

Conception d'une architecture commutée

Conception d'une architecture commutée

Définition

Motivations

- ▶ L'architecture physique d'un réseau de campus doit maintenant répondre à certains impératifs comme
 - ▶ L'adaptabilité aux topologies changeant rapidement
 - ▶ La redondance en cas de failles réseaux
 - ▶ L'agrandissement du réseau
 - ▶ Centralisation des servers et applications pour simplifier l'administration
 - ▶ Support de plusieurs protocoles routables et commutables
- ▶ Pour cela, suivant les fonctions du réseau, il existe principalement 2 architectures types
 - ▶ L'architecture AVVID pour une convergence voix, donnée, vidéo
 - ▶ L'architecture multi-couches

AVVID

- ▶ Architecture for Voice, Video, and Integrated Data
- ▶ Conçu pour faciliter l'agencement et la conception des réseaux d'entreprises
- ▶ Composé de 3 éléments principaux
 - ▶ Infrastructure réseau : le matériel et les applications nécessaires au transport entre les utilisateurs et ses ressources
 - ▶ Intelligent Network Service : Permet d'obtenir le niveau de sécurité approprié aux utilisateurs ou aux applications, ainsi que la QoS, la disponibilité des services, la redondance, ...
 - ▶ Network Solutions : Ce sont les éléments du réseau qui supporte les service du « Intelligent Network Service »

L'architecture trois couches

- ▶ Avant l'architecture réseau était composée de la manière suivante
 - ▶ Les principaux services placée au centre du réseau avec des switch niveau 2 qui assurent le transport entre les utilisateurs et les ressources
- ▶ Maintenant l'architecture réseau recommandée est en 3 couches
 - ▶ Core Layer (le coeur du réseau): fournit un backbone à haut débit
 - ▶ Distribution Layer: implémente les politiques réseaux de l'entreprise
 - ▶ Access Layer: donne aux utilisateurs l'accès aux réseaux

Conception d'une architecture commutée

Le modèle réseau

Core Layer

- ▶ L'objectif de cette couche est de permettre la commutation entre les différentes couches de distribution aussi vite que possible
- ▶ Généralement cette partie est assurée par de l'interconnexion de niveau 2 uniquement
- ▶ L'utilisation de services de niveau 3 n'est pas recommandée
 - ▶ Les fonctionnalités de sécurité comme le filtrage de paquets ne sont pas appliquées par cette couche
 - ▶ Même avec des switches multi-niveaux, cela nécessite de la manipulation de paquets: ce qui ralentit le trafic réseau
 - ▶ Exception: dans le cas d'un très grand réseaux avec des équipements dans la couche distribution nécessitant une implémentation d'une commutation de niveau 3. A utiliser avec précaution !

Distribution Layer

- ▶ Cette couche se trouve entre le coeur du réseau et la couche d'accès aux réseaux
 - ▶ Interconnecter entre-eux les switches de la couche d'accès au réseau et faire la liaison avec le coeur de réseau
- ▶ Elle doit gérer les fonctionnalités de niveau 3 et mettre en place la politique de sécurité
- ▶ Mettre en place les VLANs
- ▶ Faire le routage entre les VLANs
- ▶ Effectuer l'agrégation des routes
- ▶ Relier entre-eux les différents types de média utilisés comme FDDI, Ethernet ou Token Ring
- ▶ Comme cette couche inter-connecte le coeur de réseau à la couche d'accès, elle doit être architecturée avec de la commutation rapide de niveau 3 (ou supérieure)

Access Layer

- ▶ Sur cette couche, il est possible de mélanger des réseaux commutés (switch) et partagés (hub)
- ▶ Définir les VLANs afin d'interdire la propagation des broadcasts et des multicasts
- ▶ Filtrer le trafic en fonction des adresses MAC
- ▶ Dédier de la bande passante à destination des serveurs
- ▶ Authentifier les accès des utilisateurs au réseau
- ▶ Cette couche est généralement composée de switches mais éventuellement aussi de routeurs pour les accès distants (ISDN, frame relay, ...)

Couche physique ou logique ?

- ▶ Ces 3 couches ne représentent qu'une architecture logique
 - ▶ Pas d'obligation de faire des distinctions physiques entre ces couches
- ▶ Problème du découpage réseau de manière hiérarchique
 - ▶ Couvre uniquement l'architecture d'un campus et ne prend pas en compte les particularités fonctionnelles d'un grand réseau d'entreprises (avec firewall, VPN, IDS, ATM, ADSL, ...)
- ▶ C'est pour cette raison qu'il existe un modèle découpé par fonctionnalités

Conception d'une architecture commutée

Enterprise Composite Network Model

Enterprise Composite Network Model

- ▶ La principale proposition de ce modèle est de définir des frontières claires entre les différents modules
- ▶ Cela rend plus aisé l'analyse du réseau
- ▶ 3 zones fonctionnelles
 - ▶ Enterprise Campus
 - ▶ Enterprise Edge
 - ▶ Service Provider Edge

Enterprise Campus

- ▶ Cette zone est structurée suivant le modèle hiérarchique en 3 couches mais n'inclut ni les accès distants, ni la connexion Internet
- ▶ 3 sous-modules forment l'infrastructure
 - ▶ Building Access : équivalent à l'Access layer
 - ▶ Building Distribution : équivalent au Distribution Layer
 - ▶ Campus Core : équivalent au Core Layer
- ▶ En plus de ces 3 sous-modules
 - ▶ Un sous-module Edge Distribution est ajouté afin de faire la connexion avec le module Entreprise Edge. Il sépare les utilisateurs de l'extérieur
 - ▶ Fonction similaire au Building Distribution
 - ▶ Un sous-module Server Farm qui contient les serveurs de l'entreprise comme les serveurs de BD, DNS, email, ... Les accès à ces ressources sont critiques et donc oblige une connexion redondante avec le Campus Core
 - ▶ Un sous-module d'Administration: gestion des comptes utilisateurs, log, ...

Enterprise Edge

- ▶ Contrôle le trafic entre le Service Provider Edge et l'Enterprise Campus
- ▶ Contient 4 sous-modules
 - ▶ E-commerce: services sécurisés fournis aux publiques
 - ▶ Internet Connectivity: fournit la connexion entre l'entreprise et Internet. Il contient les serveurs DNS, FTP, mail et Web
 - ▶ Remote Access et VPN: accès distant des utilisateurs via VPN ou des connexions établies à la demande sur des serveurs
 - ▶ WAN Access: responsable de la connexion entre site distant via des réseaux privées. On n'utilise pas dans ce cas de réseaux publique comme Internet.

Service Provider Edge

- ▶ Fournit les connexions publiques et privées aux WAN et MAN
- ▶ Composé de 3 sous modules
 - ▶ ISP: fournit la connexion internet
 - ▶ PSTN: connexion de type dial-up pour les accès distants
 - ▶ WAN: fournit des connexions permanentes vers des sites distants via des lignes louées, frame relay, ATM ou autres