**Ping**

**Ping to asia : Asia-Pacific Network : www.apnic.com**

**www.apnic.com**

**PING apnic.net (202.12.29.1) 56(84) bytes of data.**

**64 bytes from ingress.public.prod.apnic.net (202.12.29.1): icmp\_seq=1 ttl=60 time=272 ms**

**Ping to Europe :www.ripe.com**

**PING www.ripe.net.cdn.cloudflare.net (104.18.20.44) 56(84) bytes of data.**

**64 bytes from 104.18.20.44 (104.18.20.44): icmp\_seq=1 ttl=59 time=5.44 ms**

**Ping to south-america : www.lacnic.net / .com**

**PING www.lacnic.net (200.3.14.145) 56(84) bytes of data.**

**64 bytes from www.lacnic.net (200.3.14.145): icmp\_seq=1 ttl=59 time=195 ms**

**ping to africa : www.afrinic.net**

**PING www.afrinic.net (196.216.2.6) 56(84) bytes of data.**

**64 bytes from www.afrinic.net (196.216.2.6): icmp\_seq=1 ttl=60 time=164 ms**

**traceroute cisco.com :**

**traceroute to www.cisco.com (184.51.105.33), 30 hops max, 60 byte packets**

**1 10.0.5.1 (10.0.5.1) 0.035 ms 0.018 ms 0.015 ms**

**2 10.10.0.143 (10.10.0.143) 0.071 ms 0.049 ms 0.050 ms**

**3 72.14.238.231 (72.14.238.231) 4.919 ms 4.668 ms 4.454 ms**

**4 ae11.r01.par01.ien.netarch.akamai.com (23.210.53.184) 4.872 ms 4.678 ms 4.496 ms**

**5 ae34.r03.border101.par02.fab.netarch.akamai.com (23.210.53.25) 5.180 ms 4.918 ms 5.644 ms**

**Trace route**

**traceRoute to asia : www.apnic.com**

**traceRoute to Europe : : www.ripe.com**

**traceRoute to South-amrica : www.lacnic.net / com**

**traceRoute to Africa : www.afrinic.net**

**traceRoute to asia : www.apnic.com**

**traceroute to www.apnic.com (202.12.29.1), 30 hops max, 60 byte packets**

**1 10.0.5.1 (10.0.5.1) 0.026 ms 0.013 ms 0.013 ms**

**2 10.10.0.143 (10.10.0.143) 0.085 ms 0.040 ms 0.035 ms**

**3 192.178.98.20 (192.178.98.20) 263.419 ms 192.178.97.80 (192.178.97.80) 265.401 ms 192.178.97.210 (192.178.97.210) 262.457 ms**

**4 4608.syd.equinix.com (45.127.172.3) 274.729 ms 270.113 ms 272.986 ms**

**5 et-1-37.nxcs1.bne.apnic.net (203.119.104.18) 273.369 ms 272.974 ms 271.388 ms**

**6 ingress.public.prod.apnic.net (202.12.29.1) 270.039 ms 272.909 ms 273.441 ms**

**traceRoute to Europe : : www.ripe.com**

**traceroute to www.ripe.com (151.101.130.159), 30 hops max, 60 byte packets**

**1 10.0.5.1 (10.0.5.1) 0.035 ms 0.014 ms 0.011 ms**

**2 10.10.0.143 (10.10.0.143) 0.062 ms 0.033 ms 0.031 ms**

**3 \* \* \***

**4 \* \* \***

**5 \* \* \***

**6 \* \* \***

**7 \* \* \***

**8 \* \* \***

**9 \* \* \***

**10 \* \* \***

**11 \* \* \***

**12 \* \* \***

**13 \* \* \***

**14 \* \* \***

**15 \* \* \***

**16 \* \* \***

**17 \* \* \***

**18 \* \* \***

**19 \* \* \***

**20 \* \* \***

**21 \* \* \***

**22 \* \* \***

**23 \* \* \***

**24 \* \* \***

**25 \* \* \***

**26 \* \* \***

**27 \* \* \***

**28 \* \* \***

**29 \* \* \***

**30 \* \* \***

**inic.net (196.216.2.6) 163.644 ms 162.843 ms 165.018 ms**

**```**

**traceRoute to asia : www.apnic.com**

**traceroute to www.apnic.com (202.12.29.1), 30 hops max, 60 byte packets**

**1 10.0.5.1 (10.0.5.1) 0.026 ms 0.013 ms 0.013 ms**

**2 10.10.0.143 (10.10.0.143) 0.085 ms 0.040 ms 0.035 ms**

**3 192.178.98.20 (192.178.98.20) 263.419 ms 192.178.97.80 (192.178.97.80) 265.401 ms 192.178.97.210 (192.178.97.210) 262.457 ms**

**4 4608.syd.equinix.com (45.127.172.3) 274.729 ms 270.113 ms 272.986 ms**

**5 et-1-37.nxcs1.bne.apnic.net (203.119.104.18) 273.369 ms 272.974 ms 271.388 ms**

**6 ingress.public.prod.apnic.net (202.12.29.1) 270.039 ms 272.909 ms 273.441 ms**

**traceRoute to Europe : : www.ripe.com**

**traceroute to www.ripe.com (151.101.130.159), 30 hops max, 60 byte packets**

**1 10.0.5.1 (10.0.5.1) 0.035 ms 0.014 ms 0.011 ms**

**2 10.10.0.143 (10.10.0.143) 0.062 ms 0.033 ms 0.031 ms**

**3 \* \* \***

**4 \* \* \***

**5 \* \* \***

**6 \* \* \***

**7 \* \* \***

**8 \* \* \***

**9 \* \* \***

**10 \* \* \***

**11 \* \* \***

**12 \* \* \***

**13 \* \* \***

**14 \* \* \***

**15 \* \* \***

**16 \* \* \***

**17 \* \* \***

**18 \* \* \***

**19 \* \* \***

**20 \* \* \***

**21 \* \* \***

**22 \* \* \***

**23 \* \* \***

**24 \* \* \***

**25 \* \* \***

**26 \* \* \***

**27 \* \* \***

**28 \* \* \***

**29 \* \* \***

**30 \* \* \***

**traceRoute to South-amrica : www.lacnic.net / com**

**traceroute to www.lacnic.net (200.3.14.145), 30 hops max, 60 byte packets**

**1 10.0.5.1 (10.0.5.1) 0.021 ms 0.017 ms 0.020 ms**

**2 10.10.0.143 (10.10.0.143) 0.044 ms 0.024 ms 0.055 ms**

**3 64.233.174.202 (64.233.174.202) 193.669 ms 197.469 ms 193.291 ms**

**4 as28001.saopaulo.sp.ix.br (187.16.216.61) 193.820 ms 193.596 ms 193.458 ms**

**5 200.3.12.41 (200.3.12.41) 193.584 ms 193.674 ms 193.534 ms**

**6 200.3.12.34 (200.3.12.34) 193.981 ms 194.023 ms 193.866 ms**

**7 www.lacnic.net (200.3.14.145) 194.095 ms 194.058 ms 193.888 ms**

**traceRoute to Africa : www.afrinic.net**

**traceroute to www.afrinic.net (196.216.2.6), 30 hops max, 60 byte packets**

**1 10.0.5.1 (10.0.5.1) 0.039 ms 0.014 ms 0.013 ms**

**2 10.10.0.143 (10.10.0.143) 0.073 ms 0.041 ms 0.037 ms**

**3 172.253.69.235 (172.253.69.235) 163.235 ms 163.701 ms 163.660 ms**

**4 afrinic-2.jinx.net.za (196.60.96.160) 162.790 ms 163.158 ms 163.911 ms**

**5 www.afrinic.net (196.216.2.6) 163.644 ms 162.843 ms 165.018 ms**

**Tous ces pings ont été effectués à partir d'un ordinateur situé aux États-Unis. Qu'advient-il du temps de**

**ping moyen en millisecondes lorsque les données voyagent à l'intérieur du même continent par rapport aux données de l'Amérique du Nord qui voyagent vers d'autres continents ?**

**Qu'y a-t-il d'intéressant dans les pings envoyés au site web européen ?**

Le temps de ping moyen en millisecondes dépend de plusieurs facteurs, dont la distance physique entre les points de communication, la capacité du réseau intermédiaire, et la charge du réseau. Lorsque les données voyagent à l'intérieur du même continent, le temps de ping peut être généralement plus court car il y a moins de "sauts" nécessaires à travers différents réseaux. Cependant, lorsque les données de l'Amérique du Nord voyagent vers d'autres continents, elles doivent traverser plusieurs réseaux et pays, ce qui augmente le temps de ping.

Lorsque vous envoyez des pings au site web européen depuis les États-Unis, vous pouvez utiliser la commande `ping` pour tester la connectivité et le temps de réponse. Par exemple, vous pouvez utiliser la commande `ping www.ripe.net`. Cette commande envoie un paquet de requête d'écho à l'adresse www.ripe.net et attend une réponse. Le temps nécessaire à la réception de la réponse d'écho est mesuré en millisecondes. Cela peut donner une idée de la latence du réseau entre les États-Unis et l'Europe.

Enfin, pour obtenir plus d'informations sur le chemin que prennent les données, vous pouvez utiliser la commande `traceroute`, qui trace le parcours que les paquets de données empruntent pour atteindre leur destination. Cela peut vous aider à identifier les points de retard ou de congestion sur le chemin des données

**Que se passe-t-il au niveau du saut 7 ? Level3.net est-il le même fournisseur d'accès que les sauts 2 à 6, ou**

**un fournisseur d'accès différent ? Utilisez l'outil whois pour répondre à cette question.**

152.63.16.185

verizon Business a ashburn

4.68.111.137

Level 3 parent llc a Monroe

ce n’est pas le meme fournisseur d'accès internet,

on passe de géorgie au missouri.

**Que se passe-t-il dans le saut 10 en ce qui concerne le temps nécessaire à un paquet pour voyager**

**entre Washington D.C. et Paris, par rapport aux sauts 1 à 9 précédents ?**

Dans le cas d'un paquet de données voyageant entre Washington D.C. et Paris, le saut 10 représente généralement le premier saut hors du réseau des États-Unis. Cela signifie qu'après avoir quitté le réseau local de Washington D.C., le paquet de données doit traverser l'Atlantique, ce qui ajoute une grande quantité de latence au temps de ping.

Par rapport aux sauts 1 à 9, où le paquet de données reste dans le réseau américain, le saut 10 introduit une augmentation significative du temps de ping. En effet, le paquet de données doit maintenant voyager à travers plusieurs réseaux internationaux, ce qui augmente la distance physique que le paquet doit parcourir et donc le temps nécessaire pour transmettre le paquet.

Il convient de noter que le temps de ping exact peut varier en fonction de nombreux facteurs, notamment la charge du réseau, la qualité de la connexion Internet et les politiques de routage des données. De plus, le fait que le paquet de données soit enregistré dans un fichier texte, comme mentionné dans votre question initiale, ne devrait pas affecter le temps de ping. Les données sont toujours transmises de la même manière, quelle que soit la nature du contenu.

**Que se passe-t-il dans le saut 18 ? Effectuez une recherche sur 168.209.201.74 à l'aide de l'outil whois.**

**Qui possède ce réseau ?**

organisation: ORG-DD1-AFRINIC

org-name: Dimension Data

org-type: LIR

country: ZA

address: The Campus,

address: 57 Sloane St,

address: Bryanston

address: Johannesburg 2021

**page 10 -> Que se passe-t-il dans le saut 7**

L'adresse IP 204.255.168.194 appartient à Verizon Business (MCICS) selon les informations fournies par l'outil WhoIs. L'adresse est située dans le bloc d'adresses 204.252.0.0/14, qui a été attribué directement à Verizon Business.

Verizon Business est une entreprise de communications basée aux États-Unis, qui offre divers services, y compris l'accès à Internet. L'adresse IP donnée semble être utilisée par Verizon pour acheminer le trafic Internet.

Quant à l'adresse IP 159.63.48.38, elle appartient à Level 3 Parent, LLC (LPL-141). Cette adresse est située dans le bloc d'adresses 159.63.0.0/16, qui a été attribué directement à Level 3 Parent, LLC. Level 3 Parent, LLC est une entreprise de télécommunications basée aux États-Unis, et cette adresse IP est probablement utilisée pour acheminer le trafic Internet

Il est important de noter que les adresses IP peuvent changer en fonction de divers facteurs, y compris les modifications des configurations de réseau et les politiques de routage des données.

**a. En utilisant http://www.subnetonline.com/pages/network-tools/online-tracepath.php pour tracer**

**l'itinéraire vers les sites web suivants :**

[**www.cisco.com**](http://www.cisco.com)

TracePath Output:

1?: [LOCALHOST] pmtu 1500

1: nova.subnetonline.com 0.107ms reached

1: nova.subnetonline.com 0.041ms reached

Resume: pmtu 1500 hops 1 back 1

---- Finished ------

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

TracePath Output:

1?: [LOCALHOST] pmtu 1500

1: nova.subnetonline.com 0.083ms reached

1: nova.subnetonline.com 0.047ms reached

Resume: pmtu 1500 hops 1 back 1

---- Finished ------

**Capturez et enregistrez le résultat dans le Bloc-notes.**

**En quoi le traceroute est-il différent lorsqu'on se rend sur www.cisco.com à partir de l'invite de**

**commande (voir partie 1) plutôt qu'à partir du site web en ligne ? (Vos résultats peuvent varier en**

**fonction de votre situation géographique et du fournisseur d'accès à Internet qui fournit la connectivité à**

**votre école).**

Lorsque vous exécutez un traceroute à partir de l'invite de commande, vous obtenez une vue plus détaillée du processus de routage des données. Chaque étape du traceroute affiche l'adresse IP du routeur ou du serveur intermédiaire à partir duquel le paquet de données est envoyé. Cela peut vous aider à identifier les points de retard ou de congestion sur le chemin des données.

D'autre part, lorsqu'un traceroute est effectué à partir d'un outil en ligne, vous obtenez une vue simplifiée du processus de routage. Ces outils en ligne ne montrent généralement que l'adresse IP du dernier hôte avant la destination finale, sans afficher les détails des hôtes intermédiaires. Ils peuvent également masquer certains détails techniques pour faciliter la compréhension des résultats.

En comparant les résultats d'un traceroute effectué à partir de l'invite de commande et ceux d'un outil en ligne, vous pouvez obtenir une meilleure compréhension du chemin que les paquets de données empruntent pour atteindre une destination spécifique. Cependant, les résultats peuvent varier en fonction de votre situation géographique et du fournisseur d'accès à Internet qui fournit la connectivité à votre école.

**Comparez le tracert de la partie 1 qui va vers l'Afrique avec le tracert qui va vers l'Afrique à partir de**

**l'interface web. Quelle différence remarquez-vous ?**

le tracert via cmd est plus détaillé que via web

**Certains tracés comportent l'abréviation asymm. Qu'est-ce que cela signifie ? Quelle est sa signification**

**?**

L'abréviation "asymm" dans le résultat d'un traceroute signifie que le chemin aller (de l'origine à la destination) et le chemin retour (de la destination à l'origine) sont différents. Cela peut être dû à plusieurs raisons, notamment le routage dynamique, où les chemins les plus courts ne sont pas toujours identiques dans les deux sens, ou des problèmes de configuration du réseau.

Dans le traceroute, chaque saut correspond à un routeur ou un autre point d'arrêt dans le chemin que les paquets de données empruntent pour atteindre leur destination. Si le chemin aller et le chemin retour passent par des routeurs différents, cela peut entraîner une différence dans le nombre de sauts et donc une différence dans le temps de réponse total.

Il est important de noter que l'asymétrie du chemin n'est pas toujours préjudiciable. Dans certains cas, elle peut même améliorer les performances du réseau en évitant les points de congestion ou les goulots d'étranglement. Cependant, si elle est significative, elle peut indiquer un problème de configuration du réseau qui pourrait nécessiter une investigation supplémentaire.

**a. Veuillez télécharger VisualRoute Lite Edition à partir du lien suivant s'il n'est pas déjà installé :**

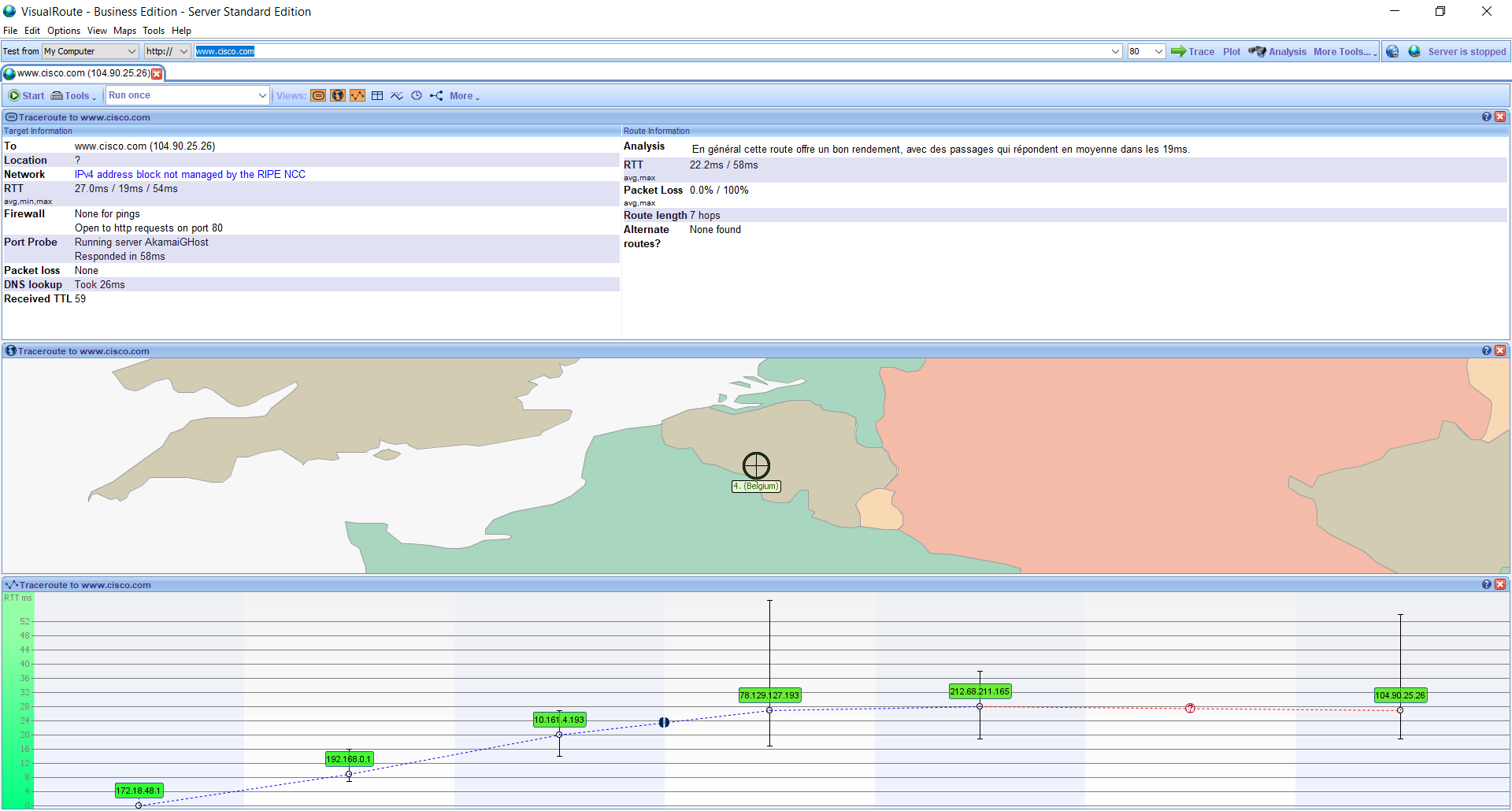
**http://www.visualroute.com/download.html**

**Si vous avez des difficultés à télécharger ou à installer VisualRoute, demandez de l'aide à votre**

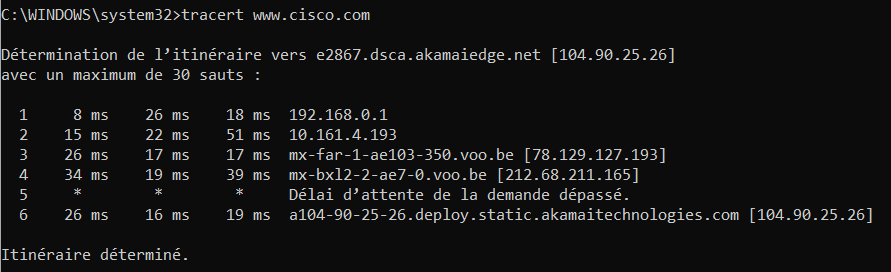
**instructeur. Veillez à télécharger l'édition Lite.**

**b. À l'aide de VisualRoute 2010 Lite Edition, tracez les itinéraires jusqu'à** [**www.cisco.com**](http://www.cisco.com)**.**

**c. Enregistrez les adresses IP dans le chemin d'accès dans le bloc-notes**

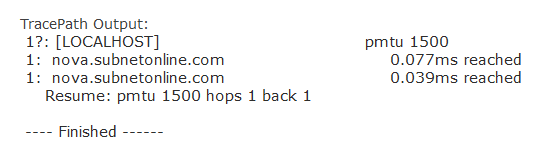
****

**Étape 1 : Dressez la liste des chemins d'accès à www.cisco.com à l'aide de tracert.**

****

**Étape 2 : Dressez la liste des chemins d'accès à www.cisco.com à l'aide de l'outil en ligne sur**

**subnetonline.com.**

****

**Étape 3 : Dressez la liste des chemins d'accès à www.cisco.com en utilisant l'édition Lite de VisualRoute.**

**Tous les utilitaires traceroute ont-ils utilisé les mêmes chemins d'accès à www.cisco.com ? Pourquoi ou pourquoi**

**pas ?**

**toutes les ips de tracert et visualroute sont pareil.**

**2.exercices CIsco packet tracer:**

**Objectifs**

**Partie 1 : Connexions de base, accès à la CLI et exploration de l'aide**

**Partie 2 : Exploration des modes d'exécution**

**Partie 3 : Régler l'horloge**

**Arrière-plan**

**Dans cette activité, vous mettrez en pratique les compétences nécessaires à la navigation dans Cisco IOS, notamment les différents modes d'accès utilisateur, les différents modes de configuration et les commandes courantes que vous utilisez régulièrement. Vous vous exercerez également à accéder à l'aide contextuelle en configurant la commande clock.**

**Partie 1 : Connexions de base, accès à la CLI et exploration de l'aide**

**Dans la première partie de cet exercice, vous connecterez un PC à un commutateur à l'aide d'une connexion de console et explorerez différents modes de commande et fonctionnalités d'aide.**

**Étape 1 : Connectez PC1 à S1 à l’aide d’un câble de console.**

**un. Cliquez sur l'icône Connexions (celle qui ressemble à un éclair) dans le coin inférieur gauche de la fenêtre Packet Tracer.**

**b. Sélectionnez le câble console bleu clair en cliquant dessus. Le pointeur de la souris se transformera en ce qui semble être un connecteur avec un câble qui pend dessus.**

**c. Cliquez sur PC1 ; une fenêtre affiche une option pour une connexion RS-232.**

**d. Faites glisser l'autre extrémité de la connexion de la console vers le commutateur S1 et cliquez sur le commutateur pour afficher la liste des connexions.**

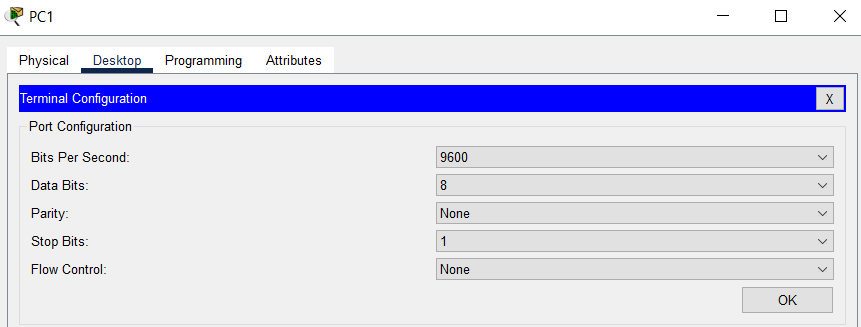
**e. Sélectionnez le port console pour terminer la connexion.**

**Étape 2 : Établissez une session de terminal avec S1.**

**un. Cliquez sur PC1, puis sélectionnez l'onglet Bureau.**

**b. Cliquez sur l'icône de l'application Terminal ; vérifiez que les paramètres par défaut de la configuration du port sont corrects.**

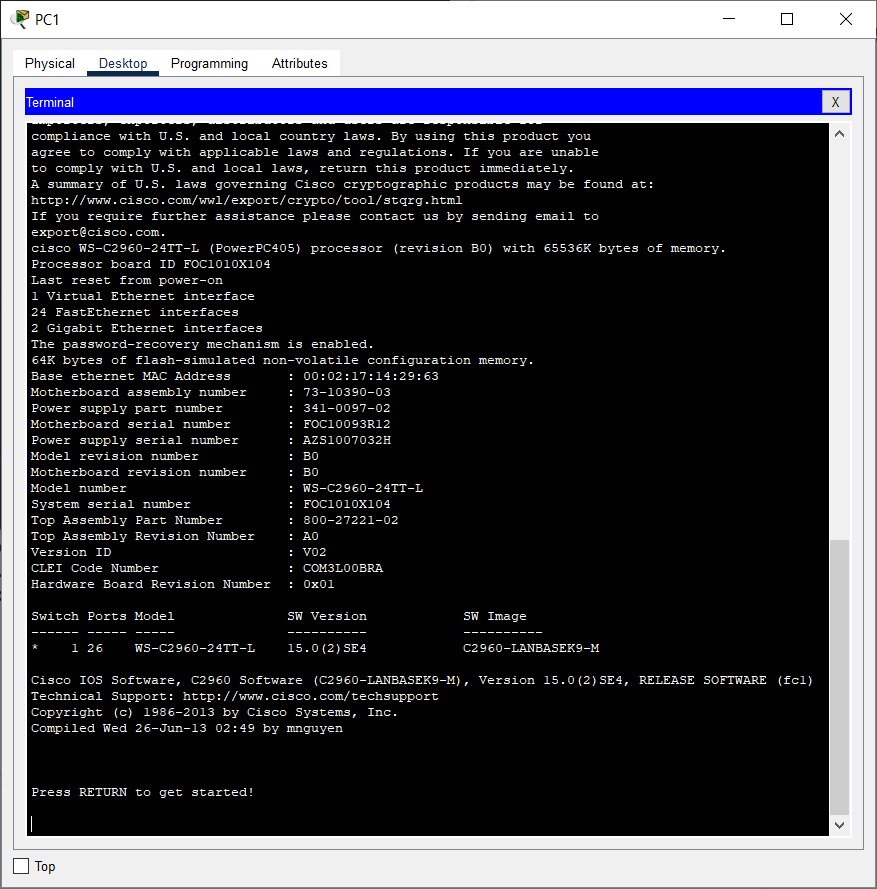
**Quel est le paramètre pour les bits par seconde ?** 9600

****

**c. Cliquez sur OK.**

**d. L'écran qui apparaît peut afficher plusieurs messages. Quelque part sur l'écran, il devrait y avoir un message Appuyez sur RETOUR pour commencer ! message. Appuyez sur Entrée.**

**Quelle est l'invite affichée à l'écran ?**

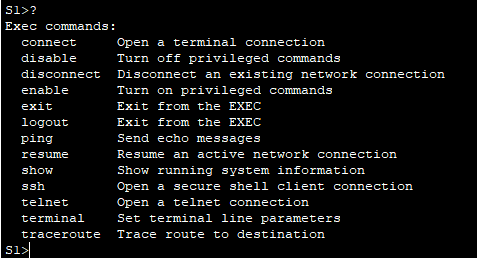
****

**Étape 3 : Explorez l'aide IOS.**

**a. L'IOS peut fournir une aide pour les commandes en fonction du niveau auquel on accède. L'invite actuellement affichée s'appelle User EXEC et l'appareil attend une commande. La forme d'aide la plus élémentaire consiste à taper un point d'interrogation (?) à l'invite pour afficher une liste de commandes.**

**S1> ?**

**Quelle commande commence par la lettre « C » ?**

****

**b. À l'invite, tapez t, suivi d'un point d'interrogation (?).**

**S1>t ?**

**Quelles commandes sont affichées ?**

****

**c. À l'invite, tapez te, suivi d'un point d'interrogation (?).**

**S1> te?e?e**

**Quelles commandes sont affichées ?**

****

**Ce type d'aide est appelé aide contextuelle et fournit davantage d'informations à mesure que les commandes sont développées.**

**Partie 2 : Exploration des modes d'exécution**

**Dans la deuxième partie de cet exercice, vous passerez en mode d'exécution privilégié et émettez des commandes supplémentaires.**

**Étape 1 : Entrez en mode d’exécution privilégié.**

**a. À l'invite, tapez le point d'interrogation (?).**

**S1> ?**

**Quelles informations sont affichées pour décrire la commande d'activation ?**

Exec commands:

connect Open a terminal connection

disable Turn off privileged commands

disconnect Disconnect an existing network connection

enable Turn on privileged commands

exit Exit from the EXEC

logout Exit from the EXEC

ping Send echo messages

resume Resume an active network connection

show Show running system information

ssh Open a secure shell client connection

telnet Open a telnet connection

terminal Set terminal line parameters

traceroute Trace route to destination

**b. Tapez fr et appuyez sur la touche Tab.**

**S1>en<Tab>**

**Qu'est-ce qui s'affiche après avoir appuyé sur la touche Tab ?**

****

**C'est ce qu'on appelle la complétion de commande ou la complétion de tabulation. Lorsqu'une partie d'une commande est saisie, la touche Tab peut être utilisée pour terminer la commande partielle. Si les caractères saisis sont suffisants pour rendre la commande unique, comme dans le cas de la commande d'activation, la partie restante est affichée.**

**Que se passerait-il si vous tapiez <Tab> à l'invite ?**

en ne tapant rien jil ne se passe rien de particulier il passe à la ligne.

**c. Entrez la commande d'activation et appuyez sur ENTRÉE. Comment l'invite change-t-elle ?**

****

**d. Lorsque vous y êtes invité, tapez le point d'interrogation (?).**

**S1# ?**

****

**Auparavant, une commande commençait par la lettre « C » en mode exécution utilisateur. Combien de commandes sont affichées maintenant que le mode d'exécution privilégié est actif ? (Indice : vous pouvez taper c? pour répertorier uniquement les commandes commençant par « C ».)**

5 

**Étape 2 : Entrez en mode de configuration globale.**

**a. L'une des commandes commençant par la lettre « C » est configurée en mode d'exécution privilégié. Tapez soit la commande complète, soit une partie suffisante de la commande pour la rendre unique, ainsi que la touche <Tab> pour émettre la commande et appuyez sur <ENTRÉE>.**

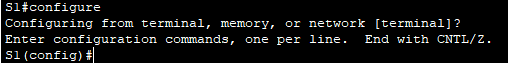
**S1# configurer**

**Quel est le message qui s'affiche ?**

****

**b. Appuyez sur la touche <ENTER> pour accepter le paramètre par défaut entre parenthèses [terminal].**

**Comment l'invite change-t-elle ?**

****

**c. C'est ce qu'on appelle le mode de configuration globale. Ce mode sera exploré plus en détail dans les activités et laboratoires à venir. Pour l'instant, revenez au mode d'exécution privilégié en tapant fin, exit ou Ctrl-Z.**

**S1(config)#sortie**

**S1#**

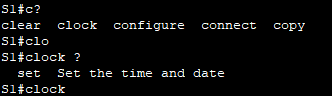
****

**Partie 3 : Régler l'horloge**

**Étape 1 : utilisez la commande clock.**

**a. Utilisez la commande clock pour explorer plus en détail la syntaxe de l’aide et des commandes. Tapez show clock à l’invite d’exécution privilégiée.**

**S1 # afficher l'horloge**

****

**Quelles informations sont affichées ? Quelle est l'année affichée ?**

****

**b. Utilisez l'aide contextuelle et la commande clock pour régler l'heure du commutateur sur l'heure actuelle. Entrez la commande d'horloge et appuyez sur ENTER.**

**S1#horloge<ENTER>**

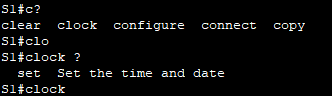
**Quelles informations sont affichées ?**

****

**c. Le message de commande % Incomplet est renvoyé par l'IOS indiquant que la commande d'horloge nécessite des paramètres supplémentaires. Chaque fois que des informations supplémentaires sont nécessaires, une aide peut être fournie en tapant un espace après la commande et le point d'interrogation (?).**

**Horloge S1# ?**

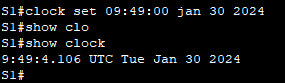
**Quelles informations sont affichées ?**

****

**d. Réglez l'horloge à l'aide de la commande clock set. Continuez à exécuter la commande une étape à la fois.**

**L'horloge S1# est réglée ?**

**Quelles informations sont demandées ?**

****

**Qu'est-ce qui aurait été affiché si seule la commande de réglage de l'horloge avait été entrée et qu'aucune demande d'aide n'avait été faite à l'aide du point d'interrogation ?**

**e. Sur la base des informations demandées lors de l'émission du réglage de l'horloge ? commande, entrez une heure de 15h00. en utilisant le format 24 heures de 15:00:00. Vérifiez si d’autres paramètres sont nécessaires.**

**L'horloge S1# est réglée à 15:00:00 ?**

**La sortie renvoie la demande pour plus d'informations :**

**<1-31> Jour du mois**

****

**MOIS Mois de l'année**

**F. Essayez de définir la date au 31/01/2035 en utilisant le format demandé. Il peut être nécessaire de demander une aide supplémentaire à l'aide de l'aide contextuelle pour terminer le processus. Une fois terminé, émettez la commande show clock pour afficher le réglage de l'horloge. Le résultat de la commande résultant doit s'afficher comme suit :**

**S1 # afficher l'horloge**

**\*15:0:4.869 UTC mar. 31 janvier 2035**

**g. Si vous n'avez pas réussi, essayez la commande suivante pour obtenir le résultat ci-dessus :**

**S1# horloge réglée à 15:00:00 31 janvier 2035**

****

**Étape 2 : Explorez les messages de commande supplémentaires.**

**a. L'IOS fournit diverses sorties pour les commandes incorrectes ou incomplètes, comme indiqué dans les sections précédentes. Continuez à utiliser la commande clock pour explorer les messages supplémentaires qui peuvent être rencontrés au fur et à mesure que vous apprenez à utiliser l'IOS.**

**b. Exécutez la commande suivante et enregistrez les messages :**

**S1#cl**

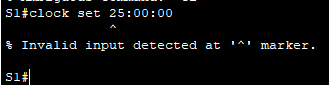
**Quelles informations ont été renvoyées ?**

****

**Horloge S1#**

**Quelles informations ont été renvoyées ?**

**S1# horloge réglée à 25:00:00**

****

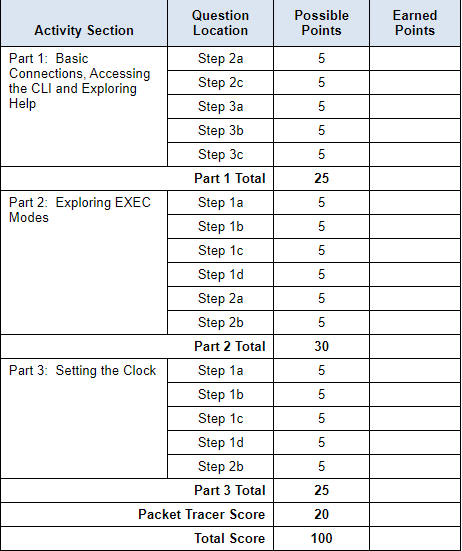
**Quelles informations ont été renvoyées ?**

**S1# horloge réglée 15:00:00 32**

**Quelles informations ont été renvoyées ?**

****

**Rubrique de notation suggérée**

****

**3.exercices CIsco packet tracer:**

**Packet Tracer - Enquête sur les modèles TCP/IP et OSI en action**

**Objectifs**

**Partie 1 : Examiner le trafic Web HTTP**

**Partie 2 : Afficher les éléments de la suite de protocoles TCP/IP**

**Arrière-plan**

**Cette activité de simulation vise à fournir une base pour comprendre la suite de protocoles TCP/IP et la relation avec le modèle OSI. Le mode simulation vous permet de visualiser le contenu des données envoyées sur le réseau à chaque couche.**

**Au fur et à mesure que les données circulent à travers le réseau, elles sont décomposées en morceaux plus petits et identifiés afin que les morceaux puissent être reconstitués lorsqu'ils arrivent à destination. Chaque élément se voit attribuer un nom spécifique (unité de données de protocole [PDU]) et est associé à une couche spécifique des modèles TCP/IP et OSI. Le mode de simulation Packet Tracer permet de visualiser chacune des couches et la PDU associée. Les étapes suivantes guident l'utilisateur tout au long du processus de demande d'une page Web à un serveur Web à l'aide de l'application de navigateur Web disponible sur un PC client.**

**Même si une grande partie des informations affichées seront abordées plus en détail ultérieurement, c'est l'occasion d'explorer les fonctionnalités de Packet Tracer et de pouvoir visualiser le processus d'encapsulation.**

**Partie 1 : Examiner le trafic Web HTTP**

**Dans la première partie de cet exercice, vous utiliserez le mode de simulation Packet Tracer (PT) pour générer du trafic Web et examiner HTTP.**

**Étape 1 : passez du mode temps réel au mode simulation.**

**Dans le coin inférieur droit de l'interface de Packet Tracer se trouvent des onglets permettant de basculer entre le mode temps réel et simulation. PT démarre toujours en mode temps réel, dans lequel les protocoles réseau fonctionnent avec des horaires réalistes. Cependant, une fonctionnalité puissante de Packet Tracer permet à l'utilisateur d'« arrêter le temps » en passant en mode Simulation. En mode Simulation, les paquets sont affichés sous forme d'enveloppes animées, le temps est déterminé par les événements et l'utilisateur peut parcourir les événements réseau.**

**a. Cliquez sur l'icône du mode Simulation pour passer du mode Temps réel au mode Simulation.**

**b. Sélectionnez HTTP dans les filtres de la liste d'événements.**

**1) HTTP est peut-être déjà le seul événement visible. Cliquez sur Modifier les filtres pour afficher les événements visibles disponibles. Activez la case à cocher Afficher tout/Aucun et remarquez comment les cases à cocher passent de non cochées à cochées ou cochées à décochées, en fonction de l'état actuel.**

**2) Cochez la case Afficher tout/Aucun jusqu'à ce que toutes les cases soient décochées, puis sélectionnez HTTP. Cliquez n’importe où en dehors de la zone Modifier les filtres pour la masquer. Les événements visibles ne devraient désormais afficher que HTTP.**

**Étape 2 : Générez du trafic Web (HTTP).**

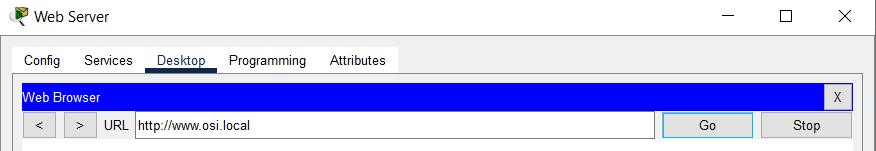
**Actuellement, le panneau de simulation est vide. Il y a six colonnes répertoriées en haut de la liste des événements dans le panneau de simulation. Au fur et à mesure que le trafic est généré et parcouru, les événements apparaissent dans la liste. La colonne Info est utilisée pour inspecter le contenu d'un événement particulier.**

**Remarque : Le serveur Web et le client Web sont affichés dans le volet de gauche. La taille des panneaux peut être ajustée en survolant la barre de défilement et en faisant glisser vers la gauche ou la droite lorsque la flèche à deux pointes apparaît.**

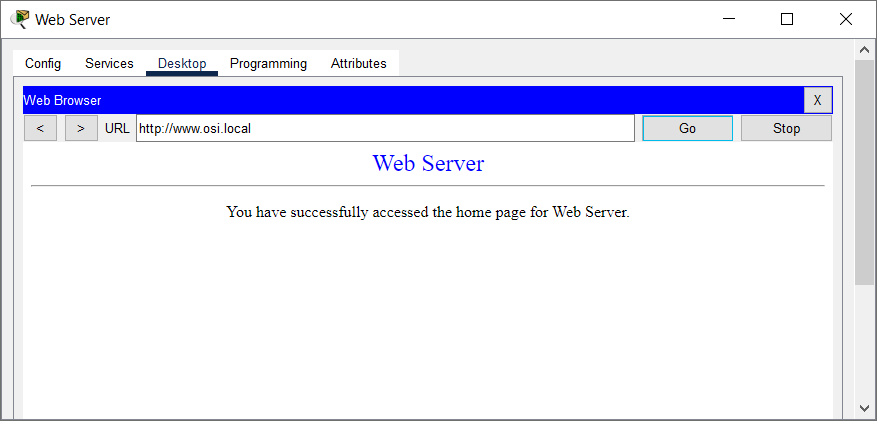
**a. Cliquez sur Client Web dans le volet le plus à gauche.**

**b. Cliquez sur l'onglet Bureau et cliquez sur l'icône du navigateur Web pour l'ouvrir.**

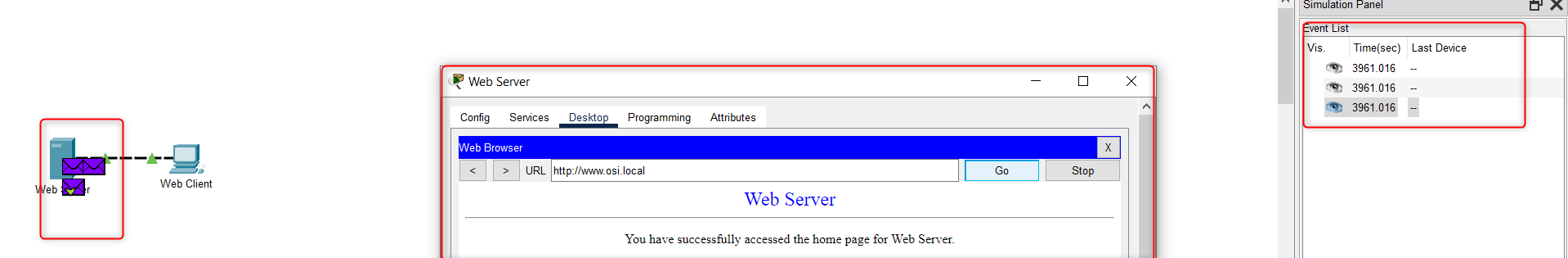
**c. Dans le champ URL, saisissez www.osi.local et cliquez sur Go.**

****

**Étant donné que le temps en mode Simulation dépend des événements, vous devez utiliser le bouton Capturer/Transférer pour afficher les événements réseau.**

****

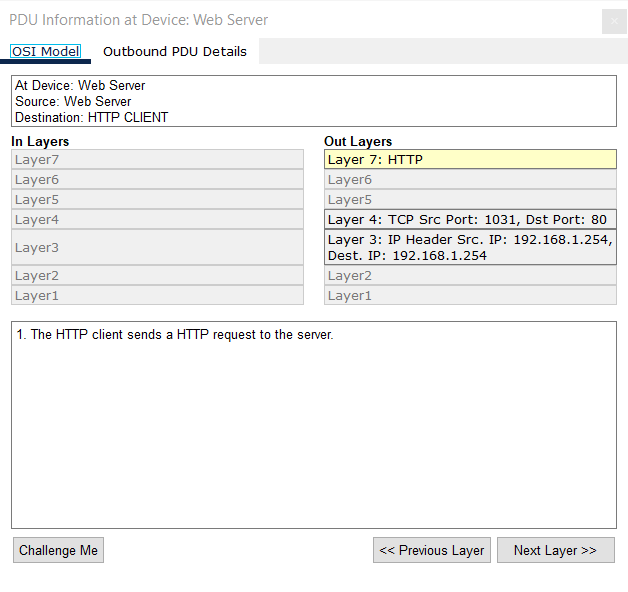
**d. Cliquez quatre fois sur Capturer/Transférer. Il devrait y avoir quatre événements dans la liste des événements.**

****

**Consultez la page du navigateur Web du client Web. Est-ce que quelque chose a changé ?**

**Étape 3 : Explorez le contenu du paquet HTTP.**

**a. Cliquez sur la première case carrée colorée sous la colonne Liste des événements > Informations. Il peut être nécessaire de développer le panneau de simulation ou d'utiliser la barre de défilement directement sous la liste des événements.**

****

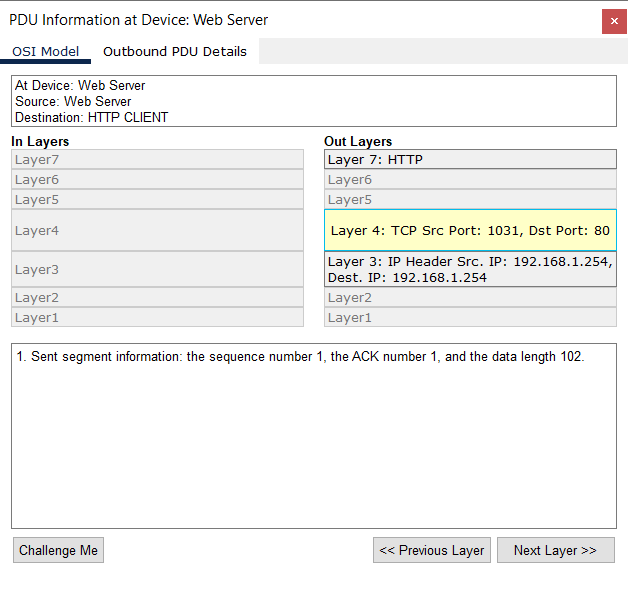
**La fenêtre Informations PDU sur le périphérique : client Web s'affiche. Dans cette fenêtre, il n'y a que deux onglets (Modèle OSI et Détails de la PDU sortante) car il s'agit du début de la transmission. Au fur et à mesure que d'autres événements sont examinés, trois onglets s'afficheront, ajoutant un onglet pour les détails de la PDU entrante. Lorsqu'un événement est le dernier événement du flux de trafic, seuls les onglets Modèle OSI et Détails de la PDU entrante sont affichés.**

**b. Assurez-vous que l'onglet Modèle OSI est sélectionné. Sous la colonne Couches sortantes, assurez-vous que la case Couche 7 est en surbrillance.**

**Quel est le texte affiché à côté de l’étiquette Layer 7 ?**

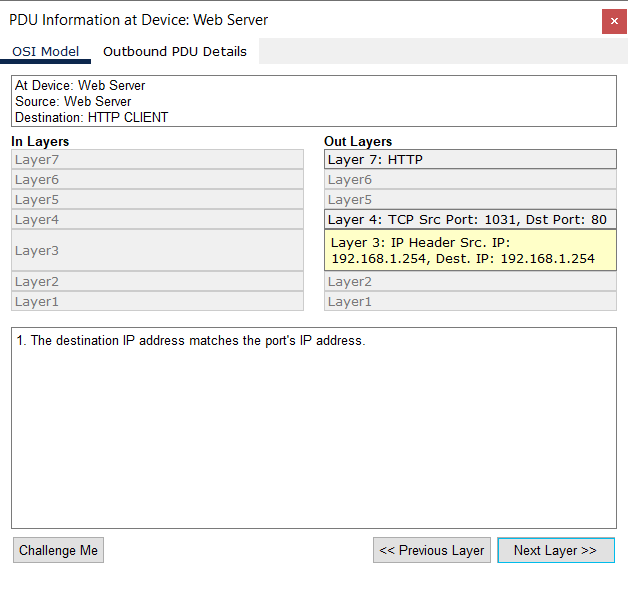
**Quelles informations sont répertoriées dans les étapes numérotées directement sous les zones Couches d'entrée et Couches de sortie ?**

**c. Cliquez sur Couche suivante. La couche 4 doit être mise en évidence. Quelle est la valeur du port Dst ?**

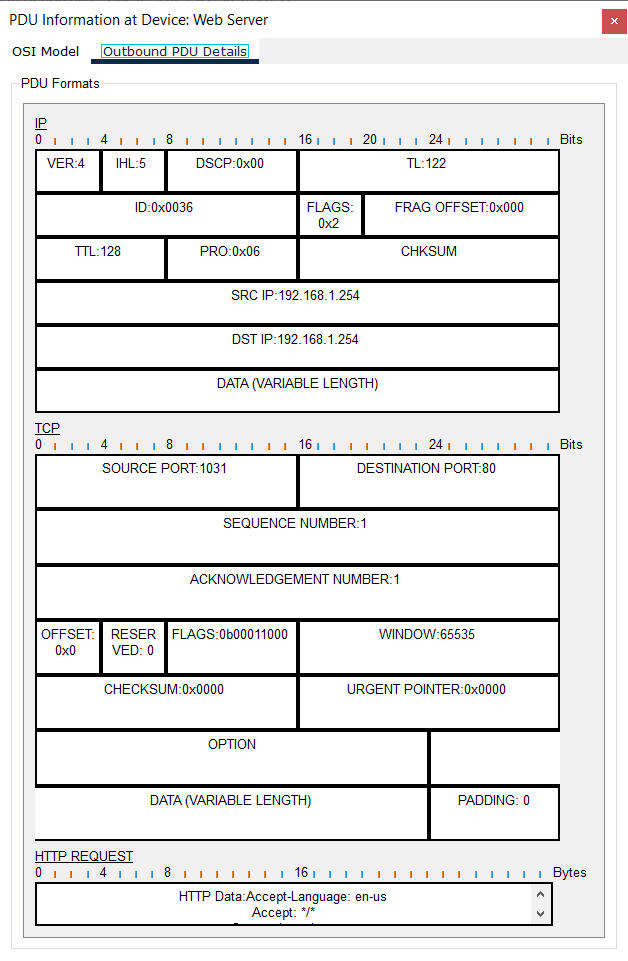
****

**d. Cliquez sur Couche suivante. La couche 3 doit être mise en évidence. Quelle est la Destinée. Valeur IP ?192.168.1.254**

**e. Cliquez sur Couche suivante. Quelles informations sont affichées sur cette couche ?**

****

**F. Cliquez sur l'onglet Détails de la PDU sortante.**

****

**Les informations répertoriées sous les détails de la PDU reflètent les couches du modèle TCP/IP.**

**Remarque : Les informations répertoriées sous la section Ethernet II fournissent des informations encore plus détaillées que celles répertoriées sous Couche 2 dans l'onglet Modèle OSI. Les détails de la PDU sortante fournissent des informations plus descriptives et détaillées. Les valeurs sous DEST MAC et SRC MAC dans la section Ethernet II des détails de la PDU apparaissent dans l'onglet Modèle OSI sous Couche 2, mais ne sont pas identifiées comme telles.**

**Quelles sont les informations communes répertoriées dans la section IP des détails de la PDU par rapport aux informations répertoriées sous l'onglet Modèle OSI ? A quelle couche est-il associé ?**

a la 3 eme

**Quelles sont les informations communes répertoriées dans la section TCP des détails de la PDU, par rapport aux informations répertoriées sous l'onglet Modèle OSI, et à quelle couche sont-elles associées ?**

l’adresse ip

**Quel est l'hôte répertorié dans la section HTTP des détails de la PDU ? À quelle couche ces informations seraient-elles associées sous l'onglet Modèle OSI ?**

couche 7

**g. Cliquez sur la case carrée colorée suivante sous la colonne Liste des événements > Informations. Seul le calque 1 est actif (non grisé). L'appareil déplace la trame du tampon et la place sur le réseau.**

**h. Passez à la zone d'informations HTTP suivante dans la liste des événements et cliquez sur la case carrée colorée. Cette fenêtre contient à la fois les calques d'entrée et les calques de sortie. Notez la direction de la flèche directement sous la colonne Dans les calques ; il pointe vers le haut, indiquant la direction dans laquelle circulent les informations. Faites défiler ces couches en notant les éléments précédemment consultés. En haut de la colonne, la flèche pointe vers la droite. Cela indique que le serveur renvoie désormais les informations au client.**

**En comparant les informations affichées dans la colonne Couches entrantes avec celles de la colonne Couches sortantes, quelles sont les principales différences ?**

**je. Cliquez sur l'onglet Détails de la PDU sortante. Faites défiler jusqu'à la section HTTP.**

**Quelle est la première ligne du message HTTP qui s'affiche ?**

**j. Cliquez sur la dernière case carrée colorée sous la colonne Informations. Combien d'onglets sont affichés avec cet événement et pourquoi ?**

**Partie 2 : Afficher les éléments de la suite de protocoles TCP/IP**

**Dans la deuxième partie de cet exercice, vous utiliserez le mode Simulation de Packet Tracer pour afficher et examiner certains des autres protocoles composant la suite TCP/IP.**

**Étape 1 : Afficher les événements supplémentaires**

**a. Fermez toutes les fenêtres d’informations de la PDU ouvertes.**

**b. Dans la section Filtres de liste d'événements > Événements visibles, cliquez sur Afficher tout.**

**Quels types d'événements supplémentaires sont affichés ?**

**Ces entrées supplémentaires jouent divers rôles au sein de la suite TCP/IP. Si le protocole ARP (Address Resolution Protocol) est répertorié, il recherche les adresses MAC. DNS est chargé de convertir un nom (par exemple, www.osi.local) en adresse IP. Les événements TCP supplémentaires sont responsables de la connexion, de l'accord sur les paramètres de communication et de la déconnexion des sessions de communication entre les appareils. Ces protocoles ont été mentionnés précédemment et seront discutés plus en détail au fur et à mesure de la progression du cours. Il existe actuellement plus de 35 protocoles possibles (types d'événements) disponibles pour la capture dans Packet Tracer.**

**c. Cliquez sur le premier événement DNS dans la colonne Info. Explorez les onglets Modèle OSI et Détails de la PDU et notez le processus d'encapsulation. Lorsque vous regardez l'onglet Modèle OSI avec la couche 7 en surbrillance, une description de ce qui se passe est répertoriée directement sous les couches d'entrée et de sortie (« 1. Le client DNS envoie une requête DNS au serveur DNS. »). Il s’agit d’informations très utiles pour aider à comprendre ce qui se passe pendant le processus de communication.**

**d. Cliquez sur l'onglet Détails de la PDU sortante. Quelles informations sont répertoriées dans le champ NOM : dans la section DNS QUERY ?**

**e. Cliquez sur la dernière case carrée colorée d’informations DNS dans la liste des événements. Quel appareil est affiché ?**

**Quelle est la valeur répertoriée à côté de ADDRESS : dans la section DNS ANSWER des détails de la PDU entrante ?**

**F. Recherchez le premier événement HTTP dans la liste et cliquez sur la case carrée colorée de l'événement TCP qui suit immédiatement cet événement. Mettez en surbrillance Couche 4 dans l'onglet Modèle OSI. Dans la liste numérotée située juste en dessous des couches d'entrée et des couches de sortie, quelles sont les informations affichées sous les éléments 4 et 5 ?**

**TCP gère la connexion et la déconnexion du canal de communication ainsi que d'autres responsabilités. Cet événement particulier montre que le canal de communication a été ÉTABLI.**

**g. Cliquez sur le dernier événement TCP. Mettez en surbrillance Couche 4 dans l'onglet Modèle OSI. Examinez les étapes répertoriées directement ci-dessous Dans les calques et Out Layers. Quel est le but de cet événement, sur la base des informations fournies dans le dernier élément de la liste (qui devrait être l'élément 4) ?**

**Défi**

**Cette simulation a fourni un exemple de session Web entre un client et un serveur sur un réseau local (LAN). Le client envoie des requêtes à des services spécifiques exécutés sur le serveur. Le serveur doit être configuré pour écouter sur des ports spécifiques une demande client. (Indice : regardez la couche 4 dans l'onglet Modèle OSI pour obtenir des informations sur le port.)**

**D'après les informations inspectées lors de la capture de Packet Tracer, sur quel numéro de port le serveur Web écoute-t-il la requête Web ?**

**Sur quel port le serveur Web écoute-t-il une requête DNS ?**

[**04-Network\_access**](https://github.com/becodeorg/CRL-Cyber-Sprint-3/tree/main/05-Networking/04-Network_access)

**/**

# **01.Network\_access.md**

**Exercices 1.1**

**Quel type de câble est actuellement utilisé dans les réseaux d'entreprise ?**

**Les réseaux d'entreprise utilisent divers types de câbles, notamment les câbles Ethernet. Selon les besoins de vitesse ou de distance, différents types de câbles peuvent être utilisés. Par exemple, si vous avez un équipement Gigabit Ethernet et que vous pouvez passer aux réseaux Multigigabit, le câble de type Cat 6 UTP est recommandé. Ce type de câble peut fournir des vitesses allant jusqu'à 10 Gbps dans de courtes sections.**

**Pour les utilisateurs plus avancés avec des équipements Multigigabit et même des équipements 10G, il est recommandé d'utiliser au moins des câbles Cat6. Un câble Cat 7 serait également recommandé pour sa protection maximale possible et sa capacité à offrir une grande vitesse****.**

**Un autre type de câble utilisé dans les réseaux informatiques est le câble à paires torsadées non blindé (UTP). Ce type de câble est le plus utilisé dans les réseaux domestiques en raison de son faible coût et de ses hautes performances. Il est utilisé pour les câbles Cat 5, Cat 5e et même Cat 6****.**

**Enfin, pour les utilisateurs très avancés qui testent constamment des commutateurs et des serveurs NAS pour vérifier la vitesse du réseau local, une bonne option serait d'acheter des câbles Cat 8 hautes performances, capables d'atteindre des vitesses allant jusqu'à 40 Gbps sur le réseau local**

**Quel est le principal problème des câbles en cuivre ?**

ca présente un problème : les perturbations. En effet, un courant électrique peut être perturbé de bien des manières mais voici les deux principales :

Les interférences électromagnétiques (EMI) et les interférences radio (RFI) \*\* Ces interférences produites par des agents extérieurs peuvent modifier le signal ; ce phénomène peut être contré en blindant les câbles du réseau.

Diaphonie\*\* Phénomène dans lequel deux câbles interfèrent l'un avec l'autre ; ce phénomène peut être contré en torsadant les câbles.

**Quelle est la portée maximale du Bluetooth ?**

Bluetooth Technologie de réseau personnel (SAN) utilisant un protocole d'appariement et permettant de communiquer sur une distance maximale de 100 m.

**Selon le modèle OSI, dans quelle couche les routeurs fonctionnent-ils ?**

Ils travaillent au niveau de la couche 3 du modèle OSI (couche réseau)

**Selon le modèle OSI, dans quelle couche les commutateurs fonctionnent-ils ?** Un commutateur (en anglais switch) est un pont multiports, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI.

**Selon le modèle OSI, dans quelle couche le câble Ethernet fonctionne-t-il ?**

Le protocole Ethernet réalise les fonctions de la couche physique (couche 1 du modèle OSI)

**Exercices 1.2**

**Téléchargez le fichier simple-test-LAN ​​et connectez les deux commutateurs et les appareils. Pour vérifier la connectivité entre les machines, utilisez la commande Ping.**

**1.1 Quel type de coin avez-vous utilisé pour connecter les PC au switch ?**

**> Votre réponse**

**1.2 Quel type de câble avez-vous utilisé pour connecter les deux interrupteurs ? Expliquez la raison de ce choix de câble.**

**> Votre réponse**

Le cable sérial avec un routage static

**Téléchargez le config\_routeur\_1.pkt et connectez les deux ordinateurs et le routeur.**

**Téléchargez le config\_routeur\_2.pkt et connectez les ordinateurs et les routeurs.**

Chapitre 5 : Technologie Ethernet

**Ethernet est la technologie LAN la plus utilisée aujourd'hui. Elle se situe sur la couche de liaison de données et prend en charge des largeurs de bande de 10, 100, 1 000, 10 000, 40 000 et 100 000 Mbps. Cette norme définit un protocole des couches 2 et 3 et est divisée en deux sous-couches :**

**LLC qui gère la communication entre les couches supérieures et inférieures. Cette couche est totalement indépendante du logiciel et du matériel. De plus, elle est assez amusante.**

**MAC La sous-couche inférieure, elle est implémentée au niveau matériel des cartes réseau de la machine.**

**Ethernet a été créé en 1973 et n'a cessé d'évoluer pour augmenter sa bande passante et devenir plus flexible.**

**Sous-couche MAC**

**Cette sous-couche a deux objectifs, encapsuler les données et contrôler l'accès au support.**

**Cette sous-couche chargée de l'encapsulation gère donc :**

**La délimitation de la trame permettant la synchronisation de l'émetteur avec le récepteur**

**L'adressage physique de la trame**

**la détection des erreurs.**

**La sous-couche gère également l'accès au support et vérifie la disponibilité du support et les éventuelles collisions.**

**La structure d'une trame Ethernet est la suivante**

**Structure de la trame**

**La structure de la trame Ethernet est la suivante, sa taille peut varier entre 64 et 1 518 octets et toute trame en dehors de ces valeurs sera considérée comme un fragment de collision.**

**Fait amusant : une trame de plus de 1 500 octets est considérée comme une "trame Jumbo" ou "trame géante".**

**Préambule Adresse de destination Adresse source Type Données Vérification de la trame**

**8 bits 6 bits 6 bits 2 bits 46 à 1.500 bits 4 bits**

**Délimiteur de trame de préambule (SFD) utilisé pour synchroniser l'émetteur avec le récepteur.**

**Adresse MAC de destination Identifiant physique du destinataire permettant l'unicast, le multicast ou le broadcast.**

**Adresse MAC source Identifiant d'origine de la trame**

**EtherType Champ identifiant le protocole de la source précédente**

**Données Données encapsulées provenant de la couche supérieure**

**Fin de trame (FCS) Utilisé pour détecter les erreurs de trame et mettre fin à la trame.**

**Exemple : Certains types de protocoles :**

**0x800 (IPv4)**

**0x86DD (IPv6)**

**0x806 (ARP)**

**Adresse MAC**

**L'hexadécimal est le système d'écriture des adresses MAC et des adresses IP. Il se présente comme un système de chiffres de 0 à 9 et de A à F dont les équivalences sont présentées dans le tableau ci-dessous.**

**Table d'équivalence hexadécimale**

**Une adresse MAC est représentée en regroupant les caractères hexadécimaux par paires et en les séparant par - ou : ou en les regroupant par 4 et en les séparant par .**

**Exemple : 00-05-9A-3C-78-00 00:05:9A:3C:78:00 0005.9A3C.7800**

**Une adresse MAC se compose de deux parties de 24 Bits, l'une définie par l'IEEE et spécifique à chaque fabricant et l'autre laissée au choix du fabricant. Ainsi, nous sommes assurés qu'une adresse MAC est unique dans le monde entier. Ce système est appelé OUI (Organizationally Unique Identifier).**

**Le plus souvent, l'adresse MAC est gravée dans la mémoire en lecture seule de la carte réseau, c'est pourquoi elle est dite non volatile (BIA). Toutefois, elle peut être modifiée par un logiciel du système d'exploitation. Au démarrage, cette adresse non volatile est stockée dans la mémoire vive pour être utilisée.**

**Lorsqu'un paquet atteint la carte réseau, celle-ci compare l'adresse MAC de destination avec celle stockée dans la RAM et interprète le paquet s'il s'agit bien de la destination.**

**Les commutateurs utilisent deux types de méthodes pour transférer les trames vers le port associé :**

**Cut-Through achemine la trame avant qu'elle ne soit complètement lue et ne vérifie pas les erreurs ; dans la variante fast-forward, les données sont immédiatement transmises, ce qui peut causer certains problèmes mais permet un débit élevé ; la seconde variante Fragment-free consiste à stocker les 64 premiers bits avant de conclure un port vers lequel communiquer et à effectuer un contrôle d'erreur sur les petites trames**

**Store and Forward Stocke la trame en mémoire et pendant que la trame est stockée, le commutateur décide vers quel port transmettre la trame et effectue un test de redondance cyclique (CRC) en analysant la queue de la trame pour vérifier que la trame est valide afin de ne pas encombrer le réseau avec des données non valides.**

**Pour permettre une bonne transmission, les commutateurs sont dotés de tampons qui peuvent être de deux types :**

**Basé sur le port Les trames sont stockées dans des files d'attente associées à chaque port entrant et sortant ; les données sont transmises dès que le port devient disponible.**

**Mémoire partagée Une seule mémoire contient toutes les trames et le port de destination est alloué dynamiquement.**

**Le protocole ethernet peut fonctionner en half-duplex ou en full-duplex, lors de la connexion à un switch ou à un autre appareil, les deux appareils s'échangent pour choisir le meilleur mode de transmission en fonction du système offrant la meilleure bande passante. Si nous ne nous mettons pas d'accord, nous risquons de nombreuses collisions sur le canal provenant du système half-duplex.**

**Un autre point sur lequel il faut se mettre d'accord est le type de câble utilisé. Pour éviter une configuration, on utilise le système Auto-MDIX qui permet, par de multiples échanges entre le switch et les autres périphériques, de conclure le type de câble utilisé et donc de modifier les configurations en conséquence.**

**ARP**

**Si l'adresse IP de destination n'appartient pas au réseau actuel, la machine l'envoie automatiquement à la passerelle, une machine de niveau 3 qui se connecte à un réseau distant.**

**Pour associer une adresse IP aux adresses MAC le long du chemin, le protocole ARP est utilisé pour résoudre les adresses MAC et conserver une table de correspondance.**

**Pour résoudre les adresses MAC à partir de l'adresse IP d'un appareil, celui-ci consulte la table de correspondance contenue dans sa mémoire vive. Si l'adresse MAC correspondante n'est pas présente, il envoie une requête ARP sur le réseau.**

**Une requête ARP contient dans son corps, soit l'adresse IP cible, soit l'adresse MAC cible qui doit être complétée. Et la trame ethernet de ce type de requête contient en en-tête :**

**l'adresse MAC de diffusion permettant à chacun de répondre**

**L'adresse MAC source de la machine émettrice**

**Le type de trame qui est 0x806 dans le cas d'une requête ARP**

**Après cette requête, seule la machine correspondant à l'IP indiquée dans le corps du message répond avec l'adresse IP de l'expéditeur et son adresse MAC. Cette réponse est accompagnée d'une trame ethnique unicast standard de type ARP. Dès que l'appareil émetteur reçoit la réponse, il l'ajoute à sa table de correspondance et envoie la trame attendue.**

**Les entrées de la table de correspondance sont rapidement supprimées si elles ne sont pas utilisées pendant un certain temps, mais cela dépend du système d'exploitation.**

**Pour afficher la table de mappage, vous pouvez utiliser la commande show ip arp sur les appareils Cisco ou arp -a sur Windows 7.**

**Si de nombreuses requêtes ARP sont diffusées en même temps sur un réseau à faible bande passante, le réseau peut être inondé, mais ce type de perte de performance est minime.**

**Certains pirates peuvent se faire passer pour un autre appareil en répondant à certaines requêtes ARP qui ne lui sont pas destinées et ainsi empoisonner la table de correspondance de l'appareil.**

**Attaques par usurpation d'adresse ARP**

**Les effets des attaques par usurpation d'adresse ARP peuvent avoir de graves conséquences pour les entreprises. Dans leur application la plus élémentaire, les attaques d'usurpation d'adresse ARP sont utilisées pour voler des informations sensibles. En outre, ces attaques sont souvent utilisées pour faciliter d'autres attaques telles que**

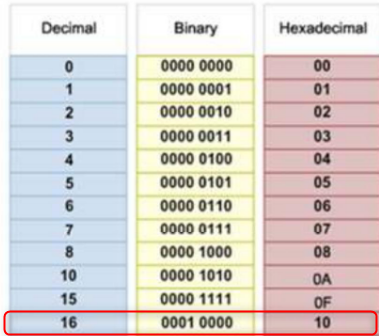
**Les attaques par déni de service : Les attaques DoS s'appuient souvent sur l'usurpation d'adresse ARP pour relier plusieurs adresses IP à l'adresse MAC d'une seule cible. En conséquence, le trafic destiné à de nombreuses adresses IP différentes est redirigé vers l'adresse MAC de la cible, ce qui a pour effet de surcharger cette dernière en trafic.**

**Détournement de session : Les attaques par détournement de session peuvent utiliser l'usurpation d'adresse ARP pour voler les identifiants de session, ce qui permet aux attaquants d'accéder à des systèmes et à des données privés.**

**Attaques de type "Man-in-the-middle" : Les attaques MITM peuvent s'appuyer sur l'usurpation d'ARP pour intercepter et modifier le trafic entre les victimes.**

**Exercices :**

**Comment écrire 16 en hexadécimal ?**

****

**Les adresses MAC sont-elles uniques ?**

Ainsi, nous sommes assurés qu'une adresse MAC est unique dans le monde entier

**Après avoir lu ceci, que représentent les 6 premiers caractères d'une adresse MAC ?**

Les 6 premiers chiffres (XX. XX. XX) permettent d'identifier le fabricant de l'appareil.

**Quelle organisation gère l'attribution des adresses MAC ?**

En tant qu'implémentation des normes IEEE 802.2/3, la trame Ethernet fournit

l'adressage MAC et la vérification des erreurs.

**A quel constructeur appartient OUID 34-FE-77 ?**

L'OUI (Organizationally Unique Identifier) 34-FE-77 appartient à Apple, Inc. Les OUI sont utilisés pour identifier de manière unique les fabricants d'équipements réseau. Ils sont composés des trois premiers octets d'une adresse MAC (Media Access Control). Dans ce cas, les trois premiers octets de l'adresse MAC (34-FE-77) correspondent à l'OUI qui est attribué à Apple, Inc.

**Si le type de la trame est 0x806, de quel type de requête s'agit-il ?**

Le type de trame 0x806 correspond au protocole ARP (Address Resolution Protocol) ou Protocole de résolution d'adresse. Ce protocole est utilisé pour mapper une adresse IP à une adresse MAC (Media Access Control) sur un réseau local.

06-Network\_Layer **01.Network\_layers.md**

## **File metadata and controls**

Couches réseau

Protocole IP

La couche réseau manipule les paquets et s'occupe de :

L'adresse des terminaux permettant de les localiser sur le réseau

Encapsulation des données PDU de la couche précédente avec des informations telles que les adresses IP source et de destination

Un routage pour orienter l'information dans le bon sens sur le réseau

Désencapsulation d'un paquet arrivant sur la machine réseau

Le protocole IP est un protocole sans connexion (qui n'établit pas de connexion avec la destination avant d'envoyer le paquet), ne permet pas de suivre les paquets et ne permet donc pas de gérer la bonne acheminement de celui-ci. Et enfin, il est indépendant du support sur lequel il est utilisé mais adapte la taille de ses paquets en fonction de celui-ci. L'en-tête IP ne contient pas beaucoup d'informations à l'exception des adresses IP de la source et de la destination.

En-têtes IPv4

Les en-têtes d'un paquet IPv4 sont les suivants :

version (4 Bits) La version de l'IP utilisée (dans ce cas 0100)

Service différent (8 Bits) Donne la priorité à certains paquets

Time-To-Live (TTL) (8 bits) Vous permet de limiter la durée de vie d'un paquet ; dès qu'un paquet est traité par un routeur, il diminue de 1

Protocole (8 bits) Le protocole utilisé par la couche précédente

Adresse IP source L'adresse IP de la machine qui envoie le paquet L'adresse IP de la machine à laquelle le paquet est destiné

Adresse IP de destination L'adresse IP de la machine à laquelle le paquet est destiné

Exemple de protocoles :

-ICMP1

-TCP2

-UDP17

Limites

Aujourd'hui, le protocole IPv4 se heurte à plusieurs limitations. Tout d’abord, les adresses IP disponibles vont s’épuiser en raison de l’augmentation du nombre d’appareils connectés. Les tables de routage des routeurs réseau se remplissent de plus en plus et cela entraîne une augmentation des ressources nécessaires. Pour éviter d'exposer un réseau entier, le système NAT est mis en place et empêche d'avoir une adresse IP publique de bout en bout.

IPv6

Pour résoudre les problèmes d'IPv4, IPv6 a été créé permettant un espace d'adressage de 128 bits au lieu de 32, ce qui permet la création de 340 Unidécilions d'adresses. Traitement plus efficace des paquets et inutilité du système NAT en raison du grand nombre d'adresses IP.

Par rapport à IPv4, les en-têtes ont été modifiés pour les simplifier. Ainsi on conserve le champ version, le champ adresse source et l'adresse destination mais on modifie la position de certains et on supprime d'autres. Ainsi, le protocole IPv6 propose :

Un format d'en-tête simplifié

Des données plus utiles

Une architecture réseau hiérarchique

Configuration automatique des adresses

Pas besoin de NAT (Magic)

En-têtes

Version (4 bits)

Classe de trafic (8 bits) Permet de prioriser le paquet

L'étiquette de flux (20 bits) permet de spécifier que tous les paquets ayant la même étiquette de flux doivent être traités de la même manière.

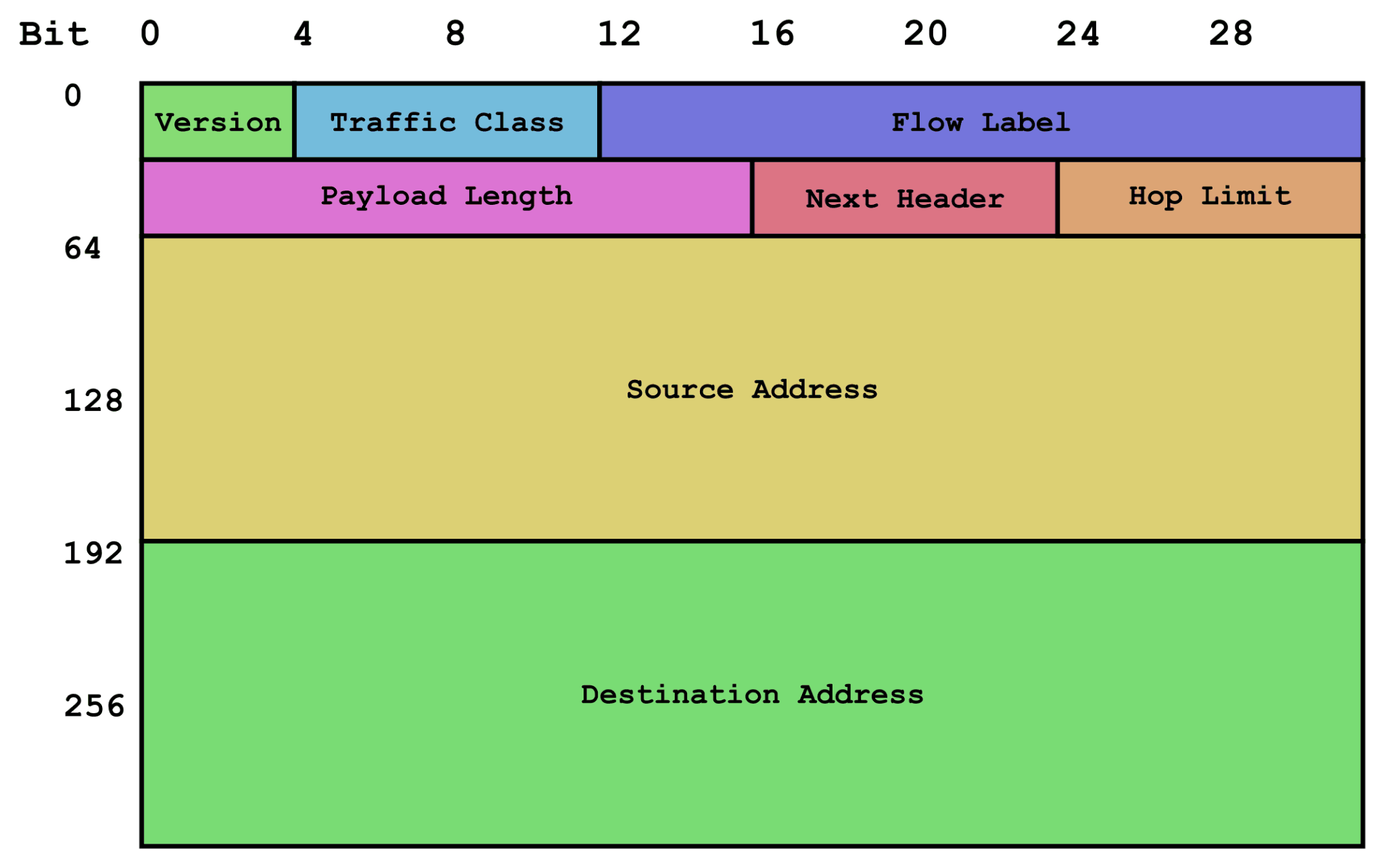
Longueur de la charge utile (16 bits)

En-tête suivant (8 bits) Indique le type de données transportées par le paquet

La limite de saut (8 bits) représente le TTL

Adresse source

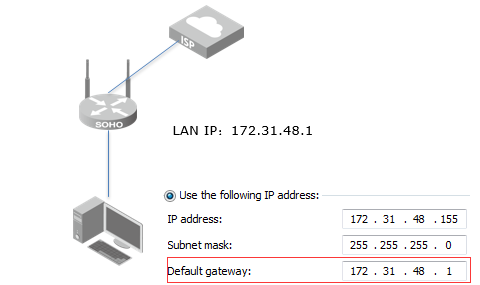
Adresse de destination



Routage

Pour communiquer, une machine peut s'envoyer des données via une adresse de bouclage ; vers un hôte local sur le même réseau que lui ou vers un hôte distant via la passerelle par défaut.

La passerelle par défaut est la machine qui achemine le trafic vers un réseau distant, elle possède une adresse IP sur les deux réseaux et peut transmettre des données de l'un à l'autre.



Chaque hôte du réseau dispose d'une table de routage sur chacune de ses interfaces pour déterminer si le paquet à envoyer se trouve ou non sur le réseau local.

La table de routage d'un routeur permet d'associer un réseau à une interface. Ce réseau peut être découvert automatiquement ou configuré manuellement.

Dans le cas d'un réseau local directement connecté à une interface, une ligne de la table de routage est constituée de la lettre C lorsqu'elle est découverte automatiquement ou L lorsqu'elle est configurée manuellement. Suivi de l'adresse IP et du masque du réseau concerné et enfin de l'interface sur laquelle ce réseau est associé.

Une ligne de routage d'un réseau distant est composée dans l'ordre des éléments suivants :

La méthode utilisée pour découvrir le réseau peut être S pour une route statique, D pour Enhaced Interior Gateway Routing Protocol ou O pour Open Shortest Path First.

Réseau de destination Le réseau vers lequel les paquets peuvent être acheminés

Distance administrative Un chiffre permettant de vérifier la fiabilité d'un itinéraire, plus le chiffre est bas, plus l'itinéraire est fiable

Métrique Une valeur pour donner une valeur pour atteindre le réseau, une valeur faible est préférable

Étape suivante L'adresse du réseau local au niveau du routeur pour atteindre le réseau spécifié

Horodatage de l'itinéraire pour spécifier quand l'itinéraire a été maintenu pour la dernière fois

Interface de sortie L'interface à laquelle envoyer le paquet pour cette route

Routeurs

Les routeurs ne sont que des ordinateurs composés d'un système d'exploitation (IOS), d'un processeur, de RAM et de ROM.

La RAM est utilisée pour stocker des informations rapidement

La mémoire morte contient des données qui ne peuvent pas être modifiées (sauf par Cisco bien sûr)

RAM non volatile utilisée comme stockage permanent pour le fichier de configuration startup-config

Mémoire flash Mémoire non volatile contenant les fichiers système et journaux

Module d'intégration avancé utilisé pour décharger le processeur des actions fastidieuses telles que la cryptographie

Au démarrage, le système contenu dans la mémoire flash est chargé dans la RAM ainsi que le fichier de configuration globale. Le processus de démarrage est le suivant

Exécution des tests POST et chargement du programme de démarrage un diagnostic technique et électrique du routeur suivi du chargement du système en RAM

Chargement d'IOS.

Localisation et chargement du fichier de configuration

LE bon fait : Pour voir la version actuelle de Cisco IOS vous devez taper la commande show version.

Configuration du routeur

Nous ne reviendrons pas ici sur la configuration de base de l'appareil car elle a déjà été vue au chapitre 2.

La configuration d'une interface passe par plusieurs commandes exécutées depuis la configuration globale.

# Entrez dans le mode de configuration de l'interface

interface gigabitethernet 0/0

# On configure le réseau de l'interface

adresse IP 192.168.10.1 255.255.255.0

# Configurer la passerelle par défaut

passerelle IP par défaut 192.168.10.50

# Donner une description de l'interface

description Lien vers LAN-10

# (Re)démarrer l'interface

Pas d'extinction

Vous pouvez ensuite vérifier sa configuration avec une des commandes

show ip interface brief Affiche un aperçu des interfaces

show ip route Affiche la table de routage

show interfaces Afficher les statistiques de l'interface

show ip interface Affiche les statistiques IPv4 pour les interfaces

**Des exercices**

**Nommez deux protocoles qui garantissent que le transfert de paquets de l’IP A vers l’IP B est terminé.**

Deux protocoles qui garantissent que le transfert de paquets de l'IP A vers l'IP B est terminé sont le protocole de contrôle de transmission (TCP) et le protocole de datagramme utilisateur (UDP).

Le protocole de contrôle de transmission (TCP) est un protocole orienté connexion qui fournit une livraison fiable, ordonnée et vérifiée d'un flux d'octets entre les applications fonctionnant sur des hôtes communiquant via un réseau IP. Il utilise une séquence de trois échanges (appelée "poignée à trois") pour établir une connexion avant que les données ne puissent être envoyées. Cette séquence est la suivante :

1. Le client envoie un SYN au serveur. Le client définit le numéro de séquence du segment à une valeur aléatoire A.
2. En réponse, le serveur répond avec un SYN-ACK. Le numéro d'accusé de réception est défini à une plus une que le numéro de séquence reçu, soit A+1, et le numéro de séquence que le serveur choisit pour le paquet est un autre nombre aléatoire, B.
3. Enfin, le client envoie un ACK au serveur. Le numéro de séquence est défini à la valeur d'accusé de réception reçue, soit A+1, et le numéro d'accusé de réception est défini à une plus une que le numéro de séquence reçu, soit B+1.

Après ces étapes, les paquets ont été reçus par le serveur et la connexion peut être fermée.

Le protocole de datagramme utilisateur (UDP) est un protocole sans connexion qui offre un service de datagramme sans connexion. Il ne garantit pas la livraison des paquets, mais il est plus rapide que TCP car il ne nécessite pas de poignée à trois pour établir une connexion. Cependant, il est souvent utilisé lorsque la rapidité est plus importante que la fiabilité

Quelle commande utilisez-vous pour voir la version actuelle de l’IOS ?

show version

