NET2 - session 1

Statut	Terminée
Commencé	lundi 23 juin 2025, 09:00
Terminé	lundi 23 juin 2025, 09:31
Durée	31 min 32 s

Question 1
Correct
Noté sur 3,00
Marquer la question

Partagez le réseau IPv4 **88.77.66.0/24** en quatre sous-réseaux disjoints de tailles égales.

Réponse : (régime de pénalités : 0 %)

Réinitialiser la réponse

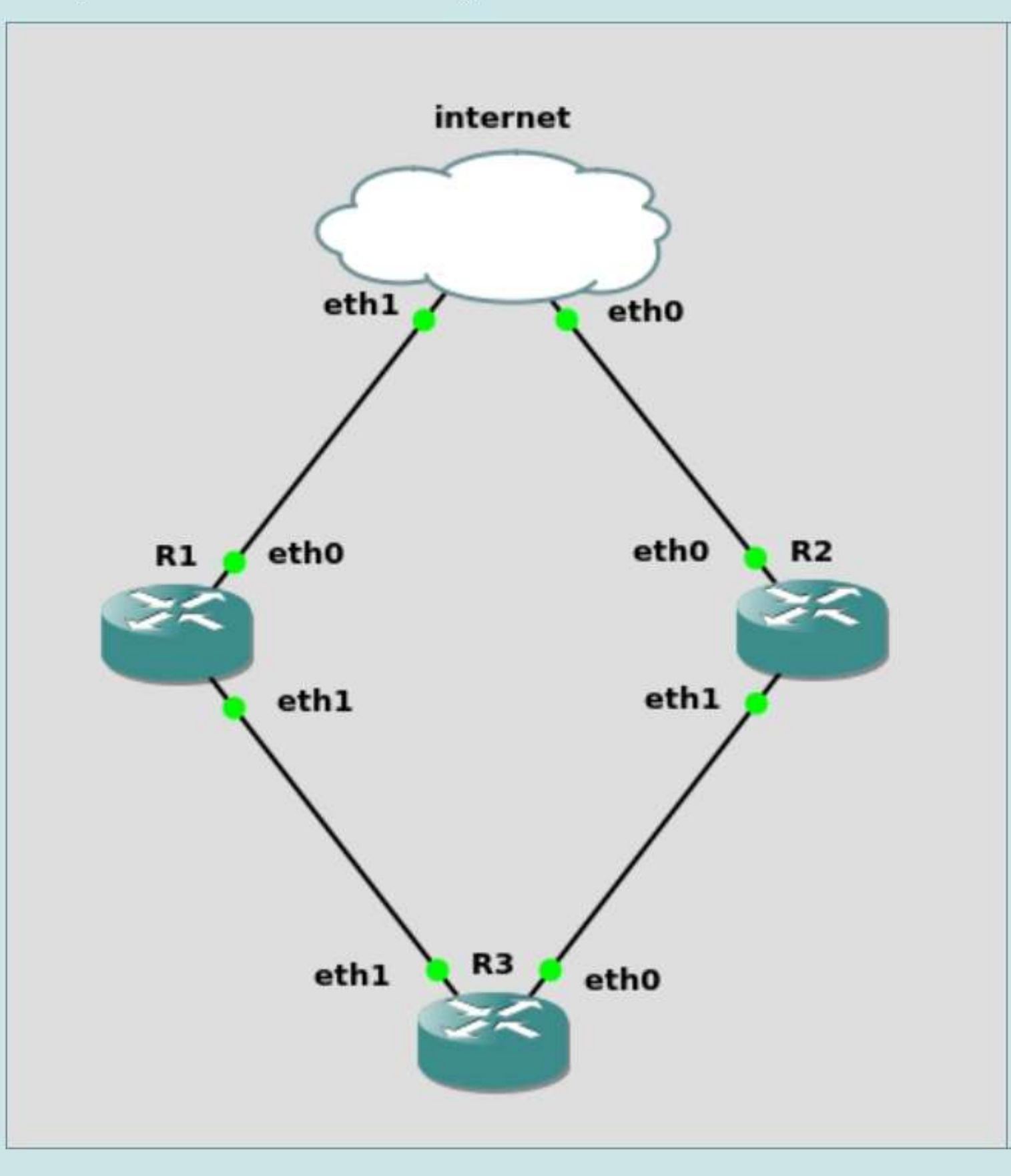
```
réseau 1: 88.77.66.0/26
réseau 2: 88.77.66.64/26
réseau 3: 88.77.66.128/26
réseau 4: 88.77.66.192/26
```

	Test	Résultat attendu	Résultat obtenu	
	`print(bool(nets and all(subnet_of(n, target) for n in nets)))`	True	True	
	`print(overlap(nets))`	6	6	
	`print(tuple(sorted(n.prefixlen for n in nets)))`	(26, 26, 26, 26)	(26, 26, 26, 26)	

Tous les tests ont été réussis !

Question 2
Terminé
Noté sur 2,00
Marquer la question

Compléter les tables de routage des différentes machines du réseau ci-dessous.



- **R1:**
  default via 2025::1
  2025::/64 dev eth 0 src 2025::1:2:3 ::2
  2025:1:2:3::/64 dev eth1 src 2025:1:2:3::1
- **R2:**
  default via 2026::1
  2026::/64 dev eth0 src 2025::1:2:3 ::2
  2026:4:5:6::/64 dev eth1 src 2026:4:5:6::1
- **R3:**
  default via 2025::1:2:3::1 dev eth1
  2025:1:2:3::/64 dev eth1 src 2025:1:2:3::2
  2026:4:5:6::/64 dev eth0 src 2026:4:5:6::2

Question 3
Terminé
Noté sur 4,00
Marquer la question

Ordonnez les couches réseau utilisées dans la consultation d'une page web (attention celle-ci utilise un VPN).

HTTP
UDP
VPN
IP (fourni par VPN)
TLS
TCP
IP
ETHERNET

Question 4
Terminé
Noté sur 4,00
Marquer la question

Nous avons vu que le DNS est un système de gestion d'enregistrements, qui sont des paires (clef, valeur), la clef étant un nom de domaine, et la valeur associée possède un type, par exemple type A pour une valeur IPv4.

Voici une requête DNS, effectuée avec dig.

```
$ dig -t PTR 35.202.240.157.in-addr.arpa

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> -t PTR 35.202.240.157.in-addr.arpa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23477
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;35.202.240.157.in-addr.arpa.   IN  PTR

;; ANSWER SECTION:
35.202.240.157.in-addr.arpa. 2365 IN    PTR edge-star-mini-shv-02-cdg4.facebook.com.
```

La requête demande une entrée de type:

● ARPA
○ PTR
○ CNAME
○ MX
○ AAAA
○ IN
○ A

La clef demandée est le nom de domaine (FQDN): facebook.com

Le domaine de premier niveau (*Top Level Domain, TLD*) est: facebook.com

La valeur obtenue en réponse est : edge-star-mini-shv-02-cdg4.facebook.com

Question 5
Terminé
Noté sur 5,00
Marquer la question

Voici ci-dessous le résultat de l'analyse d'un certificat, avec la commande **openssl**.

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number:
           7c:81:5a:6c:c1:6a:f4:6c:ed:3b:ca:c1:a5:fa:77:b6
       Signature Algorithm: sha384WithRSAEncryption
       Issuer: C = NL, O = GEANT Vereniging, CN = GEANT OV RSA CA 4
       Validity
           Not Before: Sep 18 00:00:00 2024 GMT
           Not After : Sep 18 13:59:59 2025 GMT
       Subject: C = FR, ST = Yvelines, O = INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE, CN = www.loria.fr
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
               Public-Key: (2048 bit)
               Modulus:
                   00:b4:bc:2b:5c:5a:77:e6:b2:c1:50:5e:be:4a:ec:
                   3b:70:ad:d6:43:2e:f5:45:78:87:74:bb:54:57:ce:
                   ef:95:1b:96:13:b1:fa:06:b7:eb:ec:43:00:7e:3e:
                   49:b2:51:a9:71:b2:67:16:1f:3f:5b:eb:b8:4d:0b:
                   98:97:d0:72:ae:e5:b3:56:b6:58:27:eb:f0:15:9b:
                   de:5b:55:33:0e:55:44:68:02:46:83:1c:6d:34:1c:
                   17:43:95:f8:64:8d:af:64:36:54:3b:b5:04:f0:a4:
                   10:da:2d:25:25:93:3a:de:19:4c:04:90:00:f1:e6:
                   db:24:63:4c:dd:33:74:2b:99:d5:d1:4c:53:7d:bd:
                   8d:dc:7f:02:7a:6b:cf:2f:cd:66:5f:2a:d1:0f:a0:
                   97:02:45:86:57:8a:e5:da:08:53:0f:7e:47:a2:ba:
                   7a:d2:a2:c2:82:8a:b1:7c:e0:29:0c:05:fc:f3:af:
                   42:84:62:61:d8:43:56:d6:94:0d:fb:3e:42:3a:00:
                   a1:90:41:8f:30:8e:7c:ea:d3:0b:14:eb:48:89:a3:
                   8d:68:99:33:6d:bd:9b:a4:44:72:d2:66:71:7d:87:
                   68:2d:13:cb:de:cc:eb:d2:f5:08:ec:b8:fc:29:05:
                   32:9b:0a:48:b9:90:5a:4e:22:47:4b:4c:63:50:a6:
                   d8:fb
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Authority Key Identifier:
               6F:1D:35:49:10:6C:32:FA:59:A0:9E:BC:8A:E8:1F:95:BE:71:7A:0C
           X509v3 Subject Key Identifier:
               5C:4C:BD:37:9F:2D:FB:66:08:71:8E:A4:7A:59:74:EC:D7:AC:B1:94
           X509v3 Key Usage: critical
               Digital Signature, Key Encipherment
           X509v3 Basic Constraints: critical
               CA:FALSE
           X509v3 Extended Key Usage:
               TLS Web Server Authentication, TLS Web Client Authentication
           X509v3 Certificate Policies:
               Policy: 1.3.6.1.4.1.6449.1.2.2.79
                 CPS: https://sectigo.com/CPS
               Policy: 2.23.140.1.2.2
           X509v3 CRL Distribution Points:
               Full Name:
                 URI:http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl
           Authority Information Access:
               CA Issuers - URI:http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt
               OCSP - URI:http://GEANT.ocsp.sectigo.com
           CT Precertificate SCTs:
               Signed Certificate Timestamp:
                   Version   : v1 (0x0)
                   Log ID    : DD:DC:CA:34:95:D7:E1:16:05:E7:95:32:FA:C7:9F:F8:
                               3D:1C:50:DF:DB:00:3A:14:12:76:0A:2C:AC:BB:C8:2A
                   Timestamp : Sep 18 02:26:54.432 2024 GMT
                   Extensions: none
                   Signature : ecdsa-with-SHA256
                               30:45:02:20:78:7C:1E:A0:44:BC:2A:48:27:58:27:BB:
                               B1:51:CF:4E:08:5F:1E:03:C5:75:1F:31:85:EE:8D:BC:
                               FB:9C:1E:79:02:21:00:C7:A4:A8:9B:C3:32:5A:20:C1:
                               65:C1:24:71:F0:78:23:00:E2:7C:47:38:A8:53:29:A0:
                               A9:53:CA:51:65:FE:9C
               Signed Certificate Timestamp:
                   Version   : v1 (0x0)
                   Log ID    : 0D:E1:F2:30:2B:D3:0D:C1:40:62:12:09:EA:55:2E:FC:
                               47:74:7C:B1:D7:E9:30:EF:0E:42:1E:B4:7E:4E:AA:34
                   Timestamp : Sep 18 02:26:54.328 2024 GMT
                   Extensions: none
                   Signature : ecdsa-with-SHA256
                               30:44:02:20:44:CC:19:82:34:F5:57:47:B6:1D:42:70:
                               1F:9C:D6:D3:85:04:86:79:C1:26:A6:53:A5:2A:01:64:
                               AD:4C:6C:7C:02:20:0D:F3:11:6B:58:07:E2:F9:9A:94:
                               CD:B5:54:0C:92:0D:8E:CD:23:E1:92:47:FC:12:73:EF:
                               4D:2E:7D:57:3D:09
               Signed Certificate Timestamp:
                   Version   : v1 (0x0)
                   Log ID    : 12:F1:4E:34:BD:53:72:4C:84:06:19:C3:8F:3F:7A:13:
                               F8:E7:B5:62:87:88:9C:6D:30:05:84:EB:E5:86:26:3A
                   Timestamp : Sep 18 02:26:54.327 2024 GMT
                   Extensions: none
                   Signature : ecdsa-with-SHA256
                               30:45:02:20:69:75:50:85:AA:C5:09:F7:99:85:76:94:
                               52:70:5D:0E:42:6D:BA:2B:B9:A3:43:2C:5F:38:00:70:
                               55:E2:58:06:02:21:00:B4:E1:16:D1:40:E8:51:13:57:
                               DB:86:16:0C:86:CE:BF:89:91:48:05:B3:1D:48:BD:0D:
                               69:37:F5:12:80:91:61
           X509v3 Subject Alternative Name:
               DNS:www.loria.fr, DNS:www-dev.loria.fr, DNS:www-qualif.loria.fr
   Signature Algorithm: sha384WithRSAEncryption
   Signature Value:
       13:12:53:a7:b6:a1:7f:f5:0a:7a:dd:48:ba:db:05:c9:0f:a4:
```

[…]

Donner le nom de domaine principal qui est authentifié par ce certificat
www.loria.fr

Donner un autre nom de domaine qui est authentifié par ce certificat
www-dev.loria.fr

Donner la date d'expiration du certificat.(Format: DD/MM/YYYY)
18/09/2025

L'algorithme utilisé pour signer ce certificat est:
RSA with SHA, 384bit ⬍

La clé publique contenue dans ce certificat est de type
ECDSA RSA, 2048 bit ⬍

Question 6
Non répondue
Noté sur 2,00
Marquer la question

Considérez la requête HTTPS suivante réalisée à la main depuis un ordinateur distant auquel on se connecte via SSH:

```
$ ssh myuser@XXX -L  YYY:ZZZ:TTT   openssl s_client -connect localhost:7777  -servername monipv6.org
GET / HTTP/1.1
[…]
                <h2>Connecté en IPv4</h2>
                <h3><img src="//www-cache6.stuxnet.org/monipv6-static/images/geoloc/ru.gif" alt="Russian Federation
                <p>smtp.lrde.epita.fr</p>
```

Ce site web est utilisé par les développeurs pour obtenir leur propre adresse IP. Concluez sur la commande SSH qui a très probablement été exécutée en début de ligne.

ssh myuser@ ______ -R ______ : ______ : ______

Terminer la relecture