

Introduction aux réseaux informatiques

Définition, modèles, protocoles, adressage,
systèmes et outils de diagnostic

Pourquoi relier des ordinateurs entre eux ?

OBJECTIF PRINCIPAL

La mise en réseau permet de transformer des postes de travail isolés en un système collaboratif puissant, optimisant ainsi l'utilisation du matériel et fluidifiant les échanges d'informations.



Partage de Ressources

Matériel : Imprimantes, scanners, disques de stockage (NAS).

Données : Fichiers partagés, bases de données communes.

Connexion : Partage d'une seule connexion Internet pour tous.

Applications : Logiciels réseau centralisés.



Collaboration

Communication : E-mails, messagerie instantanée, chat.

Travail d'équipe : Outils collaboratifs (ex: Teams, Slack).

Réunions : Visioconférence, partage d'écran à distance.

Organisation : Agendas et calendriers partagés.



Gestion & Économie

Centralisation : Sauvegardes des données unifiées et sécurisées.

Administration : Mises à jour et maintenance facilitées.

Sécurité : Gestion centralisée des accès utilisateurs.

Coûts : Réduction des dépenses matérielles (mutualisation).

C'est quoi un réseau informatique ?

DÉFINITION

Un réseau informatique est un ensemble d'équipements (ordinateurs, serveurs, périphériques) interconnectés les uns aux autres pour échanger des informations et partager des ressources.



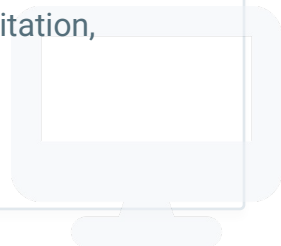
Composants

Hôtes : Ordinateurs (PC), Serveurs, Smartphones.

Interconnexion : Switchs, Routeurs, Points d'accès Wi-Fi.

Médias : Câbles Ethernet (cuivre), Fibre optique, Ondes radio.

Logiciels : Systèmes d'exploitation, Protocoles.



Types de réseaux

LAN (Local Area Network) : Réseau local (maison, bureau).

WLAN : Réseau local sans fil (Wi-Fi).

WAN (Wide Area Network) : Réseau étendu (Internet).

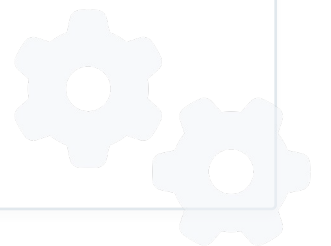


Services offerts

Communication : E-mail, Messagerie instantanée, VoIP.

Partage : Fichiers, Imprimantes, Bases de données.

Web : Navigation Internet, Applications Cloud.



Les topologies de réseau



Topologies Physiques

Comment les câbles et équipements sont connectés physiquement.

Étoile (Star) Standard actuel Tous les nœuds sont reliés à un équipement central (switch). Panne d'un câble = 1 seul PC HS.



Bus

Câble unique partagé (coaxial). Panne du câble = réseau coupé. Collisions fréquentes.



Anneau (Ring)

Chaque nœud est relié à deux voisins. Jeton (Token Ring). Redondance limitée.



Maillée (Mesh)

Connexions multiples entre les nœuds.

Les différents types de réseaux

RÉSEAUX SPÉCIALISÉS & INDUSTRIELS



CAN Bus

CONTROLLER AREA NETWORK

Standard robuste permettant aux microcontrôleurs de communiquer sans ordinateur hôte. Essentiel pour les systèmes embarqués critiques.

DÉBIT
MAX
1 Mbit/s

TOPOLOGI
E
Bus

PORTÉE
40m @ 1Mbit

FIABILITÉ
Très Haute

CAS D'USAGE PRINCIPAUX



Automobile (ABS,
Moteur)



Robotique



Ascenseurs

ISO 11898, CAN FD,
OSEK



Bus de Terrain

FIELDBUS / INDUSTRIAL ETHERNET

Famille de protocoles pour le contrôle industriel en temps réel. Relie capteurs, actionneurs et automates programmables (PLC).

DÉBIT
MAX
100Mb - 1Gb

TOPOLOGI
E
Ligne / Anneau

LATENCE
< 1 ms

TYPE
Temps Réel

CAS D'USAGE PRINCIPAUX



Usines 4.0



Automates PLC



Énergie

Modbus, Profinet,
EtherCAT



SAN

STORAGE AREA NETWORK

Réseau dédié au stockage de données haute performance. Permet de mutualiser des baies de disques accessibles par les serveurs.

DÉBIT
MAX
32-128 Gbit/s

TOPOLOGI
E
Fabric Switched

MÉDIA
Fibre Optique

ACCÈS
Bloc (Block Level)

CAS D'USAGE PRINCIPAUX



Datacenters



Cloud Privé



Virtualisation

Fibre Channel, iSCSI,
FCoE

C'est quoi un protocole réseau ?

DÉFINITION & ANALOGIE

Un protocole est un ensemble de règles et de conventions normalisées qui définissent le format et l'ordre des échanges d'informations. C'est comme la "grammaire" d'une langue : sans elle, deux ordinateurs ne pourraient pas se comprendre.

À quoi ça sert ?

Interopérabilité : Permet à un PC Windows de parler à un serveur Linux.

Standardisation : Règles communes pour tous les constructeurs.

Fiabilité : Gestion des erreurs et réassemblage des données.

Adressage : Savoir à qui envoyer les données.



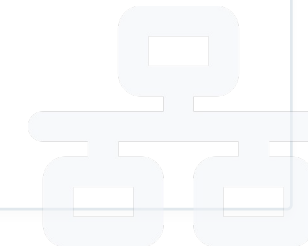
Transport & Réseau

IP Internet Protocol : Adressage et routage des paquets (le GPS du réseau).

TCP Transmission Control : Transport fiable, connecté (livraison garantie).

UDP User Datagram : Transport rapide, sans garantie (streaming, jeu).

ICMP Diagnostic : Ping, signalement d'erreurs.



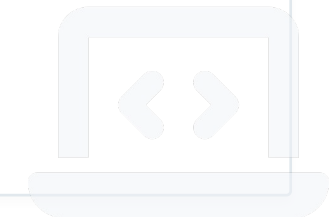
Application (Exemples)

HTTP/S Web : Affichage des pages sites internet.

DNS Domain Name System : Traduit "google.com" en IP.

DHCP Dynamic Host Config : Donne automatiquement une IP aux PC.

FTP File Transfer : Échange de fichiers.



À quoi sert une adresse IP ?



L'adresse IP (Internet Protocol) agit comme une adresse postale numérique. Elle permet d'identifier de manière unique chaque appareil connecté à un réseau informatique utilisant le protocole Internet.



Rôles Clés

Identification : Distinguer un hôte (ordinateur, serveur, imprimante) parmi des milliards d'autres.

Localisation : Indiquer sur quel réseau se trouve l'appareil (via le masque de sous-réseau).

Routage : Permettre aux routeurs d'acheminer les paquets de données vers la bonne destination.



Types & Attribution

Dynamique (DHCP) : Attribuée temporairement par un serveur (ex: Wi-Fi café).

Statique : Configurée manuellement, ne change pas (ex: Serveurs, Imprimantes réseau).

Publique vs Privée : Visible sur Internet vs Utilisable uniquement en local (LAN).

IPv4 vs IPv6 : Le changement d'échelle

IPv4

Le standard historique (1981)

STRUCTURE (32 BITS)



4 Octets

</> NOTATION DÉCIMALE

192.168.1.10

⚠ STATUT : ÉPUISÉ

4,3 Milliards



IPv6

Le standard du futur

STRUCTURE (128 BITS)



16 Octets (4x plus grand)

</> NOTATION HEXADÉCIMALE

2001:0db8:85a3::8a2e:0370

✓ STATUT : ILLIMITÉ

3,4 × 10³⁸

Internet vs Réseau Local (LAN)



Réseau Local (LAN)

Local Area Network : Votre maison, école ou bureau.

Portée géographique Limitée Restreint à un bâtiment ou un site géographique précis. Les câbles vous appartiennent.



Contrôle & Gestion

Privé. Géré par un administrateur local. Vous décidez qui se connecte.



Adressage

Utilise des adresses IP privées (ex: 192.168.x.x) non visibles directement depuis l'extérieur.



Performance

Très haut débit (1 Gbps+), latence très faible (< 1ms). Idéal pour le partage de fichiers lourds.



Internet (Public)

Le réseau des réseaux : Interconnexion mondiale.

Portée géographique Mondiale Couvre la planète. Utilise des infrastructures publiques (fibre sous-marine, satellites).



Contrôle & Gestion

Décentralisé. Géré par une multitude d'opérateurs (FAI) et organismes (ICANN).



Adressage

Utilise des adresses IP publiques uniques au monde pour être joignable de partout.



Performance

Variable selon l'abonnement et la distance. Latence plus élevée (20ms à 300ms).

Les opérations binaires & conversions

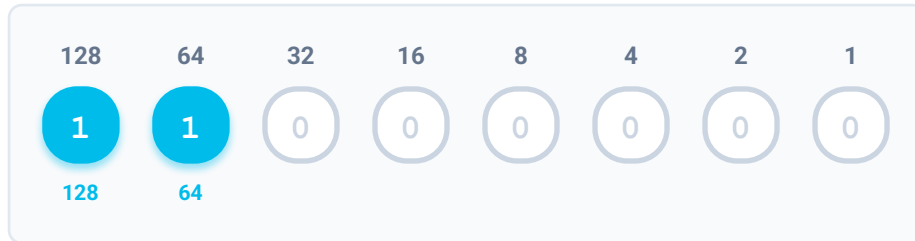


Décimal vers Binaire

Décomposition en puissances de 2 (Interrupteurs)

192

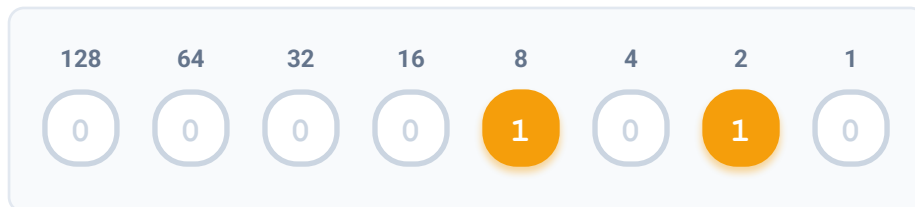
Classe C



Calcul : $128 + 64 = 192$ (Le reste est à 0)

10

Octet fin



Calcul : $8 + 2 = 10$



Masquage & Logique Réseau

Logique ET (&)

	0	1
0	0	0
1	0	1

Le Masque "Filtre" : $1 \& 1 = 1$ (Garde) $X \& 0 = 0$ (Efface)



Application : Calcul d'adresse réseau

```
IP (Hôte) 192.168.1.10 1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 1 0 0 0
Masque 255.255.255.0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0
Réseau 192.168.1.0 1 1 0 0 0 0 0 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

Opération ET

↑ Le masque à 0 "éteint" tous les bits de l'hôte dans le dernier octet.

Réseau / Masque de sous-réseau (CIDR)

1 Comprendre le rôle

Le masque sépare l'adresse IP en deux parties distinctes :

Réseau (Network)

Hôte (Host)

11111111 . 00000000

Les "1" définissent le réseau.

Les "0" définissent l'hôte.

2 Notation CIDR (/)

Le CIDR indique simplement le nombre de bits à "1" dans le masque.

/24 → 24 bits à 1

255.255.255.0

3 Calcul d'hôtes

Combien de machines peut-on brancher ?

Nb Hôtes = $2^h - 2$

h = nombre de bits "0" (bits hôte). -2 = adresse Réseau + adresse Broadcast.

Standard /24



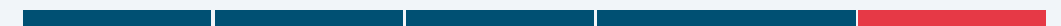
Masque 255.255.255.0

Bits Réseau (1) 24

Bits Hôte (0) 8

Calcul $2^8 - 2 = 254$ hôtes

Sous-réseau /26



Masque 255.255.255.192

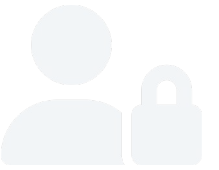
Bits Réseau (1) 26

Bits Hôte (0) 6

Calcul $2^6 - 2 = 62$ hôtes

Note: On a divisé le réseau original en 4 sous-réseaux.

Réseaux privés (RFC1918)



Ces adresses IP sont réservées pour une utilisation dans les réseaux locaux (LAN). Elles ne sont pas routables sur Internet directement. L'accès à Internet nécessite une translation d'adresse (NAT).

PRÉFIXE CIDR	PLAGE D'ADRESSES	NB. ADRESSES
10.0.0.0/8	10.0.0.0 – 10.255.255.255	16 777 216
172.16.0.0/12	172.16.0.0 – 172.31.255.255	1 048 576
192.168.0.0/16	192.168.0.0 – 192.168.255.255	65 536



Pourquoi utiliser ces adresses ?

Elles permettent d'économiser les adresses IPv4 publiques. De multiples réseaux locaux peuvent utiliser les mêmes plages privées (ex: 192.168.1.x chez vous et au bureau) sans conflit, car ils sont isolés les uns des autres par des routeurs NAT.

C'est quoi la gateway / passerelle ?

DÉFINITION

La passerelle (Gateway) est l'équipement qui agit comme une porte de sortie pour les paquets de données qui doivent quitter le réseau local pour atteindre un autre réseau (comme Internet).



Rôle Principal

Route par défaut : Si un hôte ne sait pas où envoyer un paquet, il l'envoie à la passerelle.

Interconnexion : Relie le LAN (réseau local) au WAN (Internet).

Traduction : Effectue souvent le NAT (Network Address Translation).



Configuration

Doit avoir une IP dans le même sous-réseau que les hôtes.

Exemple standard : Si IP PC est 192.168.1.10, Gateway est souvent 192.168.1.1 ou .254.

Distribuée automatiquement via DHCP.



Comment vérifier ?

Windows : Commande ipconfig ou route print.

Linux/Mac : Commande ip route ou netstat -rn.

Chercher la ligne "Default Gateway" ou "default via".

Adresse de broadcast

DÉFINITION

L'adresse de broadcast (ou diffusion) est une adresse IP spéciale permettant d'envoyer un paquet de données à tous les équipements connectés sur un même réseau ou sous-réseau logique simultanément.



Principe & Calcul

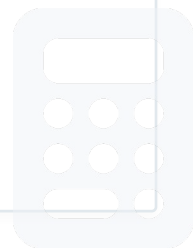
C'est toujours la dernière adresse de la plage du sous-réseau.

Règle binaire : On fixe tous les bits de la partie hôte à 1.

Elle ne peut jamais être attribuée à une machine spécifique (hôte).

Adresse réseau = Tout à 0

Adresse broadcast = Tout à 1



Exemples

Réseau Standard /24

IP: 192.168.1.0/24

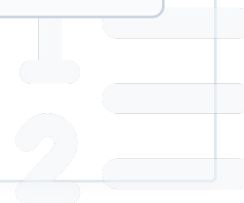
Broadcast: 192.168.1.255

Sous-réseau /26 (Divisé)

IP: 192.168.1.64/26

Plage: .65 à .126

Broadcast: 192.168.1.127



localhost / loopback

DÉFINITION

L'interface de bouclage (loopback) est une interface réseau virtuelle qui permet à un ordinateur de communiquer avec lui-même via le protocole TCP/IP, sans passer par une carte réseau physique.



IPv4 Loopback

Adresse standard : 127.0.0.1

Nom d'hôte : "localhost"

Plage réservée : Tout le bloc 127.0.0.0/8 est réservé.

127.x.x.x pointe toujours vers la machine locale.



IPv6 Loopback

Adresse : ::1

Simplification : Une seule adresse spécifique, pas de plage entière.

Équivalence : Fonctionnellement identique au 127.0.0.1 d'IPv4.

Utilisé par défaut dans les OS modernes.



À quoi ça sert ?

Tests locaux : Développer un site web sans internet (<http://localhost>).

Diagnostics : ping 127.0.0.1 vérifie si la pile TCP/IP fonctionne.

Sécurité : Les services écoutant sur localhost ne sont pas accessibles de l'extérieur.



Ping & Connectiv  

? C'est quoi Ping ?

L'outil PING (Packet Internet Groper) utilise le protocole ICMP (Internet Control Message Protocol). Il envoie un message "Echo Request" et attend un "Echo Reply".

✂ Pourquoi s'en servir ?

V  rifier si un h  te distant est joignable (Up/Down).

Mesurer le temps d'aller-retour (RTT / Latence).

D  tecter la perte de paquets (qualit   du lien).

R  soudre un nom de domaine en IP (test DNS).

Q Analyse de la d  mo (Australie)

Ping vers syd-au-ping.vultr.com. Observez le temps de r  ponse   lev   (>250ms) d      la distance g  ographique, contrairement    un ping local (<1ms) ou national (~20ms).



Command Prompt - Administrator

```
C:\Users\Admin> ping syd-au-ping.vultr.com
```

```
Pinging syd-au-ping.vultr.com [108.61.212.117] with 32 bytes of data:
```

```
Reply from 108.61.212.117: bytes=32 time=284ms TTL=52
```

```
Reply from 108.61.212.117: bytes=32 time=285ms TTL=52
```

```
Reply from 108.61.212.117: bytes=32 time=283ms TTL=52
```

```
Reply from 108.61.212.117: bytes=32 time=286ms TTL=52
```

```
Ping statistics for 108.61.212.117:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 283ms, Maximum = 286ms, Average = 284ms
```

```
C:\Users\Admin> ping 8.8.8.8
```

```
Pinging 8.8.8.8 with 32 bytes of data:
```

```
Reply from 8.8.8.8: bytes=32 time=12ms TTL=115
```

```
Reply from 8.8.8.8: bytes=32 time=13ms TTL=115
```


Traceroute : Chemin Réseau

? C'est quoi Traceroute ?

Outil permettant de visualiser le chemin emprunté par un paquet IP de la source à la destination. Il identifie chaque routeur (saut) traversé.

⚙️ Comment ça marche ?

Envoie des paquets avec un TTL (Time To Live) incrémental (1, 2, 3...).

Chaque routeur décrémente le TTL et renvoie une erreur ICMP "Time Exceeded" lorsqu'il atteint 0.

Permet d'identifier où se trouve un goulot d'étranglement ou une coupure.

>_ Commandes & Analyse

Windows : `tracert` cible (utilise ICMP)

Linux/Mac : `traceroute` cible (utilise UDP par défaut)

* = Pas de réponse (timeout/firewall)

```
Command Prompt - Network Admin

C:\Users\Admin> tracert syd-au-ping.vultr.com

Tracing route to syd-au-ping.vultr.com [108.61.212.117]
over a maximum of 30 hops:

 1 <1 ms <1 ms <1 ms 192.168.1.1 (Gateway)
 2 4 ms 3 ms 4 ms 10.125.0.1 (ISP Edge)
 3 12 ms 11 ms 14 ms mx01.paris.provider.net
 4 22 ms 21 ms 22 ms london-core.backbone.net
 5 145 ms 144 ms 146 ms singapore-transit.net
 6 * * * Request timed out.
 7 283 ms 284 ms 282 ms sydney-gw.vultr.com
 8 284 ms 285 ms 284 ms 108.61.212.117

Trace complete.

C:\Users\Admin> _
```