NETWORKS - Tools

Utilitaire réseaux....2
IP....2
IPCALC....3
PING....4
ARP....4
TRACEROUTE....5
NETSTAT....5
NMAP....6
TCPDUMP....6
WIRESHARK....6
WGET....7
TELNET....7
CURL....8
NETCAT....8
OPENSSL....9
CHRONY....9
NTP....10
WHOIS....11

Utilitaire réseaux

IP

La commande ip est l'outil standard moderne sous Linux pour gérer le réseau, remplaçant la vieille commande ifconfig

ip a (ou ip address) affiche les interfaces réseaux.

```
admin@laptop:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp5s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 84:a9:38:c7:18:6e brd ff:ff:ff:ff:ff:ff
    altname enx84a938c7186e
    inet 192.168.139.221/24 brd 192.168.139.255 scope global dynamic noprefixroute enp5s0
       valid_lft 59478sec preferred_lft 59478sec
    inet6 2a01:cb19:96fd:4500:c57e:3d87:3af3:e2cb/64 scope global dynamic noprefixroute
       valid_lft 86393sec preferred_lft 593sec
    inet6 fe80::9582:8b7d:b552:1c72/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlp6s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether ba:8c:cb:1e:c7:d2 brd ff:ff:ff:ff:ff:ff permaddr e0:0a:f6:5f:89:45
    altname wlxe00af65f8945
4: virbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 52:54:00:b8:77:45 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.250/24 brd 192.168.122.255 scope global virbr0
       valid_lft forever preferred_lft forever
5: vnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master virbr0 state UNKNOWN group
default qlen 1000
    link/ether fe:54:00:e0:79:8a brd ff:ff:ff:ff:ff:ff
    inet6 fe80::fc54:ff:fee0:798a/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

-br -brief Inverse de verbose

```
admin@laptop:~$ ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
enp5s0           UP             192.168.139.221/24 2a01:cb19:96fd:4500:c57e:3d87:3af3:e2cb/64
fe80::9582:8b7d:b552:1c72/64
wlp6s0           DOWN
virbr0           UP             192.168.122.250/24
virbr1           DOWN           192.168.100.1/24
vnet0            UNKNOWN        fe80::fc54:ff:fee0:798a/64
```

IPCALC

```
admin@laptop:~$ ipcalc 192.168.139.0/24
Address:   192.168.139.0        11000000.10101000.10001011. 00000000
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.139.0/24     11000000.10101000.10001011. 00000000
HostMin:   192.168.139.1        11000000.10101000.10001011. 00000001
HostMax:   192.168.139.254      11000000.10101000.10001011. 11111110
Broadcast: 192.168.139.255      11000000.10101000.10001011. 11111111
Hosts/Net: 254                   Class C, Private Internet
```

Ipcalc est un petit programme qui permet de dimensionner un réseau et de permetre aussi de diviser le réseau en sous-réseaux, en saisissant l'adresse et le masque du réseau d'origine et de jouer avec le second masque de réseau jusqu'à ce que le résultat correspond à ses besoins.

```
admin@laptop:~$ ipcalc 192.168.139.0 255.255.255.0 255.255.255.192
Address:   192.168.139.0        11000000.10101000.10001011. 00000000
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.139.0/24     11000000.10101000.10001011. 00000000
HostMin:   192.168.139.1        11000000.10101000.10001011. 00000001
HostMax:   192.168.139.254      11000000.10101000.10001011. 11111110
Broadcast: 192.168.139.255      11000000.10101000.10001011. 11111111
Hosts/Net: 254                   Class C, Private Internet

Subnets after transition from /24 to /26

Netmask:   255.255.255.192 = 26 11111111.11111111.11111111.11 000000
Wildcard:  0.0.0.63             00000000.00000000.00000000.00 111111

 1.
Network:   192.168.139.0/26     11000000.10101000.10001011.00 000000
HostMin:   192.168.139.1        11000000.10101000.10001011.00 000001
HostMax:   192.168.139.62       11000000.10101000.10001011.00 111110
Broadcast: 192.168.139.63       11000000.10101000.10001011.00 111111
Hosts/Net: 62                    Class C, Private Internet

 2.
Network:   192.168.139.64/26    11000000.10101000.10001011.01 000000
HostMin:   192.168.139.65       11000000.10101000.10001011.01 000001
HostMax:   192.168.139.126      11000000.10101000.10001011.01 111110
Broadcast: 192.168.139.127      11000000.10101000.10001011.01 111111
Hosts/Net: 62                    Class C, Private Internet

 3.
Network:   192.168.139.128/26   11000000.10101000.10001011.10 000000
HostMin:   192.168.139.129      11000000.10101000.10001011.10 000001
HostMax:   192.168.139.190      11000000.10101000.10001011.10 111110
Broadcast: 192.168.139.191      11000000.10101000.10001011.10 111111
Hosts/Net: 62                    Class C, Private Internet

 4.
Network:   192.168.139.192/26   11000000.10101000.10001011.11 000000
HostMin:   192.168.139.193      11000000.10101000.10001011.11 000001
HostMax:   192.168.139.254      11000000.10101000.10001011.11 111110
Broadcast: 192.168.139.255      11000000.10101000.10001011.11 111111
Hosts/Net: 62                    Class C, Private Internet


Subnets:   4
Hosts:     248
```

PING

```
admin@laptop:~$ ping -c 3 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=16.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=16.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=17.1 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 16.845/16.947/17.125/0.126 ms
```

`-c <count>` stop after <count> replies

Avec la commande ping de Linux, nous pouvons également accéder à la durée d'envoi et de réception des réponses d'un réseau. Elle fonctionne en envoyant une série de messages ICMP (Internet Control Message Protocol) à l'hôte cible et en attendant un message d'écho ICMP de et vers l'hôte et le dispositif. Cela nous informe sur l'exécution du réseau.

Essentiellement, cela envoie le message ECHO_REQUEST et attend le message ECHO_RESPONSE.

Le test Ping entre votre ordinateur et l'hôte cible vous permettra de le déterminer :

- Statut de l'hôte cible : s'il est joignable
- TTL (Time To Live): Mesure du temps entre le trajet aller-retour (Hôte-Ordinateur-Hôte)
- Pourcentage de paquets perdus
- Le Ping, la latence du réseaux

ARP

```
admin@laptop:~$ sudo arp -nv
Address                  HWtype  HWaddress           Flags Mask            Iface
192.0.0.4                ether   bc:52:74:ae:7a:0a   C                     enp5s0
192.168.139.233          ether   c0:7a:d6:bf:82:1d   C                     enp5s0
192.168.139.254          ether   18:df:26:a7:93:50   C                     enp5s0
192.168.139.223          ether   bc:52:74:ae:7a:0a   C                     enp5s0
Entries: 4     Skipped: 0     Found: 4
```

`-n` `--numeric` don't resolve names

`-v` `--verbose` be verbose

ARP n'est pas une commande de base Linux, ainsi selon votre distribution Linux, la commande arp n'est pas forcément disponible par défaut. Il est inclus dans le packet net-tools.

TRACEROUTE

```
admin@laptop:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  livebox.home (192.168.139.254)  0.565 ms  0.872 ms  1.112 ms
 2  80.10.252.37 (80.10.252.37)  10.325 ms  10.754 ms  11.039 ms
 3  ae95-0.nctou201.rbci.orange.net (80.10.154.90)  11.291 ms  11.579 ms  11.735 ms
 4  * * *
 5  * * *
 6  * * *
 7  81.52.188.174 (81.52.188.174)  17.834 ms  18.900 ms  19.028 ms
 8  108.170.255.223 (108.170.255.223)  20.521 ms 172.253.70.165 (172.253.70.165)  22.299 ms
108.170.238.45 (108.170.238.45)  22.499 ms
 9  142.251.49.137 (142.251.49.137)  22.726 ms 142.251.64.131 (142.251.64.131)  15.682 ms 108.170.235.15
(108.170.235.15)  16.539 ms
10  dns.google (8.8.8.8)  17.865 ms  18.199 ms  17.221 ms
```

traceroute (ou tracert sous Windows) est un programme utilitaire qui permet de suivre les chemins qu'un paquet de données (paquet IP) va prendre pour aller de la machine locale à une autre machine connectée au réseau IP. Il a été conçu au sein du Laboratoire national Lawrence-Berkeley.

Il existe d’autre utilitaire alternatif, comme MTR (My TraceRoute) par exemple.

NETSTAT

```
admin@laptop:~$ netstat -tlpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:8384          0.0.0.0:*               LISTEN      2184/syncthing
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:12546         0.0.0.0:*               LISTEN      2752/cli
tcp        0      0 127.0.0.1:61961         0.0.0.0:*               LISTEN      2752/cli
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 :::22000                :::*                    LISTEN      2184/syncthing
```

-a	--all	display all sockets (default: connected)
-t	--tcp	display sockets TCP
-u	--udp	display sockets UDP
-l	--listening	display listening server sockets
-p	--programs	display PID/Program name for sockets
-n	--numeric	don't resolve names

La commande netstat permet de connaître les statistiques sur les interfaces réseau actives. Il y a plusieurs option disponible, je vais vous donner la commande que j'utilise moi, mais après à vous de juger si vous en avez besoin ou non. Pour cette commande vous n'êtes pas obligé d'être root, dans se cas la il n'affichera pas toute les statistiques.

NMAP

```
admin@laptop:~$ nmap -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 11:36 CET
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds
```

-sL	List Scan - simply list targets to scan
-sS / -sT / -sA / -sW / -sM	TCP SYN / Connect() / ACK / Window / Maimon scans
-P0 / -Pn	Treat all hosts as online -- skip host discovery
-p	<port ranges>: Only scan specified ports
--traceroute	Trace hop path to each host

Le logiciel nmap permet de scanner une IP, il vous permettra de savoir quels sont les ports ouverts de votre réseaux afin de le sécuriser avec un firewall.

TCPDUMP

```
admin@laptop:~$ tcpdump -s0 -i enp5s0 -w /tmp/trafic.pcap
```

-i	interface
-s	snaplen
-w	file

Outil de capture et d'analyse réseau. Il permet d'avoir une analyse en direct du réseau ou d'enregistrer la capture dans un fichier afin de l'analyser pour plus tard. Il permet d'écrire des filtres afin de sélectionner les paquets à capturer/analyser.

WIRESHARK

```
admin@laptop:~$ sudo wireshark &
```

sudo	nécessaire pour avoir les droits d'écouter sur l'interface réseau
&	permet de lancer le logiciel en arrière-plan pour garder la main sur le terminal

Wireshark est un analyseur de protocoles réseau qui capture et affiche les données circulant sur un réseau en temps réel. Il permet une inspection minutieuse ("deep packet inspection") pour le dépannage et l'analyse de sécurité.

WGET

```
admin@laptop:~$ wget -P /home/admin/Desktop/ ftp://ftp.rs.internic.net/domain/named.root
--2025-12-05 14:37:51--  ftp://ftp.rs.internic.net/domain/named.root
           => ‘/home/admin/Desktop/named.root’
Resolving ftp.rs.internic.net (ftp.rs.internic.net)... 72.13.37.44
Connecting to ftp.rs.internic.net (ftp.rs.internic.net)|72.13.37.44|:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD (1) /domain ... done.
==> SIZE named.root ... 3314
==> PASV ... done.    ==> RETR named.root ... done.
Length: 3314 (3.2K) (unauthoritative)

named.root                          100%
[=====================================================================>]   3.24K  --.-KB/s    in 0.001s

2025-12-05 14:37:53 (2.28 MB/s) - ‘/home/admin/Desktop/named.root’ saved [3314]
```

-P	**Prefix**	Définit le **répertoire de destination** où le fichier sera enregistré. Si le dossier n'existe pas, wget le créera.
-O	**Output**	Force le nom du fichier de sortie. Indispensable quand l'URL ne contient pas un nom de fichier propre.
-c	**Continue**	Reprend un téléchargement interrompu (très utile pour les ISOs ou backups volumineux sur des connexions instables).
-b	**Background**	Lance le téléchargement en arrière-plan. Utile si tu dois fermer ta session SSH pendant un long transfert.

WGET est un utilitaire en ligne de commande robuste pour télécharger des fichiers depuis le Web (via HTTP, HTTPS ou FTP). Il est conçu pour être non interactif, ce qui signifie qu'il peut travailler en arrière-plan, et il est capable de reprendre automatiquement des téléchargements interrompus en cas de coupure réseau.

TELNET

```
admin@laptop:~$ telnet c2lr.fr 80
Trying 51.77.173.235...
Connected to 51.77.173.235.
Escape character is '^]'.
GET / HTTP/1.1
Host: c2lr.fr

HTTP/1.1 301 Moved Permanently
Date: Thu, 04 Dec 2025 10:24:39 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 SVN/1.7.14
Location: https://c2lr.fr/
Content-Length: 224
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://c2lr.fr/">here</a>.</p>
</body></html>
Connection closed by foreign host.
```

Telnet est un protocole réseau basique permettant d'établir une connexion texte interactive avec un hôte distant. Bien qu'il ne soit pas sécurisé (non chiffré), il est encore très utilisé aujourd'hui pour vérifier manuellement si un port spécifique est ouvert et accepte des connexions

CURL

```
admin@laptop:~$ curl -i google.fr
HTTP/1.1 301 Moved Permanently
Location: http://www.google.fr/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-
cS2o1yo8SXG5wmOVm9FhgQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https:
http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
Date: Fri, 05 Dec 2025 08:33:09 GMT
Expires: Sun, 04 Jan 2026 08:33:09 GMT
Cache-Control: public, max-age=2592000
Server: gws
Content-Length: 218
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN

<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.fr/">here</A>.
</BODY></HTML>
```

`-i` `--show-headers` Show response headers in output

CURL est un outil en ligne de commande puissant pour transférer des données via URL. Il est indispensable pour tester des API, télécharger des fichiers ou inspecter les réponses des serveurs web

NETCAT

```
admin@laptop:~$ nc -z -v 51.77.173.235 80
Connection to 51.77.173.235 80 port [tcp/http] succeeded!
```

`-z` zero-I/O

`-v` verbose

nc (pour netcat) est un outil qui permet de lire et écrire de la donnée en ligne de commande à travers le réseau.

OPENSSL

```
admin@laptop:~$ openssl version -a
OpenSSL 3.5.4 30 Sep 2025 (Library: OpenSSL 3.5.4 30 Sep 2025)
built on: Sat Nov  1 11:22:59 2025 UTC
platform: debian-amd64
options:  bn(64,64)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -fzero-call-used-regs=used-gpr -Wa,--
noexecstack -g -O2 -Werror=implicit-function-declaration
-ffile-prefix-map=/build/reproducible-path/openssl-3.5.4=. -fstack-protector-strong -fstack-clash-
protection -Wformat -Werror=format-security -fcf-protection -DOPENSSL_USE_NODELETE -DL_ENDIAN
-DOPENSSL_PIC -DOPENSSL_BUILDING_OPENSSL -DZLIB -DZSTD -DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
OPENSSLDIR: "/usr/lib/ssl"
ENGINESDIR: "/usr/lib/x86_64-linux-gnu/engines-3"
MODULESDIR: "/usr/lib/x86_64-linux-gnu/ossl-modules"
admining source: os-specific
CPUINFO:
OPENSSL_ia32cap=0x7ed8320b078bffff:0x0040069c219c97a9:0x0000000000000010:0x0000000000000000:0x00000000000
00000
```

version	Affiche la version du logiciel
-a	Affiche toutes les données disponibles (date de compilation, options, etc.)
s_client	Lance un outil de diagnostic client pour tester SSL/TLS
-connect hote:port	Spécifie le serveur cible et le port

OpenSSL est une boîte à outils cryptographique robuste utilisée pour implémenter les protocoles SSL/TLS, gérer les certificats numériques et tester la sécurité des connexions.

CHRONY

```
admin@laptop:~$ chronyc tracking
Reference ID    : 34F83DD6 (2001:41d0:700:6d9a::)
Stratum         : 4
Ref time (UTC)  : Mon Dec 08 16:45:46 2025
System time     : 0.000000077 seconds fast of NTP time
Last offset     : -0.000076081 seconds
RMS offset      : 0.000076081 seconds
Frequency       : 8.528 ppm slow
Residual freq   : +44.470 ppm
Skew            : 1000000.000 ppm
Root delay      : 0.041378908 seconds
Root dispersion : 31.769577026 seconds
Update interval : 2.0 seconds
Leap status     : Normal
```

tracking	affiche les informations sur la performance du système
sources	affiche la liste des serveurs de temps auxquels ton ordinateur est connecté
-v	verbose

« Mieux tes horloges tu configureras, plus sur ton cluster sera, que la force soit avec toi »

Chrony est une implémentation moderne et polyvalente du protocole NTP. Il est conçu pour synchroniser l'horloge système plus rapidement et avec une meilleure précision que les outils classiques, même sur des connexions instables ou intermittentes.

NTP

```
admin@laptop:~$ sudo systemctl status systemd-timesyncd.service
[sudo] password for admin:
● systemd-timesyncd.service - Network Time Synchronization
     Loaded: loaded (/usr/lib/systemd/system/systemd-timesyncd.service; enabled; preset: enabled)
     Active: active (running) since Fri 2025-12-05 08:38:32 CET; 4h 38min ago
 Invocation: 900814f97995403da9a022820b603f44
       Docs: man:systemd-timesyncd.service(8)
   Main PID: 533 (systemd-timesyn)
     Status: "Contacted time server [2001:41d0:801:2000::acb]:123 (2.debian.pool.ntp.org)."
      Tasks: 2 (limit: 33279)
     Memory: 2.6M (peak: 3.3M)
        CPU: 77ms
     CGroup: /system.slice/systemd-timesyncd.service
             └─533 /usr/lib/systemd/systemd-timesyncd

Dec 05 08:38:33 laptop systemd-timesyncd[533]: Network configuration changed, trying to establish
connection.
Dec 05 08:38:33 laptop systemd-timesyncd[533]: Network configuration changed, trying to establish
connection.
Dec 05 08:38:33 laptop systemd-timesyncd[533]: Network configuration changed, trying to establish
connection.
Dec 05 08:38:33 laptop systemd-timesyncd[533]: Network configuration changed, trying to establish
connection.
Dec 05 08:38:33 laptop systemd-timesyncd[533]: Network configuration changed, trying to establish
connection.
Dec 05 08:39:03 laptop systemd-timesyncd[533]: Contacted time server [2a01:cb00:129e:a803::77e]:123
(2.debian.pool.ntp.org).
Dec 05 08:39:03 laptop systemd-timesyncd[533]: Initial clock synchronization to Fri 2025-12-05
08:39:03.407743 CET.
Dec 05 09:47:34 laptop systemd-timesyncd[533]: Timed out waiting for reply from
[2a01:cb00:129e:a803::77e]:123 (2.debian.pool.ntp.org).
Dec 05 09:47:45 laptop systemd-timesyncd[533]: Timed out waiting for reply from
[2a01:cb00:129e:a803::585]:123 (2.debian.pool.ntp.org).
Dec 05 09:47:45 laptop systemd-timesyncd[533]: Contacted time server [2001:41d0:801:2000::acb]:123
(2.debian.pool.ntp.org).
```

Le protocole NTP (Network Time Protocol) permet de synchroniser l'horloge de l'ordinateur avec des serveurs de temps de référence sur Internet, garantissant une précision à la milliseconde près.

WHOIS

```
admin@laptop:~$ whois 8.8.8.8

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#


NetRange:       8.8.8.0 - 8.8.8.255
CIDR:           8.8.8.0/24
NetName:        GOGL
NetHandle:      NET-8-8-8-0-2
Parent:         NET8 (NET-8-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Google LLC (GOGL)
RegDate:        2023-12-28
Updated:        2023-12-28
Ref:            https://rdap.arin.net/registry/ip/8.8.8.0



OrgName:        Google LLC
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
RegDate:        2000-03-30
Updated:        2019-10-31
Comment:        Please note that the recommended way to file abuse complaints are located in the
following links.
Comment:
Comment:        To report abuse and illegal activity: https://www.google.com/contact/
Comment:
Comment:        For legal requests: http://support.google.com/legal
Comment:
Comment:        Regards,
Comment:        The Google Team
Ref:            https://rdap.arin.net/registry/entity/GOGL


OrgTechHandle: ZG39-ARIN
OrgTechName:   Google LLC
OrgTechPhone:  +1-650-253-0000
OrgTechEmail:  arin-contact@google.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ZG39-ARIN

OrgAbuseHandle: ABUSE5250-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-253-0000
OrgAbuseEmail:  network-abuse@google.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE5250-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#
```

Whois est un protocole de contrôle de transmission (TCP), ou protocole de requête / réponse orienté transaction, utilisé pour fournir des services d'information aux utilisateurs d'Internet.

Le whois **est utilisé pour obtenir les informations détaillées d'un domaine**, par exemple les dates de contrat, les données du registrant, le DNS attribué. Tout cela est tiré d'une base de données mondiale, où ces informations sont stockées. En même temps **Il permet à une IP de nous dire de quel pays il provient, des informations de l'opérateur Internet qui le gère et de nombreuses informations techniques supplémentaires**.