Sujet principal concours tech 2020

1- Quels composants sont nécessaires au fonctionnement et à l'utilisation d'un ordinateur ?

.....

.....

.....

2- L'ordinateur est assemblé, quelle est l'étape suivante au bon fonctionnement de celui-ci ? Quel serait votre choix et pourquoi ?

.....

.....

3- J'ai besoin d'utiliser cet ordinateur, qu'est-il nécessaire d'installer pour :

Naviguer sur internet : .....

Consulter ma messagerie : .....

Retoucher des photos : .....

Imprimer et scanner : .....

Rédiger des courriers : .....

Faire des présentations : .....

Tenir mes comptes : .....

Lire des DVD : .....

Faire des visioconférences avec mes proches : .....

4- Après 2 semaines de fonctionnement, mon ordinateur est inutilisable, tous mes fichiers ont été renommés avec des hiéroglyphes.
Pourquoi ? Quelle est la démarche pour palier au problème ?

.....

.....

.....

5- Vous êtes désigné(e) pour mettre en place une salle de formation pouvant accueillir 11 stagiaires et 1 formateur au sein de votre établissement.
Les formations ne nécessiteront pas de logiciels gourmands et votre responsable vous demande d'étudier les devis de différentes sociétés et de justifier votre choix.
Les devis se trouvent en annexe.

.....

.....

.....

.....

6- Qu'est-ce que le XMPP ?

.....

.....

7- Que vous évoque Bépo, Dvorak et Colemak ?

.....

.....

8- Qu'est-ce que l' « IoT »? Pouvez-vous citer 3 exemples d'IoT ?

.....

.....

9- Le Wifi ac est plus rapide que le Wifi n ?

.....

10- A quoi sert le « Passmark » ?

.....

.....

11- Qu'est-ce qu'une « vulnérabilité 0 day » ?

.....

.....

12- Pour désigner les « géants du web », quel acronyme est faux ? Entourez-le.
    a. NATU
    b. GAFAM
    c. FAANG
    d. NUGFAT

13- Quel(s) système(s) d'exploitation est(sont) installé(s) sur la célèbre tablette Apple ? Entourez la(les) bonne(s) réponse(s)
    a. Android
    b. iOS
    c. iPadOS
    d. AppOS

14- Dans le domaine de la téléphonie IP, citez deux clients et un serveur opensource

.....

.....

15- Faut-il utiliser un Vlan particulier pour la téléphonie ?

.....

16- En python, écrivez un script pour :
    >>> Demander à l'utilisateur d'entrer un premier nombre
    >>> Demander à l'utilisateur d'entrer un deuxième nombre
    >>> Afficher à l'écran le résultat de l'addition (exemple : 'Le résultat de l'addition de 5 + 10 est égale à 15')

.....

.....

.....

.....

.....

.....

17- Rédigez un script en php qui affiche « bonjour invité »

……

……

……

18- Que fait cette commande : tcpdump –i eth0 –n –w flux.tcpdump
Un extrait man page est disponible en annexe

……

……

19- A quoi sert la QoS (quality of service) ?

……

20- A quoi sert le masque dans une configuration TCP/IP ?

……

21- Dans quel domaine parle-t-on de la norme 802.1Q ?

……

22- A quoi sert le service WSUS ?

……

23- A quoi sert le service WDS ?

……

24- Que signifie l'acronyme SNMP ? A quoi sert-il ?

……

……

25- Ecrire une commande Windows pour atteindre le réseau 192.168.2.0/24 en utilisant la passerelle 192.168.1.1 Un extrait du man est disponible en annexe.

……

26- A quoi sert le WOL pour un PC ?

……

27- A quelle famille appartiennent les connecteurs SC ou ST ?

……

28- Quelle est la dernière version de macOS ?

……

29- Que signifie ANSSI et citez quelques missions ?

……

……

……

……

30- Quelles sont les règles d'un bon mot de passe ? Donnez un exemple.

……

……

31- Qu'est-ce que le RGPD ? Citez 3 points essentiels pour vous et argumentez-les.

……

……

……

……

……

32- Que signifie l'acronyme RSSI ? Citez 3 des missions qui y sont rattachées ?

.....

.....

.....

.....

33- Quelle politique de sécurité mettriez-vous en place pour des personnels qui utilisent des ordinateurs portables et qui voyagent ?

.....

.....

34- Quelle(s) différence(s) y a-t-il entre POP, SMTPS, et IMAP ?

.....

.....

.....

35- Vous utilisez une base de données qui contient la table Agent

Id1	Nom	Prénom	Age	Ville	Service
1	Nanasse	Juda	35	Bout du monde	Commutation
2	Vigote	Sarah	62	Bout du monde	Comptable
3	Voirrémerci	Laure	58	Au-delà	Informatique
4	Groidenmabaignoire	Gédéon	63	Centre du monde	Commercial
5	De Lune À Maubeuge	Claire	65	Bout de la terre	Pédagogie
6	Cambronne	Maude	53	Centre du monde	Administration
7	Golade	Larry	45	Bout du monde	Informatique

Quelles requêtes allez-vous écrire pour obtenir les résultats suivants :

- Connaître les noms et prénoms des agents appartenant aux services « com... » de la ville « Bout du monde »
- Connaître le nombre de d'agents de plus de 62 ans

.....

.....

36- Quelle commande permet de donner des droits sur une base MYSQL ?

.....

37- Votre responsable vous demande d'installer les 20 ordinateurs livrés qui ont été commandés pour les personnels administratifs. Le remplacement de ces postes s'intègre dans la politique de migration des postes seven Pro avec des comptes locaux en Windows 10 et de leur intégration dans un active directory. Décrivez les différentes étapes du travail que vous devez accomplir pour réaliser l'installation (matérielle et logicielle), la configuration des postes livrés aux personnels et leur recensement.

.....

.....

.....

.....

.....

.....

.....

.....

.....

38- Quelle différence faites-vous entre un incident et un problème ?

.....

.....

.....

39- Quelles différences faites-vous entre DHCP statique et dynamique ? Quels sont les avantages et inconvénients de chacun ?

.....

.....

.....

40- Vous recevez sur votre logiciel de demandes d'assistance le ticket suivant de la part d'un enseignant :

Objet : *Problème d'impression*
Description : « *Bonjour, je n'arrive pas à imprimer un document couleur urgent pour le président en salle de TP à partir de mon bureau. Merci d'intervenir même si je ne suis pas dans mon bureau*. »
Vous vous rendez dans le bureau de l'enseignant qui est absent. Vous constatez qu'il n'y a pas de message d'erreur sur son poste, et que l'imprimante ne répond pas. Puis vous vous rendez dans la salle au deuxième étage et remarquez que le câble réseau d'imprimante était débranché. Après avoir fait le nécessaire, que répondez-vous à l'utilisateur via le logiciel d'assistance.
Écrivez ci-dessous la réponse que vous lui feriez.

.....

.....

.....

.....

.....

41- Qu'est-ce qu'une charte informatique ?

.....

.....

.....

42- Votre responsable vous demande d'intervenir sur le poste du secrétaire général de l'université. Vous découvrez lors de votre intervention des choses illicites, illégales interdites par la loi (Photo à caractère pédopornographique par exemple). Comment réagissez-vous ?

.....

.....

43- Quels logiciels de sauvegardes connaissez-vous ?

.....

44- Qu'est-ce que le cloud ?

.....

45- A quoi sert IPTABLE ?

.....

.....

46- Expliquez la différence entre Système d'information et Système informatique ?

.....

.....

.....

47- Quelle différence y a-t-il entre un SAN et un NAS ? Avantages et inconvénients ?

.....

.....

.....

48- Vous êtes alerté(e) sur des lenteurs réseau, comment réagissez-vous ?

.....

.....

49- Comment nomme-t-on la poursuite des cours à distance durant le confinement ?

.....

50- Qui est le ministre de l'Education Nationale ?

.....

51- Qu'est-ce que le dispositif éducatif et ludique 2S2C ?

.....

52- Quelle est la particularité du baccalauréat 2020 ?

.....

53- Quel site permet aux élèves de terminale de postuler à des formations post-bac ?

.....

54- Quel ministère allez-vous intégrer en réussissant ce concours ?

……

55- Citez 1 droit et 1 obligation du fonctionnaire

……

……

56- Quelle est la différence entre une DSDEN et un rectorat ?

……

……

57- A quel métier se destinent les étudiants inscrits en INSPE ?

……

58- Que signifie le sigle DSI ?

……

59- Quelle est la différence entre un proviseur et un principal ?

……

……

60- Qui dirige une université ?

……

61- Vous présentez le concours pour être technicien de la filière recherche et formation. Quels sont les autres corps de cette filière ?

……

62- Le cabinet du recteur vous demande de fournir le mot de passe de la boîte mail personnelle d'un agent en vacances car un mail indispensable au recteur a été adressé par le ministère sur cette boîte. Que faites-vous ?

……

……

63- Qu’est-ce que Pronote ?

.....

64- Vous êtes affecté(e) au sein d’un service d’assistance téléphonique aux usagers. Quelles informations doit-on trouver dans un compte-rendu d’intervention ?

.....

.....

.....

65- Quelles différences y a-t-il entre : usb bleu, usb SS, usb HS ?

.....

66- Quel prérequis a-t-on pour accéder en télétravail au réseau privé de l’établissement ?

.....

67- Qu'est-ce qu'une classe d'adresses privées ? Citez-en une (avec son masque).

.....

.....

68- Citez un protocole de partage de fichiers pour chacune des familles de systèmes d’exploitation suivants :

a) Windows : .....

b) Mac OS X : .....

c) Linux : .....

69- Qu'est qu'une GPO ? A quoi est-ce que cela sert ?

.....

.....

.....

70- Pour pouvoir utiliser des GPO, que devez-vous avoir mis en place ?

.....

71- Avec quel(s) système(s) d'exploitation fonctionnent les GPO ?

.....

72- Dans le cas de la réplication avec des serveurs Active Directory est-on dans une situation de réplication maître-maître ou maître-esclave ? Argumentez.

.....

.....

.....

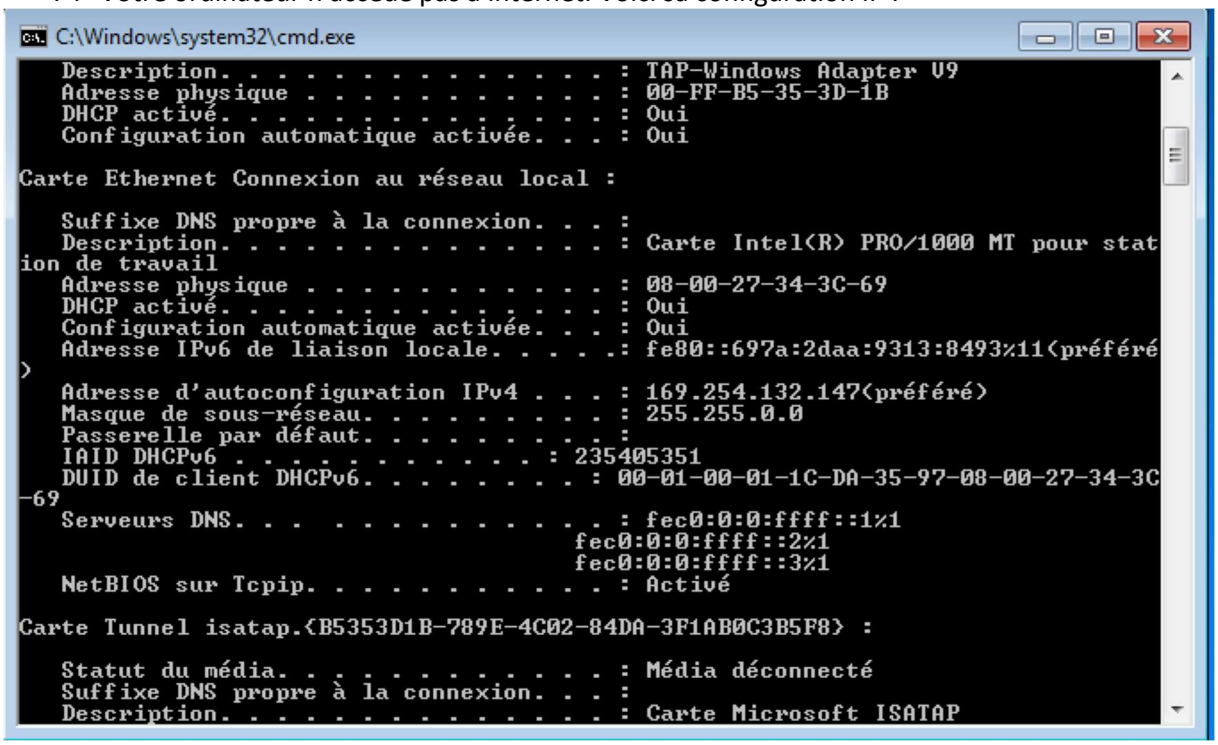
.....

73- À quoi sert samba ?

.....

.....

74- Votre ordinateur n'accède pas à internet. Voici sa configuration IP :



a) Quelle commande vous permet d'obtenir ces informations ?

.....

b) Que pouvez-vous en déduire ?

.....

75- Qu'est-ce qu'une DMZ ? Quelle est son rôle ?

.....

.....

76- Que signifie le « s » dans les droits d'accès du fichier /usr/bin/passwd ?
-r-s--x--x 1 root shadow 27144 2009-09-15 20:53 /usr/bin/passwd

.....

.....

77- Expliquez les termes suivants :

a) Phishing

.....

.....

b) Malware

.....

c) Rootkit

.....

d) Spyware

.....

.....

e) Hoax

.....

.....

f) Darkweb

.....

.....

g) deepweb

.....

.....

h) darknet

.....

.....

78- Vous recevez l'avis du CERT suivant :
Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.
Que faut-il faire ?

.....

.....

.....

79- Qu'apporte un Solid-State Drive par rapport à un disque classique ?

.....

.....

80- Configuration d'un serveur avec 2 disques rapides pour le système et 8 DD +carte RAID. Que proposez-vous comme configuration des RAID ? Justifiez votre réponse.

.....

.....

.....

.....

81- La messagerie est un outil de communication très utilisé, avec plusieurs centaines d'utilisateurs. Vous avez besoin d'interrompre l'accès à la messagerie en raison de l'application d'un patch de sécurité sur le serveur SMTP, ce qui devrait prendre moins d'une heure. Rédigez un courrier électronique pour informer les utilisateurs de cette interruption et ce en français et en anglais.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

82- Que permet la technologie " PoE " d'un switch ?

.....

.....

.....

83- Que signifie et à quoi sert un "OTP " ?

.....

.....

.....

84- Que fait cette commande? du -h –time /home/user/Desktop/

.....

.....

85- Que vous évoque « shadow IT »

……

……

……

86- Qu’est-ce que le protocole MAPI ?

……

……

87- Que permet de faire le "NAT" ?

……

……

……

88- A quoi correspondent les droits suivants sur un système Linux :

–rwxr-x--- admin appl 50001 Jan 18 2017 index.php

……

……

……

89- Quel est le rôle d’un serveur " DNS " ?

……

90- Que permet l’outil Regedit ?

……

91- Qu’est-ce qu’une distribution Linux de type « rolling release » ?

……

……

……

92- Que font les commandes :

a) wget http://cdimage.debian.org/debian-cd/4.0_r5/i386/iso-cd/debian-40r5-i386-businesscard.iso

.....

b) scp -r -p data/courant toto@10.10.10.10:data/encours

.....

.....

c) scp -r -P data/courant toto@10.10.10.10:data/encours

.....

93- Qu'est-ce qu'une adresse APIPA ? Donnez un exemple.

.....

.....

94- Que font les commandes suivantes en Linux :

a) ps -ef | grep apache2

.....

b) find . -name core -exec rm {}\ ;

.....

95- Donnez un exemple de commande pour afficher la configuration courante sur un actif réseau de type CISCO.

.....

96- Donnez différents types de sauvegarde et expliquez-les.

.....

.....

.....

.....

.....

.....

.....

.....

97- Below are all the default usernames and passwords for Nortel devices; Often default passwords are needed either when you try to access a new device you have just purchased or if you have had to do a factory reset after a failed bios update or perhaps you have forgotten the user name and or password you created for your device.
Default Admin Password
The problem is more often or not when you actually need to dig out the paperwork that came with the device you purchased 5 years ago you find it has gone walkie s. That is where the list below comes in it shows all the passwords and usernames for each model, even if your device is not mentioned as its a newer model or a new type of device by the manufacturer you should be able to see a pattern to guess the likely default password.

Faites un résumé, en français, de 5 lignes maximum de ce que vous retenez de ce texte.

.....

.....

.....

.....

.....

98- Qu'est-ce qu'un .apk ?

.....

.....

99- Pourquoi l'arrivée de la 5G fait-t-elle débat en France (maximum 5 lignes) ?

.....

.....

.....

.....

.....

100- A quoi sert l'ARCEP ?

.....

.....

Question 5 :

Devis 1 :

PAGU

DEVIS N° 2016-41

Nom commercial : PAGU
RAISON SOCIALE : SARL
Adresse : 7, rue de l'olive
84100 Orange France
Téléphone : 04.22.22.22.22
Siret 333 444 555 666 12
Contact : Ludovik Bourgeon

A : Le candidat
Adresse : Votre service

Date : 02/07/2020

Désignation

Marchandises (prix unitaire) Main d'œuvre (prix à l'heure)	Prix unitaire	Quantité	Montant HT	Remarques
Unité centrale	310,00	12,00	3 720,00	
Ecrans 22" Dell	100,00	12,00	1 200,00	
Lot claviers/souris USB	30,00	12,00	360,00	
Vidéoprojecteur et système audio	600,00	1,00	600,00	
Installation	150,00	1,00	150,00	

Assurance décennale souscrite auprès de ....., adresse,
N° TVA intracommunautaire, valable en France métropolitaine.
(uniquement pour les artisans)

TOTAL € HT	**5 880,00**
Taux de TVA : 20%	

Coordonnées bancaires :

BIC
IBAN
BANQUE ET AGENCE

Modalités de paiement :

La présente

Devis reçu avant l'exécution des travaux, bon pour accord et signature :

Devis 2 :

sarl MOCONOCE
10 boulevard des Golfs
41500 Muides-sur-Loire
Tél : 02.22.22.22.22
contact : Jean-Sebastien Bosard

DEVIS

M. Le candidat
Votre service

Référence : Dev00412
Date : 02/07/2020

Installation d'une salle de formation

Quantité	Désignation	Prix unitaire HT	Total
12	Unité centrale	285,00 €	3 420,00 €
12	Clavier USB	18,00 €	216,00 €
12	Souris USB	3,00 €	36,00 €
1	Vidéoprojecteur et système audio	610,00 €	610,00 €
1	Installation	300,00 €	300,00 €
		Total HT	4 582,00 €
		T.V.A 20%	916,40 €
		Total TTC	**5 498,40 €**

Nous restons à votre disposition pour toute information complémentaire.
Cordialement,

Si ce devis vous convient, veuillez nous le retourner signé précédé de la mention :
"BON POUR ACCORD ET EXECUTION DU DEVIS"
Date Signature

Validité du devis : 3 mois
Conditions de règlement : 40% à la commande, le solde à la livraison
Toute somme non payée à sa date d'exigibilité produira de plein droit des intérêts de retard équivalents au triple du taux d'intérêts légal de l'année en cours ainsi que le paiement d'une somme de 40 € due au titre des frais de recouvrement

Devis 3 :

LETIN Enterprise

Devis N° 169

En date du **2/7/20**

Guillaume Cradet

A l'attention de **Le candidat**

38, rue de l'ingénieur

Votre service

75000 Paris

Tel : 01.22.22.22.22

Désignation	Qté	TVA	Prix HT	Montant TTC
Unité centrale	12	20,0%	300,00 €	4 320,00 €
Écran 22 pouces	12	20,0%	90,00 €	1 296,00 €
Clavier / souris	12	20,0%	30,00 €	432,00 €
vidéoprojecteur et système audio	1	20,0%	500,00 €	600,00 €
installation	1	20,0%	240,00 €	288,00 €

Conditions de règlement :	à réception de facture
Escompte pour paiement anticipé :	non
Mode de règlement :	chèque ou virement

SOUS-TOTAL	6 936,00 €
TOTAL HT	5 780,00 €
TVA	1 156,00 €
TOTAL TTC	**6 936,00 €**

Ce devis est valable 30 jours à compter de sa date de réalisation.

Question 18 :

extrait man pages

tcpdump [**-AbdDefhHIJKlLnNOpqStuUvxX#**] [**-B** *buffer_size*]

[**-c** *count*] [**--count**] [**-C** *file_size*]
[**-E** *spi@ipaddr algo:secret,...*]
[**-F** *file*] [**-G** *rotate_seconds*] [**-i** *interface*]
[**--immediate-mode**] [**-j** *tstamp_type*] [**-m** *module*]
[**-M** *secret*] [**--number**] [**--print**] [**-Q** *in*|*out*|*inout*]
[**-r** *file*] [**-s** *snaplen*] [**-T** *type*] [**--version**]
[**-V** *file*] [**-w** *file*] [**-W** *filecount*] [**-y** *datalinktype*]
[**-z** *postrotate-command*] [**-Z** *user*]
[**--time-stamp-precision=***tstamp_precision*]
[**--micro**] [**--nano**]
[*expression*]

DESCRIPTION

Tcpdump prints out a description of the contents of packets on a network interface that match the boolean *expression*; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the **-w** flag, which causes it to save the packet data to a file for later analysis, and/or with the **-r** flag, which causes it to read from a saved packet file rather than to read packets from a network interface. It can also be run with the **-V** flag, which causes it to read a list of saved packet files. In all cases, only packets that match *expression* will be processed by *tcpdump*.

Tcpdump will, if not run with the **-c** flag, continue capturing packets until it is interrupted by a SIGINT signal (generated, for example, by typing your interrupt character, typically control-C) or a SIGTERM signal (typically generated with the **kill**(1) command); if run with the **-c** flag, it will capture packets until it is interrupted by a SIGINT or SIGTERM signal or the specified number of packets have been processed.

When *tcpdump* finishes capturing packets, it will report counts of:

packets ``captured'' (this is the number of packets that *tcpdump* has received and processed);
packets ``received by filter'' (the meaning of this depends on the OS on which you're running *tcpdump*, and possibly on the way the OS was configured - if a filter was specified on the command line, on some OSes it counts packets regardless of whether they were matched by the filter expression and, even if they were matched by the filter expression, regardless of whether *tcpdump* has read and processed them yet, on other OSes it counts only packets that were matched by the filter expression regardless of whether *tcpdump* has read and processed them yet, and on other OSes it counts only packets that were matched by the filter expression and were processed by *tcpdump*);
packets ``dropped by kernel'' (this is the number of packets that were dropped, due to a lack of buffer space, by the packet capture mechanism in the OS on which *tcpdump* is running, if the OS reports that information to applications; if not, it will be reported as 0).

On platforms that support the SIGINFO signal, such as most BSDs (including macOS) and Digital/Tru64 UNIX, it will report those counts when it receives a SIGINFO signal (generated, for example, by typing your ``status'' character, typically control-T, although on some platforms, such as macOS, the ``status'' character is not set by default, so you must set it with **stty**(1) in order to use it) and will continue capturing packets. On platforms that do not support the SIGINFO signal, the same can be achieved by using the SIGUSR1 signal.

Using the SIGUSR2 signal along with the **-w** flag will forcibly flush the packet buffer into the output file.

Reading packets from a network interface may require that you have special privileges; see the **pcap**(3PCAP) man page for details. Reading a saved packet file doesn't require special privileges.

OPTIONS

-A

Print each packet (minus its link level header) in ASCII. Handy for capturing web pages.

-b

Print the AS number in BGP packets in ASDOT notation rather than ASPLAIN notation.

-B *buffer_size*

--buffer-size=*buffer_size*

Set the operating system capture buffer size to *buffer_size*, in units of KiB (1024 bytes).

-c *count*

Exit after receiving *count* packets.

--count

Print only on stderr the packet count when reading capture file(s) instead of parsing/printing the packets. If a filter is specified on the command line, *tcpdump* counts only packets that were matched by the filter expression.

-C *file_size*

Before writing a raw packet to a savefile, check whether the file is currently larger than *file_size* and, if so, close the current savefile and open a new one. Savefiles after the first savefile will have the name specified with the **-w** flag, with a number after it, starting at 1 and continuing upward. The units of *file_size* are millions of bytes (1,000,000 bytes, not 1,048,576 bytes).

-d

Dump the compiled packet-matching code in a human readable form to standard output and stop.

-dd

Dump packet-matching code as a **C** program fragment.

-ddd

Dump packet-matching code as decimal numbers (preceded with a count).

-D

--list-interfaces

Print the list of the network interfaces available on the system and on which *tcpdump* can capture packets. For each network interface, a number and an interface name, possibly followed by a text description of the interface, are printed. The interface name or the number can be supplied to the **-i** flag to specify an interface on which to capture.

This can be useful on systems that don't have a command to list them (e.g., Windows systems, or UNIX systems lacking **ifconfig -a**); the number can be useful on Windows 2000 and later systems, where the interface name is a somewhat complex string.

The **-D** flag will not be supported if *tcpdump* was built with an older version of *libpcap* that lacks the **pcap_findalldevs(3PCAP)** function.

-e

Print the link-level header on each dump line. This can be used, for example, to print MAC layer addresses for protocols such as Ethernet and IEEE 802.11.

-E

Use *spi@ipaddr algo:secret* for decrypting IPsec ESP packets that are addressed to *addr* and contain Security Parameter Index value *spi*. This combination may be repeated with comma or newline separation.

Note that setting the secret for IPv4 ESP packets is supported at this time.

Algorithms may be **des-cbc**, **3des-cbc**, **blowfish-cbc**, **rc3-cbc**, **cast128-cbc**, or **none**. The default is **des-cbc**. The ability to decrypt packets is only present if *tcpdump* was compiled with cryptography enabled.

secret is the ASCII text for ESP secret key. If preceded by 0x, then a hex value will be read.

The option assumes RFC2406 ESP, not RFC1827 ESP. The option is only for debugging purposes, and the use of this option with a true `secret' key is discouraged. By presenting IPsec secret key onto command line you make it visible to others, via *ps*(1) and other occasions.

In addition to the above syntax, the syntax *file name* may be used to have tcpdump read the provided file in. The file is opened upon receiving the first ESP packet, so any special permissions that tcpdump may have been given should already have been given up.

-f

Print `foreign' IPv4 addresses numerically rather than symbolically (this option is intended to get around serious brain damage in Sun's NIS server --- usually it hangs forever translating non-local internet numbers).

The test for `foreign' IPv4 addresses is done using the IPv4 address and netmask of the interface on which capture is being done. If that address or netmask are not available, available, either because the interface on which capture is being done has no address or netmask or because the capture is being done on the Linux "any" interface, which can capture on more than one interface, this option will not work correctly.

-F *file*

Use *file* as input for the filter expression. An additional expression given on the command line is ignored.

-G *rotate_seconds*

If specified, rotates the dump file specified with the **-w** option every *rotate_seconds* seconds. Savefiles will have the name specified by **-w** which should include a time format as defined by **strftime**(3). If no time format is specified, each new file will overwrite the previous. Whenever a generated filename is not unique, tcpdump will overwrite the preexisting data; providing a time specification that is coarser than the capture period is therefore not advised.

If used in conjunction with the **-C** option, filenames will take the form of `*file*<count>'.

-h

--help

Print the tcpdump and libpcap version strings, print a usage message, and exit.

--version

Print the tcpdump and libpcap version strings and exit.

-H

Attempt to detect 802.11s draft mesh headers.

-i *interface*

--interface=*interface*

Listen, report the list of link-layer types, report the list of time stamp types, or report the results of compiling a filter expression on *interface*. If unspecified, *tcpdump* searches the system interface list for the lowest numbered, configured up interface (excluding loopback), which may turn out to be, for example, ``eth0''.

On Linux systems with 2.2 or later kernels, an *interface* argument of ``any'' can be used to capture packets from all interfaces. Note that captures on the ``any'' device will not be done in promiscuous mode.

If the **-D** flag is supported, an interface number as printed by that flag can be used as the *interface* argument, if no interface on the system has that number as a name.

-I

--monitor-mode

Put the interface in "monitor mode"; this is supported only on IEEE 802.11 Wi-Fi interfaces, and supported only on some operating systems.

Note that in monitor mode the adapter might disassociate from the network with which it's associated, so that you will not be able to use any wireless networks with that adapter. This could prevent accessing files on a network server, or resolving host names or network addresses, if you are capturing in monitor mode and are not connected to another network with another adapter.

This flag will affect the output of the **-L** flag. If **-I** isn't specified, only those link-layer types available when not in monitor mode will be shown; if **-I** is specified, only those link-layer types available when in monitor mode will be shown.

--immediate-mode

Capture in "immediate mode". In this mode, packets are delivered to tcpdump as soon as they arrive, rather than being buffered for efficiency. This is the default when printing packets rather than saving packets to a ``savefile'' if the packets are being printed to a terminal rather than to a file or pipe.

-j *tstamp_type*

--time-stamp-type=*tstamp_type*

Set the time stamp type for the capture to *tstamp_type*. The names to use for the time stamp types are given in **pcap-tstamp**(7); not all the types listed there will necessarily be valid for any given interface.

-J

--list-time-stamp-types

List the supported time stamp types for the interface and exit. If the time stamp type cannot be set for the interface, no time stamp types are listed.

--time-stamp-precision=*tstamp_precision*

When capturing, set the time stamp precision for the capture to *tstamp_precision*. Note that availability of high precision time stamps (nanoseconds) and their actual accuracy is platform and hardware dependent. Also note that when writing captures made with nanosecond accuracy to a savefile, the time stamps are written with nanosecond resolution, and the file is written with a different magic number, to indicate that the time stamps are in seconds and nanoseconds; not all programs that read pcap savefiles will be able to read those captures.

When reading a savefile, convert time stamps to the precision specified by *timestamp_precision*, and display them with that resolution. If the precision specified is less than the precision of time stamps in the file, the conversion will lose precision.

The supported values for *timestamp_precision* are **micro** for microsecond resolution and **nano** for nanosecond resolution. The default is microsecond resolution.

--micro

--nano

Shorthands for **--time-stamp-precision=micro** or **--time-stamp-precision=nano**, adjusting the time stamp precision accordingly. When reading packets from a savefile, using **--micro** truncates time stamps if the savefile was created with nanosecond precision. In contrast, a savefile created with microsecond precision will have trailing zeroes added to the time stamp when **--nano** is used.

-K

--dont-verify-checksums

Don't attempt to verify IP, TCP, or UDP checksums. This is useful for interfaces that perform some or all of those checksum calculation in hardware; otherwise, all outgoing TCP checksums will be flagged as bad.

-l

Make stdout line buffered. Useful if you want to see the data while capturing it. E.g.,

tcpdump -l | tee dat

or

tcpdump -l > dat & tail -f dat

Note that on Windows,``line buffered'' means ``unbuffered'', so that WinDump will write each character individually if **-l** is specified.

-U is similar to **-l** in its behavior, but it will cause output to be ``packet-buffered'', so that the output is written to stdout at the end of each packet rather than at the end of each line; this is buffered on all platforms, including Windows.

-L

--list-data-link-types

List the known data link types for the interface, in the specified mode, and exit. The list of known data link types may be dependent on the specified mode; for example, on some platforms, a Wi-Fi interface might support one set of data link types when not in monitor mode (for example, it might support only fake Ethernet headers, or might support 802.11 headers but not support 802.11 headers with radio information) and another set of data link types when in monitor mode (for example, it might support 802.11 headers, or 802.11 headers with radio information, only in monitor mode).

-m *module*

Load SMI MIB module definitions from file *module*. This option can be used several times to load several MIB modules into *tcpdump*.

-M *secret*

Use *secret* as a shared secret for validating the digests found in TCP segments with the TCP-MD5 option (RFC 2385), if present.

-n

Don't convert addresses (i.e., host addresses, port numbers, etc.) to names.

-N

Don't print domain name qualification of host names. E.g., if you give this flag then *tcpdump* will print ``nic'' instead of ``nic.ddn.mil''.

-#

--number

Print an optional packet number at the beginning of the line.

-O

--no-optimize

Do not run the packet-matching code optimizer. This is useful only if you suspect a bug in the optimizer.

-p

--no-promiscuous-mode

Don't put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, `-p' cannot be used as an abbreviation for `ether host {local-hw-addr} or ether broadcast'.

--print

Print parsed packet output, even if the raw packets are being saved to a file with the **-w** flag.

-Q *direction*

--direction=*direction*

Choose send/receive direction *direction* for which packets should be captured. Possible values are `in', `out' and `inout'. Not available on all platforms.

-q

Quick (quiet?) output. Print less protocol information so output lines are shorter.

-r *file*

Read packets from *file* (which was created with the **-w** option or by other tools that write pcap or pcapng files). Standard input is used if *file* is ``-''.

-S

--absolute-tcp-sequence-numbers

Print absolute, rather than relative, TCP sequence numbers.

-s *snaplen*

--snapshot-length=*snaplen*

Snarf *snaplen* bytes of data from each packet rather than the default of 262144 bytes. Packets truncated because of a limited snapshot are indicated in the output with ``[|*proto*]'', where *proto* is the name of the protocol level at which the truncation has occurred.

Note that taking larger snapshots both increases the amount of time it takes to process packets and, effectively, decreases the amount of packet buffering. This may cause packets to be lost. Note also that taking smaller snapshots will discard data from protocols above the transport layer, which loses information that may be important. NFS and AFS requests and replies, for example, are very large, and much of the detail won't be available if a too-short snapshot length is selected.

If you need to reduce the snapshot size below the default, you should limit *snaplen* to the smallest number that will capture the protocol information you're interested in. Setting *snaplen* to 0 sets it to the default of 262144, for backwards compatibility with recent older versions of *tcpdump*.

-T *type*

Force packets selected by "*expression*" to be interpreted the specified *type*. Currently known types are **aodv** (Ad-hoc On-demand Distance Vector protocol), **carp** (Common Address Redundancy Protocol), **cnfp** (Cisco NetFlow protocol), **domain** (Domain Name System), **lmp** (Link Management Protocol), **pgm** (Pragmatic General Multicast), **pgm_zmtp1** (ZMTP/1.0 inside PGM/EPGM), **ptp** (Precision Time Protocol), **radius** (RADIUS), **resp** (REdis Serialization Protocol), **rpc** (Remote Procedure Call), **rtcp** (Real-Time Applications control protocol), **rtp** (Real-Time Applications protocol), **snmp** (Simple Network Management Protocol), **someip** (SOME/IP), **tftp** (Trivial File Transfer Protocol), **vat** (Visual Audio Tool), **vxlan** (Virtual eXtensible Local Area Network), **wb** (distributed White Board) and **zmtp1** (ZeroMQ Message Transport Protocol 1.0).

Note that the **pgm** type above affects UDP interpretation only, the native PGM is always recognised as IP protocol 113 regardless. UDP-encapsulated PGM is often called "EPGM" or "PGM/UDP".

Note that the **pgm_zmtp1** type above affects interpretation of both native PGM and UDP at once. During the native PGM decoding the application data of an ODATA/RDATA packet would be decoded as a ZeroMQ datagram with ZMTP/1.0 frames. During the UDP decoding in addition to that any UDP packet would be treated as an encapsulated PGM packet.

-t

Don't print a timestamp on each dump line.

-tt

Print the timestamp, as seconds since January 1, 1970, 00:00:00, UTC, and fractions of a second since that time, on each dump line.

-ttt

Print a delta (microsecond or nanosecond resolution depending on the **--time-stamp-precision** option) between current and previous line on each dump line. The default is microsecond resolution.

-tttt

Print a timestamp, as hours, minutes, seconds, and fractions of a second since midnight, preceded by the date, on each dump line.

-ttttt

Print a delta (microsecond or nanosecond resolution depending on the **--time-stamp-precision** option) between current and first line on each dump line. The default is microsecond resolution.

-u

Print undecoded NFS handles.

-U

--packet-buffered

If the **-w** option is not specified, or if it is specified but the **--print** flag is also specified, make the printed packet output ``packet-buffered''; i.e., as the description of the contents of each packet is printed, it will be written to the standard output, rather than, when not writing to a terminal, being written only when the output buffer fills.

If the **-w** option is specified, make the saved raw packet output ``packet-buffered''; i.e., as each packet is saved, it will be written to the output file, rather than being written only when the output buffer fills.

The **-U** flag will not be supported if *tcpdump* was built with an older version of *libpcap* that lacks the **pcap_dump_flush(3PCAP)** function.

-v

When parsing and printing, produce (slightly more) verbose output. For example, the time to live, identification, total length and options in an IP packet are printed. Also enables additional packet integrity checks such as verifying the IP and ICMP header checksum.

When writing to a file with the **-w** option, report, once per second, the number of packets captured.

-vv

Even more verbose output. For example, additional fields are printed from NFS reply packets, and SMB packets are fully decoded.

-vvv

Even more verbose output. For example, telnet **SB** ... **SE** options are printed in full. With **-X** Telnet options are printed in hex as well.

-V *file*

Read a list of filenames from *file*. Standard input is used if *file* is ``-''.

-w *file*

Write the raw packets to *file* rather than parsing and printing them out. They can later be printed with the -r option. Standard output is used if *file* is ``-''.

This output will be buffered if written to a file or pipe, so a program reading from the file or pipe may not see packets for an arbitrary amount of time after they are received. Use the **-U** flag to cause packets to be written as soon as they are received.

The MIME type *application/vnd.tcpdump.pcap* has been registered with IANA for *pcap* files. The filename extension *.pcap* appears to be the most commonly used along with *.cap* and *.dmp*. *Tcpdump* itself doesn't check the extension when reading capture files and doesn't add an extension when writing them (it uses magic numbers in the file header instead). However, many operating systems and applications will use the extension if it is present and adding one (e.g. .pcap) is recommended.

See **pcap-savefile**(5) for a description of the file format.

-W *filecount*

Used in conjunction with the **-C** option, this will limit the number of files created to the specified number, and begin overwriting files from the beginning, thus creating a 'rotating' buffer. In addition, it will name the files with enough leading 0s to support the maximum number of files, allowing them to sort correctly.

Used in conjunction with the **-G** option, this will limit the number of rotated dump files that get created, exiting with status 0 when reaching the limit.

If used in conjunction with both **-C** and **-G,** the **-W** option will currently be ignored, and will only affect the file name.

-x

When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex. The smaller of the entire packet or *snaplen* bytes will be printed. Note that this is the entire link-layer packet, so for link layers that pad (e.g. Ethernet), the padding bytes will also be printed when the higher layer packet is shorter than the required padding.

-xx

When parsing and printing, in addition to printing the headers of each packet, print the data of each packet, *including* its link level header, in hex.

-X

When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex and ASCII. This is very handy for analysing new protocols.

-XX

When parsing and printing, in addition to printing the headers of each packet, print the data of each packet, *including* its link level header, in hex and ASCII.

-y *datalinktype*

--linktype=*datalinktype*

Set the data link type to use while capturing packets to *datalinktype*.

-z *postrotate-command*

Used in conjunction with the **-C** or **-G** options, this will make *tcpdump* run " *postrotate-command file* " where *file* is the savefile being closed after each rotation. For example, specifying **-z gzip** or **-z bzip2** will compress each savefile using gzip or bzip2.

Note that tcpdump will run the command in parallel to the capture, using the lowest priority so that this doesn't disturb the capture process.

And in case you would like to use a command that itself takes flags or different arguments, you can always write a shell script that will take the savefile name as the only argument, make the flags & arguments arrangements and execute the command that you want.

-Z *user*

--relinquish-privileges=*user*

If *tcpdump* is running as root, after opening the capture device or input savefile, but before opening any savefiles for output, change the user ID to *user* and the group ID to the primary group of *user*.

This behavior can also be enabled by default at compile time.

expression

selects which packets will be dumped. If no *expression* is given, all packets on the net will be dumped. Otherwise, only packets for which *expression* is `true' will be dumped.

For the *expression* syntax, see **pcap-filter**(7).

The *expression* argument can be passed to *tcpdump* as either a single Shell argument, or as multiple Shell arguments, whichever is more convenient. Generally, if the expression contains Shell metacharacters, such as backslashes used to escape protocol names, it is easier to pass it as a single, quoted argument rather than to escape the Shell metacharacters. Multiple arguments are concatenated with spaces before being parsed.

Question 25 :

Extrait du man

ROUTE [-f] [-p] [-4|-6] commande [destination]
[MASK masque_réseau] [passerelle] [METRIC métrique]
[IF interface]

-f Efface les tables de routage de toutes les entrées de passerelle. Si ceci est utilisé en combinaison avec une des commandes, les tables sont effacées avant l'exécution de la commande.

-p Utilisé avec la commande ADD, établit un itinéraire persistant à travers les démarrages du système. Par défaut, les itinéraires ne sont pas conservés quand le système est redémarré. Ignoré pour toutes les autres commandes, qui affectent toujours les itinéraires persistants appropriés.

-4 Force l'utilisation de IPv4.

-6 Force l'utilisation de IPv6.

commande Une des commandes suivantes :
PRINT Imprime un itinéraire
ADD Ajoute un itinéraire
DELETE Supprime un itinéraire
CHANGE Modifie un itinéraire existant

destination Spécifie l'hôte.

MASK Spécifie que le paramètre suivant est la valeur « masque_réseau ».

masque_réseau Spécifie une valeur de masque de sous-réseau pour cette entrée d'itinéraire. Si elle n'est pas spécifiée, sa valeur par défaut est 255.255.255.255.

passerelle Spécifie une passerelle.

interface le numéro d'interface pour l'itinéraire spécifié.

METRIC Spécifie la métrique, c'est-à-dire le coût pour la destination.