Télécommunications et Réseaux

Chapitre 2 : Communication et protocoles réseaux

Cours de M. Petein Thomas

Email : thomas.petein@heh.be

Communication et protocoles réseaux

Introduction

Comme nous avons eu vu précédemment, les réseaux actuels permettent de communiquer via une multitude de services différents.

Pour rendre cela possible à travers une seule structure unique, il a fallu la mise au point de modèles unanimes décrivant les règles et les fonctions du réseau.

Dans ce chapitre, vous découvrirez ces modèles, ainsi que les normes qui permettent aux réseaux de fonctionner. Vous connaîtrez également les processus de communication sur un réseau.

Règles de communication

Un réseau peut être très complexe et consister en des périphériques connectés à Internet, ou alors très simple, comme deux ordinateurs connectés directement entre eux par un seul câble.

Cependant, il ne suffit pas de connecter physiquement des périphériques finaux pour permettre la communication. Les périphériques doivent également savoir comment communiquer.

Quelle que soit la méthode choisie, tous les modes de communication ont en commun trois éléments :

- l'émetteur : il s'agit bien entendu de la source du message, ou l'expéditeur. Les sources d'un message sont les personnes, ou les périphériques électroniques, qui doivent envoyer un message à d'autres personnes ou périphériques.

- le récepteur : appelé aussi le destinataire ou la destination du message. La destination reçoit le message et l'interprète.

- le support de transmission ou canal de transmission : c'est l'élément qui fournit la voie par laquelle le message se déplace depuis la source vers la destination.

Communication et protocoles réseaux

Imaginez deux personnes communiquant face à face.
Avant de communiquer, elles doivent se mettre d'accord sur la façon de communiquer.

Si la communication fait appel à la voix, les partenaires doivent d'abord définir la langue. Ensuite, lorsqu'elles ont un message à partager, elles doivent pouvoir mettre ce message en forme de sorte qu'il soit compréhensible.

Par exemple, si une personne utilise l'anglais, mais que la structure de sa phrase est mauvaise, le message peut facilement être mal compris.

Il va donc falloir mettre en place un certain nombre de règles et de protocoles pour qu'une communication s'établissent correctement entre deux personnes.

Bien entendu il en va de même pour la communication entre deux ou plusieurs ordinateurs.

Communication et protocoles réseaux

Donc nous sommes d'accord, pour pouvoir communiquer entre elles, les personnes doivent utiliser des règles établies ou des conventions qui régissent la conversation.

Les protocoles utilisés dépendent des caractéristiques du mode de communication, notamment la source, la destination et le canal.

Ces règles ou protocoles doivent être respectés pour que le message soit correctement transmis et compris.

Il existe de nombreux protocoles qui régissent la communication humaine.
Une fois qu'une méthode de communication a été convenue (face à face, par téléphone, par lettre), les protocoles mis en place doivent répondre aux conditions suivantes :

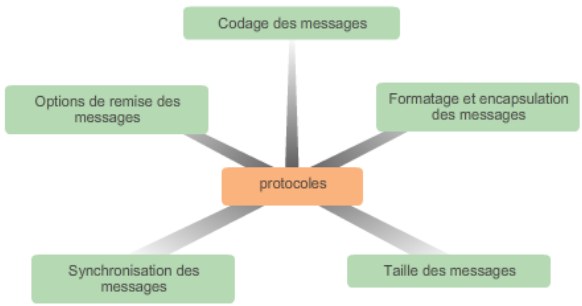
- Expéditeur et destinataire identifiés
- Même langue et syntaxe
- Vitesse et rythme d'élocution
- Demande de confirmation ou d'accusé de réception

Communication et protocoles réseaux

Concernant les protocoles utilisés dans les communications réseau, c'est à peu près la même chose que pour les communications humaines.

En plus d'identifier la source et la destination, les protocoles informatiques et réseau définissent la manière dont un message est transmis sur un réseau pour répondre aux conditions ci-dessus.

Il existe de nombreux protocoles qui doivent interagir, mais les protocoles informatiques courants sont les suivants :



Codage de message

Pour envoyer un message, il faut tout d'abord le coder !

Le **codage** est le processus de conversion des informations vers un autre format acceptable, à des fins de transmission.

Le **décodage** est le processus inverse ; il permet d'interpréter les informations.

Imaginez quelqu'un qui vous appelle pour vous expliquer quelque chose.

Pour faire passer le message, elle convertit ses pensées dans un langage convenu au préalable.

Elle prononce ensuite les mots au moyen de sons et d'inflexions, qui véhiculent le message.

Son ami écoute la description et décode les sons pour comprendre le message reçu.

Au niveau des réseaux, c'est la même chose : le format du codage entre les hôtes doit être adapté au support.

Les messages envoyés sur le réseau sont d'abord convertis en bits par l'hôte émetteur.

Chaque bit est codé en impulsions électriques, ou ondes lumineuses, selon le support sur lequel les bits sont transmis.

L'hôte de destination reçoit et décode les signaux pour interpréter le message.

Communication et protocoles réseaux

Formatage et encapsulation des messages

Lorsqu'un message est envoyé de la source à la destination, il doit respecter un format ou une structure spécifique.

Les formats des messages dépendent du type de message et du type de canal utilisés pour remettre le message.

Un exemple parlant est l'envoi d'une lettre par la poste.

Pour être envoyées, les lettres doivent également être insérées ou contenues dans une enveloppe.

L'enveloppe comporte l'adresse de l'expéditeur et celle du destinataire, chacune étant écrite à l'endroit prévu à cet effet.

Si l'adresse de destination et le format ne sont pas corrects, la lettre n'est pas remise.

Au niveau réseau, le processus consistant à placer un format de message (la lettre) dans un autre (l'enveloppe) s'appelle « encapsulation ».

Une « désencapsulation » a lieu lorsque le processus est inversé par le destinataire et que la lettre est retirée de l'enveloppe.

On peut faire une analogie avec les messages informatiques : Chaque message informatique est encapsulé dans un format spécifique, appelé **trame**, avant d'être transmis sur le réseau.

Elle fournit l'adresse de la destination souhaitée et celle de l'hôte source.

A savoir que le format et le contenu de la trame sont déterminés par le type de message envoyé et par le canal sur lequel ce dernier est transmis.

Destination (adresse matérielle/ physique)	Source (adresse matérielle/ physique)	Indicateur de début (indicateur de début du message)	Destinataire (identificateur de la destination)	Expéditeur (identificateur de la source)	Données encapsulées (bits)	Fin de la trame (indicateur de fin du message)
Adressage des trames		Message encapsulé				

Les messages qui ne sont pas correctement formatés ne sont ni livrés ni traités par l'hôte de destination.

Communication et protocoles réseaux

Taille des messages

La taille des messages fait également l'objet d'une règle de communication.

Par exemple, lorsque les personnes communiquent, les messages qu'elles envoient sont généralement limitées, en termes de taille, à ce que le destinataire peut comprendre ou traiter en une fois.

Imaginons que ce cours tienne en une seule et longue phrase. Il serait difficile à lire et à comprendre.

D'une manière identique, lorsqu'un long message est envoyé par un hôte à un autre hôte sur le réseau, il est nécessaire de décomposer le message en plusieurs petites parties.

Bien entendu, les règles qui régissent la taille de ces parties de données sont très strictes et elles peuvent être différentes selon le canal utilisé.

Par exemple, les trames trop longues ou trop courtes ne sont pas livrées.

Comme nous l'avons déjà évoqué, un hôte source doit donc segmenter son message, c'est-à-dire le décomposer en portions plus petites répondant aux impératifs de taille (minimale et maximale).

Chaque portion est encapsulée dans une trame distincte avec les informations d'adresse, puis transmise sur le réseau. Au niveau de l'hôte destinataire, les messages sont désencapsulés et recomposés pour être traités et interprétés.

Synchronisation des messages

La synchronisation affecte également la qualité de la réception et de la compréhension d'un message.

Les personnes utilisent la synchronisation pour déterminer le moment de la prise de parole, le débit de parole et le temps d'attente d'une réponse.

Au niveau réseau cela se traduit par *la méthode d'accès*, *la gestion de flux* et *le délai d'attente de la réponse.*

- *Méthode d'accès*

La méthode d'accès détermine le moment où un individu peut envoyer un message. Ces règles de synchronisation dépendent de l'environnement.

Par exemple, vous pouvez parler si vous avez quelque chose à dire.

Dans cet environnement, avant de prendre la parole, l'intervenant doit attendre que tout le monde ait fini de parler.

Si deux personnes parlent en même temps, une collision d'informations se produit et elles doivent s'arrêter et recommencer.

Pour les ordinateurs il est également nécessaire de définir une méthode d'accès pour savoir à quel moment les hôtes doivent commencer à envoyer des messages et comment réagir en cas d'erreurs.

Communication et protocoles réseaux

- *Contrôle de flux*

La synchronisation affecte également la quantité d'informations pouvant être envoyées, ainsi que leur vitesse d'acheminement.

Si une personne parle trop rapidement, l'autre personne éprouve des difficultés à entendre et à comprendre le message.

Dans une communication réseau, les hôtes source et de destination utilisent le contrôle de flux pour négocier une synchronisation correcte en vue d'établir une communication.

- *Délai d'attente de la réponse*

Si une personne pose une question et qu'elle n'a pas de réponse dans un délai acceptable, elle suppose qu'aucune réponse n'a été donnée et réagit en conséquence.

Les hôtes du réseau sont également soumis à des règles qui spécifient le délai d'attente des réponses et l'action à entreprendre en cas de dépassement du délai d'attente.

Options de remise des messages

Un message peut être transmis de différentes manières selon les besoins.

Je peux par exemple transmettre une information à une seule personne parmi vous.

Mais je peux aussi m'adresser à un groupe de personnes comme à un des groupes de laboratoire.

Finalement, mon message peut être destiné à l'ensemble des personnes présentes ici.

Les hôtes d'un réseau utilisent des options similaires de remise des messages pour communiquer :

- Lorsqu'un hôte envoie un message à destination d'un seul destinataire, on parle de **monodiffusion**.
- Lorsqu'il envoie un message à tout les destinataires présents sur le réseau, on parle de **diffusion**.
- Lorsqu'il souhaite communiquer avec un groupe d'utilisateurs, on parle de **multidiffusion**.

Parfois, l'expéditeur d'un message doit également s'assurer que le message a bien été reçu par son destinataire.
→ Dans ce cas, le destinataire doit renvoyer un accusé de réception à l'expéditeur.

Si aucun accusé de réception n'est requis, l'option de remise est dite « sans accusé de réception ».

Communication et protocoles réseaux

Monodiffusion

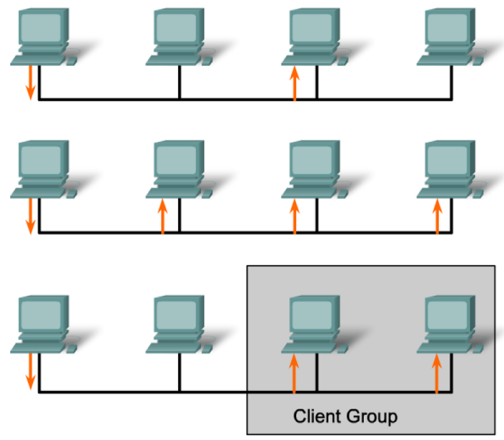
Unicast:
One sender and one receiver

Diffusion

Broadcast:
One sender to all other addresses

Multidiffusion

Multicast:
One sender to a group of addresses



Protocoles de communication

Comme dans les communications humaines, les différents protocoles réseau et informatiques doivent pouvoir interagir et œuvrer ensemble à faire aboutir la communication réseau.

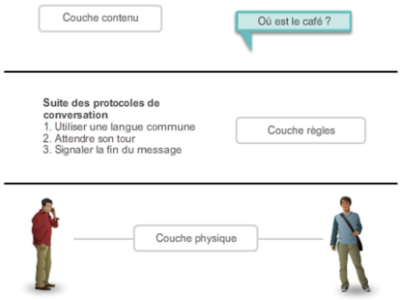
Pour remplir une fonction de communication, on a besoins de plusieurs protocoles interreliés, c'est ce qu'on appelle une **suite de protocoles**.

Les suites de protocoles sont mises en œuvre par les hôtes et les périphériques réseau dans le logiciel, le matériel ou les deux.

Pour mieux visualiser l'interaction des protocoles d'une suite, imaginez que celle-ci est une pile. Une pile de protocoles indique comment chacun des protocoles de la suite est mis en œuvre.

Les protocoles sont représentés par des couches et chaque service de niveau supérieur dépend de la fonctionnalité définie par les protocoles constituant les niveaux inférieurs.

Communication et protocoles réseaux

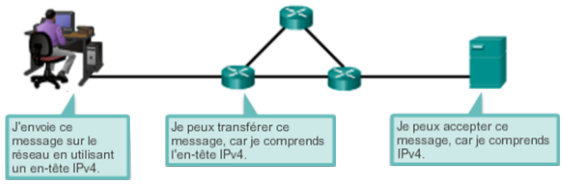


→ L'utilisation de couches permet de décomposer une tâche complexe en différentes parties simples et de décrire leur fonctionnement.

Communication et protocoles réseaux

Afin que des périphériques puissent communiquer correctement, une suite de protocoles réseau doit décrire des exigences et des interactions précises.

Les protocoles réseau définissent un format et un ensemble communs de règles d'échange des messages entre les périphériques.

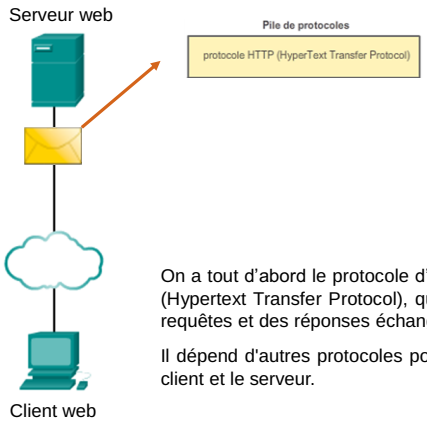


Par exemple, le protocole IP définit la façon dont un paquet de données est acheminé au sein d'un réseau ou à un réseau distant.

→ Les informations du protocole IPv4 sont transmises dans un format spécifique de sorte que le récepteur puisse les interpréter correctement.

Communication et protocoles réseaux

Exemple concret de l'utilisation d'une suite de protocoles : *la consultation de pages web* (autrement dit l'interaction entre un serveur Web et un client Web)



Même si vous ne le remarquez pas, cette interaction utilise plusieurs normes et protocoles dans le processus d'échange d'informations entre ceux-ci.

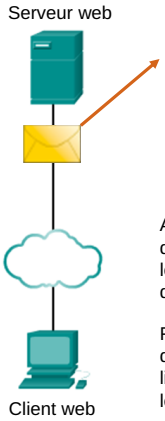
Les différents protocoles fonctionnent entre eux pour garantir que les messages sont reçus et compris par les deux parties.

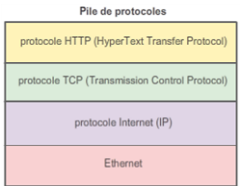
On a tout d'abord le protocole d'application, dans ce cas le **protocole HTTP** (Hypertext Transfer Protocol), qui décrit le contenu et la mise en forme des requêtes et des réponses échangées entre le client et le serveur.

Il dépend d'autres protocoles pour gérer le transport des messages entre le client et le serveur.

Communication et protocoles réseaux

Ensuite vient le **protocole TCP** (Transmission Control Protocol) qui va se charger de diviser les messages HTTP en petites parties, appelées segments.





Ces segments sont envoyés entre les processus du serveur Web et du client exécutés sur l'hôte de destination.

Ce protocole est également responsable du contrôle de la taille et du débit d'échange de messages entre le serveur et le client.

Après nous avons le **protocole IP** (Internet Protocol) qui se charge d'encapsuler en paquets les segments mis en forme par le protocole TCP, de leurs attribuer les adresses appropriées et de les remettre à l'hôte de destination en utilisant le meilleur chemin.

Finalement on a les **protocoles d'accès au réseau** (comme Ethernet) qui décrivent deux fonctions principales, d'une part la communication sur une liaison de données et d'autre part la transmission physique des données sur le support réseau.

Communication et protocoles réseaux

Les protocoles de gestion de liaison de données prennent les paquets depuis le protocole IP et les formatent pour les transmettre à travers les supports.

Les normes et les protocoles des supports physiques régissent la manière dont les signaux sont envoyés, ainsi que leur interprétation par les clients destinataires.

→ Comme on vient de le voir, **une suite de protocoles est un ensemble de protocoles qui fonctionnent ensemble pour fournir des services de communication réseau complets.**

Une suite de protocoles peut être définie par un organisme de normalisation ou développée par un constructeur.

Les protocoles basés sur des normes sont des processus ou des protocoles qui ont été validés par le secteur des réseaux et ratifiés, ou approuvés, par un organisme de normalisation.

L'utilisation de normes dans le développement et la mise en œuvre de protocoles garantit que les produits provenant de différents fabricants fonctionnent ensemble.

Attention que certains protocoles sont *propriétaires*. Propriétaire, dans ce contexte, signifie qu'une société ou qu'un fournisseur contrôle la définition du protocole et la manière dont il fonctionne. Ces protocoles propriétaires peuvent être utilisés par différentes organisations avec l'autorisation du propriétaire.

HEH be Sciences et technologies

Communication et protocoles réseaux

Suite de protocoles et normes de l'industrie

Les protocoles vus précédemment comme **HTTP**, **TCP** ou **IP** sont tous des protocoles appartenant à la *suite de protocoles TCP/IP*.

Cette suite de protocoles est une norme *ouverte*, ce qui signifie que ces protocoles peuvent être utilisés gratuitement par tous et que tous les constructeurs ont la possibilité de les mettre en œuvre sur leur matériel ou leurs logiciels.

Nom de la couche TCP/IP	TCP/IP	ISO	AppleTalk	Novell Netware
Application	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transport	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Accès réseau	Ethernet ARP WLAN			

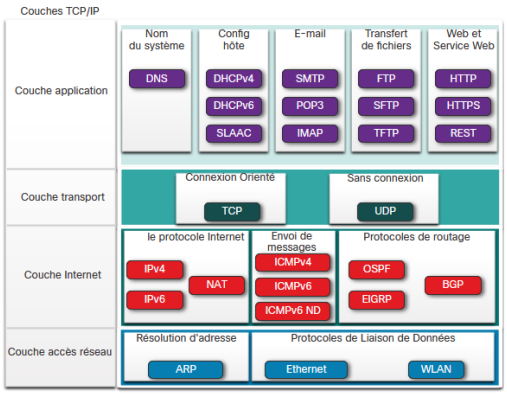
AppleTalk et Novell NetWare sont des exemples de protocoles propriétaires.

HEH be Sciences et technologies

Communication et protocoles réseaux

La suite de protocoles TCP/IP

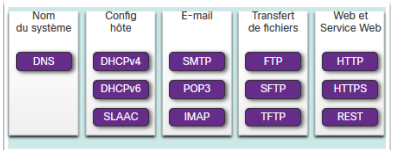
TCP/IP est la suite de protocoles utilisée par Internet et les réseaux actuels car cette suite a 2 aspects importants pour les fournisseurs et les fabricants :



- ✓ Il s'agit d'une suite de protocoles standards ouvertes : elle est donc librement accessible au public et peut être utilisée par n'importe quel fournisseur.
- ✓ Il s'agit d'une suite de protocoles basée sur des normes : elle a été approuvée par le secteur des réseaux et par des organismes de normalisation.

Communication et protocoles réseaux

Couche application



Au niveau de la couche application de ce modèle, on retrouve des protocoles tels que :

- **DNS** (Domain Name System ou Domain Name Service) qui a pour rôle de traduire les noms de domaines. Par exemple www.cisco.com en adresse IP.
- **DHCP** (Dynamic Host Configuration Protocol) qui attribue dynamiquement des adresses IP aux stations clientes au démarrage.
- **SMTP** (Simple Mail Transfert Protocol) qui permet aux clients (ou aux serveurs) d'envoyer un e-mail à un serveur de messagerie.
- **POP** (Post Office Protocol) et **IMAP** (Internet Message Access Protocol) qui permettent aux clients de récupérer des e-mails depuis un serveur de messagerie.
- **FTP** (File Transfert Protocol), **SFTP** (Secure FTP) et **TFTP** (Trivial FTP) qui permettent à un utilisateur d'accéder à des fichiers sur un autre hôte du réseau.
- **HTTP** (HyperText Transfert Protocol) et **HTTPS** (HTTP Secure) qui permettent d'échanger du texte, des graphiques, des sons, des vidéos et autres fichiers multimédias sur le Web.
- **REST** (Representational State Transfer) qui est un style d'architecture logicielle définissant un ensemble de contraintes à utiliser pour créer des services web.

Communication et protocoles réseaux

Couche transport

Par rapport à la couche transport, on retrouve deux protocoles principaux :

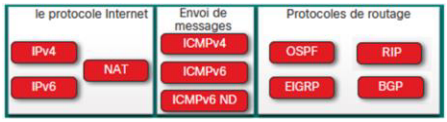
- **UDP** (User Datagram Protocol) qui permet à un processus exécuté sur un hôte d'envoyer des paquets à un processus exécuté sur un autre hôte mais sans connexion au préalable et sans confirmation de réussite de la transmission de datagrammes.

- **TCP** (Transmission Control Protocol) qui, au contraire d'UDP, permet une communication fiable entre les processus s'exécutant sur des hôtes distincts.

HEH be Sciences et technologies

Communication et protocoles réseaux

Couche Internet



Au niveau de la couche internet, on retrouve différents protocoles :

- **IP** (Internet Protocol) qui permet de recevoir des segments de message de la couche transport. Il regroupe les messages en paquets et il indique l'adresse des paquets pour permettre leur acheminement de bout en bout sur un interréseau.
- **NAT** (Network Address Translation) qui permet de convertir les adresses IP d'un réseau privé en adresses IP globales et publiques.
- **ICMP** (Internet Control Message Protocol) qui permet à un hôte de destination de signaler à l'hôte source des erreurs liées aux transmissions de paquets.
- **RIP** (Routing Information Protocol) qui est un protocole de routage dynamique à vecteur de distance.
- **OSPF** (Open Shortest Path First) qui est un protocole de routage à état de liens permettant de faire du routage dynamique.
- **EIGRP** (Enhanced Interior Gateway Routing Protocol) qui est un protocole de routage dynamique propriétaire à Cisco.
- **BGP** (Border Gateway Protocol) qui est un protocole de routage de passerelle extérieure standard ouvert utilisé entre les fournisseurs de services Internet (ISPs).

HEH be Sciences et technologies

Communication et protocoles réseaux

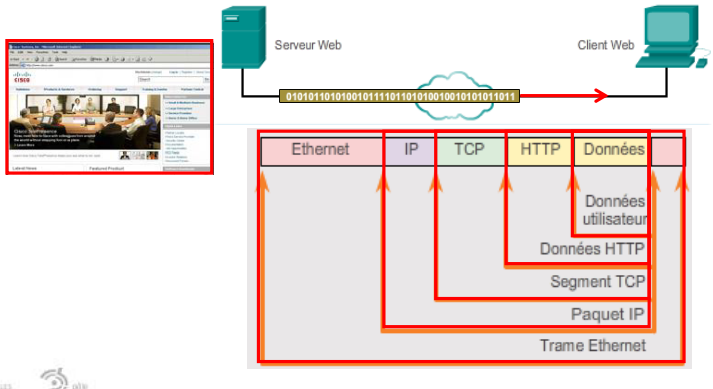
Couche accès réseau

Au niveau de la couche d'accès au réseau, on retrouve des protocoles tels que :

- **ARP** (Address Resolution Protocol) qui fournit un mappage dynamique entre une adresse logique (adresse IP) et une adresse physique (addresse MAC).
- **Ethernet** qui définit les règles de câblage et de signalisation de la couche d'accès réseau.
- **PPP** (Point to Point Protocol) qui permet d'encapsuler des paquets pour les transmettre via une connexion en série.
- **WLAN** (Wireless LAN) qui définit les règles de signalisation sans fil sur les fréquences radio 2,4 GHz et 5 GHz.
- **Pilotes d'interface** qui fournissent des instructions à un ordinateur permettant de contrôler une interface déterminée sur un périphérique réseau.

Concrètement, comment se passe un échange entre deux périphériques utilisant le modèle TCP/IP ?

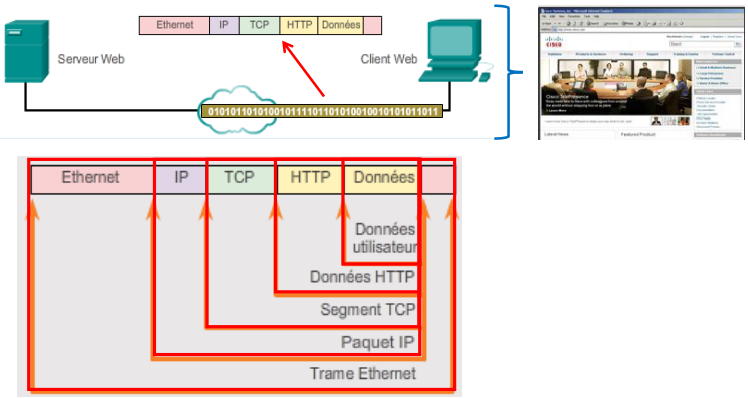
Reprenons le cas d'un client Web qui envoie une demande à un serveur Web pour consulter une page web. Le serveur lui répond en lui envoyant les données de la page en question.



HEH be Sciences et technologies

Communication et protocoles réseaux

Que se passe-t-il au niveau du client maintenant ?



Organismes de normalisation

Nous allons maintenant discuter des normes et des organismes qui mettent au point ces normes.

Tout d'abord il existe deux catégories de normes : les normes dites ouvertes et les normes propriétaires.

Les normes ouvertes favorisent la concurrence et l'innovation. Elles empêchent également qu'un seul produit d'une entreprise monopolise le marché ou puisse bénéficier d'un avantage inique sur ses concurrents.

Les normes propriétaires sont quant à eux développés et généralement utilisés par un constructeur et qui ne fonctionnent donc qu'avec le matériel de celui-ci.

Bien entendu, les organismes de normalisation sont nombreux et ils jouent un rôle important en assurant qu'Internet reste ouvert, que ses spécifications et protocoles soient accessibles librement et puissent être mis en œuvre par tous les constructeurs.

En plus, les organismes de normalisation sont généralement des associations à but non lucratif qui ne sont liées à aucun constructeur. Leur objectif est de développer et de promouvoir le concept des normes ouvertes.

Communication et protocoles réseaux

Voici les principaux organismes de normalisation :

- Internet Society (**ISOC**) qui est chargée de promouvoir le développement, l'évolution et l'utilisation ouverts d'Internet dans le monde entier.

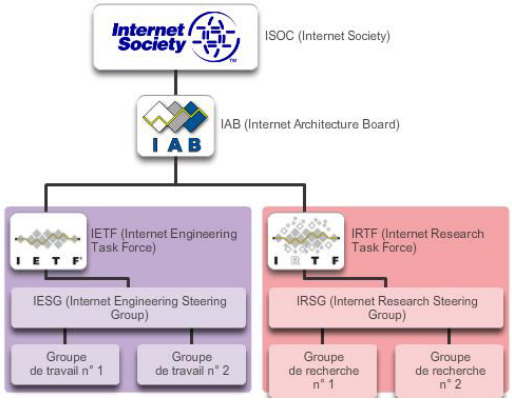
- Internet Architecture Board (**IAB**) qui s'occupe de la gestion et du développement généraux des normes Internet. Il assure la surveillance des protocoles et des procédures d'architecture utilisés par Internet. Les membres de l'IAB agissent en qualité de personne privée et ne représentent aucune entreprise, aucune institution ni aucune autre organisation.

- Internet Engineering Task Force (**IETF**) qui a pour but de de développer, de mettre à jour et d'assurer la maintenance d'Internet et les technologies TCP/IP. L'une des principales responsabilités de l'IETF est de produire des *documents RFC* (Request for Comments), c'est-à-dire des notes décrivant les protocoles, les processus et les technologies d'Internet.

L'IETF se compose de différents groupes de travail qui constituent les principales entités de développement des spécifications et des recommandations de l'organisme. Les groupes de travail sont constitués à des fins précises et dès que leurs objectifs sont remplis, ils sont dissous.

Communication et protocoles réseaux

▪ Internet Research Task Force (**IRTF**) qui se concentre sur la recherche à long terme liée à Internet et aux protocoles TCP/IP (contrairement à l'IETF qui s'intéresse surtout aux besoins à court terme), aux applications, à l'architecture et aux technologies.



HEH be Sciences et technologies

Communication et protocoles réseaux

▪ En plus de ces organismes là, il y a également l' Institute of Electrical and Electronics Engineers (**IEEE**). L'IEEE est une association américaine professionnelle s'adressant aux spécialistes du génie électrique et de l'électronique qui souhaitent se consacrer à l'innovation technologique et à la création de normes.

IEEE

L'organisme rassemble plus de 400 000 membres dans plus de 160 pays.

Il s'agit d'un organisme de normalisation majeur sur le plan international.

Il crée et gère des normes affectant un grand nombre de secteurs, notamment l'électricité et l'énergie, la santé, les télécommunications et les réseaux.

Les normes 802 de l'IEEE traitent des réseaux locaux et des réseaux métropolitains, y compris les réseaux filaires et sans fil.

WALLONIE-BRUXELLES ENSEIGNEMENT pôle hainaut

Chaque norme IEEE correspond à un groupe de travail chargé de créer et d'améliorer des normes. Au niveaux des groupes de travail des normes 802, on retrouve notamment :

- 802.1 qui est un groupe de travail sur les protocoles LAN de couche supérieure.
- 802.3 qui est un groupe de travail sur Ethernet.
- 802.11 qui est un groupe de travail sur les LAN sans fil (WLAN).
- 802.15 qui est un groupe de travail sur les réseaux personnels sans fil (WPAN).

Les normes 802.3 et 802.11 de l'IEEE jouent un rôle de premier plan dans les réseaux informatiques.

La norme 802.3 définit le contrôle d'accès au support (MAC ou Media Access Control) de l'Ethernet filaire. Cette technologie sert généralement aux réseaux locaux, mais certaines de ses applications concernent également le réseau étendu (WAN).

La norme 802.11 définit un ensemble de normes relatives à la mise en œuvre des réseaux locaux sans fil (WLAN). Elle définit la couche physique et la sous-couche de liaison de données MAC du modèle OSI pour les communications sans fil.

Communication et protocoles réseaux

- Finalement, un autre organisme bien connu est l'organisation internationale de normalisation (**ISO**). Il s'agit du plus grand concepteur de normes internationales pour une large gamme de produits et services. ISO n'est pas l'acronyme du nom de l'organisation.

Organisation internationale de normalisation

En réalité, le terme ISO provient du mot grec « isos » qui signifie « égal ». L'organisation internationale de normalisation a choisi le terme ISO pour affirmer sa volonté d'égalité envers tous les pays.

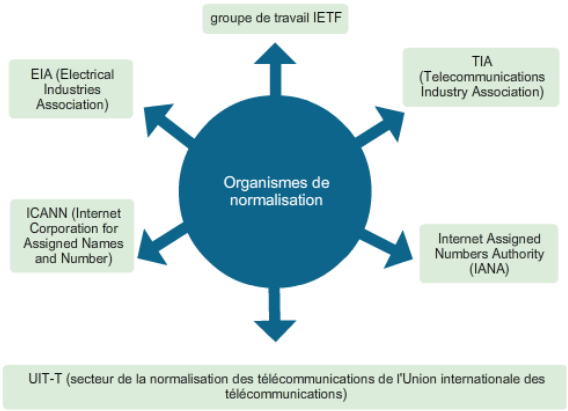
Dans le domaine des réseaux, elle est surtout célèbre pour son **modèle de référence OSI** (Open Systems Interconnection), publié en 1984 dans le but de développer un cadre composé de couches pour les protocoles réseau.

L'objectif initial de ce projet était non seulement de créer un modèle de référence, mais également de servir de base à une suite de protocoles applicables à Internet.

Toutefois, pour de multiples raisons, le choix de la suite de protocoles Internet ne s'est pas porté sur le modèle OSI, mais sur la suite TCP/IP.

Communication et protocoles réseaux

Lorsqu'on se penche sur les normes réseau, il est à noter que celles-ci font appel à plusieurs autres organismes de normalisation, dont voici les plus courants :



Communication et protocoles réseaux

- L'**EIA** (Electronic Industries Alliance), anciennement Electronics Industries Association, est une alliance commerciale internationale de normalisation dont le rôle concerne les entreprises d'électronique. L'EIA est connue pour ses normes associées au câblage électrique, aux connecteurs et aux racks 19 pouces utilisés pour monter l'équipement réseau.

- La **TIA** (Telecommunications Industry Association) est responsable du développement des normes de communication dans un grand nombre de domaines, incluant les équipements radio, les tours cellulaires, les dispositifs de VoIP et les communications par satellite. Plusieurs de ses normes sont élaborées en collaboration avec l'EIA.

- L'**ITU-T** (secteur de la normalisation des télécommunications de l'Union Internationale des Télécommunications) figure parmi les organismes de normalisation les plus grands et les plus anciens. L'ITU-T définit des normes de compression vidéo, de télévision sur IP et de communication haut débit, telles que la ligne d'abonné numérique (DSL). Par exemple, lorsque vous appelez un correspondant dans un autre pays, les codes de pays de l'ITU sont utilisés pour établir la connexion.

- L'**ICANN** (Internet Corporation for Assigned Names and Numbers) est une association à but non lucratif basée aux États-Unis qui coordonne l'attribution des adresses IP, la gestion des noms de domaine utilisés par le protocole DNS et les identificateurs de protocole ou numéros de ports utilisés par les protocoles TCP et UDP. L'ICANN crée des politiques et assume la responsabilité totale de ces attributions.

ICANN
Internet Corporation for Assigned Names and Numbers

- L'**IANA** (Internet Assigned Numbers Authority) est une composante de l'ICANN chargée de superviser et de gérer l'affectation des adresses IP, la gestion des noms de domaine et les identificateurs de protocole pour le compte de l'ICANN.

iana
Internet Assigned Numbers Authority

Communication et protocoles réseaux

Modèles de référence

On utilise souvent un modèle sous forme de couches, tel que le modèle TCP/IP ou le modèle OSI pour aider à visualiser l'interaction entre les différents protocoles.

Ce modèle illustre le fonctionnement des protocoles intervenant dans chaque couche, ainsi que leur interaction avec les couches supérieures et inférieures.

L'utilisation d'un modèle en couches présente certains avantages pour décrire des protocoles et des opérations sur un réseau :

- Aide à la conception d'un protocole, car des protocoles qui fonctionnent à un niveau de couche spécifique disposent d'informations définies à partir desquelles ils agissent, ainsi que d'une interface définie par rapport aux couches supérieures et inférieures.
- Encourage la concurrence, car les produits de différents fournisseurs peuvent fonctionner ensemble.
- Evite que des changements technologiques ou fonctionnels dans une couche ne se répercutent sur d'autres couches, supérieures et inférieures.
- Fournit un langage commun pour décrire les fonctions et les fonctionnalités réseau.

Nous allons maintenant voir les deux types de modèles réseau de base :

✓ **Le modèle de protocole**, qui suit la structure d'une suite de protocoles donnée. L'ensemble hiérarchique des protocoles associés dans une suite représente généralement toutes les fonctionnalités requises à l'interface entre le réseau humain et le réseau de données. Le ***modèle TCP/IP*** est un modèle de protocole, car il décrit les fonctions qui interviennent à chaque couche des protocoles au sein de la suite TCP/IP.

✓ **Le modèle de référence** assure la cohérence de tous les types de protocoles et services réseau en décrivant les opérations à effectuer à chaque couche, mais n'indique pas leur mise en œuvre. Un modèle de référence, comme le ***modèle OSI***, n'est pas destiné à être une spécification d'implémentation, ni à fournir un niveau de détail suffisant pour définir précisément les services de l'architecture réseau. Le principal objectif d'un modèle de référence est d'assurer une compréhension plus claire des fonctions et des processus impliqués.

Communication et protocoles réseaux

Le modèle OSI

Comme nous l'avons évoqué plus tôt, à l'origine, le modèle OSI a été conçu par l'organisation ISO pour fournir un cadre dans lequel concevoir une suite de protocoles système ouverts.

L'idée était que cet ensemble de protocoles serait utilisé pour développer un réseau international qui ne dépendrait pas de systèmes propriétaires.

Le modèle OSI est un modèle en 7 couches :

- 2 couches basses : dédiées à l'infrastructure des réseaux
- 2 couches moyennes : servant au contrôle du transport de l'information
- 3 couches hautes : liées à la gestion de l'application

Cependant, du fait de la rapidité avec laquelle Internet basé sur TCP/IP a été adopté et de sa vitesse de développement, l'élaboration et l'acceptation de la suite de protocoles OSI sont restées à la traîne.

Néanmoins, le modèle OSI a apporté des contributions essentielles au développement d'autres protocoles et produits pour tous les types de nouveaux réseaux.

HEH be Sciences et technologies

Communication et protocoles réseaux

7.	application	La ***couche application*** contient les protocoles utilisés pour les processus communications.
6.	présentation	La ***couche présentation*** fournit une représentation commune des données transférées entre des services de couche application.
5.	session	La ***couche session*** fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.
4.	transport	La ***couche transport*** définit des services pour segmenter, transférer et réassembler les données de communications individuelles entre les périphériques finaux.
3.	réseau	La ***couche réseau*** fournit des services permettant d'échanger des parties de données sur le réseau entre des périphériques finaux identifiés.
2.	liaison de données	Les protocoles de ***couche liaison de données*** décrivent des méthodes d'échange de trames de données entre des périphériques sur un support commun.
1.	physique	Les protocoles de la ***couche physique*** décrivent l'ensemble des moyens permettant de gérer des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau.

HEH be Sciences et technologies

Communication et protocoles réseaux

Modèle OSI

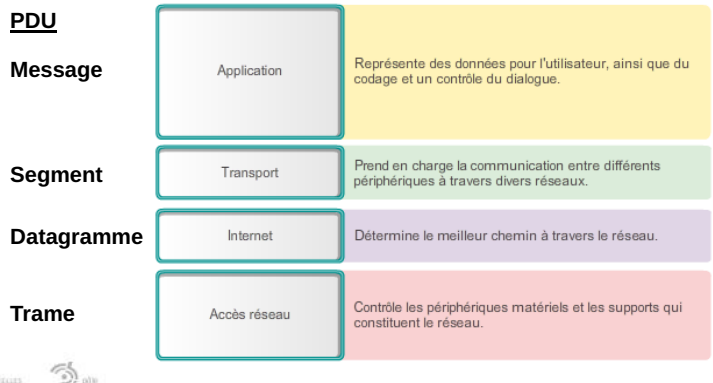
PDU (Protocol Data Unit) : « unité de données de protocole »

données	application
	présentation
	session
segment	transport
paquet	réseau
trame	liaison de données
bit	physique

Le modèle TCP/IP

Le modèle de protocole TCP/IP pour les communications interréseau fut créé au début des années 1970 et est parfois appelé modèle Internet.

Le modèle TCP/IP est un modèle en 4 couches :



Communication et protocoles réseaux

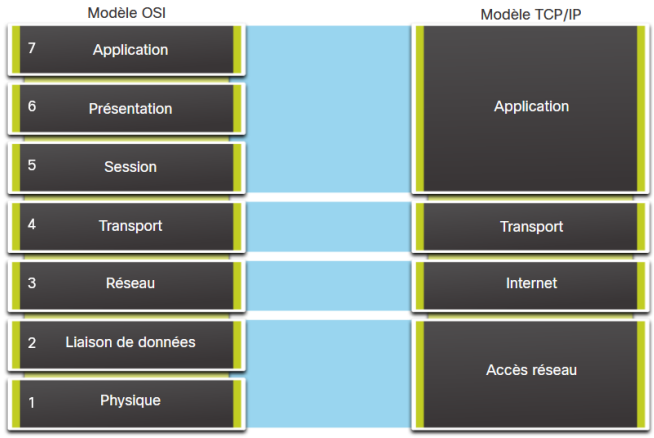
Pour rappel, le modèle TCP/IP est une norme ouverte, cela veut dire qu'aucune entreprise ne contrôle la définition du modèle.

Les définitions de la norme et des protocoles TCP/IP sont traitées dans un forum public et définies dans un ensemble de documents RFC disponible au public.

Les documents RFC contiennent les spécifications formelles des protocoles de communication de données ainsi que des ressources qui décrivent l'utilisation des protocoles.

Ils contiennent également des documents techniques et organisationnels concernant Internet, y compris les spécifications techniques et les documents relatifs aux politiques élaborés par l'IETF.

Comparaison entre le modèle OSI et le modèle TCP/IP :



Communication et protocoles réseaux

La couche application TCP/IP inclut plusieurs protocoles qui fournissent des fonctionnalités spécifiques aux applications des utilisateurs finaux. Les couches 5, 6 et 7 du modèle OSI servent de références aux développeurs et aux éditeurs de logiciels d'application pour créer des applications fonctionnant sur les réseaux.

La couche 4 du modèle OSI décrit les services et les fonctionnalités de base qui assurent l'ordre et la fiabilité des données acheminées entre les hôtes source et de destination. Ces fonctions incluent l'accusé de réception, la reprise après erreur et le séquencement. Au niveau de cette couche, les protocoles TCP et UDP de la suite TCP/IP fournissent les fonctionnalités nécessaires.

La couche 3 du modèle OSI décrit l'éventail de processus qui interviennent dans tous les réseaux de données afin d'adresser et d'acheminer les messages à travers le réseau. Le protocole IP est le protocole de la suite TCP/IP qui contient la fonctionnalité décrite à la couche 3 du modèle OSI.

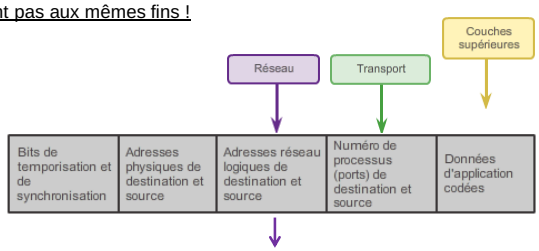
Au niveau de la couche d'accès au réseau, la suite de protocoles TCP/IP ne spécifie pas quels protocoles utiliser lors de la transmission à travers un support physique ; elle décrit uniquement la remise depuis la couche internet aux protocoles réseau physiques. Les couches OSI 1 et 2 traitent des procédures nécessaires à l'accès aux supports et des moyens physiques pour envoyer des données sur un réseau.

Communication et protocoles réseaux

Adresses réseau et adresses de liaisons de données

Dans le modèle OSI, la couche réseau et la couche liaison de données sont chargées de transmettre les données du périphérique source ou expéditeur au périphérique de destination ou récepteur.

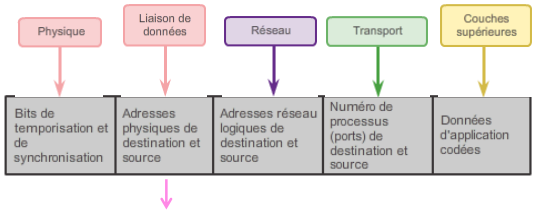
Les protocoles de ces deux couches contiennent les adresses source et de destination, mais ils ne les utilisent pas aux mêmes fins !



Sur la couche réseau, l'adresse logique contient les informations nécessaires à l'acheminement du paquet IP du périphérique source au périphérique de destination.

Dans un paquet IP, on retrouve deux adresses logiques :

- **L'adresse IP source** : il s'agit de l'adresse IP du périphérique expéditeur.
- **L'adresse IP de destination** : elle correspond à l'adresse IP du périphérique récepteur.



Sur la couche liaison de données, on retrouve d'autres types d'adresses : les adresses physiques.

Leur rôle est de transmettre la trame liaison de données d'une interface réseau à une autre, *sur un même réseau*.

Communication et protocoles réseaux

Pour qu'un paquet IP puisse être envoyé via un réseau câblé ou sans fil, il doit être encapsulé dans une trame de liaison de données qui peut être transmise à travers le support physique, c'est-à-dire le réseau réel.

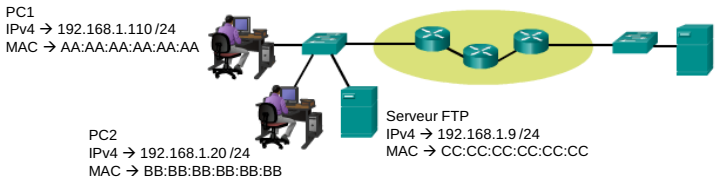
Dans une trame de liaison de données, on retrouve deux adresses physiques :

- **L'adresse de liaison de données source** : adresse physique du périphérique qui envoie le paquet. Initialement, c'est la carte réseau qui est la source du paquet IP.
- **L'adresse de liaison de données de destination** : adresse physique de l'interface réseau du routeur du tronçon suivant ou de l'interface réseau du périphérique de destination.

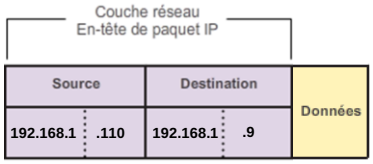
Accès aux ressources locales

Pour comprendre à quels éléments tient la réussite des communications dans le réseau, il est important de comprendre les rôles des adresses de couche réseau et des adresses de liaison de données lorsqu'un périphérique communique avec un autre *sur le même réseau*.

Pour ce faire on va prendre un exemple : PC1 veut joindre le serveur FTP



Rappel :
les adresses de couche 3 = les adresses logiques = adresses IP
les adresses de couche 2 = les adresses physiques = adresses MAC



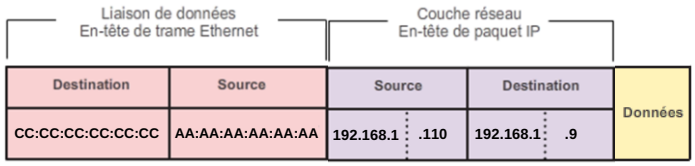
Au niveau de la couche réseau, on vient donc insérer les adresses IP dans le paquet. Une adresse IP de couche 3 se compose de deux parties :

- Le ***préfixe réseau*** est utilisé par les routeurs pour transférer le paquet au réseau approprié.
- La ***partie hôte*** est utilisée par le dernier routeur du chemin pour livrer le paquet au périphérique de destination.

Ces adresses logiques indiquent le réseau et l'adresse de l'hôte de la source et de la destination. La partie réseau de l'adresse est la même, seule la partie hôte ou périphérique de l'adresse diffère.

Dans notre exemple :

- **Adresse IP source** : adresse IP de l'ordinateur PC1 : 192.168.1.110
- **Adresse IP destination** : adresse IP du serveur FTP : 192.168.1.9



Par contre, lorsque l'expéditeur et le récepteur du paquet IP se trouvent sur le même réseau, la trame de liaison de données est envoyée directement au périphérique récepteur.

Sur un réseau Ethernet, les adresses de liaison de données sont appelées adresses MAC Ethernet et elles sont formées de 48 bits. Ces adresses sont physiquement intégrées à la carte réseau Ethernet.

- **Adresse MAC source** : il s'agit de l'adresse MAC Ethernet du périphérique qui envoie le paquet IP, c'est-à-dire PC1. L'adresse MAC de la carte réseau Ethernet de PC1 est AA-AA-AA-AA-AA-AA
- **Adresse MAC de destination** : lorsque le périphérique récepteur se trouve *sur le même réseau* que le périphérique expéditeur, il s'agit de l'adresse MAC Ethernet du périphérique récepteur. Dans notre exemple, l'adresse MAC de destination est l'adresse MAC du serveur FTP : CC-CC-CC-CC-CC-CC

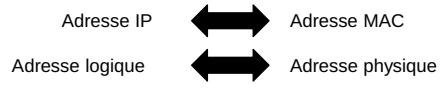
Communication et protocoles réseaux

Vous devriez maintenant savoir que pour envoyer des données à un autre hôte situé sur le même réseau local, l'hôte source doit connaître les adresses logique et physique de l'hôte de destination. Une fois ces informations acquises, il peut créer une trame et l'envoyer sur le support réseau.

Mais comment un hôte détermine-t-il l'adresse MAC Ethernet d'un autre périphérique ?

En fait l'hôte expéditeur utilise un protocole IP appelé « **protocole ARP** » pour connaître l'adresse MAC d'un hôte sur le même réseau local.

Le protocole ARP (Address Resolution Protocol) permet de déterminer l'adresse de la couche liaison de données (= adresse physique ou adresse MAC) d'une station à partir de son adresse IP (= adresse logique) en effectuant une diffusion.



L'allocation des adresses MAC est administrée par l'IEEE. Les fabricants achètent une portion de l'espace d'adressage MAC (pour garantir l'unicité).

Principe

Chaque périphérique possède donc une table ARP, stockée dans sa mémoire vive (RAM), et contenant le mappage entre l'adresse MAC et l'adresse IP.

→ Dans un tableau ARP, on a donc chaque entrée (ou ligne) qui comporte deux valeurs : une adresse IP et une adresse MAC.

Comment se construit la table ARP d'un périphérique ?

Une table ARP peut se construire de 2 manières différentes :

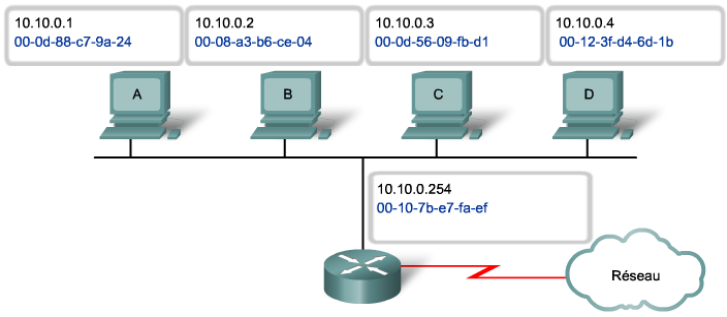
▪ Le tableau ARP peut être mis à jour de **manière dynamique**.

Dans ce cas, un périphérique dispose de deux méthodes pour obtenir des adresses MAC.

- La première consiste à surveiller le trafic sur le segment du réseau local. Quand un nœud reçoit des trames en provenance du support, il enregistre les adresses IP source et MAC dans le tableau ARP sous forme de mappage. Au fur et à mesure que les trames sont transmises sur le réseau, le périphérique remplit le tableau ARP de paires d'adresses.
- La seconde méthode consiste à diffuser une requête ARP.

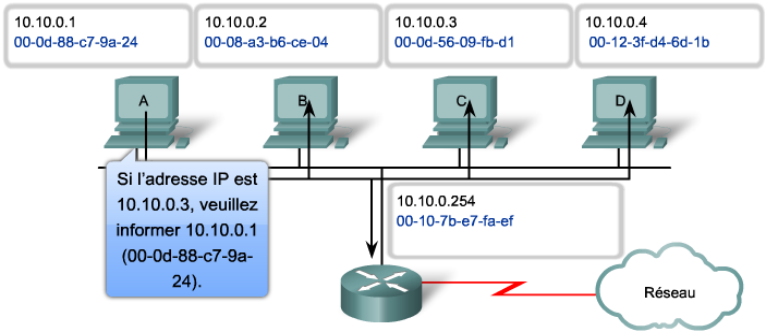
Communication et protocoles réseaux

Explication du processus dynamique utilisant une requête ARP



Dans cet exemple, nous allons regarder comment se remplit la table ARP de l'hôte A. Admettons que pour l'instant celui-ci est vide.

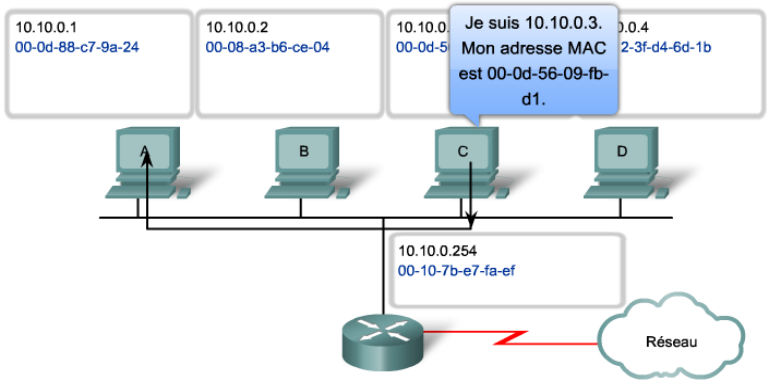
L'hôte A doit envoyer une trame vers 10.10.0.3 mais il ne connait pas l'adresse MAC du destinataire...



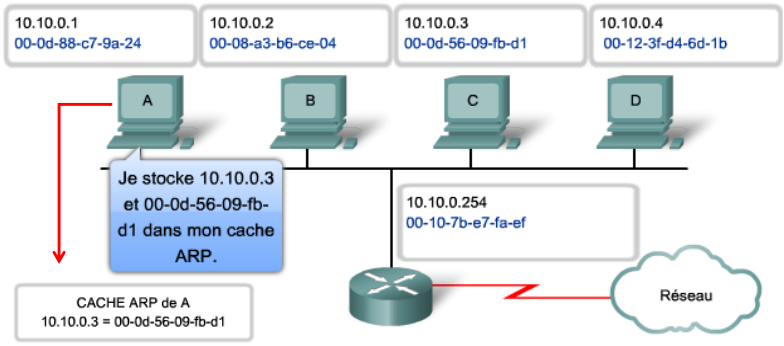
→ *l'hôte A va envoyer une requête ARP de diffusion* demandant à l'hôte réseau, qui possède l'adresse IP 10.10.0.3, de répondre en lui donnant son adresse MAC.

Communication et protocoles réseaux

L'hôte C, qui est le périphérique ayant l'adresse IP 10.10.0.3, va répondre à l'hôte A en lui fournissant son adresse MAC.

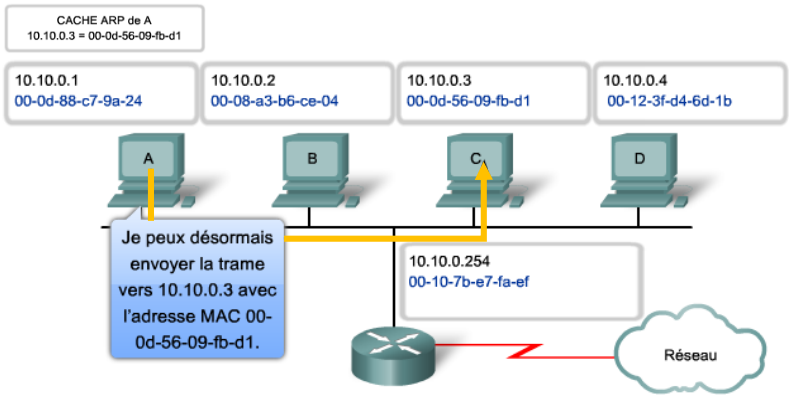


L'hôte A reçoit la réponse à sa question et la stocke dans sa table ARP.



Communication et protocoles réseaux

Maintenant que l'hôte A connait l'adresse MAC de destinataire (dans ce cas ci l'hôte C), il peut envoyer la trame qu'il souhaitait envoyer dès le départ.



Bien entendu, si un hôte possède déjà l'information dans sa table ARP, il peut directement envoyer une trame à un destinataire connu, sans passer par une requête ARP au préalable.

Maintenant, les entrées dynamiques de la table MAC sont horodatées de la même façon que les entrées de la table MAC sur les commutateurs !

→ Si le périphérique ne reçoit pas de trame d'un périphérique précis avant expiration de l'horodatage, l'entrée correspondant à ce périphérique précis est supprimée du tableau ARP.

Si un hôte souhaite envoyer une trame à un destinataire ne faisant pas partie du réseau local, il doit alors envoyer la trame à l'interface du routeur qui sert de passerelle ou de tronçon suivant pour atteindre cette destination.

Si l'entrée de la passerelle n'est pas dans la table, le processus ARP normal envoie une requête ARP pour retrouver l'adresse MAC associée à l'adresse IP de l'interface du routeur.

Communication et protocoles réseaux

Comment se construit la table ARP d'un périphérique ? (suite)

On a vu qu'une table ARP pouvait se construire de deux manières différentes.
La première étant de manière dynamique, comme on vient de le voir.

▪ La seconde étant en y ajoutant des **entrées statiques** de mappage.
Attention, les entrées statiques du tableau ARP n'expirent pas avec le temps et elles doivent être supprimées manuellement (c'est d'ailleurs assez rare).

Sécurité et protocole ARP

Dans certains cas, l'utilisation du protocole ARP peut porter atteinte à la sécurité du réseau. L'usurpation ARP ou *empoisonnement ARP*, est une technique d'attaque qui consiste à injecter un faux mappage d'adresse MAC dans un réseau en émettant de fausses requêtes ARP.

Si un pirate informatique usurpe l'adresse MAC d'un périphérique, les trames risquent d'être envoyées à la mauvaise destination.

La configuration manuelle des entrées statiques permet d'éviter l'usurpation ARP.

Accès aux ressources distantes

La méthode utilisée par un hôte pour envoyer des messages à une destination sur un réseau distant est différente de celle qu'il utilise pour envoyer des messages à une destination sur le même réseau local.

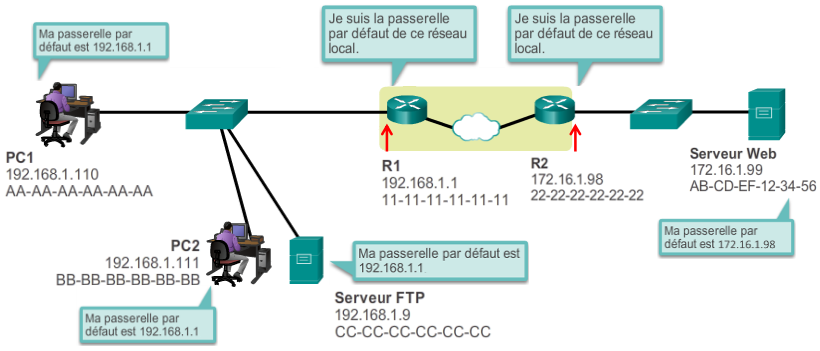
Lorsqu'un hôte doit envoyer un message à un réseau distant, il doit obligatoirement passer par un routeur, également appelé « **passerelle par défaut** ». La passerelle par défaut est l'adresse IP d'une interface d'un routeur se trouvant sur le même réseau que l'hôte expéditeur.

Il est important que l'adresse de la passerelle par défaut soit configurée sur chaque hôte du réseau local.

Si aucune adresse de passerelle par défaut n'est configurée dans les paramètres TCP/IP de l'hôte ou si une passerelle par défaut incorrecte est spécifiée, les messages adressés aux hôtes des réseaux distants ne peuvent pas être acheminés.

Et pour expliquer cela, rien de tel qu'un exemple !

Communication et protocoles réseaux

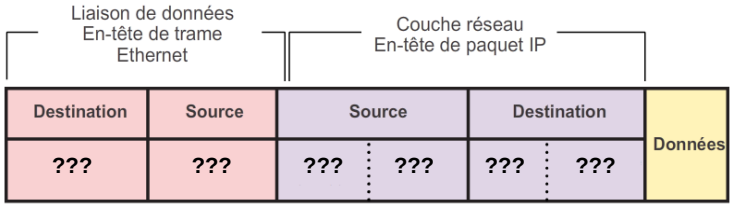


Dans cet exemple, nous avons un ordinateur client (PC1) communiquant avec un serveur appelé « Serveur Web », situé sur un autre réseau IP.

HEH.be Sciences et technologies

Communication et protocoles réseaux

Mais quels sont les adresses de couche réseau et de couche liaison de données lorsqu'un périphérique communique avec un autre périphérique situé sur un réseau distant ?



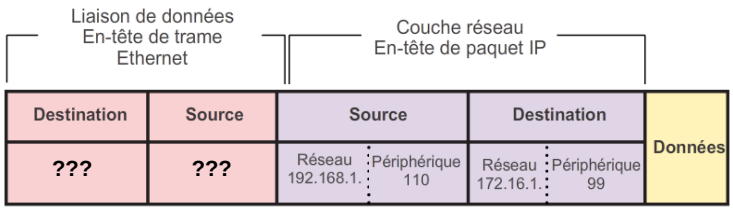
HEH.be Sciences et technologies

Communication et protocoles réseaux

Premièrement, regardons ce qui se passe au niveau de la couche réseau :

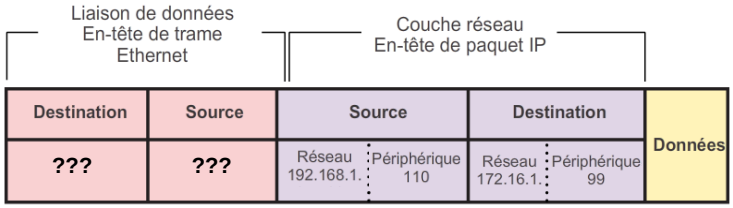
Les adresses IP indiquent les adresses des réseaux et des périphériques source et de destination. Lorsque l'expéditeur du paquet appartient à un réseau différent de celui du récepteur, les adresses IP source et de destination représentent des hôtes sur différents réseaux.

- **Adresse IP source** : adresse IP de l'ordinateur PC1 : 192.168.1.110
- **Adresse IP destination** : adresse IP du serveur Web : 172.16.1.99



Maintenant, intéressons nous à ce qui se passe au niveau de la couche liaison de données :

Lorsque l'expéditeur et le récepteur du paquet IP se trouvent sur des réseaux différents, la trame liaison de données Ethernet ne peut pas être envoyée directement à l'hôte de destination, car celui-ci n'est pas directement accessible sur le réseau de l'expéditeur.



La trame Ethernet doit être envoyée à la passerelle par défaut (routeur R1).

R1 dispose d'une interface, et d'une adresse IP qui se trouve sur le même réseau que PC1
→ Cela permet à PC1 d'accéder directement au routeur.

Communication et protocoles réseaux

Comment le périphérique destinataire détermine-t-il l'adresse MAC du routeur R1 ?

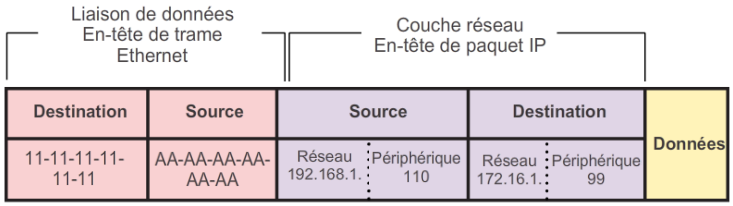
On a vu que chaque périphérique doit être configuré avec l'adresse de la passerelle par défaut dans ses paramètres TCP/IP.

Cette adresse de la passerelle par défaut est bien entendu l'adresse de l'interface du routeur connectée au même réseau local que le périphérique source.

Une fois que l'hôte connaît l'adresse IP de la passerelle par défaut, il peut utiliser le protocole ARP pour en déterminer l'adresse MAC. L'adresse MAC de la passerelle par défaut est ensuite incluse dans la trame.

Au niveau de la trame cela donne ceci :

- **Adresse MAC source** : adresse MAC Ethernet du périphérique expéditeur, PC1. L'adresse MAC de l'interface Ethernet de PC1 est AA-AA-AA-AA-AA-AA
- **Adresse MAC de destination** : adresse MAC de destination est l'adresse MAC de l'interface Ethernet de R1 qui est reliée au réseau de PC1, 11-11-11-11-11-11



La trame Ethernet contenant le paquet IP encapsulé peut être transmise à R1.

R1 achemine le paquet vers la destination, le serveur Web.
R1 peut transmettre le paquet à un autre routeur ou bien directement au serveur Web si la destination se trouve sur un réseau connecté à R1.