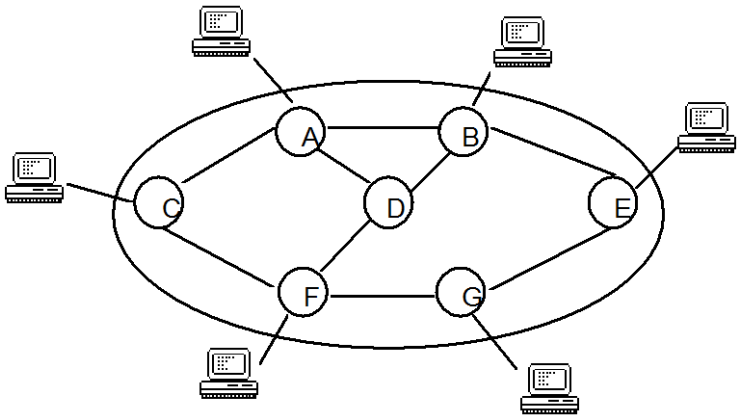
TD 5 : INTERNET, PROTOCOLE IP ET ADRESSAGE

1. GENERALITES

1.1. Rôle d'un réseau

Dans sa forme la plus simple, la communication de données prend place entre deux équipements qui sont directement reliés par un support de transmission. Néanmoins, il est souvent impossible pour deux équipements distants quelconques d'être reliés directement.

La solution consiste, pour des couvertures géographiques importantes (ceci exclut de la suite les techniques propres aux réseaux locaux ou métropolitains), à attacher les équipements à un réseau de communication, qui peut être déployé par un opérateur :



- chaque équipement (ou station) est relié à un nœud d'accès du réseau ;
- l'ensemble des nœuds d'accès constitue les frontières visibles du réseau ;
- le réseau est constitué d'un ensemble de nœuds, dits ***nœuds de commutation*** ou encore ***routeurs***, interconnectés par des liaisons.

Le réseau est un transporteur : son rôle est d'acheminer des données de leur source à leur destination. Il n'est pas concerné par la sémantique des données. Les données qui pénètrent dans le réseau en provenance d'une station sont routées vers leur destinataire en étant ***commutées*** ou ***routés*** de nœud en nœud.

Question : Du point de vue de deux stations communicantes, le réseau peut donc être considéré comme une extension d'une liaison directe. Nous avons vu précédemment les fonctionnalités assurées par une liaison de données. Sont-elles suffisantes pour permettre l'acheminement de données entre deux équipements terminaux ? Si oui, pourquoi ? Si non, que manque-t-il ?

1.2 Internet et le protocole IP

La couche Internet (Interconnection of networks) du modèle TCP/IP (RFC 1122, RFC 1123) assure les fonctionnalités de niveau 3 en mode non connecté. Ces fonctionnalités sont assurées principalement par le protocole IP (RFC 791, RFC 2474). La couche 3 contient d'autres protocoles comme : ARP, ICMP, IGMP, RIP etc.

- ARP (Adresse Resolution Protocol) : permet de faire la correspondance entre les adresses logiques Internet et les adresses physiques des interfaces réseaux.
- ICMP (Internet Control Message Protocol) : n'est pas à proprement parler un protocole de niveau 3, puisqu'il utilise l'encapsulation IP. Mais il sert à la gestion du protocole IP. Il permet par exemple de collecter les erreurs qui surviennent lors de l'émission des données.
- IGMP (Internet Group Message Protocol) est utilisé pour la gestion de groupe multicast.
- RIP (Routing Information Protocol) : comme ICMP il n'est pas un protocole de niveau 3 mais il assure des fonctionnalités de routage du niveau 3. Cependant, son utilisation n'est pas obligatoire comme IP, ICMP et ARP.

Dans les réseaux locaux filaires, l'encapsulation de paquets IP employée est généralement celle d'Ethernet. Dans les réseaux WiFi, une encapsulation possible est IEEE 802.11 PHY/IEEE 802.11 MAC/LLC/SNAP/IP. Le protocole SNAP (Sub-Network Access Protocol) permet de résoudre certains problèmes d'incompatibilité entre les protocoles IP et LLC. Bien que l'IEEE ait réservé un numéro de SAP (0x06) pour IP dans les trames LLC, l'IETF interdit rigoureusement son emploi dans les spécifications de IP. L'aiguillage entre le niveau 2 et le niveau 3 se fait en lisant soit le champ type de la trame Ethernet ou le champ code de la trame SNAP.

Questions

1. Dans l'architecture TCP/IP, est-ce qu'on peut avoir les encapsulations suivantes : Ethernet/ICMP/IP, Ethernet/IP/ICMP/IP , Ethernet/IP/IP/ICMP?
2. Donnez la pile protocolaire utilisée afin de transmettre un objet HTML entre un point d'accès WiFi et un ordinateur sans fil.
3. Peut-on dire que RIP est une application ?
4. Dans la trame Ethernet suivante, l'entête IP commence à partir de l'octet de valeur 0x45, 4 pour la version du protocole IP (IPv4), 5 pour la taille de l'entête IP (5 mots de 32 bits, donc sans options. Voir Annexe) :

```
0x0000: 0050 2282 2fb9 0004 23c3 2b52 0800 4500
0x0010: 02fc 8890 4000 4006 954b c0a8 ccc8 c0a8   Entête IP
0x0020: cc06 9805 0016 032f e60f e575 415e 8018
0x0030: 05b4 9af6 0000 0101 080a 8bf1 6d79 00bb
0x0040: 154b 0000 02c4 0514 42f7 d636 f260 b617
0x0050: 1f63 db2d 6ff9 5431 0000 0059 6469 6666
```

4.1. Quel est le protocole de niveau 4 (transport) auquel le paquet est destiné ? Voir Annexe.

4.2. Donnez en hexadécimal les deux adresses IP source et destination ? Voir Annexe.

2. ADRESSAGE ET SUBDIVISION DE RESEAU

Les adresses IP se composent de deux parties : Le numéro de réseau, appelé aussi préfixe, et le numéro de la machine (hôte) sur ce réseau. En principe, une adresse IPv4 est notée comme une suite de quatre octets en décimal séparés par des points. Elle constitue concrètement une suite de 32 bits. A noter qu'une adresse ne représente pas une machine, mais une interface de cette machine. Si un

équipement possède plusieurs interfaces réseau, il devra impérativement posséder plusieurs adresses IP, une par interface. L'adresse IP est utilisée afin de trouver un chemin pour accéder à la machine qui lui est associée, donc pour le routage (« routing »). Il existe deux types d'adressage, avec ou sans classe. Ce dernier permet de simplifier le groupement et la hiérarchisation des adresses et donc du routage, appelé en conséquence « Classless IPv4 Inter-Domain Routing » ou simplement CIDR.

Question : Donnez en notation classique en décimal les deux adresses IP source et destination de la trame précédente.

2.1. Adressage IPv4 par classes (« Classfull IPv4 network adresses »)

L'adresse de la machine PC152 sur un site est 193.55.28.152 :

- De quelle classe est cette adresse ?

- Quel est le masque du réseau (« netmask ») correspondant à cette classe d'adresses ?

- Quel est le nombre n de bits de la partie réseau ? On dit que le préfixe est sur n bits et on le note ainsi xxx.xxx.xxx.xxx/**n**. Cette notation en préfixe est plus utilisée en CIDR. Parfois, le préfixe désigne simplement le nombre n.

- Quelle est l'adresse du sous réseau auquel la machine appartient ?

- Quelle est l'adresse de diffusion sur ce réseau ?

2.2. Adressage IPv4 sans classes (« Classless IPv4 Inter-Domain Routing »)

On considère la plage d'adresses : 194.132.176.0/20

Si on utilise cette plage pour adresser (créer) un seul réseau, alors :

- Quel est le netmask de ce réseau (donc associé à cette plage d'adresses) ?

- Est-ce que la machine d'adresse 194.132.193.61 appartient à ce réseau ?

- Quelle est la première adresse de la plage ?

- Quelle est la deuxième adresse ?

- Quelle est la dernière adresse ?

- Quelle est l'avant-dernière adresse ?

- Quelle est la première adresse utilisable pour les interfaces réseaux (machines) ?

- Quelle est la dernière adresse utilisable pour les interfaces réseaux (machines) ?

- Enfin, quelle est l'adresse réseau ?

2.3 Subdivision (Subnetting)

La ***subdivision de réseau*** est un procédé qui permet de découper logiquement des réseaux de grande taille en sous-réseaux de plus petites tailles. Pour ce faire, on applique un masque de sous-réseau sur une adresse de base. Le résultat est une plage d'adresses de machines continues mais de taille réduite par rapport à la plage d'adresses initiales. Le préfixe des sous-réseaux sont alors plus longs que le préfixe du réseau subdivisé. Il y a deux types de subdivision : (1) subdivision en réseaux de tailles égales. Dans ce cas, la longueur du préfixe de chaque sous réseau est la même ; (2) subdivision en réseaux de tailles inégales. Dans ce cas, les préfixes des sous-réseaux ont des longueurs différentes, on appelle ce dernier type de subdivision en anglais « Variable Length Subnet mask » ou simplement VLSM.

4.1. On désire subdiviser le réseau 129.178.0.0/16 en 60 sous-réseaux de taille égale.

- Combien de bits a-t-on besoin afin de créer au moins 60 possibilités de combinaison de bits ? En déduire la nouvelle longueur de préfixe des sous-réseaux. Quelle est le netmask ?

- Combien de machines (interfaces réseaux), on peut adresser sur chaque sous-réseau ?

- Quelle est l'adresse du premier sous-réseau ?

- Quelle est l'adresse du deuxième ? Troisième ? 60ème ? 64ème ?

- Combien de machines au maximum pourra-t-on connecter sur chaque sous-réseau ?

- Quelle est la première adresse machine possible dans le deuxième réseau ? La dernière adresse machine ? Quelle est l'adresse de diffusion ?

4.2. VLSM : on considère l'adresse réseau 192.44.77.0/24.

On souhaite la subdiviser en 5 sous-réseaux contenant respectivement 12, 2, 8, 25 et 20 machines. Si on subdivise de manière égale comme l'exercice précédent, on doit créer des réseaux de taille $\geq 25+2$, donc de taille $2^5 = 32$. Autrement dit on a besoin de 5 bits pour adresser les machines dans chaque sous-réseau, et donc le préfixe des sous-réseaux doit être 32-5=27. Le préfixe de départ est /24, on lui rajoute donc 3 bits. Cela correspond bien puisque pour créer 5 sous-réseaux on a besoin de $2^3 = 8$ combinaisons ($2^2 = 4 < 5$). L'efficacité de cette subdivision peut se mesurer, pour chaque sous-réseau, en calculant le rapport entre le nombre d'adresses utilisées pour adresser les machines et le nombre total d'adresses allouées. Cela donne respectivement $12/2^5 = 37.5\%$, $2/2^5 = 6.25\%$, $8/2^5 = 25\%$, $25/2^5 = 78.13\%$, et $20/2^5 = 62.5\%$. Beaucoup d'adresses sont donc gaspillées.

- Proposez une subdivision du réseau en employant des préfixes différents pour chaque sous-réseau dans le but d'être au plus proche du nombre de machines dans chaque sous-réseau :

  1- Donnez les préfixes (/n) et netmasks de chaque sous-réseau

  2- Donnez l'adresse réseau de chaque sous-réseau

  3- Donnez la plage d'adresses pour les machines (1ère et dernière) et l'adresse de diffusion.

- Calculez l'efficacité de chaque sous réseau.

- Si le dernier sous-réseau doit accueillir 35 machines au lieu de 20, peut-on faire un découpage égal ? VLSM ?

2.4 Agrégation de préfixes (ou d'adresses), appelé encore supernetting

On peut considérer que l'agrégation de préfixes est l'opération inverse de la subdivision. Cette opération permet d'adresser plusieurs réseaux avec une seule adresse, à condition que les adresses de ces réseaux soient contiguës. Le préfixe obtenu est plus court que ceux des réseaux agrégés.

- Est-il possible d'agréger les réseaux suivants : 192.160.1.0/24, 192.160.2.0/24, 192.160.3.0/24 et 192.160.0.0/24 ?

- Quel est le préfixe et le netmask du réseau agrégé ?

- Donnez l'adresse du réseau agrégé

Remarque : L'agrégation de préfixe (avec l'adressage CIDR) permet de réduire le nombre d'entrée dans les tables de routage.

Annexe

Le datagramme IP

L'en-tête IP est alignée sur des mots de 32 bits. Sa longueur est donc multiple de 4 octets. Par défaut, sans option, l'en-tête IP fait 20 octets de long :

<table>
<tr><td>4 bits</td><td>4 bits</td><td>8 bits</td><td colspan="2">16 bits</td></tr>
<tr><td>Version</td><td>IHL</td><td>DS (6) ECN (2)</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
<tr><td colspan="5">Données de la couche supérieure</td></tr>
</table>

- « Version » indique le format de l'en-tête. Ce champ sert à l'identification de la version courante du protocole. La version décrite ici (et aujourd'hui utilisée) porte le n°4 ;
- « IHL (*IP Header Length*) » est la longueur de l'en-tête IP exprimée en mots de 32 bits (5 au minimum, 15 au maximum) ;
- « DS (Differentiated Services) » définit la classe de service à appliquer au paquet. Les 6 premiers bits correspondent à un code qui permet au routeur d'associer à chaque paquet d'une classe, un traitement spécifique tel que l'accélération du temps de transmission, un emplacement prioritaire en mémoire et la possibilité de rejet. « ECN (Explicit Congestion Notification) » deux bits permettant au routeur de notifier une congestion, autrement dit une charge importante de paquets à traiter. Les récepteurs et les émetteurs utilisent cette notification afin de réduire la vitesse de transmission de paquets.
- « Total Length » est la longueur totale du datagramme, en-tête et données inclus, exprimée en octets ;
- « Identification » est une valeur fournie par l'émetteur aidant au réassemblage des différents fragments du datagramme. Le seul usage de ce champ est donc de permettre à une entité réceptrice de reconnaître les datagrammes qui appartiennent à un même datagramme initial et qui doivent donc faire l'objet d'un réassemblage ;
- « Flags » est utilisé par la fragmentation. Il est composé de deux indicateurs : DF (*Don't Fragment*) pour interdire la fragmentation et de MF (*More Fragment*) pour signifier des fragments à suivre :

<table>
<tr><td>0</td><td>DF</td><td>MF</td></tr>
</table>

DF : 0 = *May Fragment*
1 = *Don't Fragment*

MP : 0 = *Last Fragment*
1 = *More Fragments*

- « Fragment offset » indique sur 13 bits la position relative du fragment dans le datagramme initial, le déplacement étant donné en unités de 64 bits (seuls un datagramme complet ou un premier fragment de datagramme peuvent avoir ce champ à 0) ;
- « TTL (*Time To Live*) » représente une indication de la limite supérieure du temps de vie d'un datagramme. Cette valeur est comprise entre 0 et 255 ;
- « Protocol » indique le protocole (de niveau supérieur) utilisé pour le champ de données du datagramme :

Code (déc)	Abréviation	Nom du protocole	Référence
1	ICMP	Internet Control Message Protocol	[RFC792]
2	IGMP	Internet Group Management Protocol	[RFC1112]
3	GGP	Gateway-to-Gateway Protocol	[RFC823]
4	IP	IP in IP (encapsulation)	
5	ST	Stream	[RFC1190]
6	TCP	Transmission Control Protocol	[RFC793]
7	UCL	UCL	
8	EGP	Exterior Gateway Protocol	[RFC888]
9	IGP	any private Interior Gateway Protocol	
10	BBN-RCC-MON	BBN RCC Monitoring	
11	NVP-II	Network Voice Protocol	[RFC741]
12	PUP	PUP	
13	ARGUS	ARGUS	
14	EMCON	EMCON	
15	XNET	Cross Net Debugger	
16	CHAOS	Chaos	
17	UDP	User Datagram Protocol	[RFC768]
46	RSVP	Reservation Protocol	
47	GRE	General Routing Encapsulation	
48	MHRP	Mobile Host Routing Protocol	
54	NHR	NBMA Next Hop Resolution Protocol	

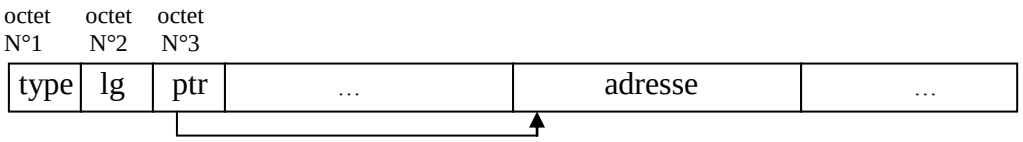
- « Header Checksum » est une zone de contrôle d'erreur portant uniquement sur l'en-tête du datagramme ;
- « Source Address » est l'adresse IP de la source du datagramme ;
- « Destination Address » est l'adresse IP de destination du datagramme ;
- « Options » sert à des fonctions de contrôle utiles dans certaines situations (estampillage temporel, sécurité, routage particulier, etc.). Le champ est donc de longueur variable. Il est constitué d'une succession d'options élémentaires, également de longueurs variables. Les options sont codées sur le principe TLV (type, longueur, valeur). La longueur indique la taille complète de l'option en octets. Les options possibles sont :

Type (déc.)	Option	Objet
0	*End of Options List* (EOOL)	Utilisée si la fin des options ne coïncide pas avec la fin de l'en-tête.
1	*No Operation* (NOP)	Pour aligner le début de l'option suivante sur 32 bits.
130	*Security* (SEC)	Permet aux hôtes d'indiquer des restrictions liées à la sécurité

		(ex : non classifié, confidentiel, restreint, top secret, etc.).
131	*Loose Source Route* (LSR)	Permet à la source du datagramme de fournir des informations à utiliser par les passerelles pour le routage du datagramme vers sa destination et d'enregistrer l'information concernant la route (série d'adresses Internet) ; un routeur ou une route peut utiliser n'importe quelle route avec un nombre quelconque de passerelles intermédiaires pour atteindre la prochaine adresse indiquée dans la route.
68	*Time Stamp* (TS)	Enregistrement de l'heure de chaque passage de passerelle.
133	*Extended Security* (E-SEC)	Notions de sécurité étendues.
7	*Record Route* (RR)	Permet d'enregistrer la route d'un datagramme (en fait, l'adresse de chaque passerelle traversée).
136	*Stream ID* (SID)	Permet de véhiculer un identifieur de flux ; utilisée à des fins de débogage et de mesure.
137	*Strict Source Route* (SSR)	Idem LSR, si ce n'est qu'un routeur ou un hôte doit envoyer directement le datagramme à la prochaine adresse indiquée dans la route.

Exemple : l'option « Record Route »

- structure de l'option :



- champ type : égal à 7 ;
- l'adresse qui est enregistrée correspond à l'interface utilisée en sortie par le routeur ;

  - « Padding » permet d'aligner l'en-tête sur 32 bits.