Gestion de la configuration : Livre blanc sur les pratiques recommandées

Contenu

Introduction

La gestion de la configuration est une collection de processus et d'outils qui favorisent la cohérence de réseau, dépistent la modification de réseau, et fournissent la documentation réseau et la visibilité à jour. En établissant et en mettant à jour des meilleures pratiques de gestion de la configuration, vous pouvez vous attendre à plusieurs avantages tels que la disponibilité améliorée du réseau et des coûts inférieurs. Ceux-ci incluent :

- Des coûts de support plus à prix réduit dus à une diminution des problèmes d'assistance réactive.
- Des coûts du réseau plus à prix réduit dus au périphérique, au circuit, et à l'utilisateur dépistant les outils et les processus qui identifient les parties du réseau inutilisées.
- Disponibilité du réseau améliorée due à une diminution des coûts d'assistance réactive et du temps amélioré des résolutions des problèmes.

Nous avons vu les questions suivantes résulter d'un manque de gestion de la configuration :

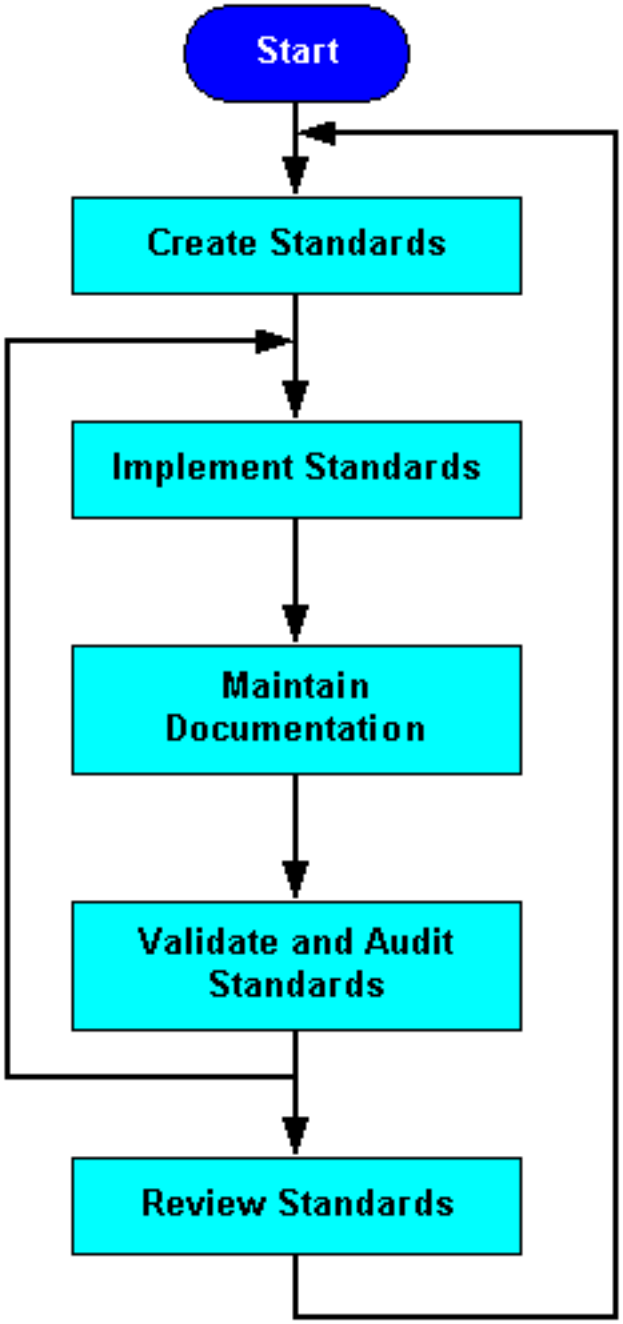
- Incapacité de déterminer l'impact pour l'utilisateur des modifications de réseau

- Problèmes d'assistance réactive et disponibilité inférieure accrus
- Temps accru aux résolutions des problèmes
- Des coûts du réseau plus élevés dus aux parties du réseau inutilisées

Ce document sur les pratiques recommandées fournit un organigramme de processus pour mettre en application un plan de gestion de la configuration réussi. Nous regarderons les étapes suivantes en détail : créez les normes, mettez à jour la documentation, et la validez et des normes d'audit.

Flux de processus à niveau élevé pour la gestion de la configuration

Le diagramme au-dessous des expositions comment vous pouvez utiliser les facteurs de succès capital suivis des indicateurs de performances pour implémenter un plan de gestion de la configuration réussi.



Créez les normes

En créant des normes pour des aides de cohérence de réseau réduisez la complexité de réseau, la quantité d'interruption imprévue, et l'exposition au réseau affectant des événements. Nous recommandons les normes suivantes pour la cohérence optimale de réseau :

- Contrôle et Gestion de version de logiciel
- Normes et Gestion d'adressage IP
- Nommer des conventions et des affectations de système de noms de domaine/protocole DHCP (DNS/DHCP)
- Configurations et descripteurs standard
- Procédures de mise à niveau de la configuration
- Modèles de solution

Contrôle et Gestion de version de logiciel

Le contrôle de version de logiciel est la pratique de déployer des versions de logiciel cohérentes sur les périphériques semblables de réseau. Ceci améliore l'occasion pour la validation et le test sur les versions du logiciel choisies et limite considérablement la quantité d'erreurs de logiciel et les problèmes d'interopérabilité fondent dans le réseau. Les versions de logiciel limitées réduisent également le risque de comportement inhabituel avec les interfaces utilisateur, la sortie de commande ou de Gestion, le comportement de mise à jour et le comportement de caractéristique. Ceci rend l'environnement moins complexe et plus facile à prendre en charge. De façon générale, le contrôle de version de logiciel améliore la Disponibilité de réseau et les aides diminuent des coûts d'assistance réactive.

Remarque: Des périphériques semblables de réseau sont définis en tant que périphériques standard de réseau avec un châssis commun fournissant un service commun.

Implémentez les étapes suivantes pour le contrôle de version de logiciel :

- Déterminez les classifications de périphérique basées sur le châssis, la stabilité, et les nouvelles exigences de fonctionnalité.
- Différentes versions de logiciel de cible pour les périphériques semblables.
- Le test, valident, et des versions du logiciel choisies de pilote.
- Versions réussies de document en tant que norme pour la classification de semblable-périphérique.
- Déployez-vous uniformément ou les périphériques semblables upgrade all vers la version de logiciel standard.

Normes et Gestion d'adressage IP

La gestion d'adresse IP est le processus d'allouer, de réutiliser et de documenter des adresses IP et des sous-réseaux dans un réseau. Les normes d'adressage IP définissent la taille de sous-réseau, affectation de sous-réseau, des affectations de périphérique de réseau et les affectations d'adresses dynamiques dans un sous-réseau s'étendent. Les normes recommandées de gestion d'adresse IP réduisent l'occasion pour superposer ou sous-réseaux en double, non-récapitulation dans le réseau, affectations de périphérique d'adresse IP en double, espace d'adresse IP gaspillé, et complexité inutile.

La première étape à la gestion d'adresse IP réussie comprend les blocs d'adresse IP utilisés dans le réseau. Dans de nombreux cas, les organismes de réseau doivent se fonder sur l'espace d'adressage RFC 1918, qui n'est pas Internet adressable, mais peuvent être utilisés pour accéder au réseau en même temps que le Traduction d'adresses de réseau (NAT). Une fois que vous avez défini les blocs d'adresses, allouez-les aux zones du réseau d'une manière dont favorise la récapitulation. Dans de nombreux cas, vous devrez plus loin subdiviser ces blocs basés sur le nombre et la taille de sous-réseaux dans la marge définie. Vous devriez définir des tailles standard de sous-réseau pour des applications standard, taille telles que des tailles de tailles de sous-réseau de bâtiment, de sous-réseau de lien WAN, la taille de sous-réseau de bouclage, ou de site du WAN sous-réseau. Vous pouvez alors allouer des sous-réseaux pour de nouvelles applications hors d'un bloc de sous-réseau dans un plus grand bloc récapitulatif.

Par exemple, permettez-nous prennent un grand réseau d'entreprise avec un campus de Côte Est, un campus de côte ouest, un WAN classique, un WAN européen, et autre des sites internationaux de commandant. L'organisation alloue les blocs contigus du routage d'interdomain

d'ip classless (CIDR) à chacune de ces zones pour favoriser la récapitulation IP. L'organisation alors définit les tailles de sous-réseau dans ces blocs et alloue des paragraphes de chaque bloc à une taille particulière d'IP de sous-réseau. Chaque principal bloc ou l'espace d'adresse IP entier peut être documenté dans des sous-réseaux alloués, utilisés, et disponibles d'une apparence de tableur pour chaque taille disponible de sous-réseau dans le bloc.

L'étape suivante est de créer des normes pour des affectations d'adresse IP dans chaque marge de sous-réseau. Des adresses virtuelles de Routeurs et de Protocole HSRP (Hot Standby Router Protocol) dans un sous-réseau pourraient être assignées les premières adresses disponibles dans la marge. Des Commutateurs et les passerelles peuvent être assignés les prochaines adresses disponibles, suivies d'autres affectations d'adresses fixes, et des adresses finalement dynamiques pour le DHCP. Par exemple, tous les sous-réseaux de l'utilisateur peuvent être des sous-réseaux de /24 avec 253 affectations d'adresses disponibles. Les Routeurs peuvent être assignés la .1 et .2 adresse, et l'adresse attribuée de HSRP la .3 adresse, les Commutateurs .5 à .9, et la plage DHCP de .10 à .253. Qu'est ce que normes vous développez, elles devraient être documentées et mises en référence sur tous les documents de plan d'ingénierie des réseaux pour aider à assurer à déploiement cohérent.

Nommer des conventions et des affectations DNS/DHCP

L'utilisation cohérente et structurée de nommer des conventions et des DN pour des périphériques vous aide à gérer le réseau des manières suivantes :

- Crée un point d'accès cohérent aux Routeurs pour toute la Gestion de réseau relative à l'information à un périphérique.
- Réduit l'occasion pour les adresses IP en double.
- Crée l'identification simple d'un périphérique affichant l'emplacement, le type de périphérique, et le but.
- Améliore la gestion des stocks en fournissant une méthode plus simple pour identifier des périphériques de réseau.

La plupart des périphériques de réseau ont une à deux interfaces pour gérer le périphérique. Ceux-ci peuvent être une intrabande ou une interface Ethernet hors bande et une interface de la console. Vous devriez établir nommer des conventions pour ces interfaces liées au type de périphérique, à l'emplacement, et au type d'interface. Sur des Routeurs, nous recommandons vivement utilisant l'interface de bouclage comme interface de gestion principale parce qu'elle peut être accédée à de différentes interfaces. Vous devriez également configurer des interfaces de bouclage comme adresse IP source pour des déroutements, SNMP et messages de Syslog. Les interfaces individuelles peuvent alors avoir une convention nommante qui identifie le périphérique, l'emplacement, le but, et l'interface.

Nous recommandons également identifier des plages DHCP et les ajouter aux DN, y compris l'emplacement des utilisateurs. Ceci peut être une partie de l'adresse IP ou d'un emplacement physique. Un exemple pourrait être "dhcp-bâtiment-c21-10" au "dhcp-bâtiment-c21-253", qui identifie des adresses IP dans le C de bâtiment, le deuxième étage, l'armoire de câblage 1. Vous pouvez également utiliser le sous-réseau précis pour l'identification. Une fois qu'une convention nommante a été créée pour des périphériques et le DHCP, vous avez besoin d'outils pour dépister et gérer des entrées, telles que le Cisco Network Registrar.

Configuration et descripteurs standard

La configuration standard s'applique au protocole et les configurations de supports, aussi bien que

les commandes de configuration globale. Les descripteurs sont des commandes d'interface utilisées pour décrire une interface.

Nous recommandons créer des configurations standard pour chaque classification de périphérique, telle que le routeur, le commutateur de RÉSEAU LOCAL, le commutateur BLÊME, ou le commutateur ATM. Chaque configuration standard devrait contenir le global, les medias, et les commandes de configuration de protocole nécessaires pour mettre à jour la cohérence de réseau. La configuration de supports inclut la configuration atmosphère, de Relais de trames, ou de Fast Ethernet. La configuration de Protocol inclut des paramètres de configuration standard de protocole de routage IP, des configurations communes de Qualité de service (QoS), des Listes d'accès communes, et d'autres configurations exigées de protocole. Les commandes de configuration globale appliquent à tous les périphériques similaires et incluent des paramètres tels que des commandes de service, des commandes IP, des commandes TACACS, la configuration vty, des bannières, la configuration SNMP, et la configuration de Protocole NTP (Network Time Protocol).

Des descripteurs sont développés en créant un format standard qui s'applique à chaque interface. Le descripteur inclut le but et l'emplacement de l'interface, d'autres périphériques ou d'emplacements connectés à l'interface, et aux identifiants de circuit. Les descripteurs aident votre organisme de support mieux à comprendre la dimension des problèmes liés à une interface et permettent une résolution plus rapide des problèmes.

Nous recommandons maintenir des paramètres de configuration standard dans un fichier de configuration standard et télécharger le fichier à chaque nouveau périphérique avant le protocole et la configuration d'interface. En outre, vous devriez documenter le fichier de configuration standard, y compris une explication de chaque paramètre de configuration globale et pourquoi il est important. Le Resource Manager Essentials de Cisco (RME) peut être utilisé pour gérer les fichiers de configuration, la configuration de protocole, et les descripteurs standard.

Procédures de mise à niveau de la configuration

Les procédures de mise à niveau aident à s'assurer que le logiciel et les mises à niveau matérielles se produisent sans à-coup avec le temps d'arrêt minimal. Les procédures de mise à niveau incluent la vérification de constructeur, des références d'installation de constructeur telles que des notes de mise à jour, des méthodologies ou des étapes de mise à jour, des instructions de configuration, et des conditions de test requises.

Les procédures de mise à niveau peuvent varier considérablement selon des types de réseau, des types de périphérique, ou de nouveaux logiciels nécessaires. Des conditions requises de mise à jour de routeur individuel ou de commutateur peuvent être développées et testées dans un groupe d'architecture et être mises en référence dans n'importe quelle documentation de modification. D'autres mises à jour, impliquant des tout le réseau, ne peuvent pas être testées en tant que facilement. Ces mises à jour peuvent exiger d'une planification plus en profondeur, d'une implication de constructeur, et des étapes supplémentaires d'assurer le succès.

Vous devriez créer ou des procédures de mise à niveau de mise à jour en même temps que n'importe quel nouveau déploiement de progiciels ou release standard identifiée. Les procédures devraient définir toutes les étapes pour la mise à jour, mettre en référence la documentation de constructeur liée à mettre à jour le périphérique, et fournir des procédures de test pour valider le périphérique après la mise à jour. Une fois que des procédures de mise à niveau sont définies et validées, la procédure de mise à niveau devrait être mise en référence dans toute la documentation de modification appropriée à la mise à jour particulière.

Modèles de solution

Vous pouvez utiliser des modèles de solution pour définir les solutions réseau modulaires standard. Un module réseau peut être une armoire de câblage, un bureau sur site BLÊME, ou un concentrateur d'accès. Dans chaque cas vous devez définir, tester et documenter la solution pour aider à s'assurer que des déploiements semblables peuvent être effectués de la même manière. Ceci s'assure que les futures modifications se produisent à un niveau beaucoup plus à faible risque à l'organisation puisque le comportement de la solution est bien défini.

Créez les modèles de solution pour tous les déploiements et solutions plus à haut risque qui seront déployés plus d'une fois. Le modèle de solution contient tous les matériel, logiciel, configuration, câblage, et conditions requises pour l'installation standard pour la solution réseau. Des détails spécifiques du modèle de solution sont affichés comme suit :

- Matériel et modules de matériel comprenant la mémoire, l'éclair, l'alimentation, et les dessins de carte.
- Topologie logique comprenant des affectations, la Connectivité, la vitesse, et le type de média de port.
- Versions de logiciel comprenant le module ou les versions de firmware.
- Tous les configuration non standard, non de périphérique-particularité comprenant des protocoles de routage, configurations de supports, configuration VLAN, Listes d'accès, Sécurité, chemins de commutation, paramètres de spanning tree, et autres.
- Les besoins en matière de gestion hors bande.
- Conditions requises de câble.
- Conditions requises pour l'installation comprenant des environmentals, l'alimentation, et des emplacements d'étagère.

Notez que le modèle de solution ne contient pas beaucoup de conditions requises. Des conditions requises spécifiques telles que l'adressage IP pour la solution, nommer, les transferts de DN, les transferts DHCP, les affectations PVC, les descripteurs d'interface, et les autres spécifiques devraient être couvertes par des pratiques de gestion globales de configuration. Des conditions plus générales, telles que des configurations standard, des plans de gestion du changement, des procédures de mise à jour de documentation, ou des procédures de mise à jour de la gestion de réseau, devraient être couvertes par des pratiques de gestion de configuration générale.

Mettez à jour la documentation

Nous recommandons documenter le réseau et les modifications qui se sont produits dans le réseau à temps le temps quasi-réel. Vous pouvez utiliser cette information réseau précise pour le dépannage, les listes de périphériques d'outil de gestion de réseau, l'inventaire, la validation, et les audits. Nous recommandons utilisant les facteurs de succès capital suivants de documentation réseau :

- Périphérique en cours, lien, et inventaire utilisateur
- Système de contrôle de version de la configuration
- Log de configuration TACACS
- Documentation de la topologie du réseau

Périphérique en cours, lien, et inventaire utilisateur

Le périphérique en cours, le lien, et les informations d'inventaire utilisateur te permet de dépister l'Inventaire réseau et les ressources, l'incidence de problème, et l'incidence de modification de réseau. La capacité de dépister l'Inventaire réseau et les ressources par rapport aux aides d'exigences de l'utilisateur s'assurent que des périphériques de réseau administré sont activement utilisés, fournissent des informations requises pour des audits, et aident à gérer des ressources du périphérique. Les données de relations d'utilisateur fournissent des informations pour définir le risque et l'incidence de modification, aussi bien que la capacité à dépannent plus rapidement et des résolutions des problèmes. Le périphérique, le lien, et les bases de données d'inventaire utilisateur sont typiquement élaborés par beaucoup de principales organisations du fournisseur de service. Le développeur principal du logiciel d'Inventaire réseau est Visionael Corporation . La base de données peut contenir des tables pour les périphériques similaires, des liens, et des données d'utilisateur de client/serveur de sorte que quand un périphérique est en baisse ou des modifications de réseau se produisent, vous puissiez facilement comprendre l'incidence d'utilisateur.

Système de contrôle de version de la configuration

Un système de contrôle de version de la configuration met à jour les configurations en cours d'exécution de tous les périphériques et d'un ensemble de versions courantes précédentes. Ces informations peuvent être utilisées pour des audits de dépannage et de configuration ou de modification. Pour le dépannage, vous pouvez comparer la configuration en cours d'exécution aux versions fonctionnelles précédentes pour aider à comprendre si la configuration est liée au problème de quelque façon. Nous recommandons mettre à jour trois à cinq versions fonctionnelles précédentes de la configuration.

Log de configuration TACACS

Pour identifier qui ont apporté les modifications de configuration et quand, vous pouvez utiliser se connecter et NTP TACACS. Quand ces services sont activés sur des périphériques de réseau de Cisco, l'ID utilisateur et l'horodateur est ajouté au fichier de configuration lorsque la modification de configuration est apportée. Cet horodatage des messages est alors copié avec le fichier de configuration sur le système de contrôle de version de la configuration. TACACS peut alors agir en tant que moyen de dissuasion pour la modification de non pris en charge et fournir un mécanisme pour apurer correctement les modifications qui se produisent. TACACS est activé utilisant le produit Cisco Secure. Quand les journaux de l'utilisateur dans le périphérique, il doivent authentifier avec le serveur TACACS en fournissant un ID utilisateur et un mot de passe. Le NTP est facilement activé sur un périphérique de réseau en indiquant le périphérique une horloge de ntp master.

Documentation de la topologie du réseau

Aides de documentation de topologie dans la compréhension et le support du réseau. Vous pouvez l'employer pour valider des directives de conception et pour comprendre mieux le réseau pour la future conception, modification, ou dépannage. La documentation de topologie devrait inclure la documentation logique et physique, y compris la Connectivité, l'adressage, les types de média, les périphériques, les affichages d'étagère, les affectations de carte, le câblage, l'identification de câble, les points d'arrêt, les informations d'alimentation, et les informations d'identification de circuit.

La mise à jour de la documentation de topologie est la clé à la bonne gestion de la configuration. Pour créer un environnement où la maintenance de documentation de topologie peut se produire,

l'importance de la documentation doit être soumise à une contrainte et les informations doivent être disponibles pour des mises à jour. Nous recommandons vivement mettre à jour la documentation de topologie toutes les fois que la modification de réseau se produit.

La documentation de la topologie du réseau est typiquement mise à jour utilisant une application graphique comme Microsoft Visio . Les autres produits comme Visionael fournissent des capacités supérieures pour gérer les informations topologiques.

Validez et des normes d'audit

Les indicateurs de performances de la gestion de la configuration fournissent un mécanisme pour valider et des normes et des facteurs de succès capital de configuration réseau d'audit. En mettant en application un programme d'amélioration du processus pour la gestion de la configuration, vous pouvez utiliser les indicateurs de performances pour identifier des questions de cohérence et pour améliorer la gestion de la configuration globale.

Nous recommandons créer une équipe croix-fonctionnelle pour mesurer le succès de gestion de la configuration et pour améliorer des processus de gestion de la configuration. Le premier objectif de l'équipe est d'implémenter des indicateurs de performances de la gestion de la configuration afin d'identifier des questions de gestion de la configuration. Nous discuterons les indicateurs de performances de la gestion de la configuration suivants en détail :

- Contrôles d'intégrité de configuration
- Périphérique, protocole, et audits de medias
- Normes et examen de documentation

Après l'évaluation des résultats de ces audits, initiez un projet pour réparer des incohérences et puis pour déterminer la cause initiale du problème. Les causes potentielles incluent un manque de documentation de normes ou un manque d'un processus cohérent. Vous pouvez améliorer la documentation de normes, implémenter la formation, ou améliorer des processus pour empêcher une incohérence plus additionnelle de configuration.

Nous recommandons des audits mensuels, ou probablement la fois par trimestre si seulement la validation est nécessaire. Passez en revue les audits passés pour confirmer que cela des problèmes de passé sont résolus. Recherchez les améliorations et les buts globaux pour expliquer la progression et la valeur. Créez les mesures pour afficher la quantité d'à haut risque, de support-risque, et d'incohérences à faible risque de configuration réseau.

Contrôles d'intégrité de configuration

Le contrôle d'intégrité de configuration devrait évaluer la configuration globale du réseau, sa complexité et cohérence, et éventuels problèmes. Pour des réseaux de Cisco, nous recommandons utilisant l'outil de validation de configuration de Netsys. Cet outil entre toutes les configurations de périphérique et crée un état de configuration qui identifie des problèmes en cours tels que les adresses IP, les non-concordances de protocole, et l'incohérence en double. L'outil signale toutes les questions de Connectivité ou de protocole, mais n'entre pas des configurations standard pour l'évaluation sur chaque périphérique. Vous pouvez manuellement passer en revue des standards de configuration ou créer un script qui signale des différences standard de configuration.

Périphérique, Protocol, et audits de medias

Le périphérique, le protocole, et les audits de medias sont un indicateur de performances pour la cohérence dans les versions de logiciel, des périphériques matériels et des modules, protocole et support, et nommer des conventions. Les audits devraient d'abord identifier toutes les questions non standard, qui devraient mener aux mises à jour de la configuration pour réparer ou améliorer les questions. Évaluez les processus globaux pour déterminer comment ils pourraient empêcher des déploiements suboptimaux ou non standard de se produire.

Cisco RME est un outil de gestion de la configuration qui peut apurer et rendre compte des versions de matériel, des modules et des versions de logiciel. Cisco développe également des audits plus complets de medias et de protocole qui signaleront l'incohérence avec l'IP, le DLSW, le Relais de trames et l'atmosphère. Si un audit de protocole ou de medias n'est pas développé, vous pouvez utiliser des audits manuels, tels que passer en revue des périphériques, des versions et des configurations pour tous les périphériques similaires dans un réseau, ou par la zone vérifiant des périphériques, des versions et des configurations.

Normes et examen de documentation

Cet indicateur de performances passe en revue la documentation de réseau et de normes pour s'assurer que les informations sont précises et à jour. L'audit devrait inclure passer en revue la documentation en cours, recommander des modifications ou des ajouts, et approuver de nouvelles normes.

Vous devriez passer en revue la documentation suivante sur une base trimestrielle : définitions standard de configuration, modèles de solution comprenant des configurations matérielles recommandées, versions de logiciel standard en cours, procédures de mise à niveau pour tous les périphériques et versions de logiciel, documentation de topologie, modèles en cours, et gestion d'adresse IP.

Informations connexes

- Support technique - Cisco Systems