NSI Terminale — Architectures matérielles, systèmes d'exploitation et réseaux

Entraînement au contrôle

Durée : 110 minutes · Sans calculatrice · Sans ordinateur · Total : 20 points

Les trois exercices sont indépendants. Toute réponse doit être justifiée par une propriété, un calcul ou une donnée de l'énoncé.

*Ce sujet porte sur les mêmes notions que le contrôle, mais elles sont posées autrement : il faut **raisonner** à partir de la situation, pas réciter le cours.*

Temps conseillé : exercice 1, 45 minutes ; exercice 2, 35 minutes ; exercice 3, 30 minutes.

Exercice 1 — Adressage et routage (8 points)

Une médiathèque intercommunale relie six sites au moyen des routeurs A, B, C, D, E et F. Dans la salle multimédia, le poste de l'animateur a pour adresse `172.16.5.141` et pour masque `255.255.255.240`.

Partie A — Adressage IPv4

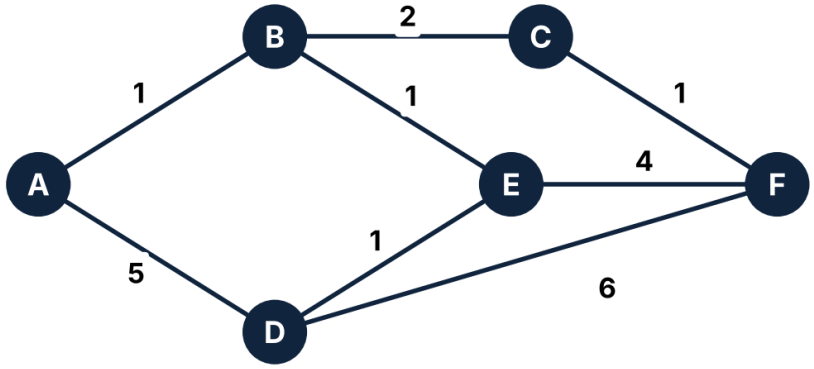
1. Écrire ce masque en notation CIDR (préfixe /n). En déduire le nombre total d'adresses du réseau et le nombre usuel d'adresses attribuables à des machines. (0,75 point)

2. Déterminer l'adresse du réseau auquel appartient le poste de l'animateur, son adresse de diffusion et la plage des adresses attribuables aux machines. (1 point)

3. Un technicien propose d'attribuer à une nouvelle imprimante l'une des adresses `172.16.5.128`, `172.16.5.139`, `172.16.5.143` ou `172.16.5.144`. Pour chacune, dire si elle convient ; sinon, expliquer pourquoi. (0,75 point)

4. La salle doit désormais accueillir 40 machines. Quel est le préfixe le plus long qui le permet ? Avec ce préfixe, le poste de l'animateur peut-il garder son adresse ? Donner alors la nouvelle adresse de diffusion. (0,5 point)

Partie B — Protocoles de routage



Le nombre placé sur chaque liaison est son coût OSPF. Pour RIP, la métrique d'un chemin est son nombre de sauts ; pour OSPF, c'est la somme des coûts des liaisons. Tous les calculs doivent apparaître.

5. Déterminer le chemin choisi par RIP pour aller de A vers F et donner sa métrique. Expliquer pourquoi aucun autre chemin ne peut faire mieux. (0,75 point)

6. Déterminer le chemin choisi par OSPF de A vers F et son coût, en présentant les coûts des chemins utiles à la comparaison. Le chemin retenu compte plus de sauts que celui de RIP : expliquer pourquoi OSPF le préfère quand même. (1,25 point)

7. Le coût OSPF d'une liaison de débit d, en bit/s, vaut $\frac{10^8}{d}$. Quel est le débit de la liaison B–C ? (0,5 point)

8. Des travaux ralentissent la liaison B–C, dont le coût augmente. À partir de quelle valeur de ce coût le chemin trouvé à la question 6 n'est-il plus le seul meilleur ? Quel chemin OSPF utilise-t-il au-delà ? (1 point)

9. Pendant la mise en route du réseau, la table RIP de B est la suivante (la route vers F n'est pas encore connue). B reçoit d'abord la table de son voisin C, puis celle de son voisin E. B ne remplace une route que par une route **strictement** plus courte. (1,5 point)

Destination	Passerelle	Distance
A	A	1
C	C	1
D	A	2
E	E	1

Distances annoncées par C : A 2 ; B 1 ; D 2 ; E 2 ; F 1.

Distances annoncées par E : A 2 ; B 1 ; C 2 ; D 1 ; F 1.

Donner la table de B après la réception de la table de C, puis après celle de E. Justifier chaque ligne qui change et chaque ligne qui ne change pas.

Exercice 2 — Processus et ressources (6 points)

1. Léa ouvre deux fois le même éditeur de texte. Le gestionnaire des tâches affiche alors deux lignes portant le même nom de programme, mais deux PID différents. Expliquer, à l'aide de cette observation, la différence entre un programme et un processus. Quel composant du système d'exploitation décide, à chaque instant, du processus exécuté ? (1 point)

2. On considère trois suites d'états d'un processus. (1 point)

(a) prêt → élu → bloqué → prêt → élu

(b) prêt → élu → bloqué → élu

(c) élu → prêt → élu

L'une de ces suites est impossible : laquelle ? Justifier. Pour la suite (a), donner un événement qui provoque le passage d'élu à bloqué, puis celui de bloqué à prêt. Pour la suite (c), quel événement fait passer d'élu à prêt ?

Trois processus arrivent dans le système. L'ordonnanceur utilise un tourniquet de quantum 1. Quand un processus arrive à l'instant où un quantum se termine, il est placé dans la file **avant** le processus interrompu.

Processus	P1	P2	P3
Date d'arrivée	0	1	2
Durée	3	2	1

3. Donner, unité de temps par unité de temps, le processus exécuté et l'état de la file, jusqu'à la fin des trois processus. En déduire l'instant de fin de chaque processus. (1,5 point)

4. Un élève affirme : « Avec un quantum plus grand, P3 finira plus tôt, puisqu'il y aura moins d'interruptions. » Tester cette affirmation avec un quantum de 3, puis conclure. (1 point)

5. Avec la politique « plus court d'abord », on élit toujours le processus le plus court parmi ceux qui attendent. Expliquer pourquoi un processus long risque alors de ne jamais être exécuté. Pourquoi le tourniquet n'a-t-il pas ce défaut ? (0,5 point)

Trois processus utilisent trois ressources non partageables : P1 détient R1 et attend R2 ; P2 détient R2 et attend R3 ; P3 détient R3 et attend R1.

6. Nommer la situation et écrire le cycle d'attente. On impose la règle suivante : un processus ne peut demander qu'une ressource de numéro plus grand que toutes celles qu'il détient. Quel processus ne respecte pas cette règle ? Expliquer pourquoi, si tous la respectent, aucun cycle ne peut se former. (1 point)

Exercice 3 — Architecture et communication sécurisée (6 points)

Un thermostat connecté est construit autour d'un système sur puce comprenant : un CPU, un GPU, une mémoire vive, un module Wi-Fi et un circuit de gestion d'énergie. Chaque heure, il envoie ses mesures au serveur `collecte.example` en HTTPS.

1. Quel bloc exécute le programme de régulation ? Quel bloc envoie les mesures au serveur ? Trois ans plus tard, le fabricant voudrait doubler la mémoire vive des thermostats déjà vendus : pourquoi est-ce impossible ? Donner en contrepartie un avantage de l'intégration sur une seule puce. (1 point)

2. Un jour, le serveur DNS est en panne. Le thermostat est bien connecté au réseau et le serveur `collecte.example` fonctionne, pourtant les envois échouent. Expliquer. Quelle information suffirait au thermostat pour se passer du DNS ? (0,5 point)

3. On admet qu'un chiffrement asymétrique est environ mille fois plus lent qu'un chiffrement symétrique. Expliquer pourquoi HTTPS n'utilise pas le chiffrement asymétrique pour toute la communication, et préciser ce qui est chiffré avec chacun des deux. (1 point)

4. Le thermostat a envoyé au serveur une clé de session chiffrée. Ève, qui espionne le réseau, intercepte ce message ; elle connaît aussi la clé publique du serveur. Peut-elle retrouver la clé de session ? Justifier en précisant avec quelle clé le message a été chiffré et quelle clé permet de le déchiffrer. (1 point)

5. Ève change de tactique : elle se place entre le thermostat et le serveur et envoie au thermostat un faux certificat contenant sa propre clé publique. Que pourrait-elle faire si le thermostat l'acceptait ? Quelle vérification l'en empêche ? (1 point)

6. Les étapes suivantes sont données dans le désordre, et l'une d'elles contient une erreur. (1 point)

A. Le serveur déchiffre la clé de session avec sa clé privée.

B. Le DNS fournit l'adresse IP du serveur.

C. La suite des échanges est chiffrée en symétrique.

D. Le serveur envoie son certificat, qui contient sa clé publique.

E. Le thermostat chiffre la clé de session avec sa propre clé privée, puis l'envoie.

Repérer et corriger l'étape erronée, puis remettre les étapes dans l'ordre chronologique.

7. Un attaquant met au plus 1 heure pour essayer toutes les clés de 40 bits. Combien de temps lui faudrait-il, au plus, pour des clés de 50 bits ? On utilisera $2^{10} \approx 10^3$. (0,5 point)

Entraînement au contrôle

Corrigé détaillé et barème — document réservé au professeur

Exercice	Points	Répartition
1. Adressage et routage	8	Adressage 3 ; routage RIP et OSPF 5
2. Processus et ressources	6	Notions 2 ; ordonnancement 3 ; interblocage 1
3. Architecture et sécurité	6	SoC et DNS 1,5 ; HTTPS et clés 4 ; force brute 0,5
Total	**20**	

Exercice 1 — Adressage et routage (8 points)

1. (0,75 point)

$240 = 128+64+32+16$, donc 240 s'écrit 11110000 en binaire : 4 bits à 1 dans le dernier octet.

$24+4=28$: **le masque s'écrit /28.**

Il reste $32-28=4$ bits pour les machines.

$2^4=16$: **16 adresses**, dont **14 attribuables** (on retire l'adresse du réseau et l'adresse de diffusion).

Le contrôle pose la question dans l'autre sens (préfixe donné, masque demandé) : savoir passer de l'un à l'autre est indispensable.

Barème : Préfixe 0,25 ; nombre total 0,25 ; nombre attribuable 0,25.

2. (1 point)

Les blocs de 16 adresses commencent aux multiples de 16 : 0, 16, …, 128, 144, …

$16 \times 8 = 128$ et $16 \times 9 = 144$: 141 est compris entre 128 et 143.

Adresse du réseau : 172.16.5.128 ; adresse de diffusion : 172.16.5.143.

Machines : de 172.16.5.129 à 172.16.5.142.

Piège fréquent : prendre 172.16.5.141 pour l'adresse du réseau. Ici, l'adresse donnée est celle d'une machine ; il faut d'abord trouver le bloc qui la contient.

Barème : Recherche du bloc 0,25 ; réseau 0,25 ; diffusion 0,25 ; plage 0,25.

3. (0,75 point)

172.16.5.128 : **non**, c'est l'adresse du réseau.

172.16.5.139 : **oui**, elle est dans la plage .129 à .142 (à condition qu'aucune autre machine ne l'utilise déjà).

172.16.5.143 : **non**, c'est l'adresse de diffusion.

172.16.5.144 : **non**, elle appartient au bloc suivant (144 à 159) : l'imprimante serait dans un autre réseau que le poste.

Barème : 0,25 pour .139 ; 0,5 pour les trois refus correctement justifiés (0,25 si une justification manque).

4. (0,5 point)

Il faut au moins $40+2=42$ adresses.

$2^5=32$ ne suffit pas ; $2^6=64$ suffit : 6 bits pour les machines.

$32-6=26$: **préfixe /26.**

Les blocs de 64 commencent à 0, 64, 128, 192 : 141 est dans le bloc 128 à 191. Le poste **garde son adresse**, dans le réseau 172.16.5.128/26.

Nouvelle adresse de diffusion : 172.16.5.191.

Barème : Préfixe justifié 0,25 ; adresse conservée et diffusion 0,25.

5. (0,75 point)

Les voisins de A sont B et D ; les voisins de F sont C, D et E.

A et F n'étant pas voisins, il faut au moins 2 sauts. Un chemin de 2 sauts passe par un voisin commun à A et à F : seul **D** convient.

RIP choisit A → D → F, métrique 2.

Barème : Chemin 0,25 ; métrique 0,25 ; justification de la minimalité 0,25.

6. (1,25 point)

A → D → F : $5+6=11$

A → D → E → F : $5+1+4=10$

A → B → E → F : $1+1+4=6$

A → B → E → D → F : $1+1+1+6=9$

A → B → C → F : $1+2+1=4$

OSPF choisit A → B → C → F, de coût 4 (3 sauts).

Pour aller vite : tout chemin qui commence par A → D coûte déjà 5, et il faut encore au moins 5 pour aller de D à F ; il ne peut donc pas descendre sous 10.

RIP ne compte que les sauts, sans tenir compte des liaisons. OSPF additionne des coûts qui dépendent du débit : **trois liaisons rapides valent mieux que deux liaisons lentes.**

Barème : Calculs des chemins utiles 0,5 ; conclusion 0,25 ; explication 0,5.

7. (0,5 point)

$\frac{10^8}{d}=2$ donc $d=\frac{10^8}{2}$.

$d=5\times10^7$ bit/s.

Le débit de B–C est 50 Mbit/s.

Barème : Équation 0,25 ; résultat avec unité 0,25.

8. (1 point)

On note x le coût de B–C. Le chemin A → B → C → F coûte $1+x+1=x+2$.

Le meilleur chemin qui n'emprunte pas B–C est A → B → E → F, de coût 6 (question 6).

$x+2=6$ pour $x=4$.

Pour un coût égal à 4, les deux chemins sont à égalité ; au-delà, OSPF passe par A → B → E → F, de coût 6.

La démarche compte plus que le résultat : exprimer le coût en fonction de x, puis le comparer au meilleur chemin qui évite la liaison.

Barème : Coût en fonction de x 0,25 ; meilleur concurrent 0,25 ; seuil 0,25 ; nouveau chemin 0,25.

9. (1,5 point)

Par un voisin, B ajoute 1 saut à la distance annoncée.

Après la table de C :

F par C : $1+1=2$. B ne connaissait pas F : **nouvelle ligne F, passerelle C, distance 2.**

D par C : $2+1=3$, et $3>2$: on garde D par A.

A par C : $2+1=3>1$; E par C : $2+1=3>1$: rien ne change.

Après la table de E :

F par E : $1+1=2$, ce n'est pas strictement mieux que 2 : **on garde F par C.**

D par E : $1+1=2$, pas strictement mieux que 2 : **on garde D par A.**

A par E : $2+1=3>1$; C par E : $2+1=3>1$: rien ne change.

Destination	Passerelle	Distance
A	A	1
C	C	1
D	A	2
E	E	1
F	C	2

Les égalités sont le piège de la question : avec la règle « strictement plus court », la première route trouvée est conservée.

Barème : Règle +1 saut 0,25 ; ligne F 0,5 ; lignes inchangées justifiées 0,5 ; table finale 0,25.

Exercice 2 — Processus et ressources (6 points)

1. (1 point)

Le **programme** est un seul fichier d'instructions, enregistré sur le disque.

Chaque lancement crée un **processus** : une exécution de ce programme, avec son propre PID, sa mémoire et son état. Un même programme a donc donné ici deux processus.

L'ordonnanceur choisit le processus exécuté.

Barème : Programme 0,25 ; processus et lien avec l'observation 0,5 ; ordonnanceur 0,25.

2. (1 point)

La suite (b) est impossible : un processus bloqué ne passe jamais directement à l'état élu. Quand l'événement attendu arrive, il redevient prêt ; c'est l'ordonnanceur qui l'élira plus tard.

Suite (a) : élu → bloqué quand le processus **demande une entrée-sortie** (lecture sur le disque, par exemple) ; bloqué → prêt quand **la donnée est disponible**.

Suite (c) : élu → prêt quand le processus est **interrompu par l'ordonnanceur** (fin du quantum, préemption).

Barème : Suite impossible et justification 0,5 ; événements de (a) 0,25 ; événement de (c) 0,25.

3. (1,5 point)

De 0 à 1 : P1 (seul arrivé). À l'instant 1, P2 arrive et passe avant P1 : file [P2, P1].

De 1 à 2 : P2. À l'instant 2, P3 arrive et passe avant P2 : file [P1, P3, P2].

De 2 à 3 : P1. File [P3, P2, P1].

De 3 à 4 : P3, qui se termine. File [P2, P1].

De 4 à 5 : P2, qui se termine. File [P1].

De 5 à 6 : P1, qui se termine.

Ordre : P1, P2, P1, P3, P2, P1.

Fins : P3 à t = 4 ; P2 à t = 5 ; P1 à t = 6.

Barème : Ordre d'exécution 0,75 (retirer 0,25 par erreur, sans descendre sous 0) ; instants de fin 0,75 (0,25 chacun).

4. (1 point)

De 0 à 3 : P1 s'exécute entièrement (durée 3) et se termine. Pendant ce temps, P2 puis P3 sont arrivés : file [P2, P3].

De 3 à 5 : P2, qui se termine.

De 5 à 6 : P3, qui se termine.

P3 finit à t = 6 au lieu de t = 4 : l'affirmation est fausse.

Avec un grand quantum, le tourniquet se comporte comme « premier arrivé, premier servi » : un processus court arrivé tard attend derrière les longs.

Barème : Simulation 0,5 ; conclusion 0,25 ; explication 0,25.

5. (0,5 point)

Si de nouveaux processus courts arrivent sans cesse, ils sont toujours élus avant le processus long, qui attend indéfiniment : c'est la **famine**.

Avec le tourniquet, chaque processus non terminé repart en fin de file : il finit toujours par revenir en tête et obtenir le processeur.

Barème : Famine expliquée 0,25 ; argument du tourniquet 0,25.

6. (1 point)

C'est un interblocage : P1 → R2 → P2 → R3 → P3 → R1 → P1.

P3 ne respecte pas la règle : il détient R3 et demande R1, de numéro plus petit.

Si tous respectent la règle, en suivant les flèches d'attente on rencontre des ressources de numéros de plus en plus grands : on ne peut jamais revenir à la ressource de départ, donc aucun cycle n'est possible.

Barème : Nom et cycle 0,5 ; processus fautif 0,25 ; explication 0,25.

Exercice 3 — Architecture et communication sécurisée (6 points)

1. (1 point)

Le **CPU** exécute le programme ; le **module Wi-Fi** envoie les mesures.

La mémoire vive est **intégrée à la puce** : on ne peut ni l'ajouter ni la remplacer.

Avantage, au choix : faible encombrement, faible consommation, échanges rapides entre blocs, coût réduit en grande série.

Barème : Deux blocs 0,5 ; limite expliquée 0,25 ; avantage 0,25.

2. (0,5 point)

Le thermostat ne connaît que le **nom** `collecte.example`. Pour envoyer des paquets, il lui faut l'**adresse IP** du serveur, que le DNS fournit à partir du nom : sans DNS, il ne sait pas où envoyer.

Il lui suffirait de connaître directement l'adresse IP du serveur.

Barème : Rôle du DNS 0,25 ; adresse IP 0,25.

3. (1 point)

Chiffrer toutes les données en asymétrique serait **beaucoup trop lent**.

Le chiffrement **asymétrique** sert seulement au début : transmettre en secret une **clé de session** et authentifier le serveur.

Le chiffrement **symétrique**, rapide, chiffre ensuite **toutes les données échangées** avec cette clé de session.

Barème : Lenteur 0,25 ; rôle de l'asymétrique 0,5 ; rôle du symétrique 0,25.

4. (1 point)

Le thermostat a chiffré la clé de session avec la **clé publique du serveur**.

Seule la **clé privée du serveur** permet de la déchiffrer.

Ève ne peut pas retrouver la clé de session : la clé publique, connue de tous, ne permet pas de déchiffrer, et elle ne possède pas la clé privée.

Barème : Clé de chiffrement 0,25 ; clé de déchiffrement 0,25 ; conclusion justifiée 0,5.

5. (1 point)

Le thermostat chiffrerait la clé de session avec la clé d'Ève : elle pourrait la déchiffrer, puis **lire et modifier toutes les mesures** en se faisant passer pour le serveur.

Le thermostat **vérifie la signature du certificat** par une autorité de certification de confiance, et vérifie qu'il correspond bien au nom `collecte.example`. Le faux certificat d'Ève n'est pas signé par une telle autorité : il est refusé.

Barème : Conséquence de l'attaque 0,5 ; vérification du certificat 0,5.

6. (1 point)

L'étape E est fausse : le thermostat chiffre la clé de session avec la **clé publique du serveur** (sinon le serveur ne pourrait pas la déchiffrer avec sa clé privée, et n'importe qui pourrait la déchiffrer).

Ordre : B, D, E, A, C.

Barème : Erreur repérée et corrigée 0,5 ; ordre 0,5 (0,25 si une seule inversion).

7. (0,5 point)

$2^{50} = 2^{40} \times 2^{10}$: il y a 2^{10} fois plus de clés.

$2^{10} \approx 10^3$: il faut environ 1 000 fois plus de temps.

Environ 1 000 heures, soit plus de 40 jours.

Ajouter 10 bits multiplie le temps de recherche par environ mille : c'est pourquoi on utilise des clés de 128 bits ou plus.

Barème : Rapport 0,25 ; ordre de grandeur 0,25.