998	99,998	99,996	99,999	99,998
Fév. 2002	99,985	99,992	99,999	99,999	99,931	99,946	99,991	99,996	99,993	99,995	99,991	99,993	99,997	99,980
Mar. 2002	99,994	99,998	99,992	99,999	99,989	99,990	99,997	99,994	99,995	99,991	99,999	99,988	99,995	99,979

Cisco IT-LAN-SJ : la haute disponibilité en quelques étapes

Avr. 2002	99,992	99,989	99,999	99,987	99,994	99,993	99,999	99,999	100,000	99,998	99,997	99,989	99,960	99,968
Mai 2002	99,994	99,998	99,999	99,994	99,999	99,999	99,998	99,998	99,998	99,969	99,994	99,997	99,990	99,892
Juin 2002	99,987	99,991	99,975	99,980	99,993	99,993	99,994	99,997	99,990	99,989	99,975	99,985	99,985	99,984
Juil. 2002	99,999	99,999	99,999	100,000	100,000	100,000	99,999	100,000	100,000	100,000	99,999	99,997	99,999	99,999
Août 2002	99,999	99,997	100,000	100,000	99,999	99,999	99,998	100,000	100,000	100,000	100,000	99,999	100,000	99,994
Sep. 2002	99,998	100,000	99,986	100,000	99,996	99,995	100,000	100,000	100,000	99,998	100,000	100,000	99,998	99,998
Oct. 2002	99,995	100,000	100,000	100,000	99,996	99,997	100,000	99,988	99,999	99,999	100,000	100,000	99,996	99,961
Nov. 2002	99,997	100,000	100,000	99,984	100,000	100,000	100,000	100,000	99,998	99,999	99,998	99,999	99,988	99,999
Déc. 2002	99,970	99,998	99,999	99,999	99,994	99,999	99,999	-	100,000	99,979	99,945	99,997	99,984	99,925
Jan. 2003	99,997	100,000	100,000	99,996	99,999	99,999	99,989	-	100,000	99,996	99,997	99,996	99,999	99,999
Fév. 2003	99,999	100,000	99,999	99,997	100,000	100,000	100,000	-	100,000	99,999	99,999	100,000	99,999	99,999
Mar. 2003	99,995	99,998	99,996	99,998	99,995	99,998	99,998	-	99,998	99,993	99,993	99,997	99,997	99,996
Avr. 2003	99,998	99,999	99,999	99,999	99,999	100,000	99,999	-	100,000	99,999	99,998	99,998	99,997	99,994
Mai 2003	99,997	100,000	99,984	99,996	99,999	99,998	100,000	-	99,999	99,997	99,999	99,996	99,990	99,985
Juin 2003	99,998	100,000	100,000	100,000	100,000	100,000	99,999	-	100,000	99,996	99,998	99,998	99,999	99,992