Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

DIRECTION GENERALE DE L'ADMINISTRATION
ET DE LA MODERNISATION

DIRECTION DES RESSOURCES HUMAINES

Sous-direction de la Formation et des Concours

Bureau des concours et examens professionnels
RH4B

CONCOURS INTERNE ET EXTERNE POUR L'ACCES A L'EMPLOI D'ATTACHE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION AU TITRE DE L'ANNEE 2019

EPREUVES ECRITES D'ADMISSIBILITE – 20 ET 21 FEVRIER 2019

EPREUVE TECHNIQUE PORTANT SUR L'OPTION CHOISIE PAR LE CANDIDAT LORS DE L'INSCRIPTION

OPTION : RESEAUX ET TELECOMMUNICATIONS

Durée : 4 heures
Coefficient : 5
Toute note inférieure à 8 sur 20 est éliminatoire.

SUJET

Voir pages suivantes.

Ce dossier comporte 13 pages (page de garde non comprise).

Partie 1 (6 POINTS)

1. Identifier et décrire succinctement les normes suivantes, définie par l'IEEE : 802.11, 802.15, 802.16

2. Rappeler les 4 premières couches du modèle OSI. Détailler leur fonction ainsi que le type de message associé (ou « Protocol Data Unit »).

3. Expliciter les acronymes des protocoles suivants, et indiquer à quoi ils servent :
   - ARP
   - DNS
   - SFTP
   - NTP

4. Une entreprise dispose du réseau suivant : 192.168.1.0/24. Il est demandé au département réseau de préparer 2 sous-réseaux d'au plus 60 machines et 1 sous-réseau d'au plus 124 machines.

   Donner le découpage à appliquer en indiquant pour chaque sous-réseau : Adresse de réseau, masque, adresse de diffusion, nombre d'hôte

5. Définissez les sigles IDS et IPS, puis explicitez et comparer ces deux systèmes

6. Quelles sont les deux types de requête DNS que l'on peut faire ? Les définir.

7. Définissez le protocole DHCP et expliciter les échanges entre une station souhaitant obtenir une adresse IP et un serveur DHCP.
   Comment une station choisi entre 2 serveurs DHCP ?
   Qu'est-ce que le DHCP spoofing ? Comment s'en prémunir ?

8. On considère la trace suivante, obtenue par l'analyseur de protocoles Ethereal installé sur la machine émettrice de la première trame Ethernet (les trames sont données sans préambule, ni CRC) :

```
Frame Number : 1
0000 00 0a b7 a3 4a 00 00 01 02 6f 5e 9b 08 00 45 00
0010 00 28 00 00 40 00 40 01 82 ae 84 00 00 01 c2 00
0020 00 01 08 00 75 da 9c 7a 00 00 d4 45 a6 3a 62 2a
0030 09 00 ff ff ff ff 00 00 00 00 00 00

Frame Number : 2
0000 00 01 02 6f 5e 9b 00 0a b7 a3 4a 00 08 00 45 00
0010 00 28 d0 92 00 00 3a 01 5a db c2 00 00 01 84 00
0020 00 01 00 00 7d da 9c 7a 00 00 d4 45 a6 3a 62 2a
0030 09 00 ff ff ff ff 00 00 00 00 00 00
```

a) Quelle est l'adresse IP (en décimal pointé) de la machine ayant initié l'échange ? Quelle est sa classe d'adresse ?

b) Quelle est « l'adresse physique » de la machine ayant initié l'échange ?
c) Quelle est l'adresse IP (en décimal pointé) de la machine ayant répondu ? Quelle est sa classe d'adresse ?
d) Quelle est « l'adresse physique » de la machine ayant répondu ?
e) En supposant que la route de retour coïncide avec la route de l'aller, combien de routeurs séparent la machine source de la machine destination ?
f) Expliquez pourquoi dans les deux trames, la fin du paquet ne coïncide pas avec la fin de la trame ?
g) D'après vous, quel genre d'application, de programme ou de commande a pu générer cet échange sur le réseau ?

Partie 2 (7 POINTS)

Responsable réseau au sein d'une entreprise disposant de quatre sites, on vous signale un dysfonctionnement entre les agences A, B, C et D. Les caractéristiques de celles-ci sont données ci-dessous.

Le site A dispose :

- d'un LAN A1 192.168.0.0/24,

Le site B dispose :

- d'un LAN B1 192.168.3.0/24
- d'un LAN B2 192.168.4.0/24

Le site C dispose :

- d'un LAN C1 192.168.5.0/24

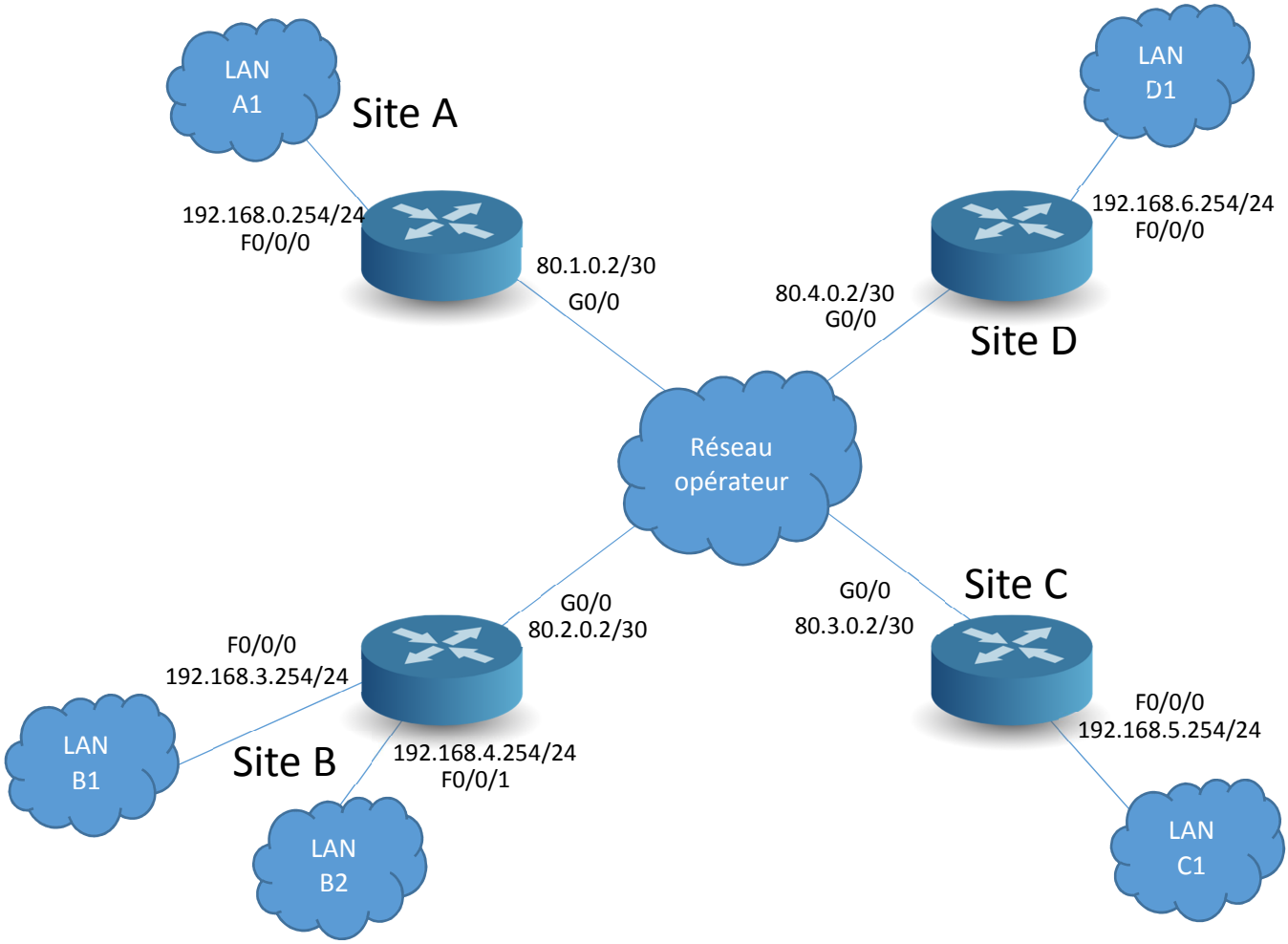
Le site D dispose :

- d'un LAN D1 192.168.6.0/24

Les règles sur les flux sont les suivantes :

- A1 peut dialoguer avec B1, C1 et D1
- B1 peut dialoguer avec A1 et C1
- B2 peut dialoguer avec C1
- C1 peut dialoguer avec A1, B1 et B2
- D1 peut dialoguer avec A1

Vous n'avez pas la main sur le réseau WAN opérer par un tiers. Des tunnels GRE ont été mis en place pour répondre aux besoins (pour simplifier l'exercice, il n'y a pas de chiffrement). Pour le routage, l'utilisation du protocole EIGRP a été imposée.



(*) Schéma simplifié réseau

Les configurations des routeurs sont les suivantes.

Routeur Site A

```
…
interface Tunnel0
ip address 10.1.1.1 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/0
tunnel destination 80.2.0.2
!
interface Tunnel1
ip address 10.1.2.1 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/0
tunnel destination 80.3.0.2
!
interface Tunnel2
ip address 10.4.1.1 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/0
tunnel destination 80.4.0.2
```

```
!
interface GigabitEthernet0/0
ip address 80.1.0.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/0/0
switchport access vlan 2
switchport mode access
switchport nonegotiate
!
interface Vlan2
ip address 192.168.0.254 255.255.255.0
!
router eigrp 90
network 10.1.1.0 0.0.0.3
network 192.168.0.0
network 10.1.2.0 0.0.0.3
!
router eigrp 95
network 10.4.1.0 0.0.0.3
network 192.168.0.0
!
ip route 0.0.0.0 0.0.0.0 80.1.0.1
…
```

Routeur Site C

```
…
interface Tunnel1
ip address 10.1.2.2 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/0
tunnel destination 80.1.0.2
!
interface Tunnel3
ip address 10.3.1.2 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/0
tunnel destination 80.2.0.2
!
interface GigabitEthernet0/0
ip address 80.3.0.2 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/0/0
switchport access vlan 2
switchport mode access
switchport nonegotiate
```

```
!
interface FastEthernet0/0/1
switchport access vlan 2
switchport mode access
switchport nonegotiate
!
interface FastEthernet0/0/2
switchport mode access
switchport nonegotiate
!
interface Vlan2
ip address 192.168.5.254 255.255.255.0
!
router eigrp 90
network 10.1.2.0 0.0.0.3
network 192.168.5.0
!
router eigrp 100
network 10.3.1.0 0.0.0.3
!
ip route 0.0.0.0 0.0.0.0 80.3.0.1

…
```

Routeur Site D

```
…
interface Tunnel2
ip address 10.4.1.5 255.255.255.252
mtu 1476
tunnel source GigabitEthernet0/0
tunnel destination 80.1.0.2
!
interface GigabitEthernet0/0
ip address 80.4.0.2 255.255.255.252
duplex auto
speed auto
!
…
interface FastEthernet0/0/0
switchport access vlan 2
switchport mode access
switchport nonegotiate
!
…
interface Vlan2
ip address 192.168.6.254 255.255.255.0
!
router eigrp 95
network 10.4.1.0 0.0.0.3
network 192.168.6.0
```

```
!
ip route 0.0.0.0 0.0.0.0 80.4.0.1

…
```

1. **Résolvez le problème entre le site A et le site C.**

Un ping sur un poste du LAN A1 ne joint pas les postes du LAN C1 alors que l'inverse fonctionne.

```
Router1#ping 192.168.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
```

```
Router3#ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

L'ensemble des interfaces et tunnels sont montés

```
Router1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     80.1.0.2        YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  down                  down
FastEthernet0/0/0      unassigned      YES unset  up                    up
FastEthernet0/0/1      unassigned      YES unset  up                    down
FastEthernet0/0/2      unassigned      YES unset  up                    down
FastEthernet0/0/3      unassigned      YES unset  up                    down
Tunnel0                10.1.1.1        YES manual up                    up
Tunnel1                10.1.2.1        YES manual up                    up
Tunnel2                10.4.1.1        YES manual up                    up
Vlan2                  192.168.0.254   YES manual up                    up
```

```
Router3#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     80.3.0.2        YES manual up                    up
GigabitEthernet0/1     unassigned      YES unset  down                  down
FastEthernet0/0/0      unassigned      YES unset  up                    up
FastEthernet0/0/1      unassigned      YES unset  up                    down
FastEthernet0/0/2      unassigned      YES unset  up                    down
FastEthernet0/0/3      unassigned      YES unset  up                    down
Tunnel1                10.1.2.2        YES manual up                    up
Tunnel3                10.3.1.2        YES manual up                    up
```

```
Vlan2                  192.168.5.254 YES  manual         up                    up
```

Les tables de routages sont les suivantes :

```
Router1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 80.1.0.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C 10.1.1.0/30 is directly connected, Tunnel0
L 10.1.1.1/32 is directly connected, Tunnel0
C 10.1.2.0/30 is directly connected, Tunnel1
L 10.1.2.1/32 is directly connected, Tunnel1
C 10.4.1.0/30 is directly connected, Tunnel2
L 10.4.1.1/32 is directly connected, Tunnel2
80.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 80.1.0.0/30 is directly connected, GigabitEthernet0/0
L 80.1.0.2/32 is directly connected, GigabitEthernet0/0
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, Vlan2
L 192.168.0.254/32 is directly connected, Vlan2
D 192.168.3.0/24 [90/52480000] via 10.1.1.2, 00:57:40, Tunnel0
D 192.168.6.0/24 [90/52480000] via 10.4.1.2, 00:57:43, Tunnel2
S* 0.0.0.0/0 [1/0] via 80.1.0.1
```

```
Router3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 80.3.0.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D 10.1.1.0/30 [90/28160000] via 10.1.2.1, 00:57:48, Tunnel1
C 10.1.2.0/30 is directly connected, Tunnel1
L 10.1.2.2/32 is directly connected, Tunnel1
C 10.3.1.0/30 is directly connected, Tunnel3
L 10.3.1.2/32 is directly connected, Tunnel3
80.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
```

```
C 80.3.0.0/30 is directly connected, GigabitEthernet0/0
L 80.3.0.2/32 is directly connected, GigabitEthernet0/0
D 192.168.0.0/24 [90/52480000] via 10.1.2.1, 00:57:48, Tunnel1
D 192.168.3.0/24 [90/53760000] via 10.1.2.1, 00:57:48, Tunnel1
D 192.168.4.0/24 [90/52480000] via 10.3.1.1, 00:57:49, Tunnel3
192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.5.0/24 is directly connected, Vlan2
L 192.168.5.254/32 is directly connected, Vlan2
S* 0.0.0.0/0 [1/0] via 80.3.0.1
```

Apportez les corrections nécessaires.

2. **Résolvez le problème entre le site A et le site D.**

Le LAN A1 ne joins pas le LAN D1.

```
Router4#show ip interface brief
Interface              IP-Address      OK?  Method  Status  Protocol
GigabitEthernet0/0     80.4.0.2        YES  manual  up      up
GigabitEthernet0/1     unassigned      YES  manuel  down    down
FastEthernet0/0/0      unassigned      YES  unset   up      up
FastEthernet0/0/1      unassigned      YES  unset   up      down
FastEthernet0/0/2      unassigned      YES  unset   up      down
FastEthernet0/0/3      unassigned      YES  unset   up      down
Tunnel0                10.4.1.5        YES  manual  up      up
Vlan2                  192.168.6.254   YES  manual  up      up

Router4#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 80.4.0.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.4.1.4/30 is directly connected, Tunnel0
L 10.4.1.5/32 is directly connected, Tunnel0
80.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 80.4.0.0/30 is directly connected, GigabitEthernet0/0
L 80.4.0.2/32 is directly connected, GigabitEthernet0/0
192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.6.0/24 is directly connected, Vlan2
L 192.168.6.254/32 is directly connected, Vlan2
S* 0.0.0.0/0 [1/0] via 80.4.0.1
```

Depuis le routeur 1, ci-dessous le résultat des ping vers les différents tunnels :

```
Router1#ping 10.1.1.2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router1#ping 10.1.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

Router1#ping 10.4.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Apportez les corrections nécessaires.

3. **Le routeur du site B doit être changé, malheureusement la sauvegarde est illisible. Proposez une configuration des interfaces GigabitEthernet 0/0 (G0/0), FastEthernet0/0/0 (F0/0/0) et FastEthernet0/0/1 (F0/0/1), des tunnels GRE nécessaires ainsi qu'une configuration du protocole de routage EIGRP répondant aux règles de flux.**

4. **Faites apparaitre sur un schéma réseau simplifié les différents tunnels ainsi que leurs adresses IP d'extrémités**

Partie 3 (7 POINTS)

Suite à plusieurs tentatives d'accès sur le réseau interne de votre entreprise, votre responsable sécurité des systèmes d'information vous demande :

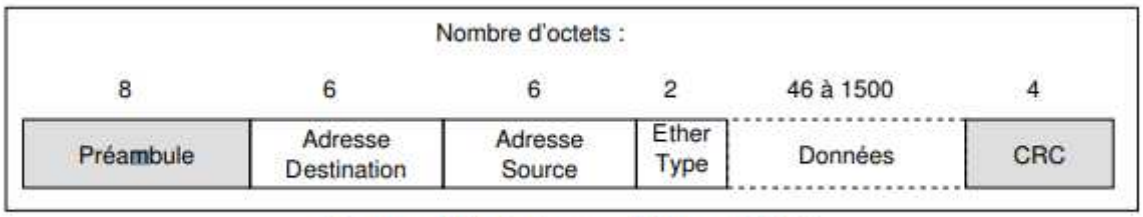
- de durcir les configurations de vos équipements réseaux,
- de mettre en place un système permettant de contrôler les différents équipements qui se connectent au réseau
- de mettre en place un outil de supervision centralisé
- de mettre en place un moyen de protection vous permettant de maîtriser les flux entrants et sortants de votre réseau sur l'internet.
- de centraliser les évènements et alarme des différents équipements.

Vous décrirez pour chacune des exigences demandées ci-dessus, les moyens que vous proposez, les configurations types de vos équipements en explicitant les règles et bonnes pratiques à mettre en place pour sécuriser vos équipements réseaux. Vous proposerez une architecture qui permettra de répondre au mieux à ces différents besoins de sécurisation.

Annexes

Format de la trame Ethernet V2

Ce sont les trames les plus couramment utilisées :



Format de la trame Ethernet V2

Description des champs de la trame Ethernet V2

Préambule : (8 octets)

Annonce le début de la trame et permet la synchronisation. Il contient 8 octets dont la valeur est 10101010 (on alterne des 1 et des 0), sauf pour le dernier octet dont les 2 derniers bits sont à 1.

Adresse Destination : (6 octets)

Adresse physique de la carte Ethernet destinataire de la trame. On représente une adresse Ethernet comme ses 6 octets en hexadécimal séparés par des ':'.

Exemple : 08:00:07:5c:10:0a

La destination peut être une adresse de (multi-)diffusion. En particulier, l'adresse ff:ff:ff:ff:ff:ff (diffusion ou broadcast) correspond à toutes les stations du réseau physique Ethernet.

Adresse Source : (6 octets)

Adresse physique de la carte Ethernet émettrice de la trame.

EtherType : ou type de trame (2 octets)

Indique quel protocole est concerné par le message. La carte réalise un démultiplexage en fournissant les données au protocole concerné.

Quelques types courants (en hexadécimal) définis par la RFC 1700

• 0x0600 : Xerox Network Systems

• 0x0800 : IP (Internet Protocol)

• 0x8100 : 802.1q (encapsulation vlan)

• 0x0806 : ARP (Address Resolution Protocol)

• 0x8035 : RARP (Reverse ARP)

• 0x8137 et 0x8138 : Novell.

Données : (46 à 1500 octets)

Les données véhiculées par la trame. Sur la station destinataire de la trame, ces octets seront communiqués à l'entité (protocole) indiquée par le champ EtherType. Notons que la taille minimale

des données est 46 octets. Des octets à 0, dits de “bourrage”, sont utilisés pour compléter des données dont la taille est inférieure à 46 octets.

CRC : (Cyclic Redundancy Code)

Champ de contrôle de la redondance cyclique. Permet de s’assurer que la trame a été correctement transmise et que les données peuvent donc être délivrées au protocole destinataire.

Les datagrammes

Les données circulent sur Internet sous forme de datagrammes (on parle aussi de paquets). Les datagrammes sont des données encapsulées, c'est-à-dire des données auxquelles on a ajouté des en-têtes correspondant à des informations sur leur transport (telles que l'adresse IP de destination).
Les données contenues dans les datagrammes sont analysées (et éventuellement modifiées) par les routeurs permettant leur transit.

Voici ce à quoi ressemble un datagramme :

<table>
<tr><th colspan="6">32 bits</th></tr>
<tr><td>Version
(4 bits)</td><td>Longue
ur d'en-
tête
(4 bits)</td><td colspan="2">Type de service
(8 bits)</td><td colspan="2">Longueur totale
(16 bits)</td></tr>
<tr><td colspan="3">Identification
(16 bits)</td><td>Drapeau
(3 bits)</td><td colspan="2">Décalage fragment
(13 bits)</td></tr>
<tr><td colspan="2">Durée de vie
(8 bits)</td><td>Protocole
(8 bits)</td><td colspan="3">Somme de contrôle en-tête
(16 bits)</td></tr>
<tr><td colspan="6">Adresse IP source
(32 bits)</td></tr>
<tr><td colspan="6">Adresse IP destination
(32 bits)</td></tr>
<tr><td colspan="6">Données</td></tr>
</table>

Voici la signification des différents champs :

Version (4 bits) :

Il s'agit de la version du protocole IP que l'on utilise (actuellement on utilise la version 4 IPv4) afin de vérifier la validité du datagramme. Elle est codée sur 4 bits.

Longueur d'en-tête, ou IHL pour Internet Header Length (4 bits) :

Il s'agit du nombre de mots de 32 bits constituant l'en-tête (nota : la valeur minimale est 5). Ce champ est codé sur 4 bits.

Type de service (8 bits) :

Il indique la façon selon laquelle le datagramme doit être traité.

Longueur totale (16 bits):

Il indique la taille totale du datagramme en octets. La taille de ce champ étant de 2 octets, la taille totale du datagramme ne peut dépasser 65536 octets. Utilisé conjointement avec la taille de l'en-tête, ce champ permet de déterminer où sont situées les données.

Identification, drapeaux (flags) et déplacement de fragment sont des champs qui permettent la fragmentation des datagrammes.

Durée de vie appelée aussi TTL, pour Time To Live (8 bits) :

Ce champ indique le nombre maximal de routeurs à travers lesquels le datagramme peut passer. Ainsi ce champ est décrémenté à chaque passage dans un routeur, lorsque celui-ci atteint la valeur critique de 0, le routeur détruit le datagramme. Cela évite l'encombrement du réseau par les datagrammes perdus.

Protocole (8 bits) :

Ce champ, en notation décimale, permet de savoir de quel protocole est issu le datagramme

- ICMP : 1
- IGMP : 2
- TCP : 6
- UDP : 17

Somme de contrôle de l'en-tête, ou en anglais *header checksum* (16 bits) :

Ce champ contient une valeur codée sur 16 bits qui permet de contrôler l'intégrité de l'en-tête afin de déterminer si celui-ci n'a pas été altéré pendant la transmission. La somme de contrôle est le complément à un de tous les mots de 16 bits de l'en-tête (champ somme de contrôle exclu). Celle-ci est en fait telle que lorsque l'on fait la somme des champs de l'en-tête (somme de contrôle incluse), on obtient un nombre avec tous les bits positionnés à 1

Adresse IP source (32 bits) :

Ce champ représente l'adresse IP de la machine émettrice, il permet au destinataire de répondre

Adresse IP destination (32 bits) :

Adresse IP du destinataire du message