Renforcement des compétences des ressources du NOC

FONDAMENTAUX DES RÉSEAUX

Informations générales sur le document et versioning

Titre du document	Fondamentaux des réseaux	
Version	1.0	
Auteurs	Steve FOTSO, Responsable NOC Edwige LONGMENE, Ing. DARS	
Date de publication	Juin 2024	
Amélioration 1 (V1.1)	Date: Juin 2024	Auteur: Steve FOTSO
Amélioration 1(V1.2)	Date:	Auteur:
Amélioration 1(V1.3)	Date:	Auteur:
Amélioration 1(V1.4)	Date:	Auteur:
Amélioration 1(V1.5)	Date:	Auteur:

Plan de la formation:

MODULE :

Fondamentaux réseaux

- Modèle OSI et TCP/IP
- Les couchs réseaux
- Protocole SNMP
- Architecture en couche du réseau
- Présentation de l’architecture de Matrix Télécoms S,A

Introduction aux réseaux (modèles TCP/IP et OSI, protocoles)

FONDAMENTAUX RESEAUX

Les modèles de référence sont des représentations conceptuelles permettant de décrire le fonctionnement des réseaux informatiques.

Les deux principaux sont :

- Le modèle OSI (Open Systems Interconnection) : Défini en 1984, il structure les réseaux en 7 couches : Physique, Liaison, Réseau, Transport, Session, Présentation et Application.

- Le modèle TCP/IP : Développé dans les années 70, il définit 4 couches : Accès réseau, Internet, Transport et Application.

Les protocoles réseaux sont des ensembles de règles qui régissent la communication entre les différents équipements. Les principaux sont : IP pour l'adressage, TCP et UDP pour le transport des données.

Les couches réseaux

FONDAMENTAUX RESEAUX

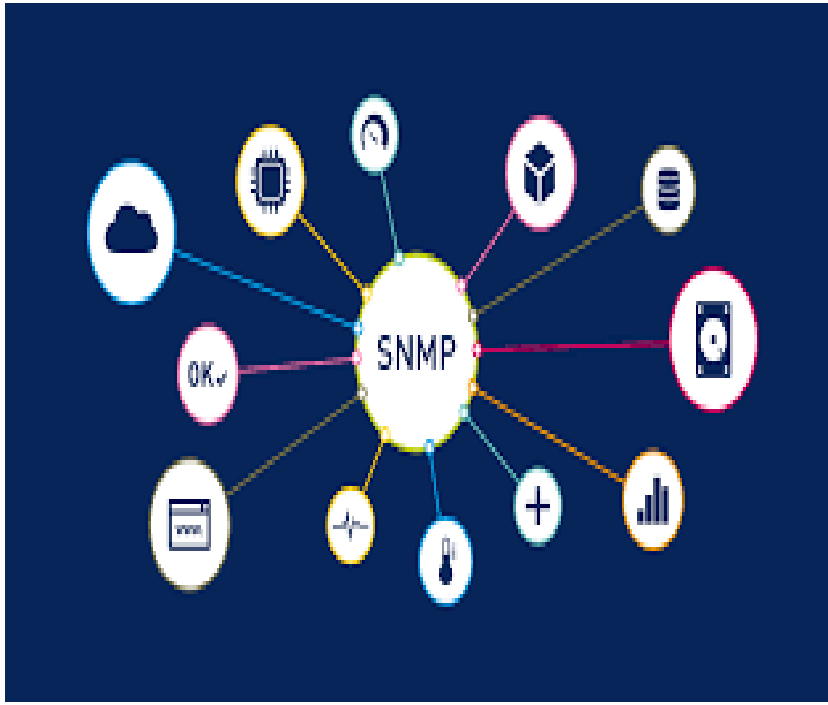
Quel que soit le modèle, on retrouve des couches similaires ayant chacune un rôle précis :

7	Application	Interface utilisateur pour les services réseau. Traduit les données dans un format reconnu. Synchronise et maintient les échanges.	DHCP BOOTP DNS FTP HTTP URL IMAP SMTP Telnet SNMP SSL TLS
6	Presentation		
5	Session		
4	Transport	Établit les circuits virtuels et contrôle la fiabilité des flux.	UDP, TCP
3	Network	Gère l'adressage logique et l'acheminement des paquets.	ICMP, IP
2	Data Link	Assure un transfert fiable entre deux nœuds directs.	PPP PPTP L2TP
1	Physical	Définit les standards de signalisation et support de transmission.	Ethernet , wifi

FONDAMENTAUX RESEAUX

Le protocole SNMP

- SNMP est un protocole standard de gestion de réseaux informatiques. Il permet de collecter des informations et de contrôler à distance les équipements réseaux tels que les routeurs, commutateurs, serveurs, imprimantes et autres périphériques.
- Le SNMP permet aux administrateurs d'avoir une vue centralisée sur l'état de leurs infrastructures et de réagir rapidement en cas d'incident. La plupart des outils de monitoring réseau comme SolarWinds, PRTG ou CACTI s'appuient sur SNMP.



FONDAMENTAUX RESEAUX

Le protocole SNMP: Caractéristiques

Caractéristiques	Description
Surveillance des équipements	• Collecter des données sur les performances (utilisation CPU, mémoire, interfaces réseau, etc.) • Récupérer des informations de configuration et d'inventaire.
Gestion des équipements	▪ Modifier la configuration des équipements à distance. ▪ Redémarrer ou arrêter des services sur les équipements.
Génération d'alertes	▪ Envoyer des notifications (traps) en cas de problème ou de dépassement de seuils.
Architecture manager/agent	▪ Les équipements hébergent un agent SNMP qui expose des données. Une station centrale (manager SNMP) interroge les agents pour collecter les informations.
Versions principales	▪ SNMPv1 et SNMPv2c (versions historiques) ▪ SNMPv3 (version récente offrant plus de sécurité avec l'authentification et le chiffrement)

FONDAMENTAUX RESEAUX

Architectures en couches du réseau

Couche cœur / Core :

C'est le cœur à haute capacité et haute disponibilité du réseau qui interconnecte les différentes zones géographiques, typiquement avec une architecture en anneaux redondants. Elle utilise des routeurs cœur très puissants optimisés pour le transit IP.

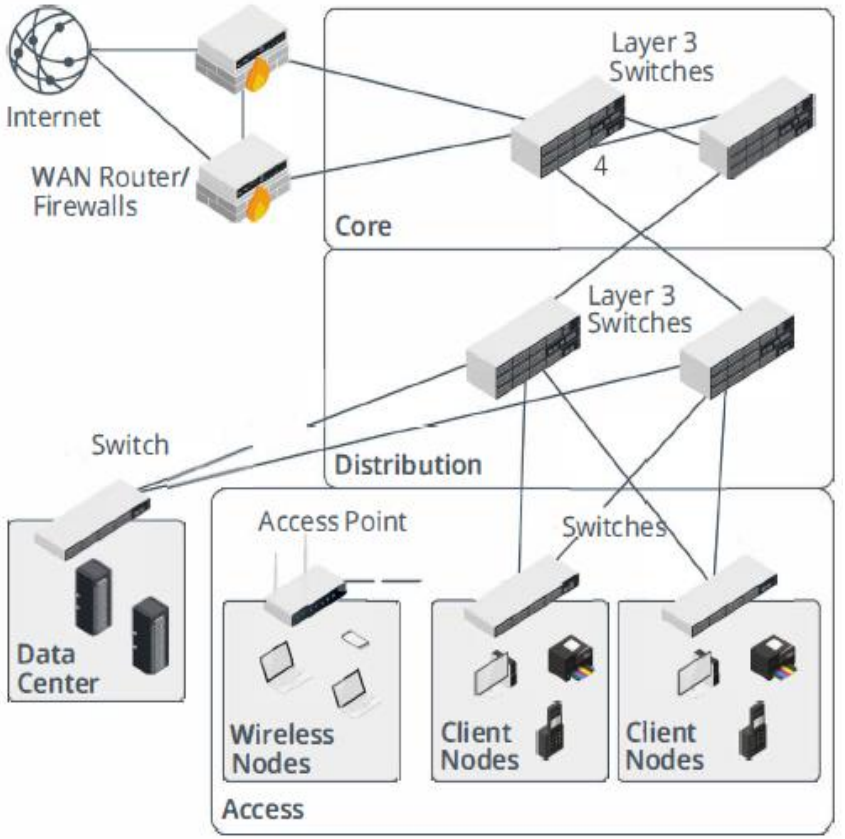
Couche distribution :

- Cette couche assure la distribution et le routage des flux dans la zone locale. Elle s'appuie sur des routeurs et commutateurs Ethernet répartis dans les différents nœuds du réseau de l'opérateur.

Couche accès :

C'est la partie du réseau qui connecte les utilisateurs finaux au réseau opérateur. Elle utilise différentes technologies d'accès :

- xDSL (ADSL, VDSL...) sur paire de cuivre
- Fibre optique (FTTH)
- Liaison spécialisée (Câble, 4G/5G, Satellite)



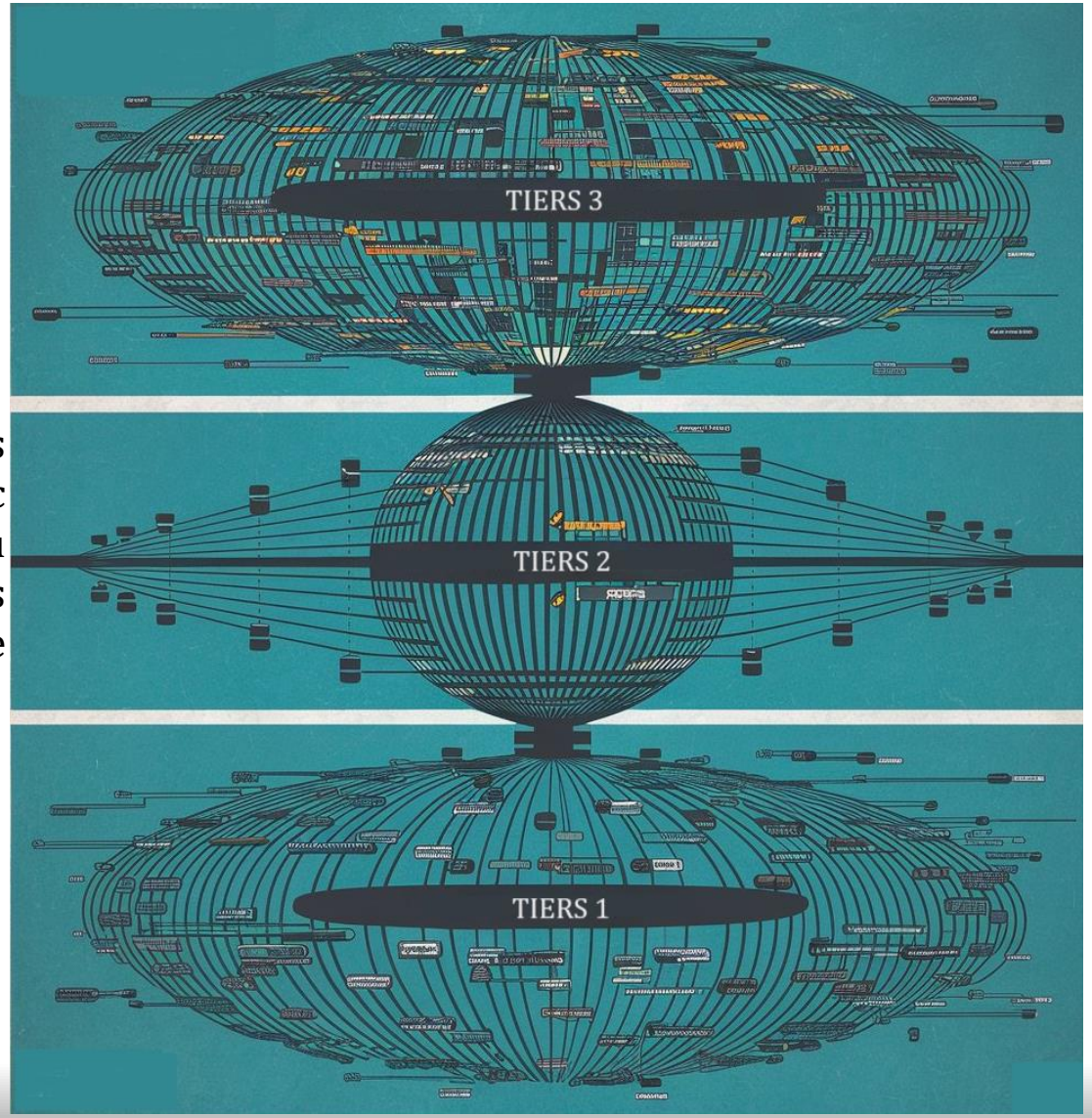
HIERACHISATION DES FAI

FONDAMENTAUX RESEAUX

Tier 3
Les FAI de niveau 3 sont les plus petits. Ils achètent de la bande passante auprès des FAI de niveau 2 ou de niveau 1 et se concentrent souvent sur des marchés locaux ou spécifiques.

Tier 2
Les FAI de niveau 2 sont de taille moyenne. Ils ont généralement des accords de peering avec certains FAI de niveau 1 et d'autres FAI de niveau 2, Ils couvrent souvent des régions spécifiques ou des pays et peuvent offrir des services de peering à des FAI de niveau 3.

Tier 1
Les FAI de niveau 1 sont les plus grands et les plus influents. Ils possèdent une infrastructure réseau mondiale et peuvent échanger du trafic internet sans frais avec d'autres FAI de niveau 1 grâce à des accords de peering.



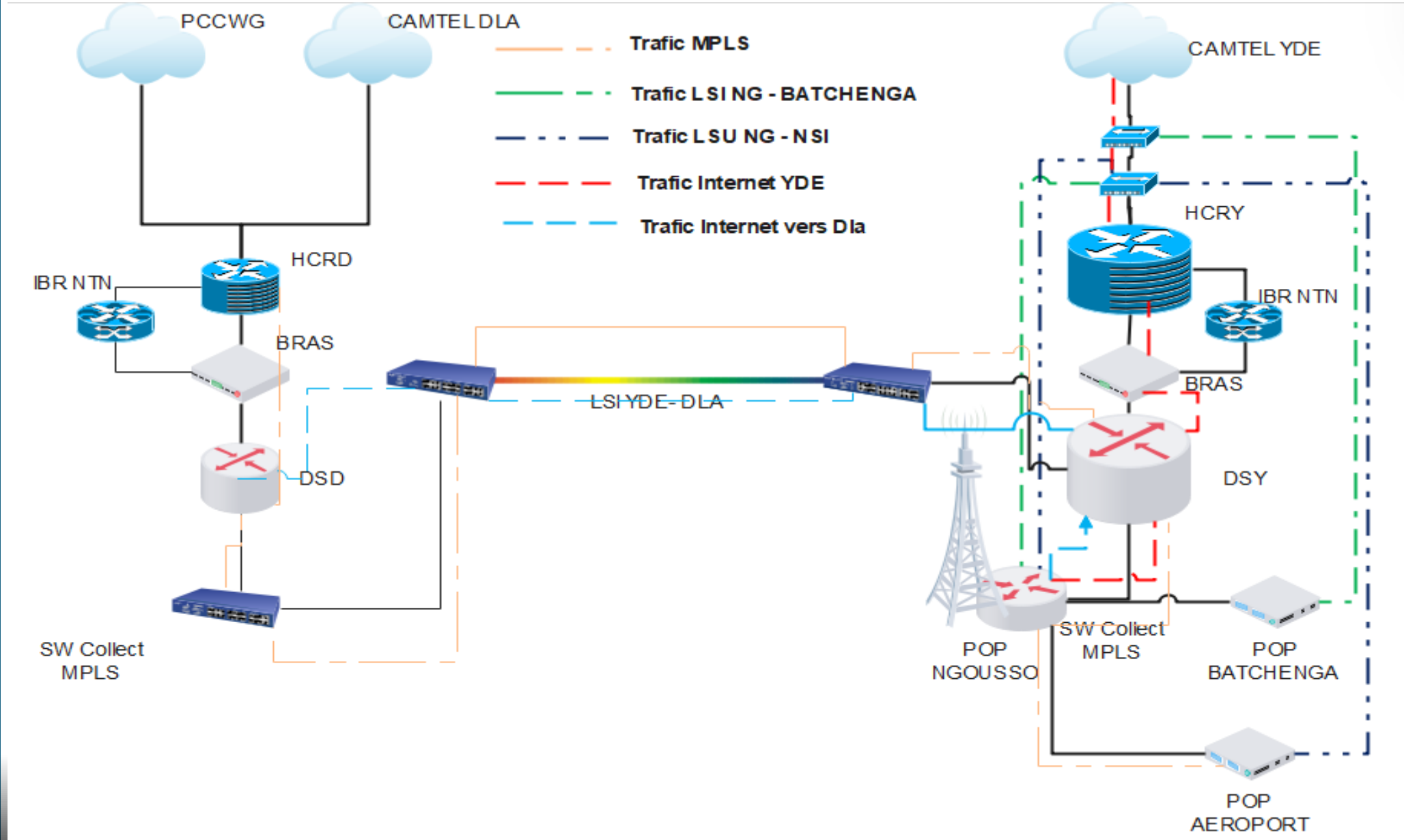
LES CABLES SOUS MARINS

FONDAMENTAUX RESEAUX

Visite guidée et explicative

Présentation de l'architecture Matrix Télécoms

FONDAMENTAUX RESEAUX



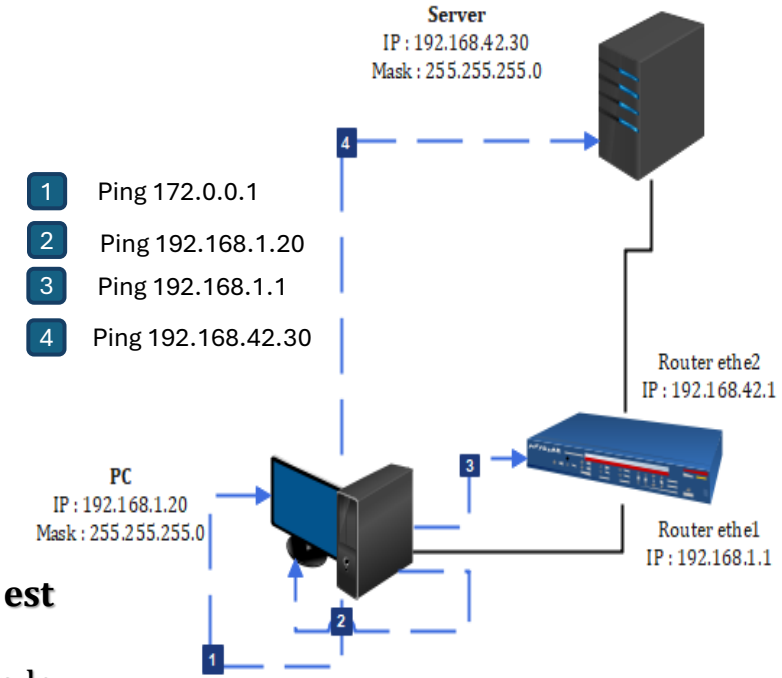
Outils de diagnostics réseaux

FONDAMENTAUX RESEAUX

Interprétation du ping

La commande ping (Packet Internet Groper) envoie des requêtes ICMP pour tester la connectivité IP avec une autre machine. Ses résultats permettent de :

- Vérifier si une machine est accessible,
- Mesurer la latence aller-retour,
- Détecter des pertes de paquets.



Si la commande ping échoue, l'un des deux messages suivants est généralement reçu :

- **La destination n'est pas accessible** : Il n'y a pas d'information sur le routage (c'est-à-dire, que l'ordinateur ne sait pas comment accéder à cette adresse IP. Si l'hôte est sur la même adresse IP réseau, vérifier le câblage physique, les dispositifs d'infrastructure tels que le commutateur et configuration IP. Si l'hôte est sur un autre réseau IP, vérifiez la configuration IP et routeur.
- **No reply (Request timed out** : L'hôte n'est pas disponible ou ne peut pas acheminer une réponse vers votre ordinateur.

***Remarque** : Soyez conscient que le trafic ICMP est souvent bloqué par des pares-feux, en faisant une réponse telle que **Request timed out**. inévitable.*

Outils de diagnostics réseaux

FONDAMENTAUX RESEAUX

Interprétation du tracert

L'outil traceroute (ou tracert sous Windows) permet de visualiser la totalité des routeurs empruntés entre deux hôtes, grâce à l'analyse des temps de latence. C'est utile pour localiser d'où provient un problème de réseau.

Interprétation du pathping

Pathping combine les fonctionnalités de ping et traceroute pour tester la connectivité mais aussi tracer le chemin emprunté par les paquets. Il indique pour chaque saut :

- L'adresse IP des routeurs traversés
- Le temps de latence jusqu'à ce nœud
- Le pourcentage de perte de paquets

Interprétation du Nslookup

NSlookup est un outil en ligne de commande permettant d'interroger le système DNS pour diverses opérations :

- Résolution directe et inverse des noms/adresses IP
- Requête sur les enregistrements DNS (MX, TXT, SOA...)
- Interrogation des serveurs DNS configurés