Solution du TP2 APR

Analyse de la commande ping :

1. Le protocole de niveau réseau est utilisé par la commande Ping c’est ICMP
2. Le rôle de la commande ping est de vérifier la connectivité réseau entre deux hôtes en envoyant des paquets ICMP Echo Request et en attendant des réponses ICMP Echo Reply. Cela permet de tester la disponibilité et la latence d'un hôte distant.
3. Lorsque l'on effectue un ping vers la passerelle( ping 192.168.165.230), on trouve un total de 8 trames ICMP. Parmi celles-ci, 4 correspondent à des demandes (requests) et 4 correspondent à des réponses (replies). Les trames de demande sont initiées depuis la machine vers la passerelle, tandis que les trames de réponse sont renvoyées par la passerelle vers la machine. Ces trames ICMP utilisent le protocole ICMP (Internet Control Message Protocol) pour établir la connectivité réseau.
4. La commande ping permet de déterminer la disponibilité d'un hôte (en fonction des réponses reçues) et de mesurer le temps de réponse (latence) entre votre machine et l'hôte distant.
5. Les codes ICMP utilisés pour déterminer la nature du message ICMP sont :

0 pour Echo Reply

8 pour Echo Request

1. Les données ICMP ("Data") dans une trame ping contiennent généralement des informations spécifiques au protocole ou des données de test, comme une séquence de caractères.
2. ICMP n'a pas de ports car il ne s'agit pas d'un protocole de transport comme TCP ou UDP. Il est principalement utilisé pour des fonctions de contrôle et de diagnostic.

Analyse de la commande Tracert :

1. La commande tracert utilise le protocole ICMP (souvent ICMP Echo Request) pour tracer le chemin entre votre machine et l'hôte distant.

La commande tracert utilise le champ TTL des paquets ICMP pour identifier les routeurs sur le chemin vers une destination. Elle commence avec un TTL faible et l'incrémente progressivement, observant les réponses "Time Exceeded" des routeurs pour déterminer les sauts successifs jusqu'à atteindre la destination. Cette méthode permet de cartographier la route réseau de votre machine vers la destination.

Analyse du protocole IP

1. Les couches OSI présentes dans les trames relevées sont généralement les couches 4 (transport) , 3 (réseau) et 7(application).
2. La version du protocole IP peut être déterminée en inspectant l'en-tête IP. Il peut s'agir d'IPv4 ou d'IPv6.
3. La taille de l'en-tête IP varie en fonction des options incluses, mais la taille minimale de l'en-tête IP est de 20 octets pour IPv4.
4. Un paquet IP peut être fragmenté si sa taille dépasse la MTU (Maximum Transmission Unit) de l'une des interfaces réseau sur le chemin de la source à la destination.
5. La valeur du champ TTL (Time To Live) de l'en-tête IP diminue à chaque saut (routeur). Il est initialement défini à une valeur fixe par l'émetteur.
6. Le protocole de niveau supérieur est indiqué dans le champ "Protocol" de l'en-tête IP. Cette valeur indique quel protocole de transport est utilisé, par exemple, TCP (6) ou UDP (17).
7. L'adresse source est généralement dans le champ "Source Address," et l'adresse de destination est dans le champ "Destination Address."

Analyse d’une connexion TCP.

* 1. Le nombre de segments d'ouverture et de fermeture de la connexion dépend du processus de connexion TCP. Il y a généralement trois segments dans une connexion TCP : SYN, SYN-ACK, et ACK pour l'ouverture, et FIN, FIN-ACK, et ACK pour la fermeture.
  2. Les valeurs des "flags" pour les segments d'ouverture sont généralement SYN (synchronisation) pour le premier segment, SYN-ACK (synchronisation + accusé de réception) pour la réponse, et ACK (accusé de réception) pour la confirmation.
  3. Les numéros de port source et destination sont utilisés pour identifier l'application ou le service sur chaque extrémité de la connexion TCP. Le port source est généralement aléatoire et le port de destination correspond au port du service auquel vous vous connectez (par exemple, le port 80 pour HTTP).

Les étudient M1 STIC :

* BELLAKHEL Anaïs
* BAKTACHE Kaouther
* DADDIOUAMER Redouane