+1/1/60+

R203 — Contrôle

Avant de commencer, lisez les consignes sur la feuille de réponse (la dernière).

Rappels : Codes d'options DHCP courantes (en *décimal*)

- 1 — *Subnet Mask*
- 3 — *Router*
- 6 — *Domain Name Server*
- 15 — *Domain Name* (nom du domaine de l'hôte)
- 42 — *NTP Servers*
- 50 — *Requested IP address* (IP demandée)
- 51 — *IP Address Lease time* (durée de bail en sec.)
- 53 — *Message type*
  1 = DISCOVER 5 = ACK
  2 = OFFER 6 = NAK
  3 = REQUEST 7 = RELEASE
- 54 — *DHCP Server identifier*
- 55 — *Parameter Request List*
- 255 — *End*

Exercice 1 — Questions générales (12 points)

Q. 1 Sur quel port un *serveur SSH* écoute-t-il, par défaut ?

[A] 80 [B] 67 [C] 443 [D] 20 [E] 68 [F] 22

Q. 2 Quelle peut être l'utilité de l'outil *rsync* ?

[A] se connecter sur un hôte distant (sans chiffrement)
[B] chiffrer le contenu d'un fichier
[C] synchroniser les horloges d'un réseau
[D] synchroniser les contenus de fichiers/répertoires
[E] ARNC

Q. 3 Dans le protocole HTTP quel code de réponse indique une erreur du client (p.ex., accès non autorisé) ?

[A] 6xx [B] 2xx [C] 3xx [D] 1xx [E] 5xx [F] 4xx

Q. 4 Quel(s) protocole(s) (TCP et/ou UDP) permet(ttent) de détecter certaines erreurs de transmission (erreur binaire) ?

[A] TCP seulement [B] UDP seulement [C] aucun des deux [D] les deux

Q. 5 Quel organisme international gère l'attribution des numéros de port aux applications et services ?

[A] IEEE [B] OSI [C] UIT [D] ISO [E] IETF [F] IANA

Q. 6 Quel est le nom du service utilisé pour envoyer des messages électroniques ?

[A] POP [B] SMTP [C] SENDP [D] MSP [E] NTP [F] NFS [G] IMAP

Q. 7 Quel champ d'en-tête HTTP est devenu obligatoire dans toute requête avec la version 1.1 ?

[A] Date [B] Host [C] User-Agent [D] Referer [E] Version [F] Server

Q. 8 Quel(s) protocole(s) (TCP et/ou UDP) inclu(en)t une fonction de contrôle de flux (pour éviter la congestion) ?

[A] UDP seulement [B] aucun des deux [C] TCP seulement [D] les deux

Q. 9 Quel protocole de transport est-il préférable d'utiliser pour des applications de transfert de fichiers (p.ex., HTTP) ?

[A] TCP [B] peu importe [C] DDP [D] UDP

Q. 10 Sur quel port un *serveur DHCP* écoute-t-il, par défaut ?

[A] 20 [B] 68 [C] 80 [D] 22 [E] 443 [F] 67

Q. 11 Quel(s) protocole(s) (TCP et/ou UDP) inclu(en)t une fonction de chiffrement des données ?

[A] aucun des deux [B] les deux [C] UDP seulement [D] TCP seulement

Q. 12 Comment appelle-t-on un port utilisé par un client web (p.ex., firefox) pour contacter un serveur ?

[A] well-known [B] éphémère [C] client [D] registered [E] statique

Exercice 2 — Chiffrement et SSH (9 points)

Q. 13 Dans SSH, de quel type une clé de session est-elle ?

A symétrique B de n'importe quel type C asymétrique/publique D asymétrique/privée

Q. 14 Alice a un compte sur la machine de Bob (1.2.3.4) et dans son répertoire personnel sur cette machine, elle a un fichier nommé `fic`. Elle est actuellement connectée sur sa machine en tant qu'utilisateur alice. Quelle commande peut-elle exécuter pour copier le fichier `fic` dans le répertoire `/tmp` de sa machine ?

A `cd tmp ; scp 1.2.3.4:fic`
B `scp 1.2.3.4@fic /tmp`
C `ssh 1.2.3.4 cp fic /tmp`
D `scp fic@1.2.3.4 /tmp`
E `scp /tmp 1.2.3.4:fic`
F `scp 1.2.3.4:fic /tmp`
G ARNC

Q. 15 Alice est connectée sur sa machine en tant qu'utilisateur alice. Quelle commande peut-elle exécuter pour ouvrir une session SSH en tant qu'utilisateur *root* sur la machine de Bob (1.2.3.4) ?

A `ssh root 1.2.3.4`
B `ssh 1.2.3.4@root`
C `ssh @1.2.3.4`
D `ssh 1.2.3.4:root`
E `ssh 1.2.3.4`
F `/etc/init.d/sshd root@1.2.3.4`
G ARNC

Q. 16 Quel(s) type(s) d'algorithme(s) de chiffrement est (sont) utilisé(s) dans SSH ?

A asymétrique uniquement
B symétrique uniquement
C symétrique puis asymétrique
D asymétrique puis symétrique

Q. 17 A ouvre une connexion SSH chez B (10.0.0.1). On note X le fichier des hôtes connus par A et K la clé reçue par A à la connexion. Dans quelle situation ssh préviendra-t-il qu'une attaque *man-in-the-middle* est peut-être en cours ?

A si K est associée à une autre IP ($\neq$ de 10.0.0.1) dans X
B si K n'est pas la clé associée à 10.0.0.1 dans X
C si l'IP 10.0.0.1 n'apparaît pas dans X
D ARNC

Q. 18 Pour éviter d'avoir à saisir son mot de passe à chaque fois qu'elle ouvre une session SSH chez Bob, Alice met en place une authentification par clé. Ses clés publique et privée sont respectivement K_A^U et K_A^R. Les clés publique et privée de Bob sont respectivement K_B^U et K_B^R. Que doit-elle faire ? (Dans les réponses `A` est le fichier `authorized_keys`.)

A copier K_B^R dans `A` sur sa machine
B copier K_A^U dans `A` sur la machine de Bob
C copier K_B^U dans `A` sur sa machine
D copier K_A^R dans `A` sur la machine de Bob

Q. 19 Alice est connectée sur sa machine en tant qu'utilisateur alice. Quelle commande peut-elle exécuter pour ouvrir une session SSH en tant qu'utilisateur *alice* sur la machine de Bob (1.2.3.4) ?

A `ssh 1.2.3.4`
B `ssh 1.2.3.4:alice`
C `/etc/init.d/sshd 1.2.3.4`
D `ssh @1.2.3.4`
E `ssh alice 1.2.3.4`
F `ssh 1.2.3.4@alice`
G ARNC

Q. 20 Vous voulez envoyer un message chiffré à Anna en utilisant un chiffrement asymétrique. Avec quelle(s) clé(s) allez vous chiffrer votre message ?

A la clé privée d'Anna
B votre clé privée + la clé publique d'Anna
C votre clé publique
D la clé publique d'Anna

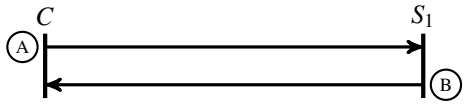
Q. 21 Alice est connectée sur sa machine en tant qu'utilisateur alice. Quelle commande peut-elle exécuter pour afficher le contenu du répertoire `/tmp/` se trouvant sur la machine de Bob (1.2.3.4) ?

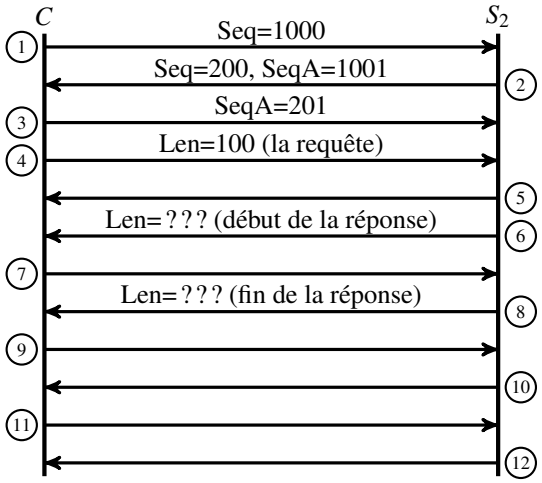
A `ssh 1.2.3.4:/tmp/`
B `scp 1.2.3.4:/tmp .`
C `ssh 1.2.3.4 ls /tmp/`
D `scp 1.2.3.4:/tmp/`
E `ssh 1.2.3.4 | ls /tmp`
F `scp 1.2.3.4 ls /tmp/`
G ARNC

Exercice 3 — Scénario TCP (10 points)

On considère dans cet exercice un processus C qui s'adresse successivement à deux serveurs TCP S_1 et S_2. Le premier lui refuse la connexion, et le second accepte. Dans son échange avec S_2, C envoie une requête de 100 octets à laquelle S_2 répond par 1470 octets de données. S_2 met ensuite fin à la connexion.

Voici les chronogrammes retraçant les échanges entre C et S_1 (à gauche) et entre C et S_2 (à droite).





Les paquets contenant les données (requête et réponse) sont les paquets 4, 6 et 8. Les autres paquets servent uniquement à contrôler l'échange (connexion, déconnexion, ...). On rappelle que :

— *Seq* = numéro de séquence d'envoi, *SeqA* = numéro de séquence d'acquittement ;
— en-tête IP = 20 octets, en-tête TCP = 20 octets, en-tête UDP = 8 octets, et en-tête + FCS ethernet = 26 octets ;
— une trame Ethernet ne peut pas encapsuler plus de 1 500 octets.

Q. 22 Parmi ceux-ci, quel bit de l'en-tête TCP est activé (i.e., vaut 1) dans les *paquets A et 1* ?

A ACK B PSH C FIN D URG E SYN F RST

Q. 23 Parmi ceux-ci, quel bit de l'en-tête TCP est activé dans le *paquet 10* ?

A SYN B RST C PSH D URG E FIN

Q. 24 Parmi ceux-ci, quel bit de l'en-tête TCP est activé dans le *paquet B* ?

A SYN B URG C RST D PSH E FIN

Q. 25 Parmi ceux-ci, quel bit de l'en-tête TCP est activé dans le *paquet 5* ?

A PSH B URG C RST D SYN E ACK F FIN

Q. 26 Que vaut le champ *Seq* dans le *paquet 4* ?

A 1001 C 1100 E 201 G 1101
B 1202 D 1000 F 301 H ARNC

Q. 27 Que vaut le champ *SeqA* dans le *paquet 5* ?

A 1101 C 1002 E 301 G 201
B 1100 D 1202 F 1000 H ARNC

Q. 28 Que vaut le champ *Seq* dans le *paquet 6* ?

A 1002 C 1002 E 1000 G 201
B 301 D 1202 F 201 H ARNC

Q. 29 Que vaut le champ *Seq* dans le *paquet 8* ?

A 1470 C 1671 E 1002 G 201
B 1661 D 202 F 1701 H ARNC

Q. 30 Que vaut le champ *SeqA* dans le *paquet 9* ?

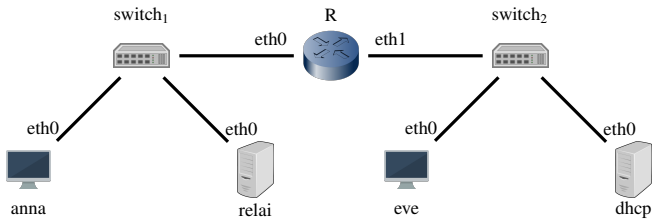
A 1471 C 203 E 1672 G 1003
B 202 D 3 F 1002 H ARNC

Q. 31 Combien de paquets auraient été échangés entre C et S_2 s'ils avaient utilisé UDP au lieu de TCP pour le transport ?

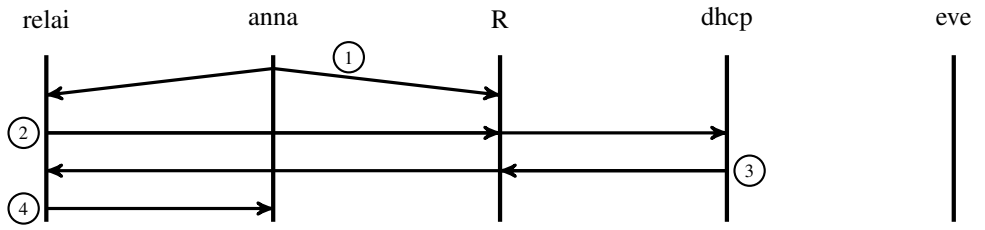
A 7 B 4 C 2 D 5 E 6 F 3 G plus de 7

Exercice 4 — Demande de bail DHCP (11 points)

On considère dans cet exercice le réseau de la figure ci-contre. Ce réseau est décomposé en deux sous-réseaux interconnectés par un routeur R. L'hôte relai est un relai DHCP pour son sous-réseau et l'hôte dhcp et un serveur DHCP pour tout le réseau. Les hôtes anna et eve sont configurées dynamiquement.



Anna demande un bail. On capture alors les messages DHCP ci-dessous. Seul le début de l'échange est représenté.



Voici les options (en hexadécimal) inclues dans le message 1 :

```
35 01 01 33 01 06 37 03 2a 0f 01 ff
```

Voici les options (en hexadécimal) inclues dans le message 3 :

```
35 01 02 33 01 03 36 04 0f 01 00 20 01 04 ff ff f0 00 2a 04 0f 01 06 2a ff
```

Q. 32 Quelle commande permet de demander un bail pour l'interface eth0 ?

A `dhcpd eth0` B `dhcp eth0` C `dhclient eth0` D `dhup eth0` E ARNC

Q. 33 Sur le relai, est-il nécessaire d'ajouter une route, et si oui avec quelle commande ?

A oui : `ip route add default via @R(eth1)`
B oui : `ip route add default via @dhcp(eth0)`
C oui : `ip route add default via @R(eth0)`
D oui : `ip route add default via @relai(eth0)`
E non : cette route lui est fournie par le DHCP

Q. 34 Quel est le type DHCP du message 2 ?

A NAK B ACK C DISCOVER D RELEASE E OFFER F REQUEST

Q. 35 Que vaut le champ *hops* du message DHCP dans le paquet 2 ?

A `03` B `04` C `00` D `02` E `01` F ARNC

Q. 36 Quelle adresse IP apparaît dans le champ *giaddr* (gateway internet address) du message DHCP dans le paquet 2 ?

A 0.0.0.0
B celle de dhcp(eth0)
C celle de R(eth0)
D celle de relai(eth0)
E celle de R(eth1)
F ARNC

Q. 37 Anna a-t-elle demandé une durée de bail particulière ?

A oui : 22 s. B non C oui : 16 s. D oui : 106 s. E oui : 6 s. F oui : 261 s.

Q. 38 À part une IP, combien d'informations (p.ex., un routeur, un serveur DNS) Anna a-t-elle demandé au serveur ?

A 3 B 4 C 6 D 1 E 5 F 2

Q. 39 Parmi celles-ci, laquelle Anna a-t-elle effectivement demandé au serveur ?

A un serveur DNS B un serveur NTP C une adresse de diffusion D un routeur

Q. 40 Quel est le masque du réseau d'Anna ?

A /12 B /24 C /10 D /20 E /8 F /16 G /14 H /18

Q. 41 Quel est l'IP du serveur DHCP ?

A 4.15.1.0 B 15.1.6.32 C 15.1.0.20 D 1.0.32.1 E 15.1.6.42 F 15.1.0.32

Q. 42 Quel autre IP a été fournie à Anna ?

A une adr. de diffusion : 1.4.255.255
B un routeur : 36.4.15.1
C un serveur DNS : 4.15.1.6
D un routeur : 54.4.15.1
E un serveur NTP : 15.1.6.42

Feuille de réponses

- Le barème est sur 42 points (42 questions, 1 point par question).
- Le sigle ARNC qui est proposé pour certaines questions en dernier choix signifie *Aucune des Réponses précédentes Ne Convient.*
- Il n'y a pas de points négatifs (i.e., pas de malus si vous vous trompez).
- Pour toutes les questions il y a une et une seule réponse correcte (il n'y donc aucune question pour laquelle il faut remplir plusieurs cases).
- Si vous vous trompez de case, plutôt que de raturer, écrivez la lettre que vous pensez être la bonne réponse à côté du numéro de la question.
- Utilisez un stylo bille (ou un stylo plume), mais pas de crayon de papier ni de feutre.
- Remplissez au stylo bille la case que vous pensez être la bonne réponse, mais ne faites pas de croix et n'entourez pas la case.

Prénom et nom :

Q. 1 [A] [B] [C] [D] [E] [F]
Q. 2 [A] [B] [C] [D] [E]
Q. 3 [A] [B] [C] [D] [E] [F]
Q. 4 [A] [B] [C] [D]
Q. 5 [A] [B] [C] [D] [E] [F]
Q. 6 [A] [B] [C] [D] [E] [F] [G]
Q. 7 [A] [B] [C] [D] [E] [F]
Q. 8 [A] [B] [C] [D]
Q. 9 [A] [B] [C] [D]
Q. 10 [A] [B] [C] [D] [E] [F]
Q. 11 [A] [B] [C] [D]
Q. 12 [A] [B] [C] [D] [E]
Q. 13 [A] [B] [C] [D]
Q. 14 [A] [B] [C] [D] [E] [F] [G]
Q. 15 [A] [B] [C] [D] [E] [F] [G]
Q. 16 [A] [B] [C] [D]
Q. 17 [A] [B] [C] [D]
Q. 18 [A] [B] [C] [D]
Q. 19 [A] [B] [C] [D] [E] [F] [G]
Q. 20 [A] [B] [C] [D]
Q. 21 [A] [B] [C] [D] [E] [F] [G]
Q. 22 [A] [B] [C] [D] [E] [F]
Q. 23 [A] [B] [C] [D] [E]
Q. 24 [A] [B] [C] [D] [E]
Q. 25 [A] [B] [C] [D] [E] [F]
Q. 26 [A] [B] [C] [D] [E] [F] [G] [H]
Q. 27 [A] [B] [C] [D] [E] [F] [G] [H]
Q. 28 [A] [B] [C] [D] [E] [F] [G] [H]
Q. 29 [A] [B] [C] [D] [E] [F] [G] [H]
Q. 30 [A] [B] [C] [D] [E] [F] [G] [H]
Q. 31 [A] [B] [C] [D] [E] [F] [G]
Q. 32 [A] [B] [C] [D] [E]
Q. 33 [A] [B] [C] [D] [E]
Q. 34 [A] [B] [C] [D] [E] [F]
Q. 35 [A] [B] [C] [D] [E] [F]
Q. 36 [A] [B] [C] [D] [E] [F]
Q. 37 [A] [B] [C] [D] [E] [F]
Q. 38 [A] [B] [C] [D] [E] [F]
Q. 39 [A] [B] [C] [D]
Q. 40 [A] [B] [C] [D] [E] [F] [G] [H]
Q. 41 [A] [B] [C] [D] [E] [F]
Q. 42 [A] [B] [C] [D] [E]