Administration et sécurité des réseaux

Plan du cours

- Chap1: Introduction à l'administration des réseaux
- Chap2: Le protocole SNMP
- Chap3: Le service DHCP
- Chap4: Le service DNS
- Chap5: Le service FTP
- Chap6: introduction à la sécurité des réseaux
- Chap7: Les attaques réseaux
- Chap8: mécanismes cryptographiques de la sécurité
- Chap9: Autres mécanismes de sécurité
  - Filtrage, ACL et proxy
  - Les VLAN

Chapitre 1

Introduction à l'Administration des Réseaux

principes, modèles et standards

Introduction

- Besoin d'une administration des réseaux: pourquoi?
  - Passage d'une administration de quelques ordinateurs (multi-utilisateurs) à l'administration d'un réseau d'ordinateurs et d'équipements variés (périphériques, commutateurs, ponts, routeurs …) provenant de différents constructeurs et ayant différents systèmes d'exploitations
  - De nouveaux services réseaux doivent être mis en place (supports pour le développement d'application client serveurs, serveurs de noms, serveurs de disques, serveurs de bases de données ...)
- La nécessité d'outils inter-opérables d'administration et donc de standards
  - Modèle de l'ISO : CMIP, CMISE …
  - Modèle de de l'Internet : SNMP

Introduction

- L'administration d'un réseau ?
  - Ensemble des activités nécessaires afin d'offrir aux utilisateurs un service de qualité
- La qualité s'exprime en termes de
  - adéquation des services aux besoins
  - disponibilité
  - performance
  - efficacité
- Les domaines d'activités (selon l 'OSI)
  - Gestion des pannes
  - Gestion de la comptabilité
  - Gestion des configurations
  - Audit des performances
  - Gestion de la sécurité

Les domaines d'activités

- La gestion des pannes:
  - Détection, localisation, isolation, réparation
- Gestion des configurations
  - Identification des ressources
  - Installation, initialisation, paramétrage, reconfiguration.
  - Collecte des informations utiles et sauvegarde d'un historique.
- Audit des performances
  - Évaluation: collecter les données et établir des statistiques sur les performances (temps de réponse, taux d'utilisation, débit, taux d'erreur, disponibilité)
  - Gestion de trafic : satisfaire les besoins des users (à qui attribuer un grand dédit…)

Les domaines d'activités

- Gestion de la comptabilité:
  - Gérer la charge des ressources pour empêcher toute surcharge (congestion).
  - Gérer le coût d'utilisation des ressources et les facturer
  - Gérer le quota d'exploitation de la ressources (imprimante, disques…)
- Gestion de la sécurité
  - **But**: protéger les ressources du réseau et du système d'administration
  - **Comment**: Assurer les services de la sécurité (authentification, confidentialité, intégrité, disponibilité et non répudiation).
  - Moyen : cryptographie + logiciel de supervision + audit + firewall + surveillance des journaux d'évènements.
    - Journal de sécurité
    - Journal système
    - Journal application

Critères pour une organisation logique

- Critères informationnels:
  - Ensembles des informations servant à gérer le réseau
    - Information en provenance des équipements du réseau, des utilisateurs, des mesures effectuées.
    - Informations décrivant les différents composants du système (adresses, comptes utilisateurs, données de droit d'accès…)
- Critères fonctionnels:
  - Ensembles des fonctions servant à gérer le réseau
    - Ajout d'utilisateur, définition des droit d'accès, autorisation à un port, augmentation du débit d'un port…

Critères pour une organisation logique

- Critères temporels:
  - Évolution du système (matériel + logiciel)
    - À court terme (journalière)
    - Moyen terme : des jours → quelques mois
    - Long terme : des mois → année
- Critères de discipline:
  - Administration des utilisateurs, des fournisseur de services

Organisation logique

- Doit respecter les quatre critères déjà cités
  - Informationnels
  - Fonctionnel
  - Temporel
  - discipline
- Englobe (plan):
  - Les services de gestion du réseau réel
  - Les services de gestion du réseau logique
  - La gestion des performance
  - La gestion de la planification

Organisation logique

- Les services de gestion du réseau réel : activités à court terme qui gère les données en provenance du système
  - Collecter les données
  - Exécuter toutes les fonction du service
  - Prendre en compte les alertes et notifier les évènements
  - Déterminer et identifier les problèmes
  - Contrôler la configuration du système
  - Activer/ désactiver un élément du système
  - Assurer la maintenance technique.

Organisation logique

- Les services de gestion du réseau logique : activité à moyen terme basé sur les information stockées
  - Supprimer les information de gestion inutiles
  - Évaluer le niveau de la QOS.
  - Pouvoir maintenir un inventaire complet du système.
  - Gérer et interpréter les problèmes et les anomalies répertoriées
  - Pouvoir évaluer le trafic
  - Contrôler la sécurité (essayer d'exécuter des attaques)
  - Faire la comptabilité du système
  - Gérer la modification (conserver des traces).

Organisation logique

- La gestion des performance :
  - Établir et maintenir une BD des performances
  - Analyser et réguler le réseau
  - Définir les indicateurs de performances
- La gestion de la planification:
  - Établir les besoins
  - Étudier et déterminer une solution
  - Planifier l'implantation de cette solution

Les types de décisions

- Décisions opérationnelles : **à court terme**, journalière
  - suivi du fonctionnement du réseau
  - ajout / retrait / remise en fonctionnement d 'un service
  - réponse aux besoins des utilisateurs
  - mise en place des contrôles de sécurité et gestion des droits d 'accès
  - mesure de l'état de charge des ressources
  - gestion des évolutions immédiates nécessaires
  - comptabilisation des ressources
- Décisions tactiques :
  - → **à moyen terme**, concernant l'évolution du réseau et l'application des politiques de long terme
- Décisions stratégiques
  - → **à long terme**, stratégie pour le future

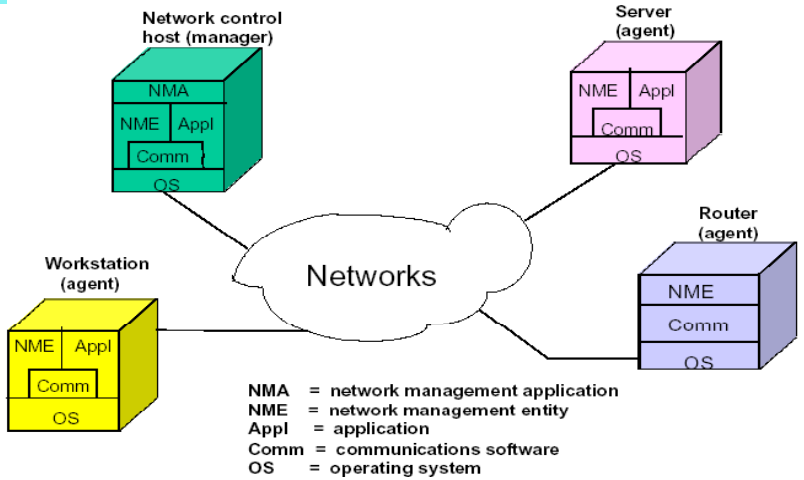
Caractéristiques d'un système d'administration

- Un système de gestion de réseau est une collection d'outils pour
  - observer et suivre l'état des ressources du réseau
  - contrôler le réseau en modifiant ses paramètres de fonctionnement
- Ces outils doivent
  - disposer d 'une seule interface conviviale pour l'opérateur et offrant un ensemble de commandes pour exécuter la plupart des tâches d 'administration
  - minimiser les équipements séparés en intégrant les composantes matérielles et logicielles dans les équipements existants

Architecture

- NMS : « Network Management System »
  - composé d'éléments incrémental matériel et logiciel
  - Il doit permettre une vision unifiée et globale du réseau
- NME « Network Management Entity »
  - extraction et collecte des statistiques relatives aux activités réseau
  - stockage des informations dans une base de données locale
  - réponse aux requêtes provenant d'un hôte de contrôle du réseau
    - transmettre les statistiques
    - transmettre la valeur de certains paramètres de fonctionnement
    - changer la valeur d 'un paramètre
    - générer un trafic artificiel pour effectuer certain test
    - générer des notifications sous certaines conditions

Architecture



- Il est possible de prévoir plusieurs hôte de contrôle dans l 'optique d 'une gestion distribuée du réseau

Modèles d'administration

- L'administration peut être vue au travers de 3 modèles (selon l'ISO)
  - Modèle organisationnel
  - Modèle fonctionnel
  - Modèles d'information

Modèles d'administration

- Modèle organisationnel
  - notion de domaine d'administration
  - Utilité : mise à l'échelle, sécurité, autonomie d'administration
    - Répartition des agents / « managers »
    - Un domaine peut comporter plusieurs agents / managers
    - Un agent / « manager »peut être partagé entre plusieurs domaines
    - Système d'administration coopératif et distribué

Modèles d'administration

- Modèle fonctionnel (SMFA « Specific Management Functionnal Areas »)
  - Gestion des erreurs : détecter, isoler, corriger les erreurs du réseau
  - Gestion de la configuration : configuration distante d'éléments du réseau
  - Gestion des performances : évaluation des performances
  - Gestion de comptes utilisateurs : faire payer l'utilisation du réseau en fonction de son utilisation, limiter l'utilisation des ressources
  - Gestion de la sécurité : contrôle d'accès, authentification, cryptage

Modèles d'administration

- Modèle d'information SMI « Structure of Management Information »
  - Ensemble de conventions pour la description et l'identification des données
  - Permet à n'importe quel type de protocole de manipuler les données (CMIP ou SNMP)
  - Management Information Base (MIB)
    - Dépôt conceptuel d'information de gestion
    - Ensemble des informations nécessaires à l'administration
    - Ne se préoccupe pas de l'aspect stockage des informations

Standards

- Pourquoi les standards?
  - Pour les utiliser dans une large gamme de produits (terminaux, ponts, routeurs …) et dans un environnement multi-constructeurs.
- Familles de standards
  - Internet Network Management Framework (IETF)
    - SNMPv1, SNMPv2, SNMPv3
  - OSI Network Management Framework (ISO/ITU-T)
    - CMISE/CMIP : common Management Information Service Element / CMI Protocol
  - Telecommunication Management Network (ITU-T)
    - TMN (M.3000 Series)
  - Distributed Management Task Force (DMTF)
    - DMI, CIM, WBEM