

L'ESSENTIEL D'UN RÉSEAU D'ENTREPRISE (IGT-CONGOSERVE)

Mr Boris Mikamona

DG @Congoserve

bmikamona@congoserve.com

Mr Mael Nzila

Responsable Technique @Congoserve

mael@congoserve.com

- **les vlans**
- **les interfaces trunk**
- **le routage avec OSPF**
- **le HSRP**
- **Active Directory**
- **DHCP & DNS**
- **MPLS**
- **SD-WAN**
- **SD-LAN**
- **VXLAN**

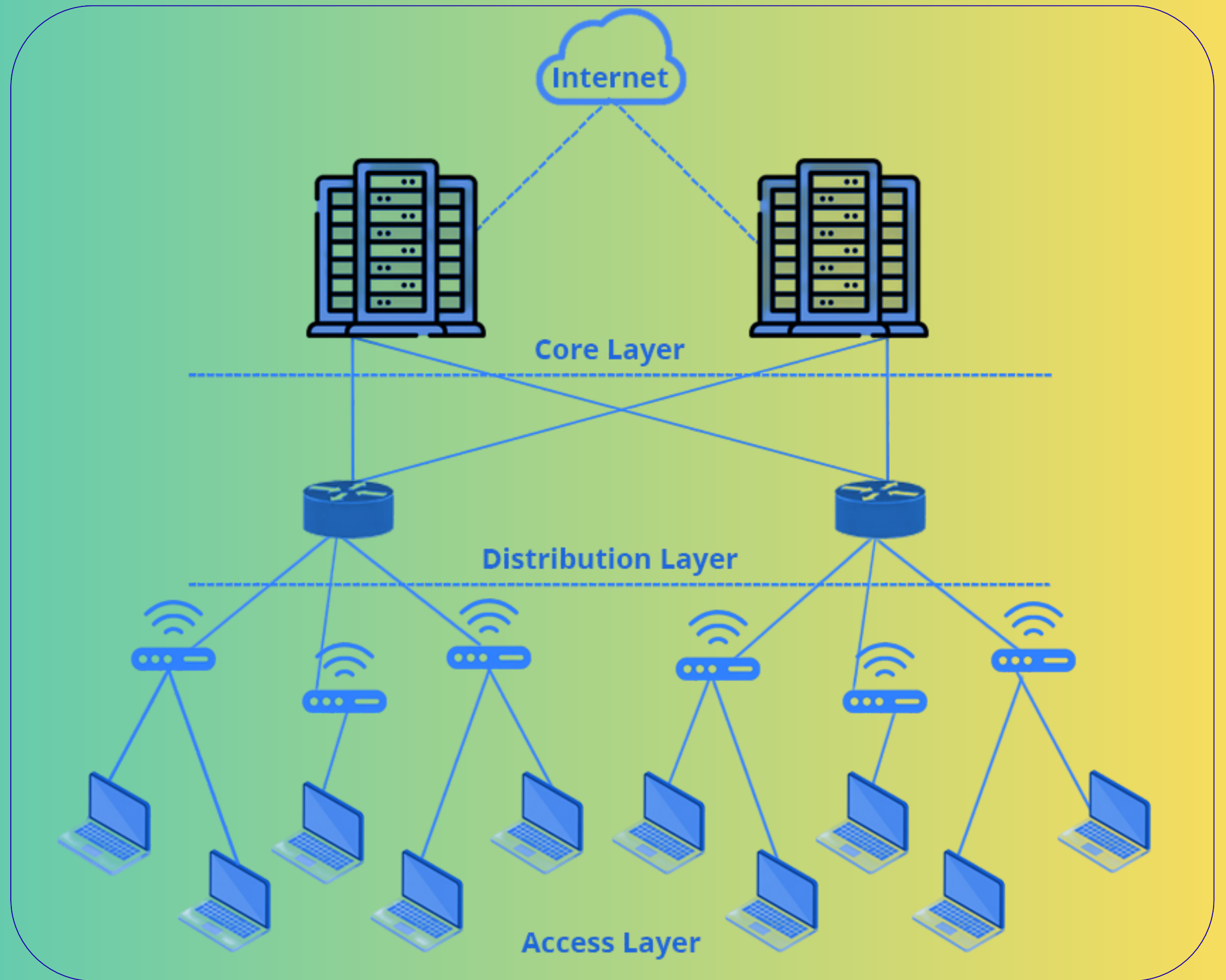
La topologie réseau hiérarchique (ou en arbre)

Cette structure en étoile hiérarchique permet de sécuriser le réseau en cloisonnant les accès, par exemple en séparant le trafic de bureau, les serveurs et la téléphonie.

Couche Coeur ->

Couche Distribution ->

Couche Accès ->



Structure et Fonctionnement :

Couche Cœur (Core) :

Le sommet de la hiérarchie, backbone à haute vitesse, responsable du transport rapide des données entre les sites.

Couche Distribution (Distribution) :

Intermédiaire entre le cœur et l'accès, elle gère le routage, le filtrage et les politiques de sécurité (VLANs).

Couche Accès (Access) :

Connecte les terminaux finaux (ordinateurs, imprimantes) au réseau.

Avantages :

Évolutivité : Facile à étendre en ajoutant des niveaux.

Gestion simplifiée : La structuration par niveaux facilite l'administration.

Performance : Optimise le flux de données en hiérarchisant le trafic.

Inconvénients

Dépendance : Une panne au niveau du cœur peut paralyser tout le réseau.

Coût : Plus complexe et coûteux à mettre en place qu'une structure simple.

les vlans

Un VLAN (Virtual Local Area Network) est une technologie réseau qui segmente logiquement un commutateur physique en plusieurs réseaux locaux indépendants.

les interfaces trunk

Une interface trunk est un port réseau configuré pour transporter le trafic de plusieurs VLANs (réseaux locaux virtuels) simultanément sur une seule liaison physique. Utilisée principalement entre commutateurs (switches) ou entre un switch et un routeur, elle utilise le tagging (étiquetage) 802.1Q pour identifier à quel VLAN appartient chaque trame.

le routage avec OSPF

Le routage avec OSPF (Open Shortest Path First) est un protocole de routage dynamique interne (IGP) qui permet aux routeurs de découvrir automatiquement les chemins les plus courts et les plus rapides dans un réseau IP. Il utilise l'algorithme de Dijkstra (SPF) pour calculer la topologie optimale et s'adapte rapidement aux changements, idéal pour les grands réseaux.

Caractéristiques principales :

- **Protocole à état de liens** : Chaque routeur construit une carte complète du réseau, pas seulement ses voisins directs.
- **Calcul du coût** : OSPF choisit la meilleure route en se basant sur la bande passante (coût) plutôt que sur le nombre de sauts.
- **Hiérarchique** : Il fonctionne en zones (Areas) pour optimiser les performances et limiter la propagation des mises à jour.
- **Standard Ouvert** : Non-propriétaire, il est utilisable sur du matériel hétérogène (Cisco, Juniper, etc.)

Fonctionnement :

- **Voisinage** : Les routeurs échangent des paquets « Hello » pour découvrir leurs voisins.
- **Synchronisation** : Ils synchronisent leurs bases de données d'état de lien (LSDB) pour avoir une vue commune.
- **Calcul** : Chaque routeur applique l'algorithme de Dijkstra pour trouver le chemin le plus court

le HSRP :

Le HSRP (Hot Standby Router Protocol) est un protocole propriétaire de Cisco, de type FHRP, conçu pour garantir la haute disponibilité de la passerelle par défaut dans un réseau local. Il permet à plusieurs routeurs d'utiliser une adresse IP et MAC virtuelle partagée, assurant une continuité de service transparente si le routeur actif tombe en panne.

Points clés du HSRP:

- **Fonctionnement Actif/Passif** : Un routeur "Actif" traite le trafic tandis qu'un routeur "Standby" (veille) attend de prendre le relais.
- **Adresse Virtuelle** : Les PC pointent vers une adresse IP unique, qui reste inchangée même en cas de basculement.
- **Fiabilité** : Des messages "Hello" (UDP 1985) sont échangés pour surveiller l'état des routeurs.
- **Élection** : Le routeur avec la priorité la plus élevée devient actif.
- **Usage** : Idéal pour éviter qu'une panne de routeur n'isole un réseau local

HSRP est une solution mature et robuste pour la redondance au premier saut.

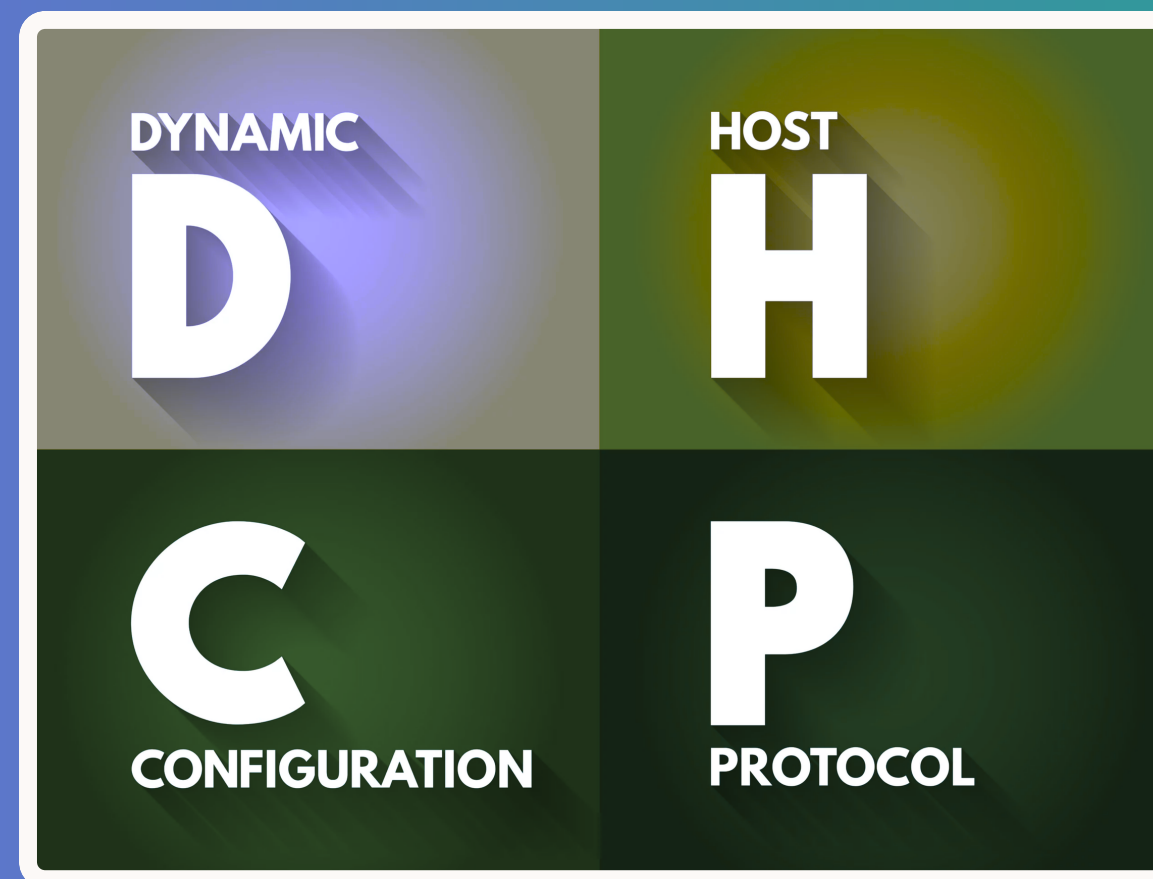
Le domaine Active Directory (AD)

Microsoft
Active Directory

Active Directory:

Active Directory (AD) est un service d'annuaire Microsoft centralisé, essentiel en entreprise pour gérer les identités, les accès et la sécurité du réseau. Il organise les utilisateurs, ordinateurs et ressources en domaines et unités d'organisation (OU), simplifiant l'administration et permettant l'authentification sécurisée (single sign-on).

Le service DHCP



Le DHCP:

Le DHCP (Dynamic Host Configuration Protocol) est un protocole réseau essentiel qui automatise la configuration IP des appareils (ordinateurs, smartphones, imprimantes). Il attribue dynamiquement des adresses IP, des masques de sous-réseau, des passerelles par défaut et des serveurs DNS, évitant ainsi la configuration manuelle et les conflits d'adresses.

Le service DNS



Le DNS:

Le service DNS (Domain Name System) est l'annuaire décentralisé d'Internet. Il traduit les noms de domaine compréhensibles (ex: google.com) en adresses IP numériques (ex: 142.250.179.196) nécessaires aux ordinateurs pour se connecter. Sans lui, il faudrait mémoriser des suites de chiffres complexes pour chaque site web.

```
C:\Users\researchadmin>nslookup google.com
Server:  hub.home.arpa
Address:  192.168.1.254

Non-authoritative answer:
Name:     google.com
Addresses: 2a00:1450:4009:c0b::65
           2a00:1450:4009:c0b::8a
           2a00:1450:4009:c0b::64
           2a00:1450:4009:c0b::8b
           142.251.29.102
           142.251.29.100
           142.251.29.101
           142.251.29.138
           142.251.29.139
           142.251.29.113

C:\Users\researchadmin>
```

```
C:\Users\researchadmin>nslookup facebook.com
Server:  hub.home.arpa
Address:  192.168.1.254

Non-authoritative answer:
Name:     facebook.com
Addresses: 2a03:2880:f189:184:face:b00c:0:25de
           157.240.214.35

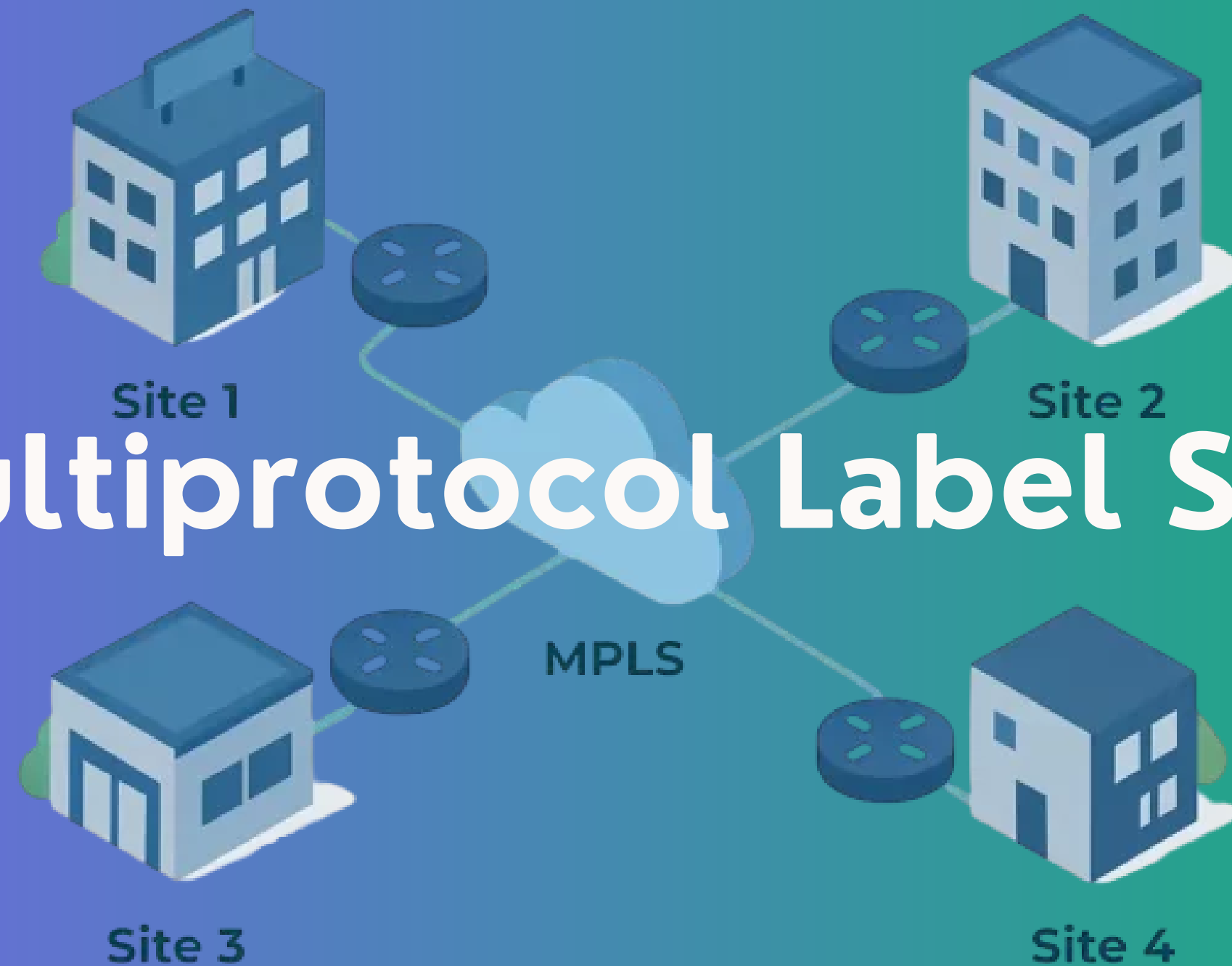
C:\Users\researchadmin>
```

```
C:\Users\researchadmin>nslookup congotelecom.com
Server:  hub.home.arpa
Address:  192.168.1.254

Non-authoritative answer:
Name:     congotelecom.com
Addresses: 76.223.54.146
           13.248.169.48

C:\Users\researchadmin>
```

Le MPLS (Multiprotocol Label Switching)



Le MPLS:

Le MPLS (Multiprotocol Label Switching) est une technique de routage haute performance pour réseaux d'entreprise, acheminant les données via des étiquettes (labels) plutôt que des adresses IP. Il permet de créer des réseaux privés sécurisés, garantissant qualité de service (QoS) et faible latence, idéal pour les applications temps réel comme la voix sur IP

Caractéristiques principal:

- **Fonctionnement par étiquettes :** Les routeurs MPLS (LER/LSR) utilisent des labels pour diriger les paquets, accélérant le transfert et contournant les recherches complexes dans les tables de routage IP.
- **Haute Fiabilité et QoS :** Idéal pour la voix, la vidéo et les applications critiques, il permet de prioriser certains flux.
- **Réseau Privé (VPN MPLS) :** Offre une étanchéité des flux, assurant une sécurité supérieure à celle d'Internet, idéale pour connecter des succursales à un siège social.
- **Gestion Opérateur :** Solution infogérée de bout en bout par l'opérateur, garantissant performance et disponibilité

Avantages et Limites:

Avantages : Fiabilité, performance, sécurité, priorisation du trafic.

Inconvénients : Coût élevé, déploiement lent, moins flexible que le SD-WAN pour le Cloud

Aujourd'hui, le MPLS est de plus en plus remplacé ou complété par le SD-WAN pour mieux s'adapter aux architectures Cloud, bien qu'il reste pertinent pour les besoins de très haute performance et de sécurisation maximale.

Le SD-WAN (Software-defined Wide Area Network)

Le SD-WAN (Software-Defined Wide Area Network) est une approche logicielle de gestion des réseaux étendus (WAN) qui centralise le contrôle, simplifie l'architecture et optimise la performance. Il permet de combiner plusieurs types de connexions (MPLS, internet, 4G/5G) de manière intelligente et sécurisée pour relier des sites distants, réduisant ainsi les coûts et la dépendance aux opérateurs classiques

Le SD-LAN (Software-defined Local Area Network)

Le SD-LAN (Software-Defined Local Area Network) applique les principes du SDN (contrôle logiciel centralisé) aux réseaux locaux filaires et Wi-Fi. Il permet de gérer, configurer et sécuriser l'ensemble des équipements (switches, points d'accès) depuis une interface unique, généralement dans le cloud, offrant une flexibilité, une visibilité et une automatisation bien supérieures aux réseaux LAN traditionne

Le VXLAN (Virtual Extensible Local Area Network)

Le VXLAN (Virtual Extensible LAN) est une technologie de virtualisation réseau qui étend les réseaux de couche 2 (Ethernet) sur une infrastructure de couche 3 (IP). Il encapsule les trames Ethernet dans des paquets UDP (MAC-in-UDP), permettant de créer jusqu'à 16 millions de réseaux virtuels isolés (VNI), surmontant la limite de 4 094 VLANs du standard IEEE 802.1Q.