

## Travaux pratiques – Tracer une route

### Objectifs

**Partie 1 : vérifier la connectivité réseau à l'aide de la commande ping**

**Partie 2 : effectuer le suivi d'une route vers un serveur distant à l'aide de l'outil Traceroute**

**Partie 3 : effectuer le suivi d'une route vers un serveur distant à l'aide de l'outil web Traceroute**

### Contexte

Le suivi d'une route répertorie chaque appareil de routage qui achemine un paquet de la source à la destination sur un réseau. Ce logiciel de suivi s'exécute généralement dans une ligne de commande comme suit :

```
tracert <nom du réseau de destination ou adresse du périphérique final>
```

(Systèmes Microsoft Windows)

ou

```
traceroute <nom du réseau de destination ou adresse du périphérique final>
```

(Unix et systèmes identiques)

L'outil **traceroute** (ou **tracert**) est souvent utilisé pour dépanner les réseaux. En affichant la liste des routeurs traversés, il permet à l'utilisateur d'identifier le chemin pris pour atteindre une destination particulière sur le réseau ou les interréseaux. Chaque routeur représente un point de connexion entre deux réseaux par lequel a été transféré le paquet de données. Le nombre de routeurs correspond au nombre de « tronçons » effectués par les données depuis la source jusqu'à la destination.

La liste affichée permet d'identifier les problèmes de flux de données lors de la tentative d'accès à un service tel qu'un site Web. Elle permet également d'effectuer des tâches telles que le téléchargement de données. Si plusieurs sites web (miroirs) sont disponibles pour le même fichier de données, il est possible de tracer chaque miroir pour déterminer le plus rapide.

Deux commandes traceroute entre la même source et la même destination exécutées à des moments différents peuvent produire des résultats différents. Cela s'explique par la structure de « maillage » des réseaux interconnectés qui constituent Internet et du fait que les protocoles Internet sont capables de choisir différents chemins pour envoyer des paquets.

Les outils de traçage de route basés sur une interface en ligne de commande sont généralement intégrés au système d'exploitation du périphérique final.

### Scénario

Via une connexion Internet, vous allez utiliser deux programmes de suivi de route pour examiner le chemin Internet menant aux réseaux de destination. Tout d'abord, vous allez vérifier la connectivité à un site web. Ensuite, vous allez utiliser l'utilitaire **tracert** sur la ligne de commande Linux. Enfin, vous allez utiliser un outil traceroute basé sur le web (<https://gsuite.tools/traceroute>).

### Ressources requises

- Poste de travail virtuel Linux (Kali par exemple)
- Accès Internet

### Instructions

#### Étape 1: Vérifier la connectivité réseau à l'aide de la commande ping

- Démarrez le poste de travail virtuel Kali.
- Ouvrez une fenêtre de terminal dans la machine virtuelle pour envoyer une requête ping à un serveur distant, tel que [www.cisco.com](http://www.cisco.com).

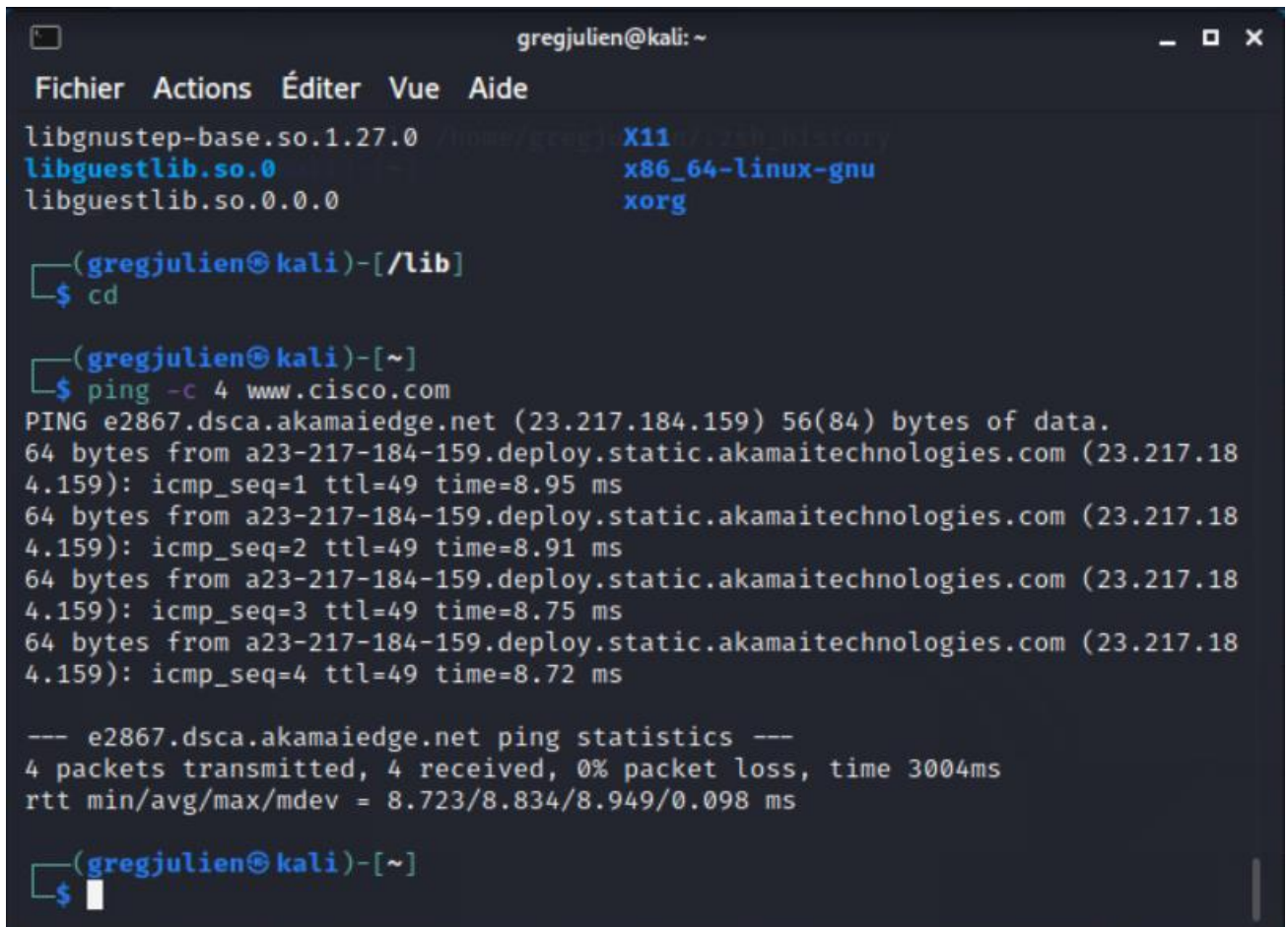
```
[kali@root ~]$ ping -c 4 www.cisco.com

PING e2867.dsca.akamaiedge.net (184.24.123.103) 56(84) bytes of data.
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=1 ttl=59 time=13.0 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=2 ttl=59 time=12.5 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=3 ttl=59 time=14.9 ms
64 bytes from a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103):
icmp_seq=4 ttl=59 time=11.9 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 11.976/13.143/14.967/1.132 ms
```

- La première ligne affiche le nom de domaine complet (FQDN) e2867.dsca.akamaiedge.net. Elle est suivie de l'adresse IP 184.24.123.103. Cisco héberge le même contenu web sur différents serveurs dans le monde entier (appelés miroirs). Par conséquent, selon votre emplacement géographique, le nom de domaine complet et l'adresse IP seront différents.

Quatre requêtes ping ont été envoyées et une réponse a été reçue pour chaque requête ping. Étant donné que chaque requête ping a reçu une réponse, la perte de paquets correspond à 0 %. En moyenne, il a fallu 3005 ms (3005 millisecondes) pour acheminer les paquets sur le réseau. Une milliseconde correspond à 1/1 000<sup>e</sup> de seconde. Vos résultats seront probablement différents.



```
gregjulien@kali: ~  
Fichier Actions Éditer Vue Aide  
libgustep-base.so.1.27.0 /usr/lib/x86_64-linux-gnu  
libgustep-base.so.0 /usr/lib/x86_64-linux-gnu  
libgustep-base.so.0.0.0 /usr/lib/x86_64-linux-gnu  
  
(gregjulien@kali)-[/lib]  
$ cd  
  
(gregjulien@kali)-[~]  
$ ping -c 4 www.cisco.com  
PING e2867.dsca.akamaiedge.net (23.217.184.159) 56(84) bytes of data.  
64 bytes from a23-217-184-159.deploy.static.akamaitechnologies.com (23.217.184.159): icmp_seq=1 ttl=49 time=8.95 ms  
64 bytes from a23-217-184-159.deploy.static.akamaitechnologies.com (23.217.184.159): icmp_seq=2 ttl=49 time=8.91 ms  
64 bytes from a23-217-184-159.deploy.static.akamaitechnologies.com (23.217.184.159): icmp_seq=3 ttl=49 time=8.75 ms  
64 bytes from a23-217-184-159.deploy.static.akamaitechnologies.com (23.217.184.159): icmp_seq=4 ttl=49 time=8.72 ms  
  
--- e2867.dsca.akamaiedge.net ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 8.723/8.834/8.949/0.098 ms  
  
(gregjulien@kali)-[~]  
$
```

## Étape 2: Effectuer le suivi d'une route vers un serveur distant à l'aide de l'outil Traceroute

Maintenant que l'accessibilité de base a été vérifiée à l'aide de l'outil ping, il est utile d'examiner de plus près chaque segment de réseau qui est traversé.

Suivant la taille de votre fournisseur d'accès Internet (FAI) et l'emplacement des hôtes source et de destination, les routes tracées peuvent passer par des sauts et des FAI différents. Chaque « saut » représente un routeur. Un routeur est un type d'ordinateur spécialisé qui permet de diriger le trafic sur Internet. Imaginez que vous effectuez un voyage en voiture dans plusieurs pays en utilisant de nombreuses autoroutes. À plusieurs endroits pendant le voyage, vous arrivez à des embranchements sur la route où vous avez la possibilité de choisir entre plusieurs autoroutes. Maintenant, imaginez qu'à chaque embranchement sur la route se trouve un dispositif qui vous oriente vers l'autoroute correcte vous permettant ainsi d'accéder à votre destination finale. C'est exactement le rôle d'un routeur pour les paquets sur un réseau.

Étant donné que les ordinateurs communiquent avec des nombres binaires ou hexadécimaux, plutôt qu'avec des mots, les routeurs sont identifiés grâce à leur adresse IP. L'outil **tracert** indique le chemin emprunté par un paquet de données sur le réseau pour atteindre sa destination finale. L'outil **tracert** vous donne également une idée de la vitesse du trafic sur chaque segment du réseau. Des paquets sont envoyés à chaque routeur sur le chemin et le temps de retour est mesuré en millisecondes.

Pour ce faire, c'est l'outil **tracert** qui est utilisé.

- a. À l'invite du terminal, tapez **tracert www.cisco.com**.

```
[kali@root ~]$ tracert www.cisco.com

tracert to www.cisco.com (184.24.123.103), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1) 6.527 ms 6.783 ms 6.826 ms
 2 10.39.176.1 (10.39.176.1) 27.748 ms 27.533 ms 27.480 ms
 3 100.127.65.250 (100.127.65.250) 27.864 ms 28.570 ms 28.566 ms
 4 70.169.73.196 (70.169.73.196) 29.063 ms 35.025 ms 33.976 ms
 5 fed1bbrj01.xe110.0.rd.sd.cox.net (68.1.0.155) 39.101 ms 39.120 ms 39.108 ms
 6 a184-24-123-103.deploy.static.akamaitechnologies.com (184.24.123.103) 38.004 ms
 13.583 ms 13.612 ms
```

```
gregjulien@kali:~$ traceroute www.cisco.com
traceroute to www.cisco.com (23.217.184.159), 30 hops max, 60 byte packets
 1 192.168.1.1 (192.168.1.1) 0.440 ms 0.443 ms 0.515 ms
 2 172.16.100.1 (172.16.100.1) 1.250 ms 1.250 ms 1.261 ms
 3 10.254.254.254 (10.254.254.254) 7.771 ms 9.170 ms 7.845 ms
 4 10.0.0.30 (10.0.0.30) 9.475 ms 10.0.0.22 (10.0.0.22) 8.027 ms 10.0.0.30
 (10.0.0.30) 10.487 ms
 5 10.0.0.21 (10.0.0.21) 8.034 ms 10.0.0.29 (10.0.0.29) 10.139 ms 10.0.0.2
 1 (10.0.0.21) 8.558 ms
 6 10.0.2.13 (10.0.2.13) 10.540 ms 8.304 ms 10.0.2.5 (10.0.2.5) 7.971 ms
 7 xe-4-3-1.tcr1.rb.par.core.as8218.eu (213.152.16.10) 8.950 ms 10.0.2.2 (1
 0.0.2.2) 7.783 ms xe-4-3-1.tcr1.rb.par.core.as8218.eu (213.152.16.10) 8.877
 ms
 8 xe-4-3-1.tcr1.rb.par.core.as8218.eu (213.152.16.10) 7.922 ms ae24.ter3.e
 qx2.par.core.as8218.eu (83.107.56.141) 8.853 ms xe-4-3-1.tcr1.rb.par.core.as
 8218.eu (213.152.16.10) 8.091 ms
 9 v3.ae10.mcs1.cdg12.fr.zip.zayo.com (64.125.30.182) 10.037 ms ae24.ter3.e
 qx2.par.core.as8218.eu (83.107.56.141) 8.440 ms v3.ae10.mcs1.cdg12.fr.zip.za
 yo.com (64.125.30.182) 9.979 ms
10 v3.ae10.mcs1.cdg12.fr.zip.zayo.com (64.125.30.182) 8.702 ms ae0.mcs1.cdg
11.fr.eth.zayo.com (64.125.29.117) 10.156 ms v3.ae10.mcs1.cdg12.fr.zip.zayo.
com (64.125.30.182) 8.937 ms
11 ae0.mcs1.cdg11.fr.eth.zayo.com (64.125.29.117) 8.301 ms 213.161.08.242.I
PYX-282803-902-ZY0.zip.zayo.com (213.161.08.242) 142.056 ms ae0.mcs1.cdg11.f
r.eth.zayo.com (64.125.29.117) 8.517 ms
12 ***
13 ***
14 ***
15 ***
16 ***
17 ***
18 ***
19 ***
20 ***
21 ***
22 ***
23 ***
24 ***
25 ***
26 ***
27 ***
28 ***
29 ***
30 ***

gregjulien@kali:~$
```

- b. Si vous souhaitez enregistrer la sortie de traceroute dans un fichier texte pour l'examiner ultérieurement, utilisez le caret de droite (>), nommez le fichier de la sortie comme il convient, puis enregistrez-le dans le répertoire actuel. Dans cet exemple, la sortie de traceroute est enregistrée dans le fichier `/home/analyst/cisco-traceroute.txt`.

```
[kali@root ~]$ traceroute www.cisco.com > cisco-traceroute.txt
```

Vous pouvez maintenant saisir la commande `cat cisco-traceroute.txt` pour afficher la sortie de traceroute stockée dans le fichier texte.

- c. Exécutez l'outil traceroute et enregistrez ses résultats pour l'un des sites web suivants. Il s'agit des sites web des organismes d'enregistrement Internet locaux de différentes parties du monde :

Afrique : [www.afrinic.net](http://www.afrinic.net)

Australie : [www.apnic.net](http://www.apnic.net)

Europe : [www.ripe.net](http://www.ripe.net)

Amérique du Sud : [www.lacnic.net](http://www.lacnic.net)

**Remarque :** il est possible que certains de ces routeurs sur la route ne répondent pas à traceroute.

### Étape 3: Effectuer le suivi d'une route vers un serveur distant à l'aide de l'outil web Traceroute

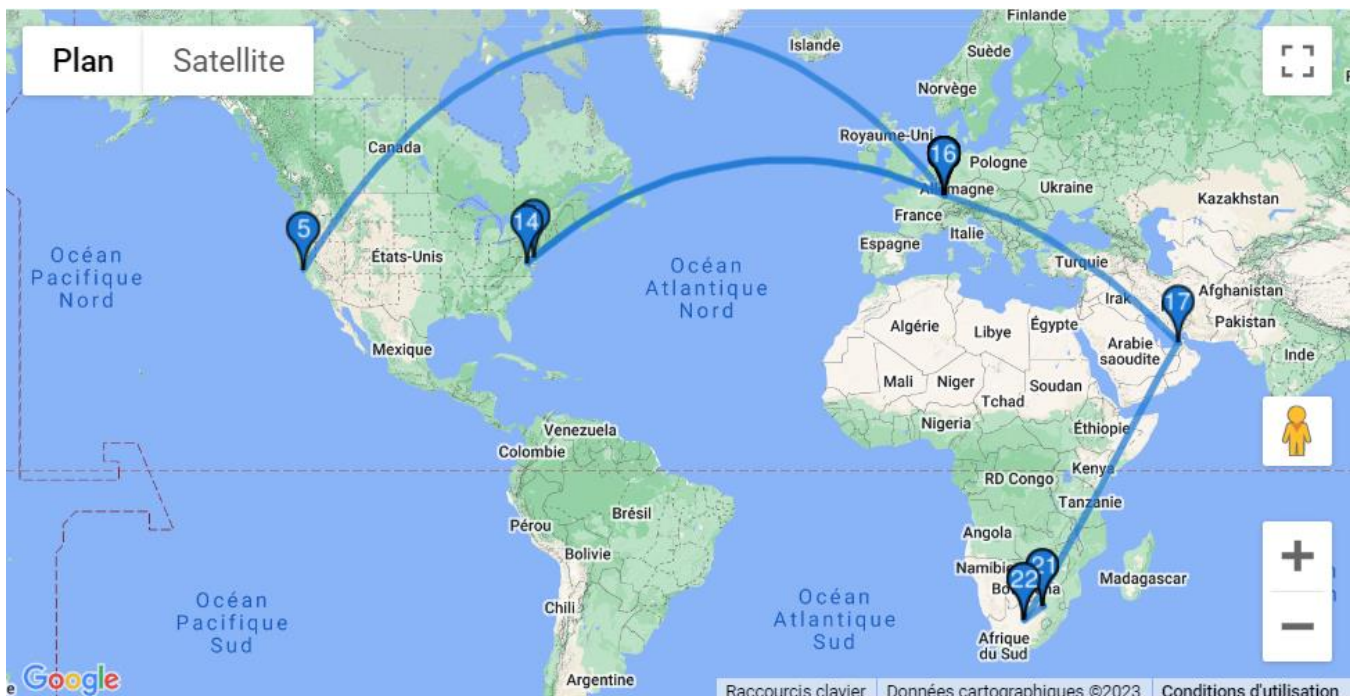
- Ouvrez un navigateur Web dans la machine virtuelle et recherchez un outil de traceroute visuel que vous pouvez utiliser dans le navigateur Web. Essayez d'accéder le site Web suivant:  
<https://gsuite.tools/traceroute>
- Entrez n'importe quel site Web que vous souhaitez. **Exemple: [www.cisco.com](http://www.cisco.com)** et appuyez sur **Trace**.

**Remarque:** Si vous obtenez l'erreur «SEC\_ERROR\_OCSP\_FUTURE\_RESPONSE» dans Firefox, alors l'horloge/heure de la station de travail CyberOps est incorrecte. Pour corriger l'heure, saisissez la commande suivante pour mettre à jour l'horloge/heure, puis actualisez le navigateur Web et entrez la trace visuelle:

```
[kali@root~]$ sudo ntpd -qq
```

Vérifiez l'emplacement géographique des sauts correspondants. Qu'avez-vous remarqué concernant le chemin ?

Le chemin fait début à New-York pour ensuite partir sur l'Europe, puis à Dubaï pour finir en Afrique du Sud.





tracert to www.afrinic.net (196.216.2.6), 30 hops max

Hop	Host	IP	Time (ms)
1	_gateway	209.151.144.1	0.096ms
2	100.70.163.241	100.70.163.241	0.336ms
3	172.23.255.89	172.23.255.89	0.149ms
4	172.23.255.238	172.23.255.238	0.149ms
5	te0-3-1-3.rcr51.b034314-0.sjc01.atlas.cogentco.com	38.104.135.225	0.848ms
6	be2297.ccr21.sjc01.atlas.cogentco.com	154.54.90.181	1.025ms
7	be3178.ccr21.sfo01.atlas.cogentco.com	154.54.43.69	2.118ms
8	be3109.ccr21.slc01.atlas.cogentco.com	154.54.44.138	16.425ms
9	be3037.ccr21.den01.atlas.cogentco.com	154.54.41.146	26.659ms
10	be3035.ccr21.mci01.atlas.cogentco.com	154.54.5.90	38.055ms
11	be2831.ccr41.ord01.atlas.cogentco.com	154.54.42.166	49.715ms
12	be2717.ccr21.cle04.atlas.cogentco.com	154.54.6.222	56.225ms
13	be2878.ccr21.alb02.atlas.cogentco.com	154.54.26.130	66.715ms
14	be3599.ccr31.bos01.atlas.cogentco.com	66.28.4.238	70.199ms
15	be2099.ccr41.lon13.atlas.cogentco.com	154.54.82.33	132.418ms
16	be2375.rcr21.b015533-1.lon13.atlas.cogentco.com	154.54.61.158	132.695ms
17	149.14.227.58	149.14.227.58	132.148ms
18	cr1-mrs-et49-1.wolcomm.net	41.78.188.221	318.758ms
19	*	*	*
20	esr1-isd-cr1-te0-0-26.wolcomm.net	197.157.77.97	305.896ms
21	197.157.64.195	197.157.64.195	307.064ms
22	www.afrinic.net	196.216.2.6	305.826ms

## Question de réflexion

En quoi la sortie de traceroute est-elle différente lorsque vous accédez à [www.cisco.com](http://www.cisco.com) à partir du terminal (voir la partie 2) plutôt qu'à partir du site web en ligne ? (Vos résultats peuvent varier selon votre emplacement géographique et selon le FAI fournissant la connexion de votre école.)

### Réponse :

Lorsque nous exécutons la commande traceroute sur notre terminal, celle-ci est exécutée depuis notre machine donc la route commencera à partir de notre adresse ip tandis que depuis un navigateur web, la commande est exécutée sur le serveur qui héberge le site web, donc la route commencera depuis le serveur et non notre machine.

En conclusion, la sortie de traceroute sera différente en fonction de si la commande est exécutée sur notre machine ou bien depuis un site web car le chemin d'accès sera lui aussi différent.

Important : La Kali étant K.O au moment du TP, j'ai effectué ces commandes depuis mon pc personnel.

Commande exécutée sur ma machine :

```
PS C:\Users\jbert> tracert www.cisco.com

Détermination de l'itinéraire vers e2867.dsca.akamaiedge.net [104.69.2.211]
avec un maximum de 30 sauts :

  1    4 ms    8 ms    1 ms  172.16.1.1
  2   14 ms   14 ms   13 ms  10.254.254.254
  3   31 ms   17 ms   19 ms  10.0.6.30
  4   13 ms   11 ms   15 ms  10.0.6.29
  5   13 ms   12 ms   13 ms  10.0.2.13
  6   11 ms   12 ms   12 ms  10.0.2.1
  7   15 ms   13 ms   12 ms  ae75-0.noidf001.rbc1.orange.net [193.253.12.85]
  8   12 ms   14 ms   17 ms  ae43-0.niidf101.rbc1.orange.net [193.252.98.113]
  9   14 ms   15 ms   12 ms  193.252.137.10
 10   14 ms   13 ms   13 ms  193.251.133.141
 11   12 ms   15 ms   12 ms  193.251.144.100
 12   *       *       *      Délai d'attente de la demande dépassé.
 13   *       *       *      Délai d'attente de la demande dépassé.
 14   *       *       *      Délai d'attente de la demande dépassé.
 15   14 ms   19 ms   15 ms  a104-69-2-211.deploy.static.akamaitechnologies.com [104.69.2.211]

Itinéraire déterminé.
```

Commande exécutée depuis <https://gsuite.tools> :

traceroute to e2867.dsca.akamaiedge.net (23.218.68.242), 30 hops max

Hop	Host	IP	Time (ms)
1	_gateway	209.151.144.1	0.107ms
2	100.70.134.65	100.70.134.65	0.255ms
3	172.23.255.37	172.23.255.37	0.223ms
4	172.23.255.234	172.23.255.234	0.167ms
5	ae17-727.cr0-sjc1.ip4.gtt.net	69.174.20.9	0.693ms
6	ae6.cr3-lon8.ip4.gtt.net	213.200.112.210	136.066ms
7	ip4.gtt.net	154.14.69.238	137.552ms
8	ae8.r01.lon01.icn.netarch.akamai.com	23.210.49.36	137.413ms
9	ae9.r02.ams01.icn.netarch.akamai.com	95.100.192.125	157.882ms
10	ae2.r02.ams01.iem.netarch.akamai.com	23.210.55.41	149.678ms
11	ae35.r02.border101.ams01.fab.netarch.akamai.com	23.210.55.185	146.674ms
12	*	*	*
13	*	*	*
14	*	*	*
15	a23-218-68-242.deploy.static.akamaitechnologies.com	23.218.68.242	146.493ms