Chapitre 02: Les couches Liaison et Internet

Table des matières

Objectifs....2
Rappels : couches des modèles OSI et TCP/IP....2
Classification des réseaux....2
Réseau local de référence....3
La couche Liaison....4
La couche Internet....4
- Adresse IPv4....4
- Adresse IPv6....5
- Contournement de l'épuisement des adresses IPv4....5
- Adresse statique et adresse dynamique....6
- Routage....6
- Adresses spéciales....9

DNS....9
Index....9
Références....10

© 2024 Pier-Luc Brault

Ce document est mis à disposition selon les termes de la licence Creative Commons - Attribution - Partage dans les Mêmes Conditions 4.0 International (CC BY-SA 4.0).

Objectifs

- Distinguer les couches Liaison et Internet du modèle TCP/IP
- Comprendre la différence entre un LAN, un MAN et un WAN
- Comprendre les notions de base du protocole IP
- Connaître les notions de DHCP et DNS

Rappels : couches des modèles OSI et TCP/IP

Dans le premier chapitre, nous avons vu la correspondance suivante entre les couches des modèles OSI et TCP/IP:

OSI	TCP/IP
7 – Application	4 - Application
6 – Présentation	
5 – Session	
4 – Transport	3 - Transport
3 – Réseau	2 - Internet
2 – Liaison de données	1 - Liaison
1 – Physique	

Dans le modèle OSI, la couche physique permet de transmettre des bits sur un canal de communication, par exemple un câble en cuivre, une fibre optique, un réseau Wi-Fi, etc. Le modèle TCP/IP ne se préoccupe pas de la couche physique.

La **couche Liaison** du modèle TCP/IP correspond essentiellement à la couche Liaison de données du modèle OSI. Celle-ci permet de transmettre des données sous forme de groupes de bits, appelés **trames**, entre deux machines adjacentes. Chaque trame inclut l'identification de la machine à laquelle elle s'adresse, puisque plusieurs machines peuvent se trouver sur un même canal de communication.

La **couche Internet** du modèle TCP/IP correspond pour sa part à la couche Réseau du modèle OSI. Cette dernière attribue des adresses aux hôtes du réseau, et détermine la route que les données, appelées **paquets**, doivent emprunter pour parvenir de l'adresse source à l'adresse de destination.

Les couches Liaison et Internet du modèle TCP/IP sont celles que nous explorerons dans ce chapitre.

Classification des réseaux

Il existe principalement trois catégories de réseaux selon l'étendue géographique de chacune: **LAN**, **MAN** et **WAN**.

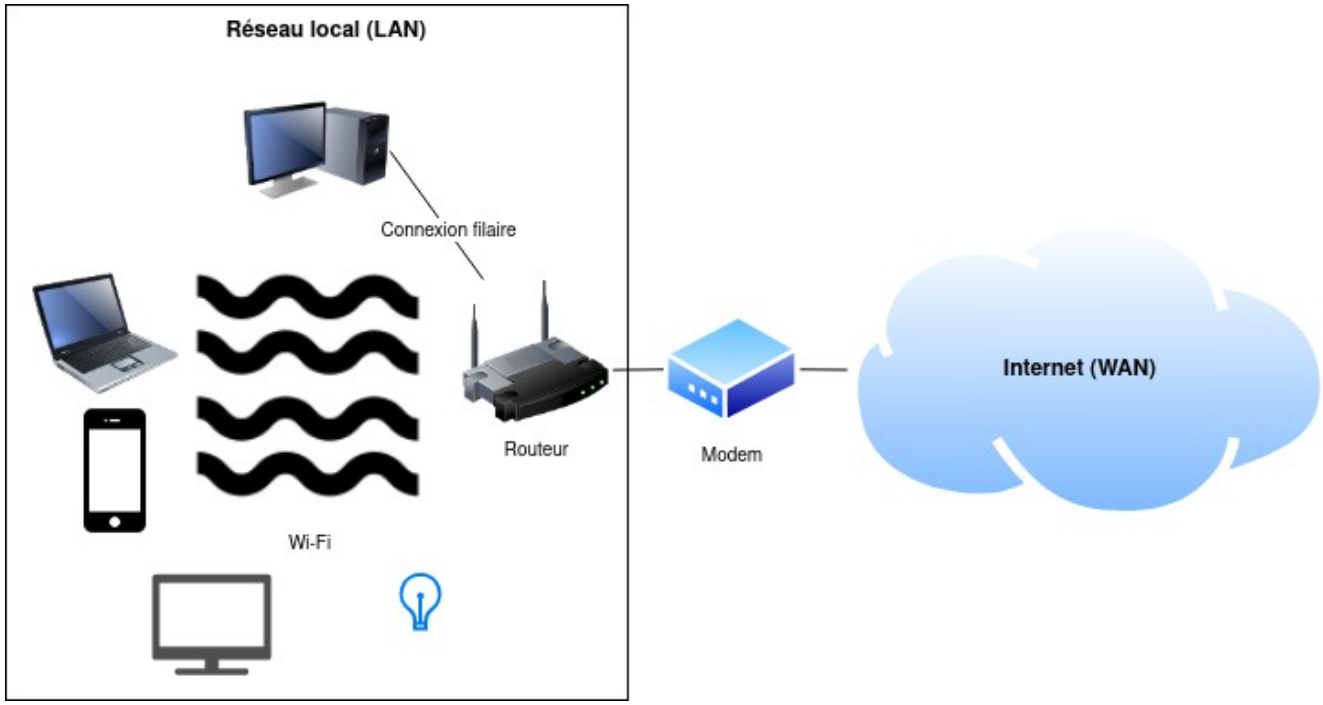
© 2024 Pier-Luc Brault

- **LAN** pour *Local Area Network* : c'est un réseau local, par exemple dans une résidence ou un bureau d'entreprise.
- **MAN** pour *Metropolitan Area Network* (réseau métropolitain): c'est un réseau regroupant plusieurs LAN au sein d'un espace géographique plus grand, par exemple à l'échelle d'une ville ou d'un campus.
- **WAN** pour *Wide Area Network* (réseau étendu): c'est un réseau couvrant une grande zone géographique, par exemple à l'échelle d'un pays ou d'un continent, voire du monde entier.

À toutes fins pratiques, la distinction entre MAN et WAN n'est pas vraiment utile pour la programmation d'applications réseau, et nous parlerons donc simplement de WAN pour désigner Internet, et de LAN pour ce qui est du réseau local. C'est d'ailleurs ce que font de nombreux logiciels et équipements réseaux, tels que des routeurs résidentiels.

Réseau local de référence

L'exemple le plus simple d'un réseau local est celui qu'on retrouve typiquement en milieu résidentiel: plusieurs machines sont mises en réseau en étant connectées par Wi-Fi ou de manière filaire à un **routeur**, qui lui-même est connecté à Internet par le biais d'un modem[1] (parfois intégré au routeur). Un routeur est un appareil qui permet de faire transiter des paquets entre plusieurs réseaux, dans ce cas-ci un LAN et un WAN. Un modem est nécessaire pour assurer la connexion au fournisseur d'accès Internet (**FAI**), par exemple par câble coaxial ou fibre optique.



1 « Modem » est l'acronyme de « **Mod**ulateur-**Dém**odulateur ». Dans le cas d'un accès Internet par fibre optique, l'équipement utilisé pour se raccorder à la fibre n'est pas, strictement parlant, un modem. On parle plutôt d'un **ONT** (*Optical Network Termination*). Cette distinction n'est pas particulièrement importante dans le cadre du cours.

Cet exemple est celui que nous utiliserons comme réseau local de référence pour la suite du chapitre.

La couche Liaison

Puisque la couche Liaison gère la transmission de données sur des canaux de communication de toutes sortes, elle utilise de nombreux protocoles. Sur notre réseau local de référence, les protocoles utilisés sont **Ethernet**, et sa version sans fil, **IEEE 802.11**, communément appelée **Wi-Fi**.

Selon ces protocoles, chaque hôte possède une **adresse physique**, aussi appelée **adresse MAC** (*Media Access Control*) qui permet de l'identifier sur le réseau local. Une adresse MAC est composée de six octets, et est généralement représentée par six paires de caractères hexadécimaux séparés par des « : ». Par exemple:

5E:FF:56:A2:AF:15

Les adresses MAC sont en principe uniques. Des blocs d'adresses sont attribués aux fabricants de matériel par l'*Institute of Electrical and Electronics Engineers* (IEEE).

Ce sont ces adresses qui sont utilisées par la couche Liaison pour indiquer à quel hôte est destinée chaque trame. Ainsi, sur un réseau Wi-Fi, par exemple, chaque interface réseau ne se préoccupe que des trames destinées à son adresse MAC, et ignore les autres. Ces adresses ne permettent cependant pas de router des paquets à travers Internet, et ne sont donc pas celles qui sont utilisées par la couche Internet.

La couche Liaison ayant peu d'intérêt pour la programmation d'applications réseau, nous n'élaborerons pas davantage à son sujet dans ce cours.

La couche Internet

La couche Internet du modèle TCP/IP est celle qui achemine les paquets de leur source à leur destination, que ce soit sur le réseau local ou à travers Internet. Pour ce faire, elle s'en remet principalement au protocole **IP** (pour *Internet Protocol*), qui existe en deux versions: **IPv4** et **IPv6**.

Adresse IPv4

Le protocole IP repose d'abord sur des **adresses logiques** permettant d'identifier les hôtes sur un réseau (ou sur un inter-réseau) et de déterminer la route à emprunter pour y acheminer des paquets (ce que les adresses MAC ne permettent pas). Chaque paquet comprend un en-tête qui contient notamment une adresse source et une adresse de destination. En IPv4, les adresses ressemblent à ceci:

192.168.1.10

Une adresse IPv4 est codée sur quatre octets, et on peut donc la représenter par quatre nombres entre 0 et 255. Cela nous limite à un peu plus de 4 milliards d'adresses possibles, ce qui n'est plus suffisant aujourd'hui. Le protocole IPv6 fût imaginé en réponse à ce problème.

Adresse IPv6

Une adresse IPv6 comprend 16 octets au lieu de 4. On la représente sous la forme de huit groupes de quatre caractères hexadécimaux, comme ceci:

2001:0db8:0000:85a3:0000:0000:ac1f:8001

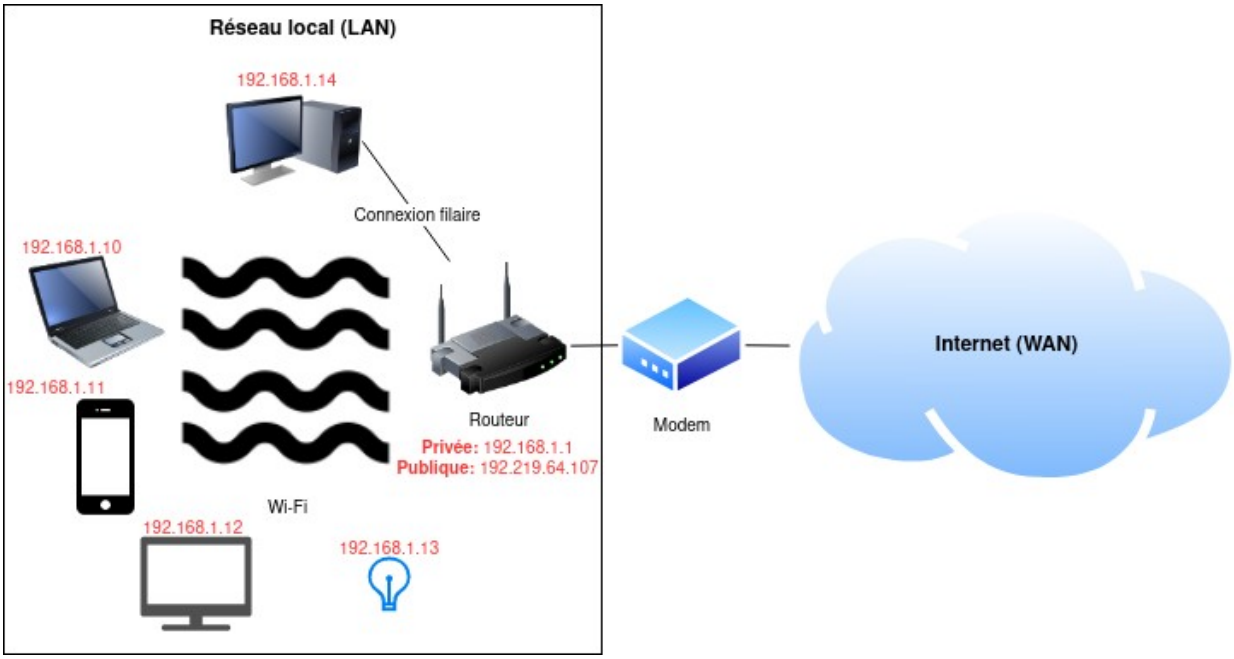
En IPv6, le nombre maximal d'adresses est de 340 sextillons (340 x 10^{36}).

Contournement de l'épuisement des adresses IPv4

Les derniers blocs d'adresses IPv4 disponibles ont été assignés par l'*Internet Assigned Numbers Authority* (IANA) en février 2011. Pourtant, IPv4 demeure largement répandu et IPv6 tarde à être déployé de manière généralisée. Cela s'explique en partie parce que des moyens techniques ont été mis en place pour pallier à la pénurie d'adresses IPv4. Un de ces moyens est le **NAT**, pour *Network Address Translation*, soit « traduction d'adresses réseau ».

Avec le NAT, les adresses IP des hôtes d'un réseau local ne sont pas exposées à Internet. On dit que ce sont des **adresses IP privées**. Le réseau, lui, possède une **adresse IP publique**, qui elle est joignable sur Internet. Le routeur effectue la traduction entre l'adresse IP publique et les adresses IP privées en modifiant les en-têtes des paquets. Ainsi, un même réseau local pourrait comprendre des centaines d'hôtes, et n'utiliser qu'une seule[2] adresse IP publique. Puisque les adresses privées doivent seulement être uniques sur leur propre réseau local, cela réduit considérablement le nombre d'adresses uniques nécessaires pour connecter tous les hôtes à Internet.

Exemple de LAN avec des adresses privées et une adresse publique :



2 Dans le cas d'un gros réseau comme celui du Cégep de Sherbrooke, il peut y avoir plusieurs adresses publiques. Un petit réseau (par exemple, un réseau résidentiel) n'en possède habituellement qu'une seule.

© 2024 Pier-Luc Brault

Les plages d'adresses IPv4 suivantes peuvent être utilisées comme adresses privées:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

Nous en apprendrons un peu plus sur le fonctionnement du NAT dans le chapitre 3.

Adresse statique et adresse dynamique

Si on devait configurer manuellement une adresse IP sur chaque appareil connecté à un réseau, cela ne serait pas pratique, d'autant plus que les appareils portatifs qui se déplacent entre plusieurs réseaux sont très courants de nos jours. C'est pourquoi on laisse généralement le réseau attribuer automatiquement une adresse IP à un hôte. On dit alors qu'on utilise une **adresse IP dynamique**. Celle-ci est attribuée par **DHCP** (*Dynamic Host Configuration Protocol*), un protocole de la couche Application prévu à cet effet. Sur un réseau local domestique, le routeur agit habituellement comme serveur DHCP.

Cependant, il peut être nécessaire d'attribuer soi-même une adresse IP à un hôte spécifique, par exemple un serveur qui doit conserver toujours la même adresse. Dans ce cas, on configure l'adresse IP de l'hôte à l'aide de son système d'exploitation. On dit alors que cet hôte possède une **adresse IP statique**.

Une adresse IP publique est le plus souvent dynamique, et est attribuée par un serveur DHCP du FAI. Pour obtenir une adresse publique statique, il faut généralement payer des frais supplémentaires à son FAI. Cela peut être nécessaire, par exemple si on héberge un serveur qui doit toujours être accessible sur Internet via la même adresse IP.

Routage

La conception des adresses IP aide la couche Internet à déterminer quelle route prendre pour acheminer les paquets à leur destination. Nous nous concentrerons ici sur les adresses IPv4, mais des principes similaires ou équivalents s'appliquent à IPv6.

Adresse du réseau ou du sous-réseau

Les adresses IP sont hiérarchiques. Ainsi, sur un même réseau local, les premiers bits des adresses IP sont toujours les mêmes. Par exemple, on pourrait avoir un réseau sur lequel toutes les adresses commencent par « 10 » ou par « 192.168.1 ». On représente l'**adresse du réseau** en complétant avec des zéros, donc « 10.0.0.0 » et « 192.168.1.0 » dans nos exemples.

On peut aussi diviser un réseau en **sous-réseaux**. On pourrait donc avoir, pour le réseau « 10.0.0.0 », les sous-réseaux « 10.1.0.0 », « 10.2.0.0 », et ainsi de suite.

On dit qu'une adresse IP est constituée en deux parties: un sous-réseau (les premiers bits, partagés avec les autres hôtes du sous-réseau) et un hôte (les derniers bits). On pourrait par exemple avoir une adresse

« 10.1.5.13 » dont la partie sous-réseau est « 10.1 » et la partie hôte est « 5.13 ». Pour simplifier les choses, on utilise le terme « sous-réseau » même lorsque le réseau n'est pas divisé en sous-réseaux (le sous-réseau correspond alors au réseau).

Un hôte doit connaître le nombre de bits de son adresse IP qui identifient le sous-réseau (soit la **longueur du préfixe de sous-réseau**). Par exemple, pour l'adresse « 10.1.5.13 » appartenant au sous-réseau « 10.1.0.0 », ce sont les deux premiers octets de l'adresse, c'est-à-dire ses 16 premiers bits, qui désignent le sous-réseau. On peut représenter cette information par la notation « 10.1.5.13/16 », soit l'adresse IP suivie d'une barre oblique et du nombre de bits identifiant le sous-réseau.

La longueur du préfixe de sous-réseau ne correspond pas nécessairement à un nombre entier d'octets. On pourrait par exemple créer de plus petits sous-réseaux en utilisant 20 bits. Pour 10.1.5.13/20, on obtiendrait ceci en binaire (la partie surlignée correspond au sous-réseau):

00001010.00000001.00000101.11111111

Si on remplace le troisième octet par « 00001111 » (c'est-à-dire 15) et le quatrième par « 11111111 », on obtient la plus grande adresse IP faisant partie de ce même sous-réseau (soit 10.1.15.255/20). Lorsque le troisième octet est à 16 (00010000), on change un bit du sous-réseau, et on se trouve donc dans un autre sous-réseau.

Cependant, dans le cadre du cours, nous utiliserons toujours un nombre entier d'octets comme longueur de préfixe. Le nombre de bits identifiant le sous-réseau sera donc soit 8, 16 ou 24.

Masque de sous-réseau

Un **masque de sous-réseau** est une autre façon d'identifier les bits d'une adresse IP qui désignent le sous-réseau. Il a le même format qu'une adresse IP, et est formé en mettant les bits du sous-réseau à 1 et ceux de l'hôte à 0. Par exemple, pour l'adresse « 10.1.5.13/16 », on obtient, en binaire:

11111111.11111111.00000000.00000000

Soit, en décimal:

255.255.0.0

Le masque de sous-réseau est demandé par certains systèmes d'exploitation pour configurer une adresse IP statique, tandis que d’autres demandent plutôt la longueur du préfixe de sous-réseau.

Dans le cadre du cours, puisque nos sous-réseaux utiliseront toujours soit 8, 16 ou 24 bits, les masques de sous-réseau possibles seront les suivants:

255.0.0.0

255.255.0.0

255.255.255.0

© 2024 Pier-Luc Brault

Routage des paquets sur le même sous-réseau

Lorsqu'une application sur un hôte source veut transmettre un paquet à un hôte de destination, la couche Internet sur l'hôte source utilise le masque de sous-réseau de celui-ci pour déterminer si l'adresse de destination fait partie du même sous-réseau. Si c'est le cas, le paquet est transféré à la couche Liaison qui y ajoute l'adresse MAC de destination pour en faire une trame qu'elle transmet sur la couche physique (par exemple, sur un câble Ethernet ou un réseau Wi-Fi).

Dans le cas où l'hôte source ne connaît pas l'adresse MAC qui correspond à l'adresse IP de destination (et toujours à condition que celle-ci soit sur le même sous-réseau), il envoie un appel à tous sur le sous-réseau pour demander: « À qui appartient cette adresse IP? », et il reçoit une réponse de l'hôte concerné. Ce processus fait partie du protocole **ARP** (*Address Resolution Protocol*).

La carte réseau de chaque hôte, qui fonctionne sur la couche Liaison, surveille les trames qui passent sur le canal de communication auquel elle est branchée. Lorsqu'une trame est destinée à son adresse MAC, elle en extrait le paquet et le transmet à sa couche Internet. Dans le cas d'un réseau Wi-Fi, cette trame peut provenir directement d'un autre hôte sur le même réseau Wi-Fi. Dans le cas d'une connexion Ethernet filaire, la trame lui aura été transférée par l'équipement réseau auquel la carte réseau est directement connectée (par exemple, un routeur ou un commutateur réseau (*network switch*)).

Routage des paquets à l'extérieur du sous-réseau

Lorsqu'un hôte veut envoyer un paquet à une adresse IP qui ne se trouve pas sur son sous-réseau (par exemple, une adresse publique sur Internet), il doit faire appel à un autre hôte, qui sait comment transmettre des paquets à l'extérieur du sous-réseau. On appelle cet hôte la **passerelle par défaut**. Dans ce cas, c'est l'adresse MAC de la passerelle par défaut qui est incluse dans la trame transmise par la couche Liaison. Sur notre réseau local de référence, c'est le routeur qui agit comme passerelle par défaut.

Un hôte doit donc minimalement connaître les trois informations suivantes pour pouvoir utiliser le réseau et accéder à Internet:

- Son adresse IP
- Son masque de sous-réseau (ou la longueur du préfixe de sous-réseau)
- Sa passerelle par défaut

Lorsqu'on utilise une adresse IP dynamique, ces trois informations sont transmises à l'hôte par le serveur DHCP.

Si l'hôte de destination se trouve sur Internet, le paquet, une fois sorti du réseau local, transite d'abord par un routeur du FAI. Le mot « routeur » fait ici référence à un équipement beaucoup plus sophistiqué et coûteux qu'un routeur résidentiel! Les routeurs des FAI maintiennent des tables de routage complexes permettant de déterminer le chemin optimal qu'un paquet devrait emprunter selon son adresse de destination. Le paquet est ensuite dirigé vers le prochain routeur sur ce chemin, et ainsi de

suite jusqu’à ce qu’il atteigne l’hôte voulu. Ce processus, appelé « routage », est rendu possible grâce à la structure hiérarchique des adresses IP.

Adresses spéciales

Adresse de l'hôte local

L'adresse **127.0.0.1**, aussi appelée **localhost**, est une adresse spéciale permettant à un hôte de communiquer avec lui-même. Par exemple, pendant le développement d'une application réseau, il est courant d'exécuter le programme serveur et le programme client sur la même machine. Dans ce cas, on donne cette adresse au programme client pour lui indiquer l'adresse du serveur.

L'adresse équivalente en IPv6 est **::1**, représentée ainsi parce que les sept premiers octets ne contiennent que des zéros.

Adresse de diffusion

L'**adresse de diffusion** (ou **adresse de broadcast**) est une adresse permettant de transmettre un même paquet à tous les hôtes du sous-réseau. Il s'agit de la plus grande adresse IP possible sur le sous-réseau. Par exemple, pour le sous-réseau « 192.168.1.0/24 », l'adresse de diffusion est « 192.168.1.255 ».

DNS

Il serait bien peu pratique de devoir connaître l'adresse IP de chaque serveur avec lequel on peut vouloir communiquer sur Internet. Pensons par exemple à un serveur Web: il faudrait taper « 192.219.64.107 » dans la barre d'adresse de son navigateur pour accéder au site Web du Cégep de Sherbrooke. Il va sans dire que l'adresse « www.cegepsherbrooke.qc.ca » est beaucoup plus facile à retenir!

Le **DNS**, pour *Domain Name System*, est un système permettant de faire la correspondance entre des noms de domaine (comme « www.cegepsherbrooke.qc.ca ») et des adresses IP. Pour résoudre les noms de domaine, on fait appel à un **serveur DNS**, dont on doit connaître l'adresse IP.

Lorsqu'un hôte utilise une adresse IP dynamique, les adresses des serveurs DNS à utiliser (généralement deux, au cas où le premier serait en panne) font partie des informations qui lui sont transmises par le serveur DHCP. La plupart des FAI possèdent leurs propres serveurs DNS, dont les adresses sont justement acheminées à leurs clients par DHCP. Il est aussi possible d'utiliser d'autres serveurs DNS, tels que ceux de Google (8.8.8.8 et 8.8.4.4) ou de Cloudflare (1.1.1.1 et 1.0.0.1).

Lorsqu'on accède à un site Web (par exemple), une requête DNS est d'abord effectuée pour récupérer l'adresse IP correspondant à son nom de domaine. L'adresse IP est ensuite utilisée pour communiquer avec le serveur.

Le protocole DNS appartient à la couche Application.

Index

::1 9
127.0.0.1 9
adresse de broadcast 9
adresse de diffusion 9
adresse du réseau 7
adresse IP dynamique 6
adresse IP publique 5
adresse IP statique 6
adresse MAC 4
adresse physique 4
adresses IP privées 5
adresses logiques 4
ARP 8
couche Internet 2
couche Liaison 2
DHCP 6
DNS 9
Ethernet 4
FAI 3
IEEE 802.11 4
IP 4
IPv4 4
IPv6 4
LAN 3
localhost 9
longueur du préfixe de sous-réseau 7
MAN 3
masque de sous-réseau 8
NAT 5
paquets 2
passerelle par défaut 9
routeur 3
serveur DNS 9
sous-réseaux 7
trames 2
WAN 3
Wi-Fi 4

Références

- TANENBAUM, Andrew et WETHERALL, David, *Réseaux, 5e édition*, Paris, Pearson Education France, 2011, p. 465-500.
- https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/
- https://www.it-connect.fr/les-types-de-reseaux-lan-man-wan-et-pan-pour-les-debutants/
- https://fr.wikipedia.org/wiki/R%C3%A9seau_m%C3%A9tropolitain

© 2024 Pier-Luc Brault

- https://fr.wikipedia.org/wiki/Adresse_MAC
- https://fr.wikipedia.org/wiki/Adresse_IPv6
- https://fr.wikipedia.org/wiki/%C3%89puisement_des_adresses_IPv4
- https://en.wikipedia.org/wiki/Address_Resolution_Protocol
- https://fr.wikipedia.org/wiki/Localhost
- https://fr.wikipedia.org/wiki/Broadcast_(informatique)
- https://www.youtube.com/watch?v=1pZNjRZLNqI
- https://fr.wikipedia.org/wiki/Optical_Network_Termination

© 2024 Pier-Luc Brault