Nguyen Anh Dung et Zoe LE BARILLEC – Group 1.1 3INFO

Q1:
Commande pour le nom de ma machine: hostname -> Résultat: nguyen-anh-dung
Commande pour l'adresse IP de ma machine: ip -a addr ou ip a | grep "inet" ou ifconfig (avec installation sudo apt install net-tools) -> Résultat: 10.9.29.36

Q2:
Le nombre d'interfaces: ip link show
lo: mtu 65536 bytes
eno2: mtu 1500 bytes
wlo1: mtu 1500 bytes

Q3:
La table de routage: route
Informations obtenues:

- Destination - indique la destination réseau de la route, une route par défaut
- Gateway - la passerelle
- Genmask
- Flags
- Metric - une métrique de coût
- Ref
- Use
- Iface - l'index d'interface pour l'interface sur laquelle la destination est accessible

Résultat:
Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	_gateway	0.0.0.0	UG	600	0	0	wlo1
10.9.24.0	0.0.0.0	255.255.248.0	U	600	0	0	wlo1

Q4:
sudo apt install openssh-server
ssh nom-machine@ip-adresse
Informations obtenues: c'est l'information de la machine de mon binôme

Q5:
La table (cache) ARP: arp
Résultat:

Address	HWtype	HWaddress	Flags Mask	Iface
10.9.24.87	ether	a8:7e:ea:b4:40:47	C	wlo1
_gateway	ether	00:09:0f:09:00:1a	C	wlo1

Q6:
sudo apt install wireshark
sudo wireshark

Q7:
sudo wireshark

Q8:
ping 10.9.24.87

Q9:
Arrêté

Q10:
Le message ARP est broadcast sur le réseau
Un message ARP contient les champs suivants :
- Adresse MAC source
- Adresse MAC destination
- Adresse IP source
- Adresse IP destination
- Type d'opération (requête ou réponse)

Q11:
785 125.553397924 CloudNetwork_0f:19:3d Broadcast ARP 60 ARP Announcement for 10.9.29.240
786 125.553398016 Intel_24:54:a5 Broadcast ARP 60 Who has 10.9.24.238? (ARP Probe)
787 125.553398092 Intel_24:54:a5 Broadcast ARP 60 Who has 10.9.24.238? (ARP Probe)
788 126.249963616 Fortinet_09:00:1a Broadcast ARP 56 Who has 10.9.30.95? Tell 10.9.31.254
789 126.249963863 Fortinet_09:00:1a Broadcast ARP 56 Who has 10.9.30.95? Tell 10.9.31.254
790 126.296315252 ce:22:b7:de:56:d4 Broadcast ARP 60 Gratuitous ARP for 10.9.29.174 (Reply)
791 126.296315338 ce:22:b7:de:56:d4 Broadcast ARP 60 Gratuitous ARP for 10.9.29.174 (Reply)
792 126.318478820 ce:22:b7:de:56:d4 Broadcast ARP 60 Gratuitous ARP for 10.9.29.174 (Request)
793 126.318479020 ce:22:b7:de:56:d4 Broadcast ARP 60 Gratuitous ARP for 10.9.29.174 (Request)
794 126.619675901 Fortinet_09:00:1a Broadcast ARP 56 Who has 10.9.28.9? Tell 10.9.31.254

Q12:
Un message ICMP contient :
- Type
- Code
- Checksum
- Identifiant et numéro de séquence

Q13:
L'Echo Request est envoyé au destinataire.
L'Echo Reply est retourné avec les mêmes données.

Q14:
ping -c 1 -s 2000 10.9.24.87

Q15:
Je ne sais pas

Q16:
Flag MF (More Fragments) → indique s'il y a d'autres fragments.
Offset → position du fragment dans le message.
ID de fragmentation → identifiant commun à tous les fragments du même paquet.

Q17:
ping www.google.com -> Envoie des requêtes à un serveur de Google, il renvoie une réponse ICMP Echo Reply avec le temps de réponse
ping www.nust.na et ping www.nmmu.ac.za-> Envoie des requêtes à un serveur, cela permet de vérifier la connexion avec un serveur en Afrique
ping www.kitakyu-u.ac.jp et ping www.kyoto-u.ac.jp -> Vérifie l'accessibilité d'un serveur universitaire au Japon, le délai de réponse sera plus long en raison de la distance géographique.

Si un site ne répond pas, il peut être inaccessible depuis votre réseau.
Si les temps de réponse varient, c'est dû aux distances géographiques et aux performances des réseaux.
Si la latence est élevée (>200 ms), le serveur est probablement situé loin ou le réseau est congestionné.

Q18:
sudo apt install traceroute
J'ai déjà essayé mais ca marche pas, il retourne "You do not have enough privileges to use this traceroute method. Socket: Operation not permitted"

Q19:
host www.free.fr -> IP: 212.27.48.10
host www.insa-rennes.fr -> IP: 193.52.94.58

nslookup www.free.fr -> Nom: www.free.fr
nslookup www.insa-rennes.fr -> Nom: www-vmp-app01.insa-rennes.fr (nom canonique: www-vmp-app01.insa-rennes.fr)

dig -> permet d'interroger un serveur DNS pour obtenir des informations sur le domaine, il renvoie principalement l'adresse IP
dig www.free.fr
-> ANSWER SECTION: indique que www.free.fr correspond à l'adresse IP 212.27.48.10.
-> Query time: 0 msec signifie que la requête a pris 0 millisecondes.
-> SERVER: 127.0.0.53 indique que la requête a été résolue par Google Public DNS.
dig www.insa-rennes.fr
-> ANSWER SECTION: indique que www.free.fr correspond à l'adresse IP 193.52.94.58.
-> Query time: 0 msec signifie que la requête a pris 0 millisecondes.
-> SERVER: 127.0.0.53 indique que la requête a été résolue par Google Public DNS.

Q20:
Port de destination : souvent 80 (HTTP)

Q21:
La longueur d'entête est 40 bytes

Q22:
La longueur du segment TCP: taille des données + taile d'entête

Q23:
paquet TCP (SYN)
Le numéro de séquence TCP du premier paquet (du client vers le serveur): 172.18.15.155
La taille de la fen^etre TCP annonc´ee par le client: 32120 bytes
Cela signifie que le client recoit 32120 bytes de données

Q24:
paquet SYN-ACK (Ethernet)
Destination: f0:77:c3:db:a0:ec
Source: 4c:5e:0c:c9:4f:1d
Type: IPv6 (0x86dd)

paquet SYN-ACK (IP)
Source: 2600:1f13:37c:1400:ba21:7165:5fc7:736e
Destination: 2a06:e040:3502:4000:489e:4702:99a7:97cc
Type: TCP(6)

paquet SYN-ACK (TCP)
Source: 80
Destination: 40948
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 4071951760
TCP Segment Len: 0
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 628501767
Calculated window size: 26847

Q25:
MSS Value: 1440 octets

Q26:
paquet ACK
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 628501768
Next Sequence Number: 1 (relative sequence number)
Acknowledgment Number: 490 (relative ack number)
Acknowledgment number (raw): 4071952249
La taille: 32 bytes

Q27:
Ils augmentent en fonction de la quantité de données échangées.

Q28:
La taille de données applicatives de HTTP du 200 OK est: 1632 bits

Q29:
La fragmentation des données peut se produire à deux niveaux principaux :

+ Au niveau de la couche Transport (TCP):
    + TCP segmente les données en fonction du MSS (Maximum Segment Size).
    + Le MSS est négocié lors du three-way handshake et définit la taille maximale d'un segment TCP sans fragmentation IP.
+ Au niveau de la couche Réseau (IP):
    + Si un paquet IP dépasse la MTU (Maximum Transmission Unit) du réseau, il est fragmenté par l'IP.
    + La MTU typique d'Ethernet est 1500 octets (hors en-têtes).

Constatations dans Wireshark:
+ Le paquet ICMP est fragmenté en plusieurs paquets IP.
+ Les indicateurs de fragmentation dans l'en-tête IP