Côté cours - Les principes de la communication dans un réseau local : les protocoles mis en œuvre.

Description du thème

Propriétés	
Intitulé long	Les principes de la communication dans un réseau local : les protocoles mis en œuvre
Formation(s) concernée(s)	BTS Services Informatiques aux Organisations
Matière(s)	SI2
Présentation	L'objectif général est de découvrir et d'approfondir les notions inhérentes aux protocoles nécessaires au fonctionnement d'un réseau local. Cette ressource fournit des indications sur la façon d'introduire ces notions en BTS SIO. Elle correspond à une séance réelle qui peut faire suite à la séance sur « Les principes de la communication dans un réseau local : les éléments physiques ».
Savoirs	**Savoir-faire** • Caractériser les éléments d'interconnexion d'un réseau • Analyser des unités de données de protocole **Savoirs associés** • Modèles de référence associés aux architectures réseaux • Rôle et positionnement des éléments d'interconnexion dans les modèles de référence • Services de base et unités de données de protocole associées • Technologies et techniques d'adressage et de nommage
Compétences	
Transversalité	
Prérequis	Les éléments physiques dans un réseau local
Outils	Simulateur Réseau. Nous fournissons : • Les fichiers exploitables avec Sopirem en version 2 ou 3. La version 2 est disponible sur le site du réseau Certa. • Les vidéos retraçant les manipulations sur Sopirem : ◦ Démonstration Collision ◦ Démonstration Half-Duplex ◦ Démonstration Full-Duplex
Mots-clés	réseau normes protocoles ethernet 802.3 802.11 ARP adresses MAC
Durée	8/10 heures
Auteur.e(s)	Apollonie Raffalli et David Duron
Version	v 1.0
Date de publication	Novembre 2017

Indications à destination des enseignants

Nous supposons que la séance précédente a porté sur les éléments physiques constituant un réseau local.

Cette séance peut débuter (éventuellement à la maison) par la visualisation de deux vidéos :

- Les diverses normes réseaux (7mn 04) qui retracent brièvement la succession des normes réseaux : https://www.youtube.com/watch?v=ICjWM7YkQQw.
- Une présentation succincte de la norme Ethernet (4mn 43) : https://youtu.be/nRbIvkTgggg

Ce cours comprend :

- une activité sur l'analyse d'une trame ARP avec Wireshark sur Ubuntu 17.04 (fichier activite-analyseTrameWireshark.odt) ;
- un QCM permettant de valider les notions acquises (fichier qcm-reseauLocalProtocoles.odt).

Vous disposez également de deux vidéos visant notamment à expliquer les principes de base de la commutation (table MAC/PORT, ARP, etc.), la première s'appuie sur le simulateur réseau SOPIREM et la deuxième sur Packet Tracer : https://youtu.be/I8H0n91grec et https://youtu.be/aUKGECkMhjM

Contexte

Nous avons vu que pour qu'une information circule entre deux éléments du réseau, il faut :

- un support matériel qui véhicule le signal électrique (un câble par exemple) ;
- des codes de signalisation, qui organisent la manière dont ce signal informatique est véhiculé afin que les ordinateurs qui envoient ou reçoivent cette information se comprennent.

Mais ce n'est pas suffisant : comment un message envoyé d'un hôte à un autre à travers un réseau peut-il arriver sans encombre à destination et être parfaitement compris ?

La problématique que nous soulevons ici est la même à l'échelle d'Internet qui est le plus grand des réseaux sachant qu'en avril 2017, il y avait plus de 3,8 milliards d'internautes dans le monde interconnectés (https://www.blogdumoderateur.com/chiffres-internet/) !

Des organismes ont ainsi été mis en place pour s'assurer que les technologies, développées et mises en œuvre dans différents pays par de nombreux constructeurs concurrents, partagent les mêmes règles (protocoles), les mêmes principes de fonctionnement, d'interaction et de régulation.

Toutes les communications sont régies par des **règles prédéterminées appelées protocoles** implémentés dans des logiciels et du matériel chargés sur chaque hôte et périphérique réseau. Les protocoles appliqués dans un réseau local sont les mêmes que ceux appliqués sur Internet.
L'utilisation de normes dans le développement et l'implémentation de protocoles garantit que les produits provenant de différents fabricants peuvent fonctionner ensemble pour créer des communications efficaces.

Les règles de fonctionnement des réseaux locaux et de l'internet sont issues de normes[1] définies au niveau mondial. On trouve notamment 3 organisations complémentaires :

- l'**EIA/TIA** (Electronics Inidustry Alliance et Telecommunications Industry Association) édite des **normes de câbles** transportant les signaux électriques (par exemple les câbles croisés et câbles droits vus dans la séance précédente) ;
- l'**IEEE** (Institute of Electrical and Electronics Engineers) est connu pour ses travaux relatifs à la **norme Ethernet** et autres technologies de réseaux locaux ;
- l'**IETF** (Internet Engineering Task Force - Détachement d'ingénierie d'Internet) se consacre à Internet ainsi qu'à la communication entre LAN, autrement dit à l'interconnexion de réseaux : il a pour rôle d'établir les normes relatives au protocole TCP/IP (que nous avons commencé à étudier dans le thème 2), protocole implémenté dans les réseaux locaux et sur Internet.

Les règles sont applicables à tous les opérateurs qui interviennent au sein des réseaux.

Nous nous intéresserons particulièrement dans cette séance au protocole Ethernet utilisé dans les réseaux locaux.

1 Une norme est un processus ou un protocole reconnu par l'industrie du réseau et ratifié par une organisation de normes.

I Le protocole Ethernet

95 % des réseaux locaux sont aujourd'hui régis par le protocole Ethernet qui déterminent les capacités et les limites du système et en décrivent les règles de fonctionnement comme :

- l'association possible entre un support, une bande passante et une manière de transmettre l'information ;
- la définition des processus qui permettent aux périphériques réseau d'accéder aux supports réseau et de transmettre des trames dans des environnements réseaux hétérogènes.

Pour garantir la compatibilité de tous les périphériques Ethernet, l'IEEE a mis au point des normes que les fabricants et les développeurs doivent respecter lors de la conception de périphériques Ethernet.

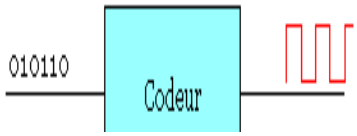
À chaque norme technologique correspond un numéro, qui fait référence au comité responsable de l'approbation et de la maintenance de la norme. **Le comité responsable des normes Ethernet est le 802.3 pour le filaire** et 802.11 pour le WiFi.

Depuis la création d'Ethernet en 1973, les normes se sont développées et spécifient désormais des versions plus rapides et plus flexibles. Chaque version d'Ethernet comporte une norme.

Par exemple, la norme **802.3u** créée en 1995 **notée 100BASE-TX représente les normes d'Ethernet 100 mégabits avec câbles à paires torsadées**. La notation standard se traduit comme suit :

- **100** est la vitesse en Mbit/s (bande passante).
- **BASE** désigne la transmission en bande de base.
- **TX** désigne le type de câble, dans ce cas, les paires torsadées : X signifie l'utilisation de 2 paires sur les 4.

La transmission en bande de base consiste à transmettre directement (sans modulation) les signaux numériques (suites de bits) sur le support selon une méthode de codage (NRZ, NRZI, Manchester, MLT3, nB/mB, etc.) déterminée en partie selon la vitesse désirée (4B/5B: Fast Ethernet ; 8B/10B :Gigabit Ethernet).



Elle peut transporter les signaux électriques ou lumineux dans les deux sens (transmission bidirectionnelle) et, comme nous l'avons vu avec le commutateur, certains équipements d'un réseau en bande de base transmettent les signaux numériques dans les deux sens simultanément.

1 Quelques normes Ethernet filaires 802.3

Nom commercial	Vitesse	Dénomination physique	Standard	Support, longueur
Ethernet	10 Mbps	10BASE-T	IEEE 802.3	Cuivre, 100 m
Fast Ethernet	100 Mbps	100BASE-TX	IEEE 802.3u	Cuivre, 100 m
Gigabit Ethernet	1 Gbps	1000BASE-SX, 1000BASE-LX	IEEE 802.3z	Fibre, 550 m, 5 Km
Gigabit Ethernet	1 Gbps	1000BASE-T	IEEE 802.3ab	Cuivre, 100 m
10Gigabit Ethernet	10 Gbps	10GBASE-SR, 10GBASE-LR	IEEE 802.3ae	Fibre, 300 m, 25 Km
10Gigabit Ethernet	10 Gbps	10GBASE-T	IEEE 802.3an	Cuivre, 100 m

NB 1 : un câble en cuivre est certifié pour 100 m (ça ne veut pas dire qu'en pratique on ne peut pas dépasser mais si on le fait on est "hors bonnes pratiques").

NB 2 : la longueur de la fibre est donnée pour la fibre multimode (la plus faible longueur) et pour la fibre monomode (la plus grande longueur).

NB 3 : il existe d'autres normes qui autorisent d'autres distances selon le débit.

2 Les normes Ethernet sans fil

Trois normes de communications de données courantes s'appliquent aux supports sans fil.

Quelles sont les normes WiFi rencontrées le plus souvent actuellement ?

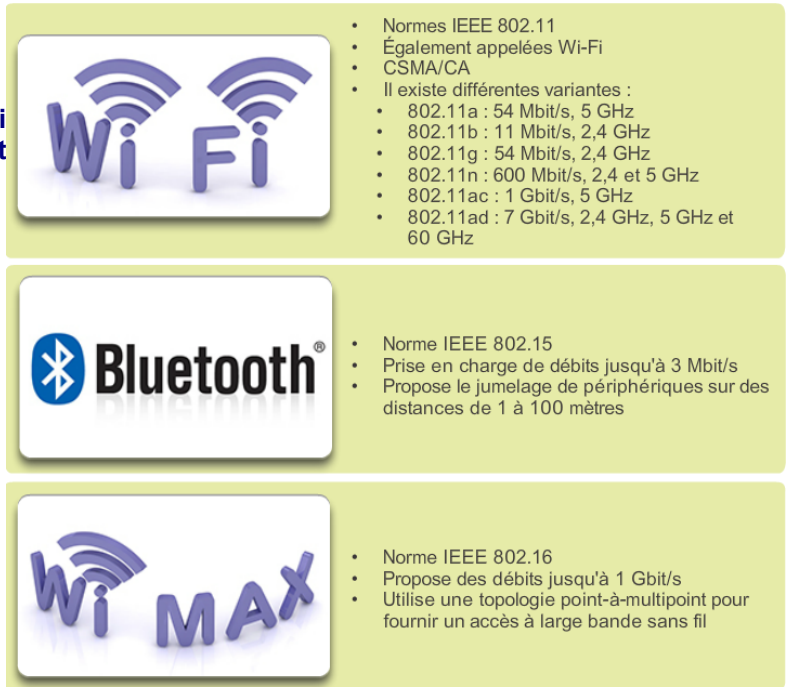


Schéma issu du cours Cisco CCNA Discovery

II Le fonctionnement d'Ethernet

Dans un réseau de type Ethernet, **les informations circulent sous forme d'une trame Ethernet** normalisée 802.3 et/ou Ethernet II (suite de bits transmis en série les uns après les autres).

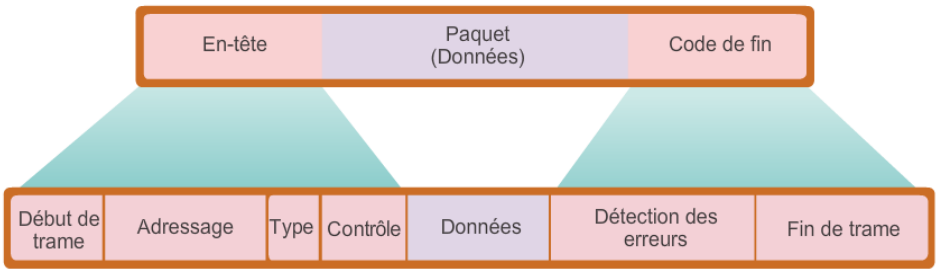
Par exemple, un fichier envoyé d'un hôte à un autre est **encapsulé** dans une ou plusieurs trames avant d'être envoyé sur le support.

Le contenu d'une trame permet de répondre notamment aux **problématiques suivantes :**

- Quels nœuds sont en communication ?
- Quand la communication entre les nœuds individuels commence-t-elle et quand se termine-t-elle ?
- Y a-t-il eu des erreurs lorsque les nœuds communiquaient ?
- Quelles sont les données transportées ?
- Quelles sont les applications du système concernées par les données transportées ?

1 La trame Ethernet v2

Les différentes informations présentes dans une trame sont de nature à faciliter leur traitement par les équipements intermédiaires (commutateur, routeur, etc.) car elle contient des données qui seront analysées par les différentes applications du récepteur.

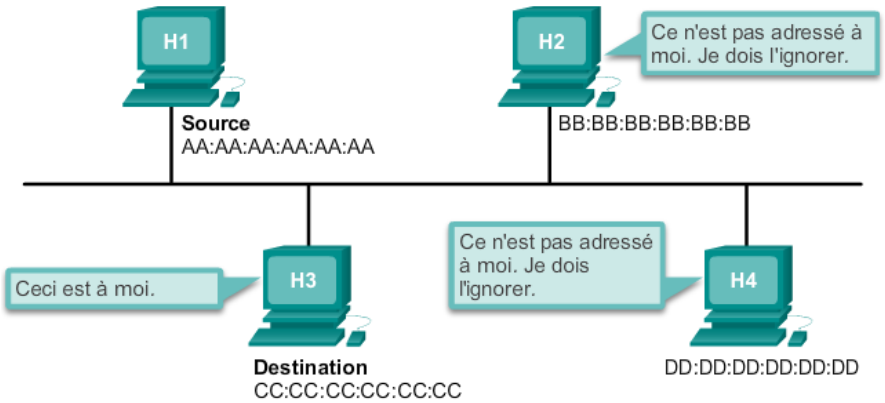


La trame comprend les éléments suivants :

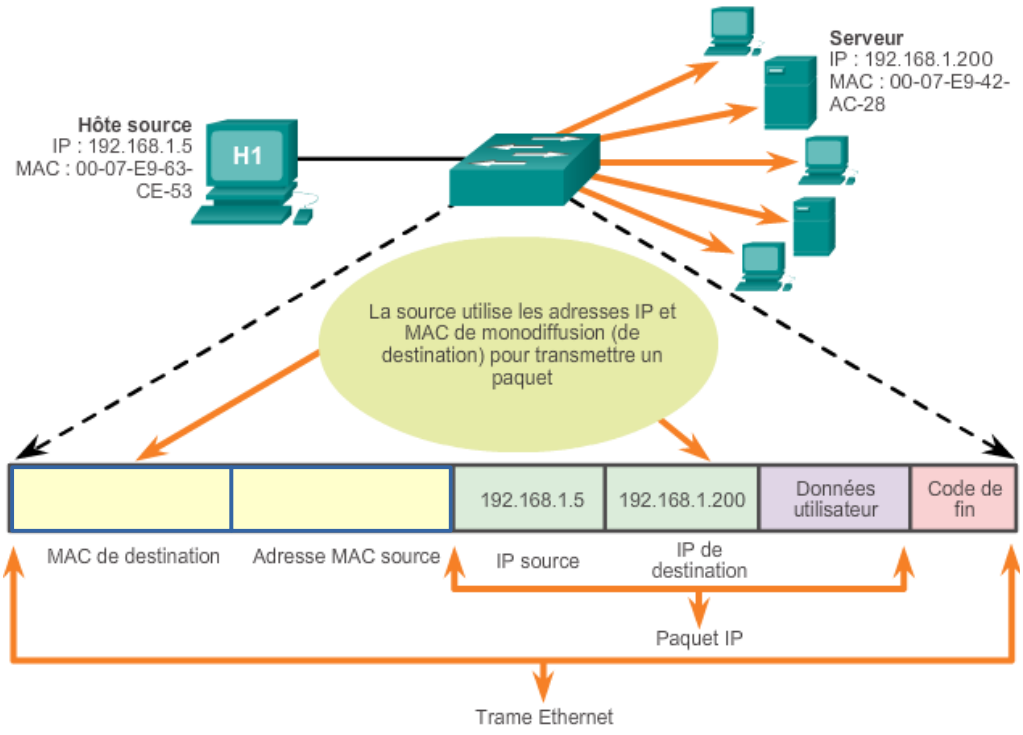
- Le *début de trame* (appelé aussi préambule) permet de synchroniser les horloges des interfaces réseaux. Il n'est pas lu par l'interface réseau.
- L'*adressage* permet d'identifier les nœuds source et de destination (voir schéma ci-dessous).
- Le *type* permet d'identifier le protocole inséré dans le champ "données" : en fonction du type, la suite de la trame sera interprétée en conséquence.
- Le *contrôle* permet d'identifier les services de contrôle de flux spécifiques.
- Les *données* contiennent l'en-tête IP, l'en-tête de la couche transport et les données d'application.
- La *détection d'erreur* permet de contrôler qu'une trame est valide.
- La *fin de trame* contient des informations de contrôle pour la détection d'erreurs.

Les éléments de la trame Ethernet qui permettent d'identifier les nœuds participant à l'échange sont les adresses MAC (Media Acces Control) de destination et source :

Adresse de destination	Adresse source	Données
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Données encapsulées
Adressage des trames		



Q1. H1 envoie un message au serveur. Reconstituez ci-dessous les champs relatifs à l'adressage



1.1 Les adresses MAC

Q2. Comment une carte réseau sait-elle qu'une trame lui est destinée ?

Les adresses MAC (Media Acces Control) sont attribuées physiquement par le constructeur à toutes les cartes réseaux des périphériques susceptibles de devoir envoyer et/ou recevoir des données sur le réseau : postes de travail, serveurs, imprimantes, routeurs, etc. **Tous les périphériques connectés à un réseau ont donc des interfaces dotées d'une adresse MAC.**

Une adresse MAC (par exemple 5c514f7c0777 en hexadécimal) est composée de 48 bits :

- elle est généralement donnée sous forme hexadécimale de 6 octets (1 octet = 2 symboles hexadécimaux compris entre 0 et 9 et entre A et F) séparés de 2 points 5c:51:4f:7c:07:77 ;
- les 24 premiers bits (3 octets = 6 symboles hexa) identifient le constructeur de la carte : la Zone OUI (Organizationally Unique Identifier) est un identifiant sur 3 octets attribué par l'IEEE ;
- les 24 derniers bits identifient la carte chez le constructeur.

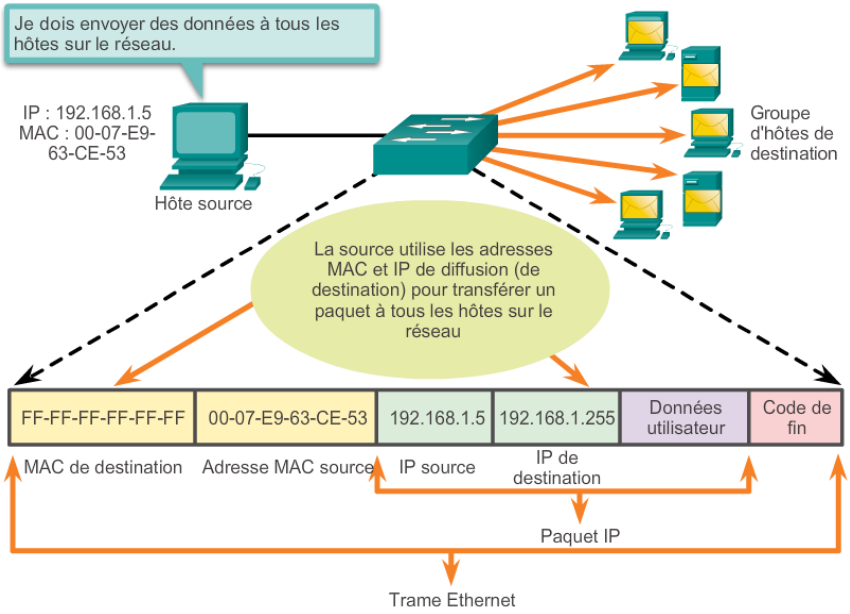
5c	51	4f	7c	07	77
Constructeur de la carte (Zone OUI)			Identification de la carte		

Q3. À partir du site https://standards.ieee.org/develop/regauth/oui/public.html, trouvez le constructeur de la carte qui a pour adresse MAC 5c514f7c0777 ?

1.2 Adresse MAC et adresse de diffusion

Lorsqu'un hôte veut envoyer un message à tous les autres éléments du réseau, il utilise une adresse IP spéciale (où tous les bits de l'hôte sont à 1) appelée "adresse IP de diffusion". L'adresse MAC correspondante est donc forcément "virtuelle" puisqu'elle ne correspond pas à une carte réseau unique et formellement identifiée.

Q4. À partir du l'exemple ci-contre, dire quelle est l'adresse MAC de diffusion en Hexadécimal et en bits.



Q5. Peut-on trouver cette adresse MAC de diffusion dans le champ "adresse MAC source" ? Justifiez votre réponse.

1.3 La longueur d'une trame

Une transmission entre deux postes d'un gros fichier ne doit pas monopoliser la bande passante pendant tout l'échange : une trame a donc une taille limite maximum appelée MTU (Maximum Transfert Unit).

Lors de l'envoi d'un message (un fichier par exemple), celui-ci sera découpé en plusieurs trames ; le récepteur devra reconstituer le message d'origine à partir de toutes les trames.

La **longueur d'une trame** est constituée comme présentée ci-dessous :

8	6	6	2	46à1500	4
Préambule	Adresse de destination	Adresse source	Type	Données	Séquence de contrôle de trame2

Q6. Quelles sont, en octets, les tailles minimum et maximum d'une trame (hors préambule) ?

2 Le contrôle d'accès au support

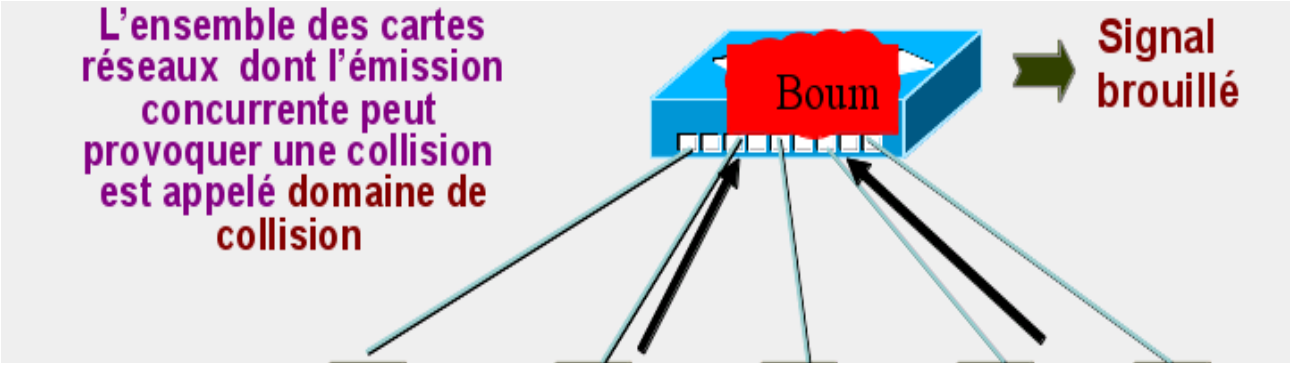
Après **l'encapsulation du message** dans une ou plusieurs trames, le protocole Ethernet gère le placement de la ou les trames sur le support et, éventuellement, leur suppression : c'est ce qu'on appelle le **contrôle d'accès au support.**

La topologie logique sous-jacente d'Ethernet est un bus à accès multiple. Par conséquent, tous les nœuds (périphériques) d'un même segment de réseau doivent partager le support.

2.1 Concentrateur et collision de données

Le concentrateur (hub) répète les signaux qu'il reçoit sur un port, sur tous ses autres ports.

Ainsi, si deux stations émettent en même temps, il y a collision des données.



Une méthode d'accès permettant de gérer les conflits est donc nécessaire.

Principes de la méthode d'accès CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Les formes traditionnelles d'Ethernet ont été développées pour utiliser cette méthode la méthode d'accès CSMA/CD :

Écoute de la porteuse : si une station veut émettre, elle écoute le réseau pour savoir s'il y a déjà une autre émission en cours. Si elle détecte un signal, elle attend, sinon elle émet.

Émission du signal : la station émet, mais elle continue à écouter pendant son émission afin de vérifier que ses données n'ont pas été perturbées (subit une collision).

En cas de collision : si une collision a lieu (par exemple si deux stations émettent en même temps), les deux machines interrompent leur communication et attendent un délai aléatoire, puis la première ayant passé ce délai peut alors réémettre.
Si le nombre de collisions successives dépasse un certain seuil (généralement 16), on considère qu'il y a une erreur fatale et l'émission s'interrompt avec la condition "excessive collisions".

Collision et half-duplex

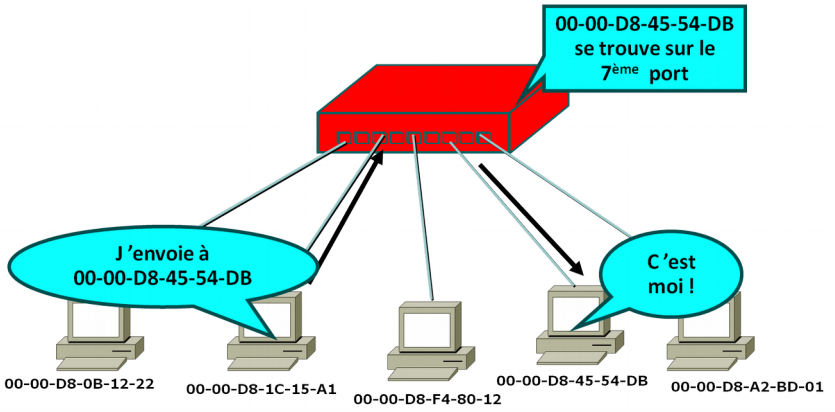
La détection de collision oblige l'interface réseau à écouter le média pendant l'émission d'une trame.

Une interface réseau a deux circuits, un circuit pour l'émission (TX) et un circuit pour la réception (RX).

Pendant l'émission sur TX, le circuit de réception RX est monopolisé par la détection de collision ==> on ne peut donc pas recevoir et émettre en même temps avec cette méthode d'accès.
==> La transmission en Ethernet de base (basée sur les concentrateurs) est donc Half-Duplex.

2.2 Fonctionnement avec un commutateur

Lorsque le commutateur reçoit un message, il lit l'adresse MAC destinataire, inspecte chacun de ses ports pour déterminer où est connecté le poste destinataire et ré-émet le message seulement vers celui-ci.



Q7. Comment les commutateurs connaissent-ils les adresses MAC associés à chaque port ?

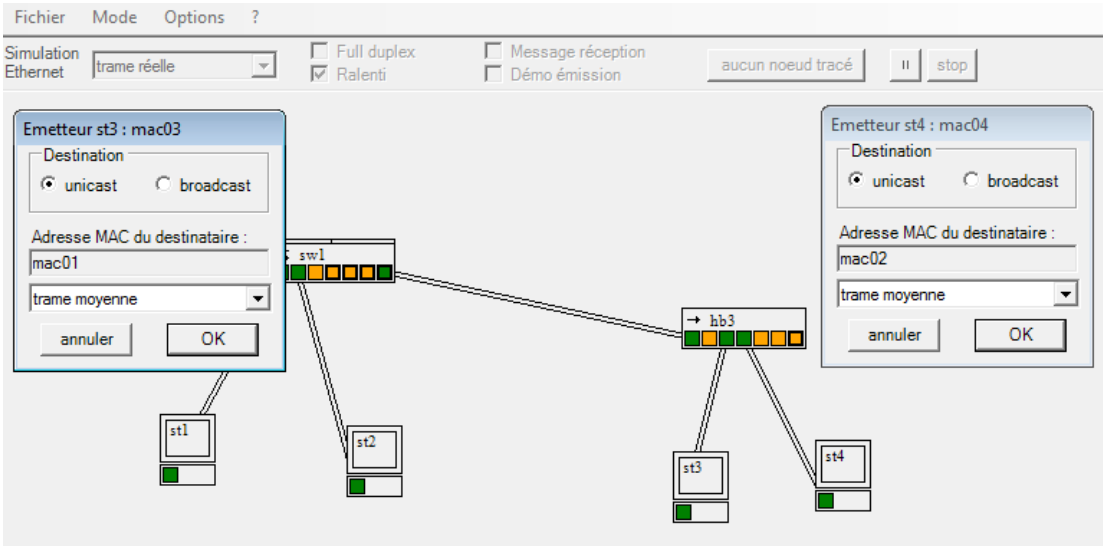
Un commutateur a deux modes de fonctionnement :

- **Store and forward** : les commutateurs ne transmettent que les trames valides (FCS contrôlé) : ils stockent donc les données dans des mémoires tampons : ceci entraîne certes un retard mais évite la retransmission de trames défectueuses. C'est un mode de fonctionnement obligatoire pour l'analyse de la qualité de service.
- **On the fly** : les commutateurs n'attendent pas d'avoir lu toute la trame pour la transmettre ==> solution avantageuse lorsqu'un grand nombre de données doit être transféré, entre des nœuds peu nombreux..

Activité

Lancez le simulateur réseau (icône « Simulateur réseau 3 » sur le bureau et ouvrir le fichier xml.

A1 - Fichier à utiliser : unHubUnSwitch – Passer en mode Ethernet



*Vous utilisez le **mode trame réelle** pour essayer de provoquer une collision (il y a un concentrateur, vous devriez y arriver). **Pour cela, vous allez envoyer des trames simultanément : les deux trames doivent être préparées avant tout envoi** (le mode "trame réelle" permet cela).*

A2 - Fichier à utiliser : fedeSwitch.xml.
L'architecture est entièrement commutée, mais on est quand même en half-duplex car les cartes réseaux ne supportent pas le full-duplex : vous décochez la case « Full duplex ».
Le commutateur est configuré en mode « store and forward ».

- Envoyez par exemple :
  - une trame de st1 vers st5 et en même temps une trame de st5 vers st1 ;
  - une trame de broadcast de st1 et en même temps une trame de broadcast de st5 ;

  Que constatez-vous ?

- Refaites la même démonstration en configurant les commutateurs en mode « on the fly ». Que constatez-vous ?

A3 - Fichier à utiliser : full.xml
Dans une architecture entièrement commutée, il n'y a plus de collision. On peut donc travailler en mode full-duplex car la paire de réception n'est plus monopolisée pendant l'envoi pour détecter la collision.
Les commutateurs sont ici configurés en mode « on the fly » .

Attention « on the fly » et « full duplex » sont des techniques indépendantes, on peut être à la fois en mode « store and forward » et en mode « full duplex ».

- Refaites les manipulations précédentes. Envoyez par exemple :
  - une trame de st1 vers st5 et en même temps une trame de st5 vers st1 ;
  - une trame de broadcast de st1 et en même temps une trame de broadcast de st5 ;

  Répondez aux questions suivantes.

- Quels sont les avantages et les inconvénients du type « on the fly » ?

- Quel est l'intérêt du « full duplex » ?

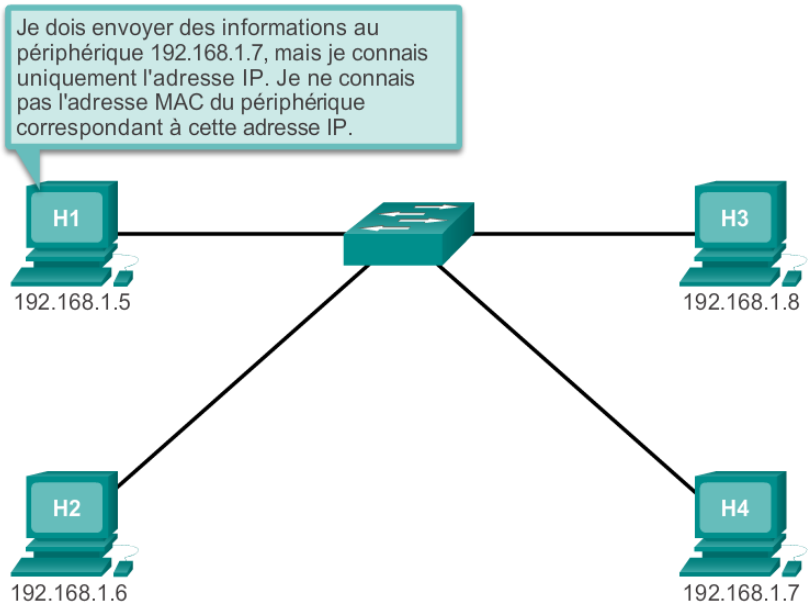
Avant de réémettre une trame, un commutateur vérifie que les liaisons RX sont libres => il évite ainsi les collisions ==> Dans un environnement entièrement commuté, c'est-à-dire sans concentrateur, il ne peut pas se produire de collision.
==> On peut dans ce dernier cas désactiver la détection de collision sur la paire RX et travailler en full duplex.

Actuellement, la quasi-totalité des connexions filaires entre les périphériques d'un réseau local sont des connexions bidirectionnelles simultanées (un périphérique envoie et reçoit des données simultanément). Ainsi, même si les réseaux Ethernet actuels sont conçus avec la technologie CSMA/CD, avec les périphériques récents, aucune collision ne se produit et les processus CSMA/CD sont devenus inutiles.

Les collisions sont toujours possibles sur les connexions sans fil. Les périphériques des réseaux locaux sans fil (Ethernet 802.11) utilisent la **méthode CSMA/CA (CSMA/Collision Avoidance) :** le périphérique examine le support pour établir si celui-ci comporte un signal de données. Si le support est libre, le périphérique envoie une notification à travers celui-ci pour indiquer son intention de l'utiliser. Le périphérique transmet alors ses données.

III Adresses IP et adresses MAC : le protocole ARP

Chaque hôte dispose d'une adresse IP et d'une adresse MAC. Pour envoyer des données, le nœud utilise ces deux adresses.



Au niveau logique, lorsqu'un hôte du réseau s'adresse à un autre hôte (ou à un ensemble d'hôte), il utilise l'adressage IP.
Et au final, au niveau physique, comme nous venons de le voir, c'est l'adresse MAC qui est utilisé.

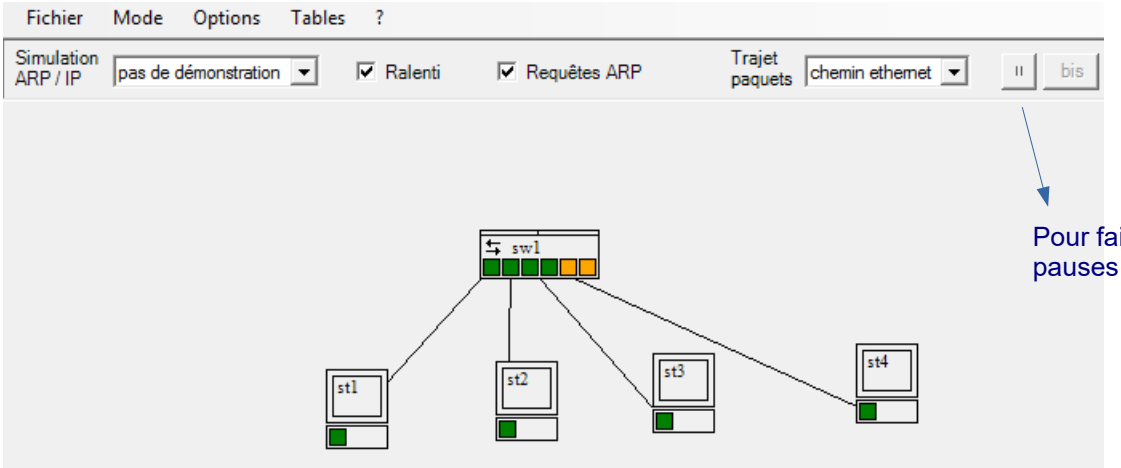
Lorsqu'un hôte transmet un message sur un réseau Ethernet, il doit intégrer des informations d'en-tête dont l'adresse MAC source et de destination. L'hôte connaît bien évidemment l'adresse MAC source puisqu'il s'agit de la sienne. Mais il ne connaît pas forcément l'adresse MAC de destination, il connaît juste l'adresse IP de destination.

Il existe un protocole qui permet d'obtenir l'adresse physique d'un élément à partir de son adresse IP : c'est le protocole ARP (Address Resolution Protocol)

Activité

Lancez le simulateur réseau Sopirem et ouvrez le fichier unSwitchIP.xml.

Vous vous mettez en mode IP, vous activez le type de simulation « pas de démonstration » et vous cochez les cases "ralenti" et "Requêtes ARP"



Rappel :

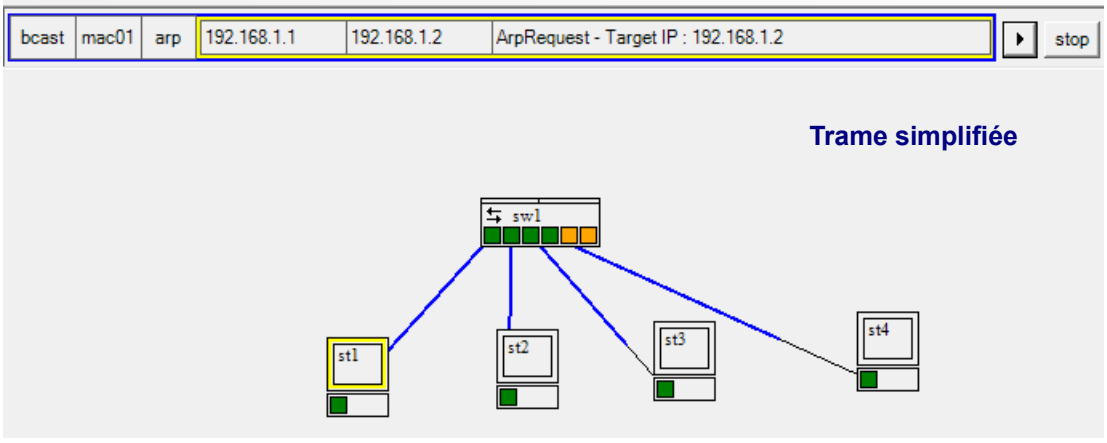
- pour faire un ping on clique droit sur le poste (et non sur la carte) ;
- Les lignes bleues représentent la communication physique (Ethernet) ;
- les lignes jaunes la communication logique (IP).
- L'option « Les stations s'annoncent » au niveau de la configuration générale Ethernet a été activée (menu options / configurer, onglet Ethernet).

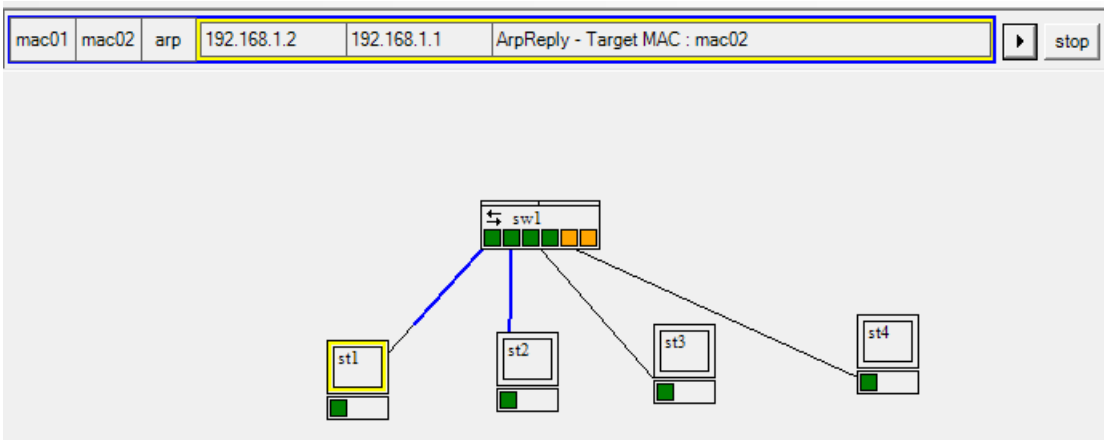
Q8. Quelles sont les conséquences sur le fait que l'option « Les stations s'annoncent » ait été activée ?

Le fait de cocher la case « Requetes ARP » a pour effet de vider tous les caches ARP des postes mais ceux-ci se remplissent au fur et à mesure des manipulations. Pour observer les requêtes ARP, il vous faudra donc, dans certains cas, vider le cache ARP.

Faites un ping de st1 vers st2. *N'hésitez pas à recommencer (sans oublier de vider le cache ARP, dans ce cas) et/ou à faire des pauses).*

Vous constatez les premier et deuxième échanges suivants :





Q9. Quelle adresse a-t-on utilisé pour initier l'échange ?

Q10. Y a-t-il une diffusion Ethernet (broadcast) avant que le ping ne soit effectivement effectué ?

Q11. En consultant les contenus des deux trames simplifiées, dire quel est l'objectif de cette diffusion.

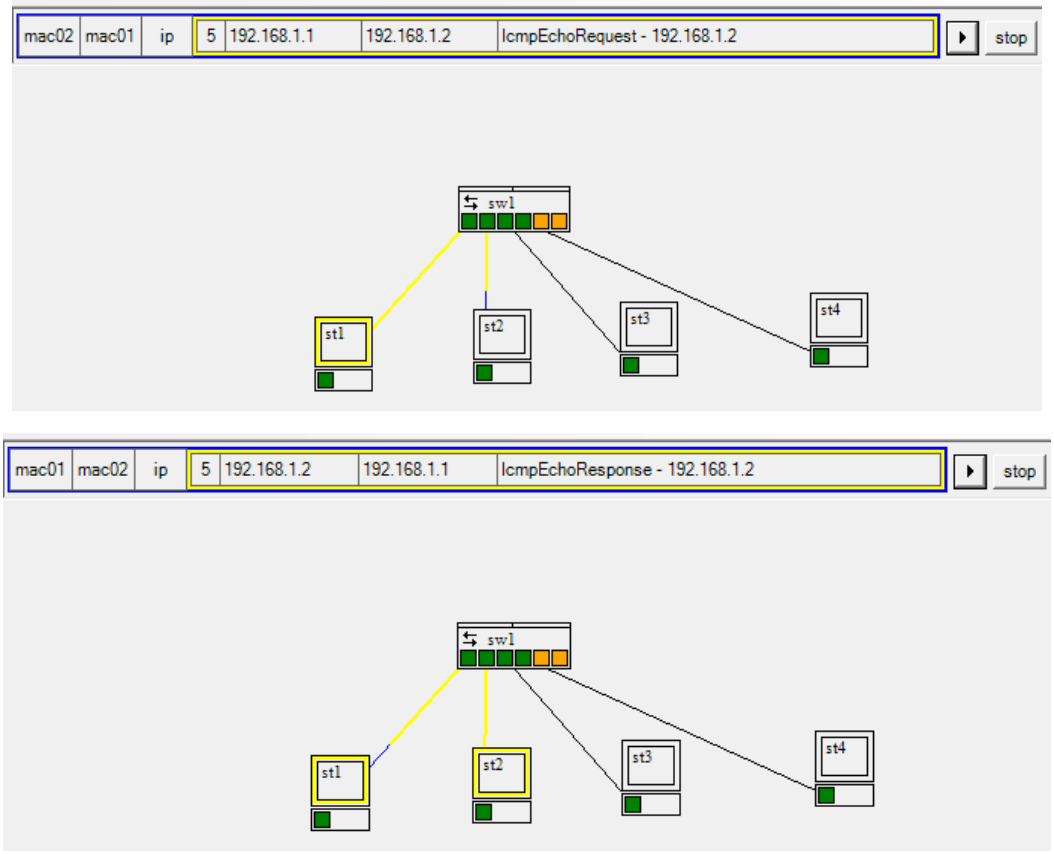
La station st1 a envoyé une requête de diffusion demandant à quelle adresse mac correspondait l'adresse IP 192.168.1.2 et st2 (qui a reconnu son adresse IP) lui a répondu en lui envoyant son adresse mac.

Q12. À qui est adressée la trame "ArpRequest" ?

Q13. À qui est adressée la trame "ArpReply" ?

Q14. En consultant les contenus des deux trames simplifiées, dire quel est le contenu du champ "type" et ce qu'il annonce dans ce cas précis.

Vous constatez ensuite les deux échanges unicast suivants :



Q15. En consultant les contenus des deux trames simplifiées, dire quel est le contenu du champ "type" et expliquez pourquoi il a changé.

↗ **Consultez le cache arp (clic droit puis Tables/Cache ARP) du poste st1. Que contient-il ?**

Q16. Quels sont les postes dont les caches ARP ont été mis à jour et pourquoi ?

↗ **Refaites le même ping sans vider le cache et répondez aux questions suivantes.**

Q17. Le paquet ICMP est-il transmis immédiatement ?

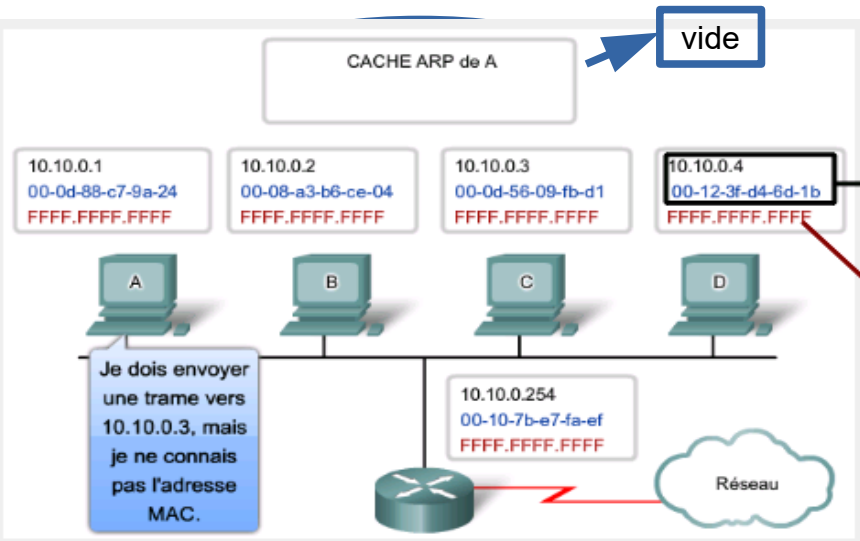
Q18. Pourquoi n'y a-t-il pas eu d'échanges ARP ?

↗ Mettez-vous en mode IP et activez le type de simulation « automatique » (de manière à pouvoir observez chaque étape). Décochez « ralenti » et activez « Requête arp ». Videz le cache ARP de st1. Après un ping de st1 vers st2, vous observez les étapes suivantes :

- recherche du destinataire qui a pour adresse IP 192.168.1.2 ;
- examen de la table de routage du poste pour déterminer s'il s'agit d'un paquet destiné au réseau ;
- examen du cache ARP ==> aucune correspondance trouvée ;
- mise en attente du paquet jusqu'à ce que l'adresse MAC de destination soit trouvée ;
- envoi d'un Arp Request sur le réseau ;
- les postes qui reçoivent le paquet mettent en cache la correspondance entre mac01 et son adresse IP ;
- chaque poste inspecte ensuite le paquet pour voir s'ils doivent le traiter ;
- seul le poste st2 qui a reconnu son adresse IP le traite, les autres l'abandonnent ;
- st2 envoie un ArpReply à st1 pour lui donner son adresse MAC ;
- st1 met en cache à son tour l'adresse mac de st2 ;
- st1 utilise l'adresse MAC en cache pour finir de reconstituer la trame et envoyer le ping ;
- st2 répond au ping en utilisant le cache arp qui contient l'association entre st1 et son adresse IP.

Q19. Videz de nouveau le cache ARP de st1. Éteignez le poste st4 puis faites un ping de st1 vers ce poste. Quelles sont les étapes qui ne sont pas réalisées ?

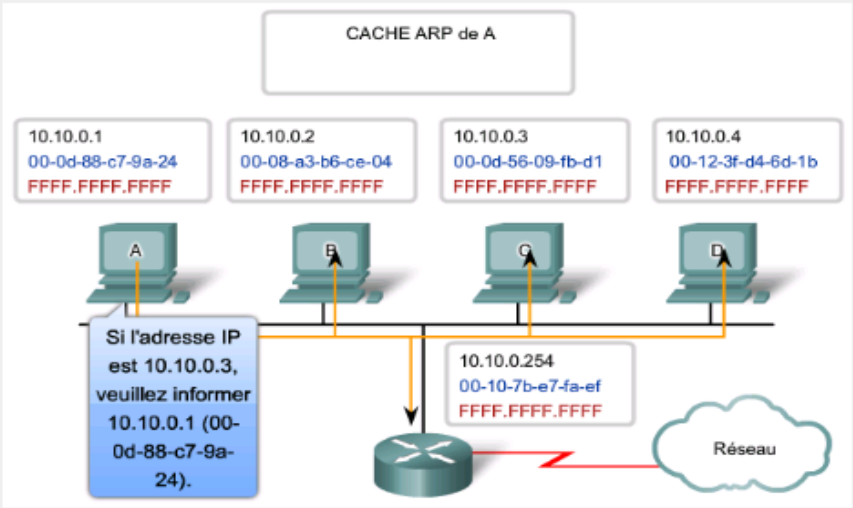
Récapitulatif sur le protocole ARP



Une interface réseau connaît :

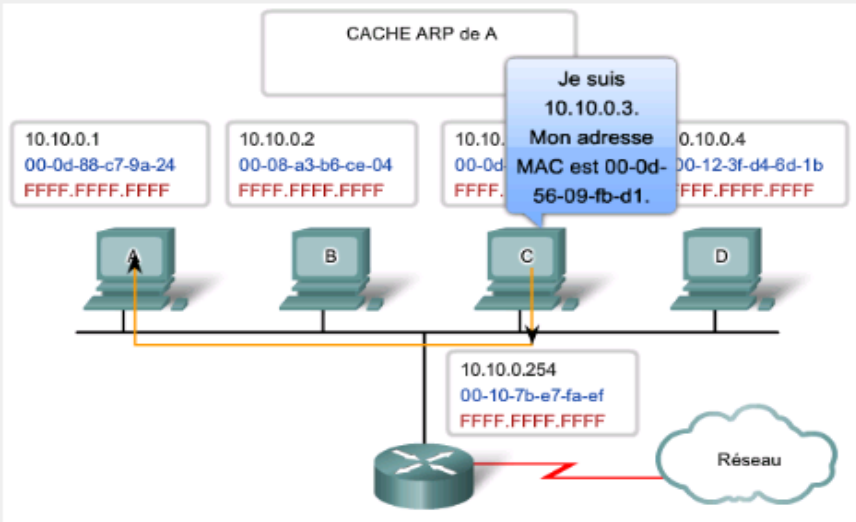
- son adresse IP
- son adresse MAC
- l'adresse MAC de diffusion

Adresse MAC qui permet la diffusion



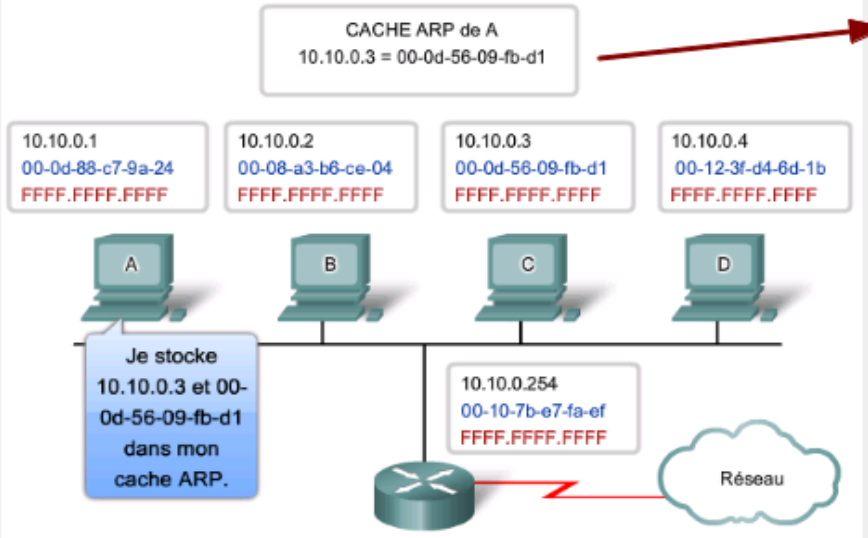
Si le processus ARP ne trouve pas dans le cache l'adresse MAC correspondante à l'adresse IP recherchée, il envoie alors un paquet de requête ARP (requête de diffusion utilisant l'adresse MAC FFFFFFFFFFFF pour trouver l'adresse MAC du périphérique de destination sur le réseau local.

Tous les éléments sur le réseau local lisent cette requête

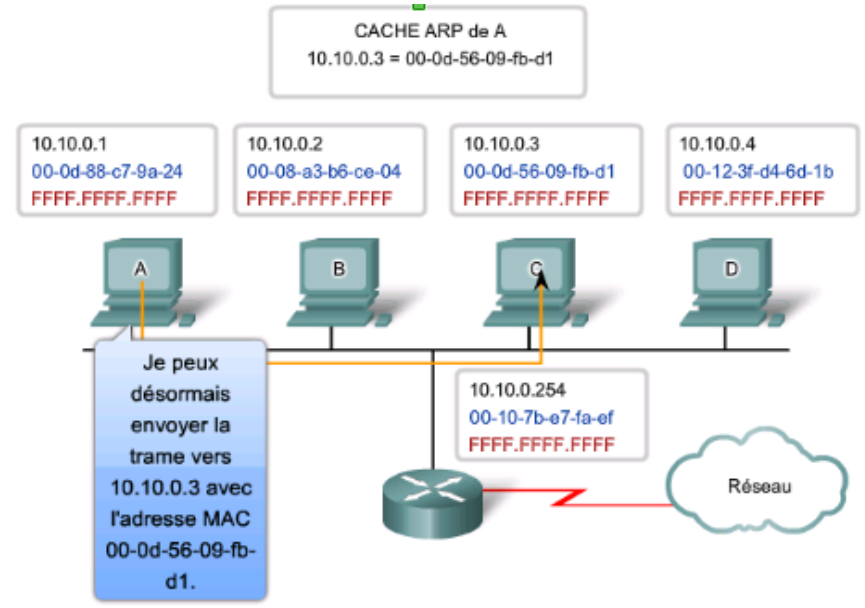


Si le périphérique qui reçoit la requête possède l'adresse IP de destination, il répond à l'aide d'une réponse ARP dans laquelle il insère son adresse MAC

Si aucun périphérique ne répond à la requête ARP, le paquet est abandonné car il est impossible de créer une trame ==> possibilité de message d'erreur (cf quand on « pingue » une adresse qui n'existe pas)



- Une entrée est créée dans la table ARP. Les paquets à destination de cette adresse IPv4 peuvent à présent être encapsulés dans des trames.
- Chaque entrée ou ligne de la table ARP comporte deux valeurs : une adresse IP et une adresse MAC.
- La table ARP garde en mémoire cache un certain temps le mappage des périphériques du réseau local (LAN



Le paquet IP comportant les adresses IP source et destination est encapsulé dans la trame comportant les adresses MAC source et destination

Dans un réseau local il y a deux systèmes d'adressage :

- physique : adresse MAC ;
- logique : adresse IP

Le protocole ARP (Address Résolution Protocol) est un processus qui permet de passer de l'adresse IP logique à l'adresse MAC Physique :

1. quand un hôte veut envoyer une trame à un destinataire, il regarde dans son cache ARP s'il a une correspondance entre l'adresse mac du destinataire et son adresse IP ;
2. s'il n'a pas cette correspondance, l'émetteur crée et envoie une trame de diffusion dont le message contient l'adresse IP du destinataire ;
3. chaque hôte reçoit la trame et compare l'adresse IP contenu dans le message à sa propre adresse et seul l'hôte dont l'adresse correspond renvoie son adresse MAC ;
4. l'hôte émetteur reçoit le message et enregistre l'adresse MAC et l'adresse IP momentanément dans une table appelée « Table ARP ».

Une fois que l'hôte émetteur dispose de l'adresse MAC dans sa table il n'a plus besoin d'envoyer de requête ARP et peut envoyer directement des trames à l'adresse de destination.

Il ne faut pas confondre le cache ARP d'un poste avec la table d'adresses MAC/PORT d'un commutateur.