

DIU Bloc3 – Réseaux

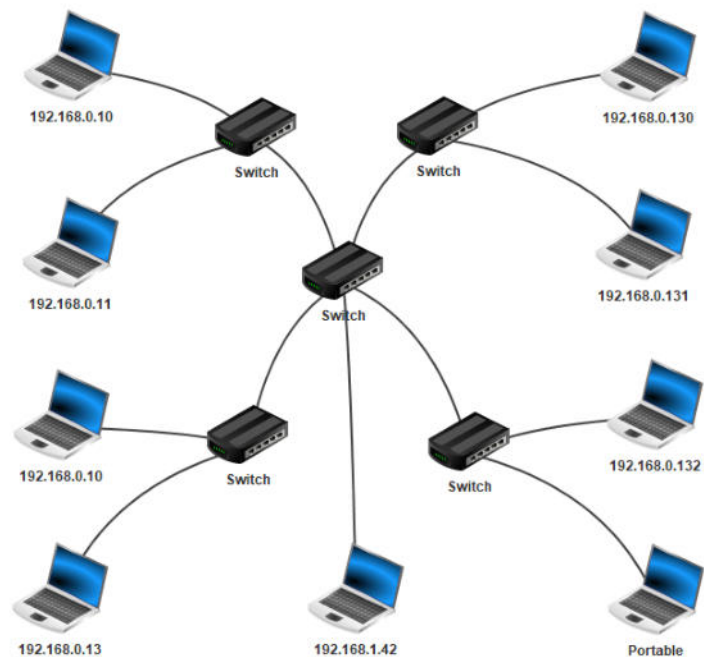
Lemoine Ghislaine

TP – switch – arp – ping

Construction du réseau

(avec le logiciel Filius)

Aperçu de la configuration réseau pour la machine 192.168.0.10



Premières informations

@ip.0.10 = 192.168.0.10

Masque = 255.255.255.0

@ip.0.10 = 192.168.0.10/24 (avec la notation CIDR)

La machine M.0.10 appartient à un réseau R tel que : @R = 192.168.0.0

Les adresses des machines du réseau sont codées avec le dernier octet = 8 bits.

Ce réseau peut contenir : $2^8 - 2 = 254$ machines

L'adresse IP de la première machine : @R_first = 192.168.0.1

L'adresse IP de diffusion : @R_diff = 192.168.255.255

L'adresse IP de la dernière machine : @R_end = @R_diff - 1 = 192.168.255.254

Exercice 1 :

Ping 192.168.0.10 vers 192.168.0.133

```
root /> ipconfig
Adresse IP . . . : 192.168.0.10
Masque . . . . . : 255.255.255.0
Adresse MAC. . . : 2C:5B:E8:B8:01:42
Passerelle . . . :
Serveur DNS. . . :

root /> ping 192.168.0.133
PING 192.168.0.133 (192.168.0.133): icmp_seq=1 ttl=64 time=8103ms
From 192.168.0.133 (192.168.0.133): icmp_seq=2 ttl=64 time=4011ms
From 192.168.0.133 (192.168.0.133): icmp_seq=3 ttl=64 time=4011ms
From 192.168.0.133 (192.168.0.133): icmp_seq=4 ttl=64 time=4011ms
--- 192.168.0.133 Statistiques des paquets ---
4 paquets transmis, 4 paquets reçus, 0% paquets perdus
```

Échanges de données						
192.168.0.10						
No.	Date	Source	Destination	Protocole	Couche	Commentaire
1	21:31:19.639	192.168.0.10	192.168.0.133	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.1
2	21:31:23.731	192.168.0.133	192.168.0.10	ARP	Internet	192.168.0.133: 73:B7:3D:73:4C:DB
3	21:31:23.731	192.168.0.10	192.168.0.133	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 1
4	21:31:27.742	192.168.0.133	192.168.0.10	ICMP	Internet	ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 1
5	21:31:27.942	192.168.0.10	192.168.0.133	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 2
6	21:31:31.953	192.168.0.133	192.168.0.10	ICMP	Internet	ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 2
7	21:31:32.153	192.168.0.10	192.168.0.133	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 3
8	21:31:36.164	192.168.0.133	192.168.0.10	ICMP	Internet	ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 3
9	21:31:36.364	192.168.0.10	192.168.0.133	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 4
10	21:31:40.375	192.168.0.133	192.168.0.10	ICMP	Internet	ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 4

Analyse des échanges :

No.: 1 / Date: 21:31:19.639	
⊖ Réseau	
Source:	2C:5B:E8:B8:01:42
Destination:	FF:FF:FF:FF:FF:FF
Commentaire:	0x806
⊖ Internet	
Source:	192.168.0.10
Destination:	192.168.0.133
Protocole:	ARP
Commentaire:	Recherche de l'adresse MAC associée à 192.168.0.133, 192.168.0.10: 2C:5B:E8:B8:01:42

La machine M.0.10 dont l'adresse MAC est @M.0.10 =2c:5b:e8:b8:01:42 ne connaît pas l'adresse MAC du destinataire.

La diffusion s'effectue pour tous les postes du réseau en utilisant @R_diff : adresse identifiée dans le réseau par ff:ff:ff:ff:ff:ff.

Donc toutes les liaisons ont clignoté, lors de l'exécution du ping.

Le protocole utilisé est ARP : protocole qui permet d'associer @MAC (unique pour chaque machine lors de sa construction) et @IP (utilisée dans la couche internet) et d'identifier l'adresse physique d'une machine particulière dans le réseau à partir de son adresse IP.

No.: 2 / Date: 21:31:23.731	
⊖ Réseau	
Source:	73:B7:3D:73:4C:DB
Destination:	2C:5B:E8:B8:01:42
Commentaire:	0x806
⊖ Internet	
Source:	192.168.0.133
Destination:	192.168.0.10
Protocole:	ARP
Commentaire:	192.168.0.133: 73:B7:3D:73:4C:DB

La réponse est l'envoi à la source initiale (qui devient le destinataire de la réponse) de l'adresse physique de la machine auquel est destiné le message.

Ici, @MAC = 73:b7:3d:73:4c:db qui correspond à @IP =192.168.0.133 recherchée.

Une fois les deux machines parfaitement identifiées, l'envoi de la trame d'un ping est gérée par le protocole ICMP et concerne uniquement ces deux machines.

Un ping permet de s'assurer que les deux machines identifiées peuvent échanger des trames.

Il y a 4 demandes envoyées par la machine source

Cela correspond dans la table d'échange des données aux lignes 3; 5 ; 7 et 9 que l'on peut identifier par l'intitulé « Echo Request (ping) ».

En retour, la machine destinataire confirme la bonne réception de chaque demande. Cela correspond dans la table d'échange des données aux lignes 4 ; 6 ; 8 et 10 que l'on peut identifier par l'intitulé « Echo Reply (pong) ».

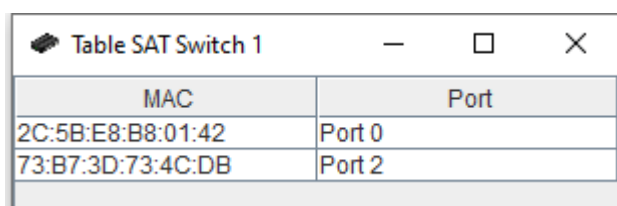
Si toutes les demandes ont reçu une réponse, le ping fonctionne et l'échange de trames entre les deux machines est possible.

Le TTL indiqué correspond au temps de transfert limite et est utilisé pour la gestion des transmissions de paquets.

Les switches sont des commutateurs permettant de relier plusieurs machines entre elles afin d'acheminer des trames d'une machine « source » vers une machine « destinataire ». Le switch aiguille les trames grâce à @MAC qui figure dans l'en-tête de la trame. Pour envoyer l'information à la bonne machine, le switch fabrique de façon dynamique sa table SAT, qui lui permet de garder en mémoire, pendant la transmission, les ports utilisés et les machines concernées, en établissant une table de correspondance entre @CAM et le port du switch utilisé. Cela permet une transmission rapide en évitant les collisions.

Après le ping, les switches 1 ; 3 et 5 du réseau ont dans leur table SAT les ports utilisés pour la communication entre les deux machines.

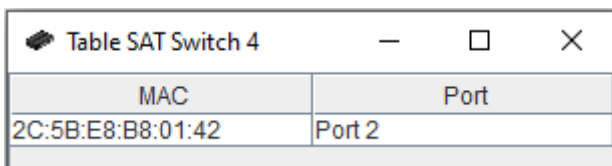
Dans chaque switch, deux ports ont été associés à une @MAC (respectivement un port pour la source et un pour le destinataire).



MAC	Port
2C:5B:E8:B8:01:42	Port 0
73:B7:3D:73:4C:DB	Port 2

Pour les switches 2 et 4, un seul port est gardé en mémoire et est associé à @MAC de la source. La diffusion de la demande dans tout le réseau a été effectué initialement, et seule la machine qui correspond à @IP de la demande répond.

Les switches qui n'ont pas été utilisés lors de la communication entre les deux machines identifiées, ne connaissent que @MAC de la source.



MAC	Port
2C:5B:E8:B8:01:42	Port 2

Les switches permettent de gérer dans la couche internet des communications rapides en évitant les collisions de paquets. Les trames n'étant échangées qu'entre les machines identifiées.

Dans la couche internet, les machines communiquent entre-elles à l'aide des @IP. C'est le protocole ARP qui permet d'établir la correspondance entre @IP et @MAC.

C'est le protocole IMCP qui gère l'acheminement des trames dans le réseau en utilisant les @MAC

Les switches conservent de manière provisoire dans leur table SAT des adresses physiques de machines ou @MAC.

No.: 10 / Date: 21:31:40.375

⚙ Réseau

— Source: 73:B7:3D:73:4C:DB
— Destination: 2C:5B:E8:B8:01:42
— Commentaire: 0x800

⚙ Internet

— Source: 192.168.0.133
— Destination: 192.168.0.10
— Protocole: ICMP
— Commentaire: ICMP Echo Reply (pong), TTL: 64, Seq.-Nr.: 4

Niveau 1 – COUCHE « PHYSIQUE »

Acheminement des bits

Elle effectue l'adaptation des bits pour la transmission sur le support physique (câbles, fibre optique, liaison Wi-fi)

L'unité d'échange est le bit.

Éléments de niveau 1 : les câbles (câble coaxial, paire torsadée, fibre optique), liaison Wi-Fi, concentrateur (Hub),... travaillent au niveau 1 ISO.

Niveau 2 – COUCHE « LIAISON DE DONNEES »

Acheminement sans erreur des trames

Elle assure un transfert fiable des trames sur une liaison physique.

Elle s'occupe également de la topologie du réseau, de l'accès au réseau, de la notification des erreurs, de la livraison ordonnée des trames et du contrôle de flux.

Pour vous souvenir facilement des fonctions de la couche 2, pensez aux trames et aux adresses MAC.

Éléments de niveau 2 : Commutateur (Switch), adresse MAC

Niveau 3 – COUCHE « RESEAU »

ADRESSAGE, ROUTAGE, SEGMENTATION

Elle assure l'acheminement ou le routage (choix des chemins à partir des adresses IP) des paquets à travers les réseaux.

Pour vous souvenir facilement des fonctions de la couche 3, pensez à la sélection du chemin, au routage et à l'adressage.

Éléments de niveau 3 : **Les protocoles : IP, IPX, ARP, RARP,...**

Matériel : Routeur , commutateur de niveau 3

Sites consultés :

<http://maurise-softawre1.e-monsite.com/medias/files/not-fond-chap2-modeles-osi-tcpip-v2.pdf>

https://dept-info.labri.fr/~felix/Annee2007-08/A2/ASR3/TD1/A2-Cours1_OSI.pdf

https://www.unilim.fr/pages_perso/deneuille/docs/reseaux1/2-physique-liaison.pdf

Exercice 2 :

ping de 192.168.0.10 vers 192.168.0.14 (machine qui n'existe pas)

```
root /> ping 192.168.0.14
PING 192.168.0.14 (192.168.0.14)
From 192.168.0.14 (192.168.0.14): icmp_seq=1 -- Timeout!
From 192.168.0.14 (192.168.0.14): icmp_seq=2 -- Timeout!
From 192.168.0.14 (192.168.0.14): icmp_seq=3 -- Timeout!
From 192.168.0.14 (192.168.0.14): icmp_seq=4 -- Timeout!
--- 192.168.0.14 Statistiques des paquets ---
4 paquets transmis, 0 paquets reçus, 100% paquets perdus
```

Échanges de données						
192.168.0.10						
No.	Date	Source	Destination	Protocole	Couche	Commentaire
1	13:04:31.395	192.168.0.10	192.168.0.14	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.14, 192.168.0.10: 2C:5B:E8:B8:01:42
2	13:04:43.906	192.168.0.10	192.168.0.14	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.14, 192.168.0.10: 2C:5B:E8:B8:01:42
3	13:04:56.618	192.168.0.10	192.168.0.14	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.14, 192.168.0.10: 2C:5B:E8:B8:01:42
4	13:05:09.123	192.168.0.10	192.168.0.14	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.14, 192.168.0.10: 2C:5B:E8:B8:01:42
5	13:05:21.824	192.168.0.10	192.168.0.14	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.14, 192.168.0.10: 2C:5B:E8:B8:01:42
6	13:05:34.329	192.168.0.10	192.168.0.14	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.14, 192.168.0.10: 2C:5B:E8:B8:01:42
7	13:05:47.043	192.168.0.10	192.168.0.14	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.14, 192.168.0.10: 2C:5B:E8:B8:01:42
8	13:05:59.558	192.168.0.10	192.168.0.14	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.14, 192.168.0.10: 2C:5B:E8:B8:01:42

Analyse des échanges :

Sans compter les doublons, au minimum 5 recherches de l'adresse @MAC associée à @IP sont effectuées. (la recherche initiale à laquelle s'ajoute les 4 séquence ICMP liées à l'envoi d'un ping).

L'affichage « Timeout ! » indique que l'adresse MAC n'a pas été trouvée dans les délais impartis. Cela ne donne aucune précision sur l'existence ou non de la machine cible, ni sur la raison de sa non identification.

Seule la machine source émet et renouvelle les demandes.

Toutes les autres machines reçoivent (au minimum 5 fois) les demandes, mais restent muettes, car l'adresse du destinataire est différente de la leur.

Exercice 3 :

ping de 192.168.0.10 vers 192.168.1.42

```
root /> ping 192.168.1.42
Destination inaccessible
```

ping de 192.168.1.42 vers 192.168.0.10

```
root /> ping 192.168.0.10
Destination inaccessible
root /> |
```

Analyse des échanges et corrections apportées :

Les machines ne font pas partie du même réseau, les tables d'échange des données reste vide.

En changeant le netmask de la machine source ou de la machine destinataire, on peut agrandir la taille du réseau dans lequel elles appartiennent (nombres d'adresses machines possibles avec lesquelles elles peuvent communiquer)

Par exemple, si on change le masque le masque de la machine destinataire on peut l'intégrer au réseau de la machine source. En effet :

	Avant	Après
@ipMachine	192.168.1.42/24	192.168.1.42/23
Masque	255.255.255.0	255.255.254.0
@R	192.168.1.0	192.168.0.0
@ipR_diff	192.168.1.255	192.168.1.255

ping de 192.168.1.42 vers 192.168.0.10

```
root /> ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10)
From 192.168.0.10 (192.168.0.10): icmp_seq=1 -- Timeout!
From 192.168.0.10 (192.168.0.10): icmp_seq=2 -- Timeout!
From 192.168.0.10 (192.168.0.10): icmp_seq=3 -- Timeout!
From 192.168.0.10 (192.168.0.10): icmp_seq=4 -- Timeout!
--- 192.168.0.10 Statistiques des paquets ---
4 paquets transmis, 0 paquets reçus, 100% paquets perdus
```

Échanges de données						
192.168.0.10						
No.	Date	Source	Destination	Protocole	Couche	Commentaire
1	13:48:16.362	192.168.1.42	192.168.0.10	ARP	Internet	Recherche de l'adresse MAC associée à 192.168.0.10, 192.168.1.42: EA:15:F3:64:00:10
2	13:48:16.362	192.168.0.10	192.168.1.42	ARP	Internet	192.168.0.10: 2C:5B:E8:B8:01:42
3	13:48:44.577	192.168.1.42	192.168.0.10	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 2
4	13:49:09.787	192.168.1.42	192.168.0.10	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 3
5	13:49:34.993	192.168.1.42	192.168.0.10	ICMP	Internet	ICMP Echo Request (ping), TTL: 64, Seq.-Nr.: 4

Dans la table d'échange, on constate que les deux machines sont bien identifiées grâce au protocole ARP

Par contre, même si la machine M.0.10 reçoit bien les trames de la machine M.1.42, elle ne peut envoyer d'accusé de réception car pour elle, la machine M.0.10 demeure inaccessible.

Il faut donc changer aussi le masque de la machine M.0.10

	Avant	Après
@ipMachine	192.168.0.10/24	192.168.0.10/23
Masque	255.255.255.0	255.255.254.0
@R	192.168.0.0	192.168.0.0
@ipR_diff	192.168.0.255	192.168.1.255

De manière plus générale, il faudrait changer tous les netmask de toutes les machines. Elles seront intégrées alors dans un réseau de 510 adresses machine disponibles ($2^9 - 2 = 510$). En effet, un masque 255.255.254.0 permet de coder les adresses machines sur 9 bits.

D'un point de vue pratique, pour la maintenance du réseau, il faudra évaluer le coût en temps pour configurer les machines et le coût matériel (en tenant compte des besoins en poste et de l'évolution possible de ces besoins) pour savoir s'il est préférable de conserver deux sous-réseaux de 254 adresses interconnectés avec un routeur ou de les fusionner en changeant le masque de chacune des machines pour obtenir un réseau de 510 adresses.