MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

Liberté
Égalité
Fraternité

DIRECTION DES RESSOURCES HUMAINES

SOUS-DIRECTION DE L'ATTRACTIVITÉ ET DES RECRUTEMENTS

Bureau des concours et examens professionnels

Concours externe et interne pour le recrutement dans le grade d'attaché des systèmes d'information et de communication au titre de l'année 2026

Épreuve écrite d'admissibilité n°2

Mardi 17 février 2026

Réseaux et télécommunications

Durée totale de l'épreuve : 4 heures - Coefficient : 5
Toute note inférieure à 8 sur 20 est éliminatoire.

Épreuve technique portant sur l'option choisie par le candidat lors de l'inscription au concours :
Option « réseaux et télécommunications »

Ce dossier comporte 6 pages (page de garde et sommaire non compris)

Sommaire

Le sujet comporte 6 parties notées respectivement sur 3, 2, 2, 2, 3 et 6 points.

2 points seront réservés à la qualité de la copie (présentation, orthographe et la syntaxe).

Exercice 1 (3 points)

1. Quel est le rôle du routage dynamique ? Vous expliquerez les différences entre les protocoles de routage OSPF et BGP, et vous présenterez des cas d'usage actuels pour chacun d'eux.

2. Qu'est-ce qu'un réseau underlay et un réseau overlay ? Vous expliciterez l'usage de ces types de réseaux dans les infrastructures actuelles.

3. Qu'est-ce qu'un réseau de service opérateur ? Quels types de services y sont proposés ?

Exercice 2 (2 points)

1. Quels sont les principaux avantages des nouveaux réseaux satellitaires d'orbites basses (LEO) ?

2. Quelles sont les principales différences entre le VXLAN et le VLAN ?

3. QCM sur le protocole SIP :

   3.1. A quelle couche du modèle OSI appartient le protocole SIP ?

   a) Session
   b) Application
   c) Transport

   3.2. Quel est le port utilisé par le protocole SIP ?

   a) 5060
   b) 5061
   c) 5062

   3.3. Indiquez si les phrases suivantes sur le protocole SIP sont vraies ou fausses :

   a) Il permet d'établir des communications.
   b) Il permet de transporter les données des communications temps réel.
   c) Il permet de monter des tunnels chiffrés.

4. Quelle est la différence entre décrypter et déchiffrer une donnée ?

5. En quoi la journalisation est-elle un élément clé de la supervision et de la sécurité d'un système d'information, et quels types d'événements doivent être prioritairement journalisés ?

6. Donner une commande Linux permettant d'effectuer une recherche récursive d'une chaîne de caractère dans un dossier et ses sous-dossiers, en affichant les numéros de ligne et en ignorant la casse.

7. Qu'est-ce que le principe de défense en profondeur ?

8. A quoi font référence les acronymes PCA, PRA, PCI et PRI ?

Exercice 3 (2 points)

A partir de la capture Wireshark suivante, que pouvez-vous déduire de la tentative de connexion du client au serveur web portal.abcd.com ?

Expliquer d'où vient le problème et proposer une solution pour le résoudre.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.0.2.10	198.51.100.20	TCP	54	52360 → 443 [SYN] Seq=0 Win=64240 Len=0
2	0.020000	198.51.100.20	192.0.2.10	TCP	54	443 → 52360 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.040000	192.0.2.10	198.51.100.20	TCP	54	52360 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.080000	192.0.2.10	198.51.100.20	TLSv1	151	Client Hello (SNI=portal.abcd.com)
5	0.110000	198.51.100.20	192.0.2.10	TLSv1	61	Alert (Level: Fatal, Description: Protocol Version)
6	0.130001	192.0.2.10	198.51.100.20	TCP	54	52360 → 443 [RST, ACK] Seq=98 Ack=8 Win=64240 Len=0

```
> Frame 4: Packet, 151 bytes on wire (1208 bits), 151 bytes captured (1208 bits)
> Ethernet II, Src: MS-NLB-PhysServer-17_22:33:44:55 (02:11:22:33:44:55), Dst: 02:aa:bb:cc:dd:ee (02:aa:bb:cc:dd:ee)
> Internet Protocol Version 4, Src: 192.0.2.10, Dst: 198.51.100.20
v Transmission Control Protocol, Src Port: 52360, Dst Port: 443, Seq: 1, Ack: 1, Len: 97
    Source Port: 52360
    Destination Port: 443
    [Stream index: 0]
    [Stream Packet Number: 4]
  > [Conversation completeness: Complete, WITH_DATA (47)]
    [TCP Segment Len: 97]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 200001
    [Next Sequence Number: 98    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 990001
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x4e73 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
    TCP payload (97 bytes)
v Transport Layer Security
    [Stream index: 0]
  v TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 92
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 88
      > Version: TLS 1.2 (0x0303)
      > Random: 1a892cd0883713c2aaae1a5145acaa7d5300df2cc12303a1e534162f48400a95
        Session ID Length: 0
        Cipher Suites Length: 12
      > Cipher Suites (6 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 35
      > Extension: server_name (len=20) name=portal.abcd.com
      > Extension: supported_versions (len=7) TLS 1.3, TLS 1.2, TLS 1.1
        [JA4: t13d060200_9c75f1e755ed_b9a491fefe05]
        [JA4_r: t13d060200_002f,009c,009d,1301,1302,1303_002b]
        [JA3 Fullstring: 771,4865-4866-4867-156-157-47,0-43,,]
        [JA3: c6aa9ce16a7d178c54c18225b37d8130]
```

```
> Frame 5: Packet, 61 bytes on wire (488 bits), 61 bytes captured (488 bits)
> Ethernet II, Src: 02:aa:bb:cc:dd:ee (02:aa:bb:cc:dd:ee), Dst: MS-NLB-PhysServer-17_22:33:44:55 (02:11:22:33:44:55)
> Internet Protocol Version 4, Src: 198.51.100.20, Dst: 192.0.2.10
v Transmission Control Protocol, Src Port: 443, Dst Port: 52360, Seq: 1, Ack: 98, Len: 7
    Source Port: 443
    Destination Port: 52360
    [Stream index: 0]
    [Stream Packet Number: 5]
  > [Conversation completeness: Complete, WITH_DATA (47)]
    [TCP Segment Len: 7]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 990001
    [Next Sequence Number: 8    (relative sequence number)]
    Acknowledgment Number: 98    (relative ack number)
    Acknowledgment number (raw): 200098
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x7354 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [Timestamps]
  > [SEQ/ACK analysis]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
    TCP payload (7 bytes)
v Transport Layer Security
    [Stream index: 0]
  v TLSv1 Record Layer: Alert (Level: Fatal, Description: Protocol Version)
      Content Type: Alert (21)
      Version: TLS 1.0 (0x0301)
      Length: 2
    > Alert Message
```

Exercice 4 (2 points)

Un site institutionnel exposé sur internet subit un déni de service distribué (DDoS) de type « SYN flood » depuis des centaines de milliers d'adresses IP réparties dans le monde.

1. Expliquer en quoi consiste ce type d'attaque et la particularité de celle-ci.
2. Proposer des actions de mitigation ayant pour objectif de circonscrire cette attaque.
3. Proposer des mesures de remédiation pour se prémunir de futures attaques.
4. Expliquer les différences avec une attaque de type HTTP flood.

Exercice 5 (3 points)

1. Citer des algorithmes vulnérables à la puissance d'un ordinateur quantique.
2. Qu'est-ce que l'algorithme de Shor ?
3. Quels sont les enjeux principaux de la cryptographie post-quantique ?

Exercice 6 (6 points)

Vous êtes responsable informatique au sein d'un Centre régional d'assistance des systèmes d'information et de communication (CRASIC) dans une ambassade de France à l'étranger. Un projet de déménagement de l'ambassade, prévu dans un horizon de trois ans, est actuellement à l'étude.

Dans ce contexte, l'Ambassadeur vous demande de préparer une note identifiant les principaux éléments techniques, contraintes et prérequis à prendre en compte pour la conception et l'aménagement des futurs locaux, afin de garantir le bon fonctionnement des systèmes d'information et de communication.

L'ambassade compte environ 100 agents et assure des missions diplomatiques, consulaires et administratives nécessitant un haut niveau de disponibilité, de sécurité et de confidentialité.

La note que vous rédigerez sera accompagnée d'un macro-planning et devra notamment prendre en compte :

- Les principaux enjeux techniques liés au déménagement ;
- Les prérequis à anticiper pour les futurs locaux ;
- Les mesures permettant d'assurer la sécurité, la disponibilité et la continuité des services.

Une attention particulière doit être portée sur les points suivants :

- Couverture Wi-Fi complète et sécurisée de l'ensemble de l'ambassade, y compris sur plusieurs étages ;
- Gestion et protection des informations classifiées, conformément aux exigences de sécurité ;
- Locaux techniques dédiés, sécurisés et adaptés aux contraintes climatiques, notamment en cas de fortes chaleurs ;
- Maintien des moyens de communication sécurisés avec la Centrale pendant toute la durée du déménagement ;
- Continuité des services et des moyens de communication en cas de coupure d'alimentation électrique.

A noter que des missions de renfort de la Centrale pour le déménagement et l'accompagnement technique pourront être sollicitées.