Collection Formation Réseau Cisco CCNA

TCP/IP

TCP/IP Fondamental

François-Emmanuel Goffinet
Formateur IT
Version 15.10

Objectifs du cours

Ce cours TCP/IP Fondamental est une **introduction large, un aperçu** sur les technologies des réseaux.

Il a pour ambition de fournir une boîte à outil de concepts et de méthodes de diagnostic pour comprendre les réseaux TCP/IP. Il s'accompagne d'exercices de laboratoires en Linux, en Windows, en Mac OS X, en Cisco IOS.

Il permet d'accéder aux cours plus avancés sur le routage et la commutation (CCENT/CCNA/CCNP), sur les mécanismes d'adressage IPv4/IPv6, la sécurité des réseaux, les réseaux sans-fil, la téléphonie IP (UC), la mise en place de services réseaux, l'architecture des réseaux, etc.

Il peut être utilisé comme cours de lissage sur la matière des fondamentaux des réseaux.

Un quiz vous offre la possibilité d'évaluer les sujets de connaissance évoqués dans les diapositives suivantes : http://cisco.goffinet.org/quiz/quiz-tcp-ip-fondamental

ICND1 100-101/CCNA 200-101

Sujet 1. L'exploitation de réseaux de données IP

- Reconnaître le but et les fonctions des divers périphériques réseau tels que les routeurs , commutateurs, ponts et concentrateurs.
- Sélectionner les composants nécessaires pour répondre à une spécification de réseau donné.
- Identifier les applications courantes et leur impact sur le réseau.
- Décrire le but et le fonctionnement de base des modèles et protocoles OSI et TCP/IP.
- Prédire le flux de données entre deux ordinateurs sur un réseau.
- Identifier les médias, les câbles, les ports et connecteurs pour connecter des périphériques de réseau Cisco à d'autres périphériques réseau et des hôtes sur un réseau local.

Table des matières

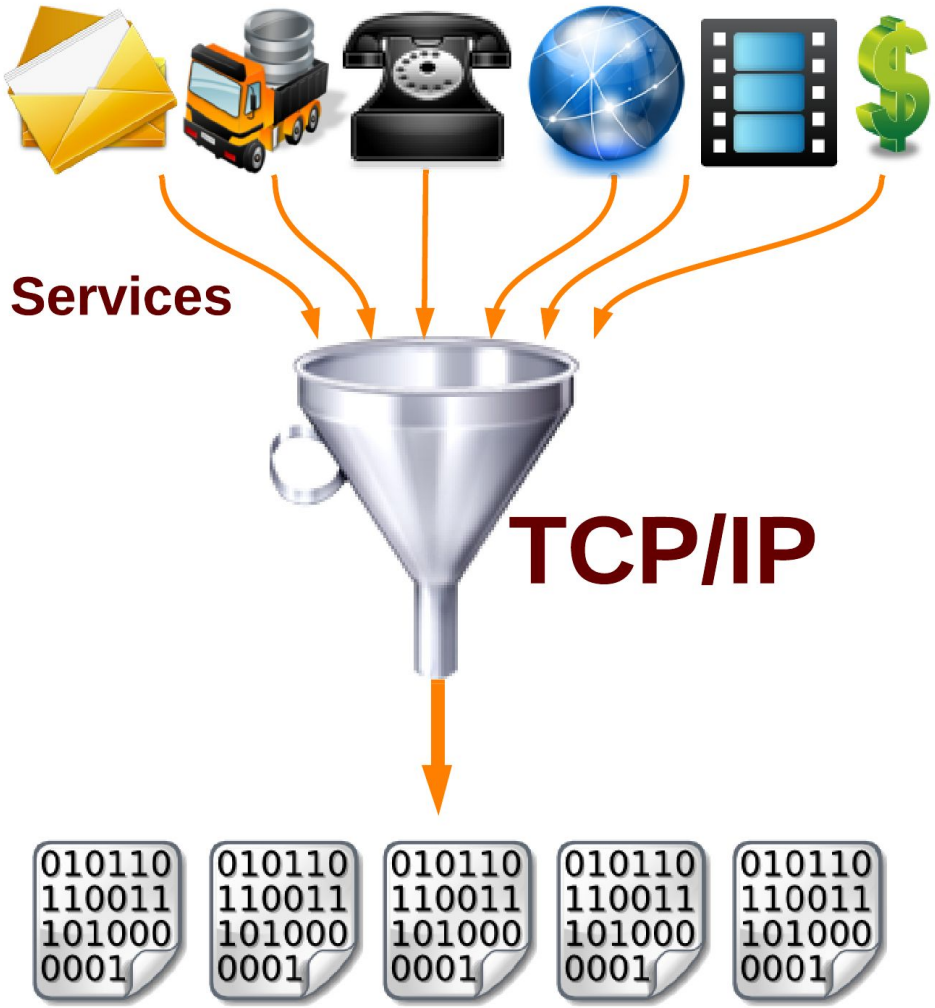
1. TCP/IP : Introduction

Qu’est-ce que l’Internet ? Technologie et terminologie

TCP/IP

- Un ensemble (pile) de protocoles de communication.
- Ne se préoccupe pas du contenu.
- Technologie planétaire qui interface directement n'importe quelle machine dans le Monde.
- Technologie de l'Internet, en son coeur
- Impact sociétal, économique, social : une révolution contemporaine.

Convergence TCP/IP



Un grand nombre de tâches courantes (des services) sont réalisées en tant que données

A travers une seule technologie :

TCP/IP

Objectifs de TCP/IP

1. Communiquer
2. à l'échelle du globe
3. de manière libérale

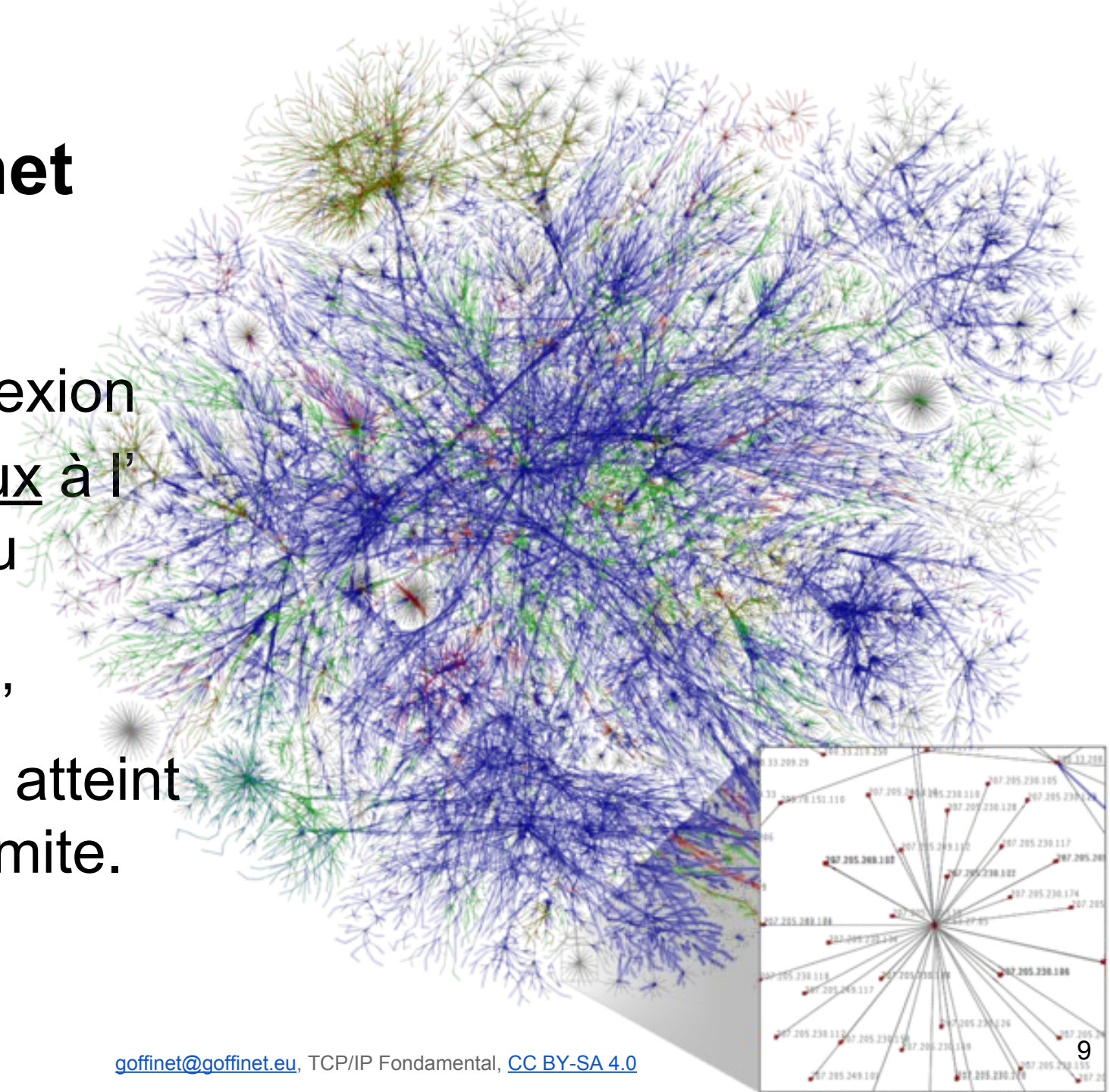
<u>quel que soit</u>

1. le contenu
2. le support
3. les hôtes

L’Internet

Il est l’ interconnexion de réseaux à l’ échelle du globe.

En IPv4, l’ Internet a atteint sa taille limite.



Facteurs de succès

- Assure des communications robustes (infrastructure réseaux redondantes)
- Donnant accès à un contenu riche
- Démocratisation des accès, des périphériques, des services
- Standard industriel ouvert, adoption forte du marché
- Indépendant des services ou des supports
- Usage mondial/global

Principes

Communication de bout en bout

- Grâce aux routeurs, le réseau Internet se contente d'assurer le transfert rapide des paquets d'une extrémité à l'autre (où se situe l'intelligence). *Les routeurs NAT, les pare-feux, bref la réalité, contredisent ce principe.*

Robustesse

- Être conservateur avec les messages envoyés et libéral avec les messages reçus.

Les hôtes terminaux

Les hôtes terminaux sont les ordinateurs connectés au réseau. On peut les classer en différentes catégories :

- Ordinateurs de bureau,
- Ordinateurs légers,
- Matériel embarqué,
- Smartphones et tablettes,
- Téléphone et caméras
- Serveurs

Périphériques intermédiaires

Les périphériques intermédiaires sont ceux qui assurent la connectivité entre les hôtes terminaux.

- Les **routeurs** sont les périphériques qui interconnectent le réseau local à l'Internet. L'Internet est constitué de routeurs.
- Au sein du réseau local, les **commutateurs** et les points d'accès Wi-Fi partagent rapidement la connectivité locale.
- On rencontre bien d'autres périphériques réseau tels que des **pare-feux**, des **mandataires** et divers serveurs.

Bande passante

- En conception des réseaux, le critère le plus important est la **bande passante**. Il s'agit de quantité de données qu'une technologie est capable de transporter. Elle s' exprime en **bits/s** et avec ses préfixes Kb/s, Mb/s, Gb/s, …
- On distinguera la bande passante, mesure théorique, du **débit réel** qui est la vitesse réellement mesurée.
- On sera attentif sur le fait que les systèmes d' exploitation peuvent exprimer le poids des données en octets en non en bits.

Organismes de standardisation

La gestion de l'Internet et des standards se répartissent entre diverses organisations

Registry	Area Covered
AfriNIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	North America Region
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

L'Internet, ses protocoles et son fonctionnement sont formalisés par l'IETF dans des documents numérotés appelés des Requests for Comments (RFC).

Activités

- Collecter et interpréter les informations sur sa connexion Internet sur : http://ipv6-test.com/, sur http://test-ipv6.com/ et sur https://stat.ripe.net/
- Effectuer un “ping” et un “traceroute” vers Google.
- S’informer sur les termes RFC, IETF, IANA, RIRs, IEEE 802.

2. Modèles en couches

Modèles TCP/IP et OSI, Protocoles, Encapsulation, Modes de communication, PDU, Adresses et identifiants

Modèle en couche

TCP/IP est fondé sur un modèle de communication divisé en **quatre couches**.

Chaque couche remplit une **fonction** assurée par un **protocole**.

A chaque couche on peut aussi associer :

- du matériel;
- une encapsulation, un PDU;
- un élément d'identification.

Protocole

- Un protocole est une règle de communication.
- Si on peut avoir le choix entre plusieurs protocoles au sein d'une couche, chacun n' est associé qu'à une seule couche.
- Un protocole embarque les messages des utilisateurs mais aussi les messages des systèmes (transparents aux utilisateurs lambda).

Quatre couches

Couche Application

- Elle est la couche de communication qui s'interface avec les utilisateurs.
- Exemples de protocoles applicatifs : HTTP, DNS, DHCP, FTP, ...
- S'exécute **sur les machines hôtes**.

Couche Transport : TCP

- Elle est responsable du dialogue entre les hôtes terminaux d'une communication.
- Les applications utiliseront TCP pour un transport fiable et UDP sans ce service.
- Les **routeurs NAT** et les **pare-feu** opèrent un filtrage au niveau de la couche transport.

Couche Internet : IP

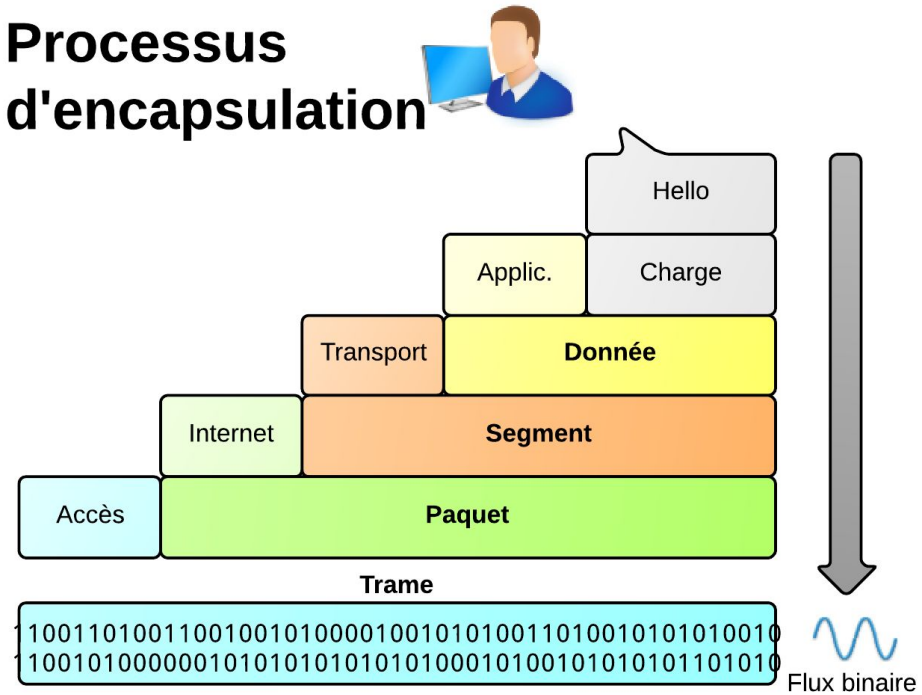
- Elle permet de déterminer les meilleurs chemins à travers les réseaux en fonction des adresses IPv4 ou IPv6.
- Les **routeurs** transfèrent le trafic IP qui ne leur est pas destiné.

Couche Accès au réseau

- TCP/IP ne s'occupe pas de la couche Accès Réseau
- Elle organise le flux binaire et identifie physiquement les hôtes
- Elle place le flux binaire sur les support physique
- Les **commutateurs, cartes réseau, connecteurs, câbles, etc.** font partie de cette couche

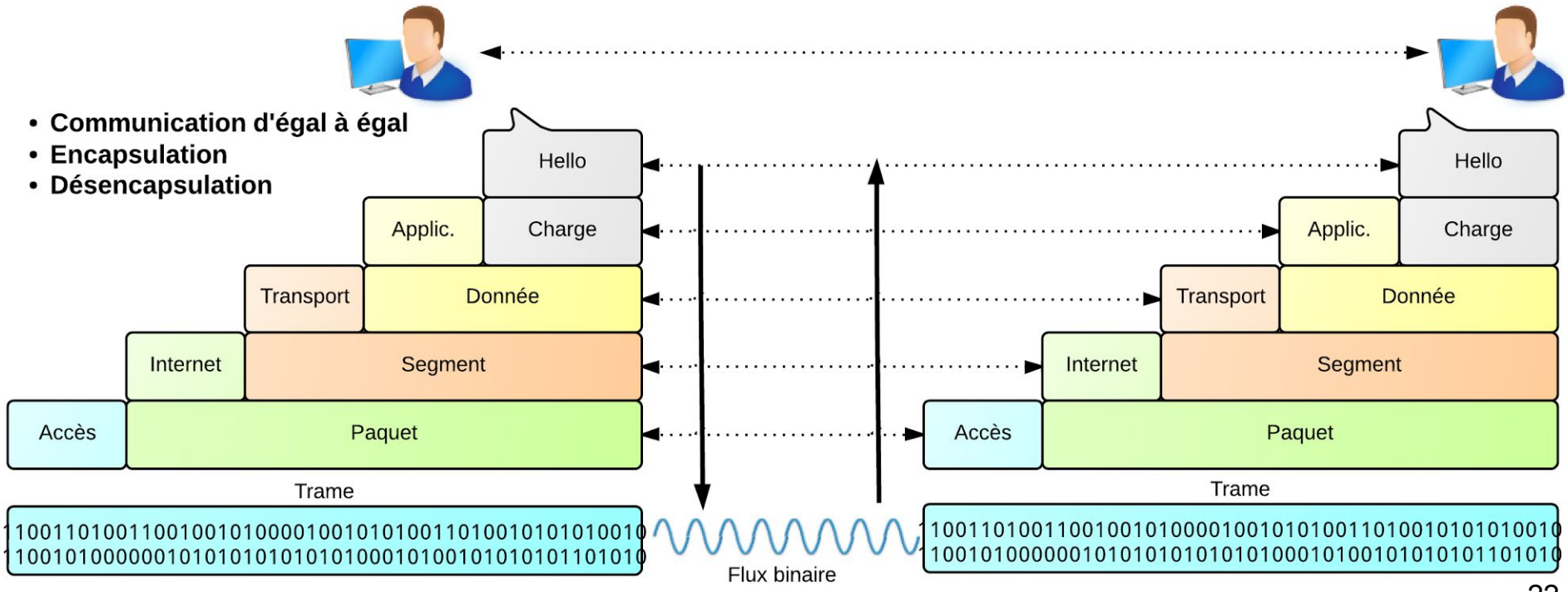
Encapsulation

- Pour transmettre du contenu d'un ordinateur à un autre, l'utilisateur va utiliser un programme qui construit un message enveloppé par un en-tête applicatif, SMTP par exemple. Le message subit une première encapsulation.
- Le logiciel va utiliser un protocole de couche transport correspondant pour établir la communication avec l'hôte distant en ajoutant un en-tête TCP ou UDP.
- Ensuite, l'ordinateur va ajouter un en-tête de couche Internet, IPv4 ou IPv6 qui servira à la livraison des informations auprès de l'hôte destinataire. L'en-tête contient les adresses d' origine et de destination des hôtes.
- Enfin, ces informations seront encapsulées au niveau de la couche Accès qui s'occupera de livrer physiquement le message.

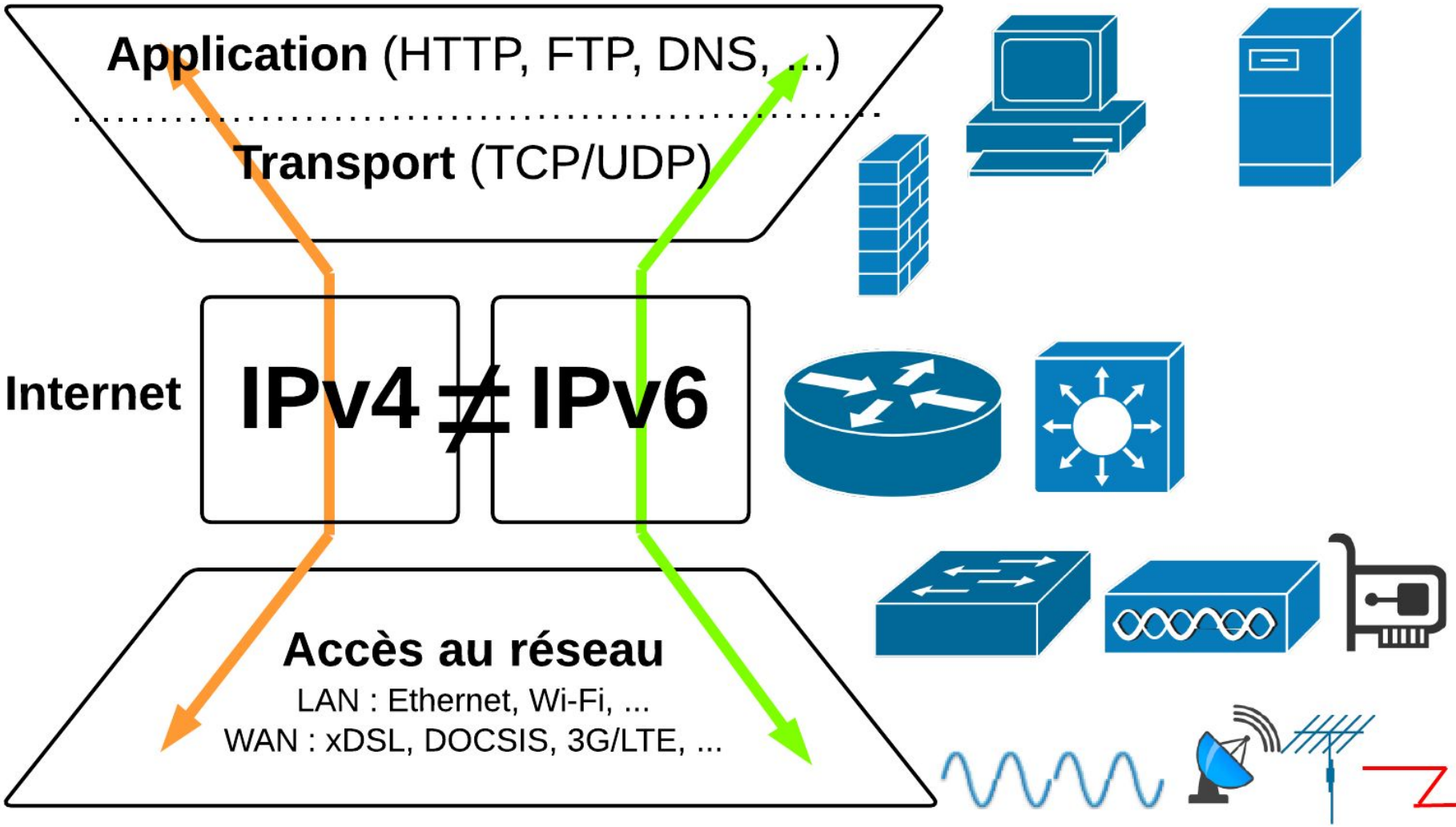


Processus de communication

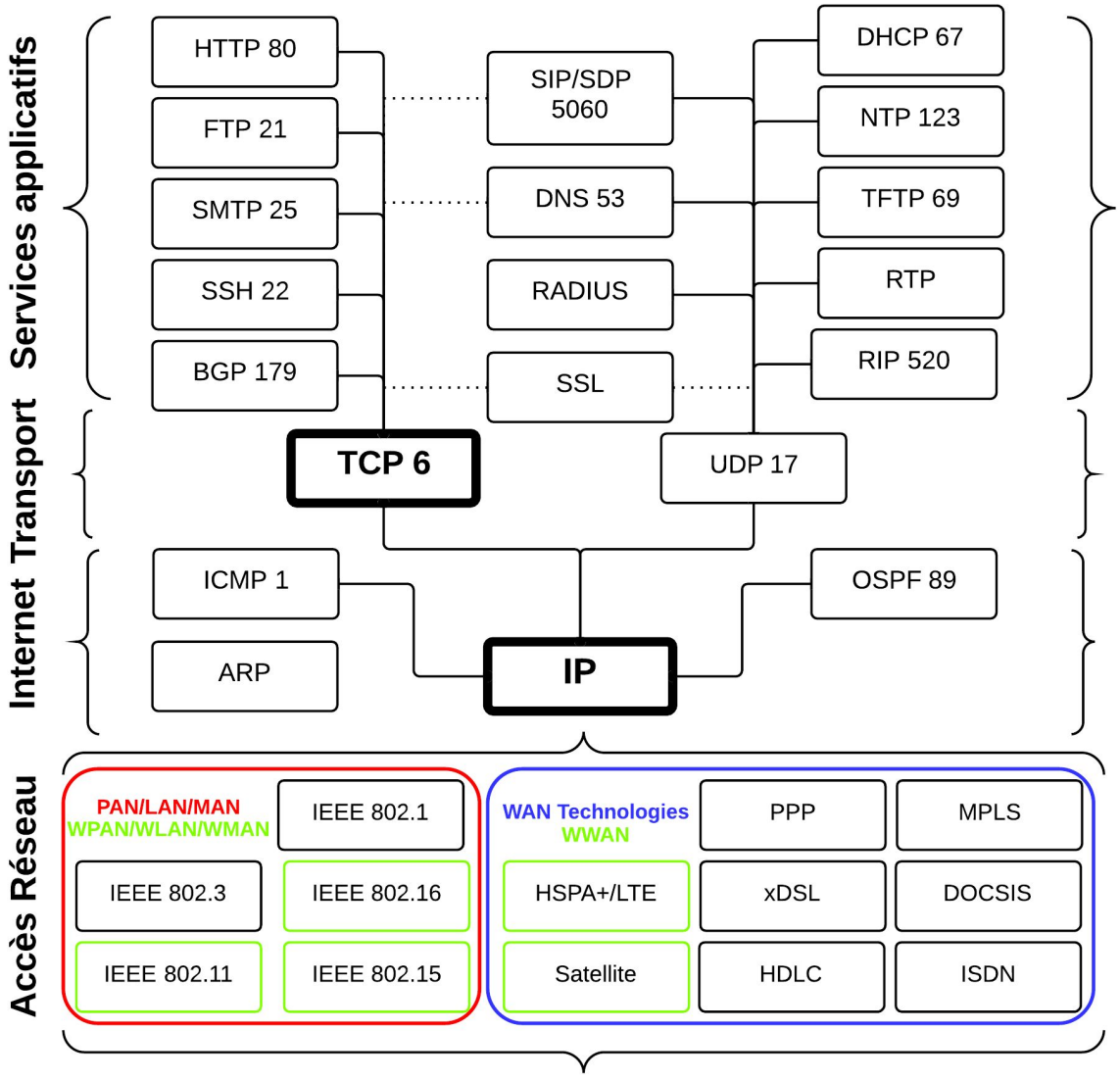
Chaque couche ajoute une information fonctionnelle au message original. A la réception, l'hôte examine chaque couche et prend une décision quant à ce trafic.



Modèle TCP/IP simplifié



Modèle TCP/IPv4 détaillé



Modèles de communication

1. Client / Serveur :

- Le client élabore des requêtes, entame les dialogues à destination du serveur.
- Le serveur donne des réponses suite à un dialogue initié par le client : le serveur rend des services.

2. Pair-à-pair (peer-to-peer)

- Les machines émettent des requêtes et rendent des services.

Caractéristiques des protocoles

Un protocole est un ensemble de règles de communication. Il peut avoir les caractéristiques suivantes :

- In-Band : signalisation avec les données (HTTP)
- Out-of-Band : signalisation dans un autre protocole (FTP, SIP/SDP/RTP)

- de Gestion : protocoles d'accès distant, de résolution de noms, d'attributions d'adresses, de voisinage.
- de Contrôle : protocoles de routage, IEEE 802.1

- Orientés Connexion : Établissement, maintien et fermeture d'un canal au préalable de l'envoi des données (TCP, FTP)
- Fiables : mettant en oeuvre des mécanismes de fiablilité tel que la reprise sur erreur, des accusés de réception, du contrôle de flux, etc.

PDU

Chaque contenu encapsulé par une couche est une unité de donnée (Data Unit) qui prend un nom (PDU), **Protocol Data Unit** :

- Couche Application : **Donnée**
- Couche Transport : **Segment**
- Couche Internet : **Paquet ou Datagramme**
- Couche Accès : **Trame et Bit**

Le signal binaire contient des trames contenant des paquets contenant des segments contenant des données

Adressage et identifiants

Les machines et leurs interfaces disposent d' identifiants au niveau de chaque couche :

- Couche Application : **Nom de domaine**
  par exemple : www.goffinet.eu
- Couche Transport : **Port TCP ou UDP**
  par exemple : TCP80
- Couche Internet : **Adresse IPv4 et/ou IPv6**
  par exemple : 192.168.150.252/24 ou 2001:db8::1/64
- Couche Accès : **adresse physique (MAC)**
  par exemple une adresse MAC 802 : 70:56:81:bf:7c:37

URI-URL

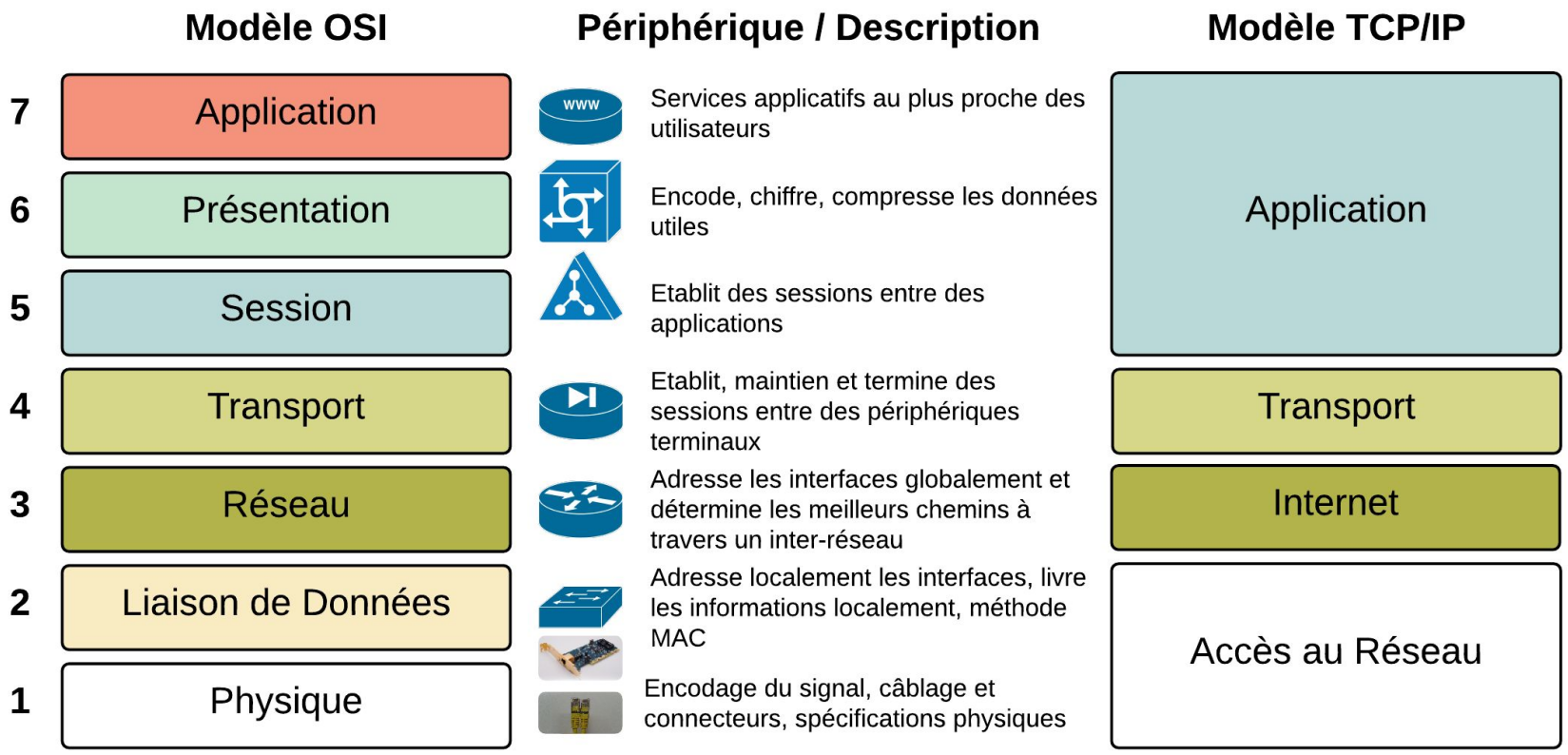
Le sigle URL (de l'anglais Uniform Resource Locator, littéralement « localisateur uniforme de ressource »), auquel se substitue le terme adresse web, désigne **une chaîne de caractères utilisée pour adresser les ressources du World Wide Web** : document HTML, image, son, forum Usenet, boîte aux lettres électronique, entre autres. Les URL constituent un sous-ensemble des identifiants uniformisés de ressource (URI). La syntaxe d'une URL est décrite dans la RFC 3986. Par exemple,

`http://cisco.goffinet.org:9080/Plone/index.html`

On trouvera d’autres exemples ici.

OSI et TCP/IP

Les deux modèles trouvent leurs correspondances, mais c'est TCP/IP qui est utilisé dans la pratique.



Activités

- Commencer à compléter le tableau de synthèse.
- S’intéresser aux commutateurs et aux routeurs, aux serveurs, aux terminaux clients, aux grands constructeurs (Cisco, Microsoft, VMWare, HP, Dell, IBM, etc.)

3. Couches Application et Transport

Protocoles de couche application, TCP, UDP, numéros de ports

Couche Application

La couche application est celle qui s'interface directement avec les logiciels utilisateurs. Elle embarque le message original et ajoute des commandes diverses du type :

- Donne-moi ceci
- Je te donne cela
- Je suis ici
- Donne moi cette liste
- Exécute telle commande
- Donne-moi telle donnée
- Quelle heure est-il ?
- Donne moi une adresse
- Je demande un accès
- etc.

Couche application : protocoles

- Rendre des pages Web : **HTTP**
- Transférer du courrier : **SMTP**
- Transférer des fichiers : **FTP**, **TFTP**
- Résoudre des noms : **DNS**
- Distribuer des adresses IP : **DHCP**, **DHCPv6**
- Accéder à une console : **Telnet**, **SSH**, **MS-RPC**
- Etablir des appels : **SIP/SDP**, **H.323**
- Communiquer de la voix/vidéo : **RTP**
- Rapatrier du courrier : **POP3**, **IMAP**

Couche application : protocoles

- Synchronisation du temps : **NTP**
- Partager des fichiers : **SMB/CIFS**, **NFS**
- Gérer des périphériques : **SNMP**
- Bureaux distants : **VNC**, **RDP**
- Authentification : **Radius**, **Kerberos**
- Tunnel sécurisé : **TLS/SSL**
- NAT Traversal : **ICE/STUN**
- Messagerie instantanée (IM) : **jabber**, **ICQ**
- Service de base de données : MS-SQL, MySQL, Oracle, PGSQL

Couche application : compétences

Les compétences à développer dans le cadre du déploiement de services applicatifs relèvent plutôt de l'administration des systèmes :

- Utiliser un service applicatif
- Mettre en place un service applicatif
- Avoir un bon aperçu des systèmes d'exploitation et des architectures matérielles

Dans les domaines :

- d'usage courant
- de gestion du réseau
- de la téléphonie

Couche Transport

La couche Transport est responsable des **dialogues** (sessions) entre les hôtes terminaux. Elle permet de **multiplexer** les communications en offrant un support à la couche application de manière :

- Fiable : **TCP**
- Non-fiable : **UDP**

Les ports TCP ou UDP (65536 sur chaque interface) permettent aux hôtes terminaux d'identifier les dialogues.

TCP

TCP, Transmission **Control** Protocol, offre des services d'établissement et de fin de dialogue ainsi que des messages de maintenance de la communication en mode fiable et connecté avec :

- des accusés de réception
- du séquençace, de l'ordonnancement
- du contrôle de flux (fenêtrage)
- de la reprise sur erreur
- du contrôle de congestion
- de la temporisation

UDP

UDP, User **Datagram** Protocol, s'occupe uniquement du transport non fiable.

Il est une simple passerelle entre IP et l'application.

Il est conseillé pour les applications transmettant du trafic en temps réel, à taille fixe et régulier (voix, vidéo).

Il supporte des protocoles simples (TFTP, SNMP) ou souffrant des délais (DHCP, DNS, NTP).

Il est utile de comparer UDP et TCP :

- UDP est un en-tête amoindri des fonctionnalités TCP.
- UDP dispose presqu'uniquement des champs port source et port destination.

Numéros de ports

Les ports sont des portes d'entrée entre les hôtes terminaux. Ils sont codés sur 16 bits de 0 à 65535.

Un client IP ouvre un port d'origine pour communiquer avec un serveur IP à l'écoute sur un port de destination. La réponse émane du port de l'application sur le serveur à destination du port client ouvert à l'origine.

La commande **netstat -a** sur un PC permet de connaître tous les ports à l'écoute et les liasions maintenues à l' instant (UDP et TCP sur IPv4 et IPv6).

C'est ce qu'on appelle un "socket" : l'adresse IP combinée au port identifie chaque partenaire de communciation.

La liste des des ports se trouve ici.

Numéros de ports de services bien connus

HTTP→	**TCP80**
HTTPS→	TCP443
TELNET→	**TCP23**
SSH→	TCP22
SMTP→	TCP25
POP3→	**TCP110**
FTP→	**TCP21, TCP20**
TFTP→	**UDP69**
DNS→	**UDP53, TCP53**
DHCP→	**UDP67, UDP68**
NTP→	**UDP123**
RIP→	**UDP520**

Les hôtes utilisent les ports TCP ou UDP pour identifier les sessions à l'origine (port source) et à la destination.

Par exemple, pour établir une session HTTP, l'hôte utilisera un port local au-delà de TCP1024 et le port TCP80 en destination

Les numéros de ports par défaut des services applicatifs sont gérés par l' IANA

Activités

Document **Labs TCP** avec les outils :

- netstat -a
- netcat
- wireshark
- nmap/zenmap

4. Couche Internet

Réseau, Routeurs, Mode de livraison, Adresses IPv4/IPv6, Masque d'adresse, NAT et adresses privées/publiques, passerelle par défaut, pare-feu

Internet : réseau

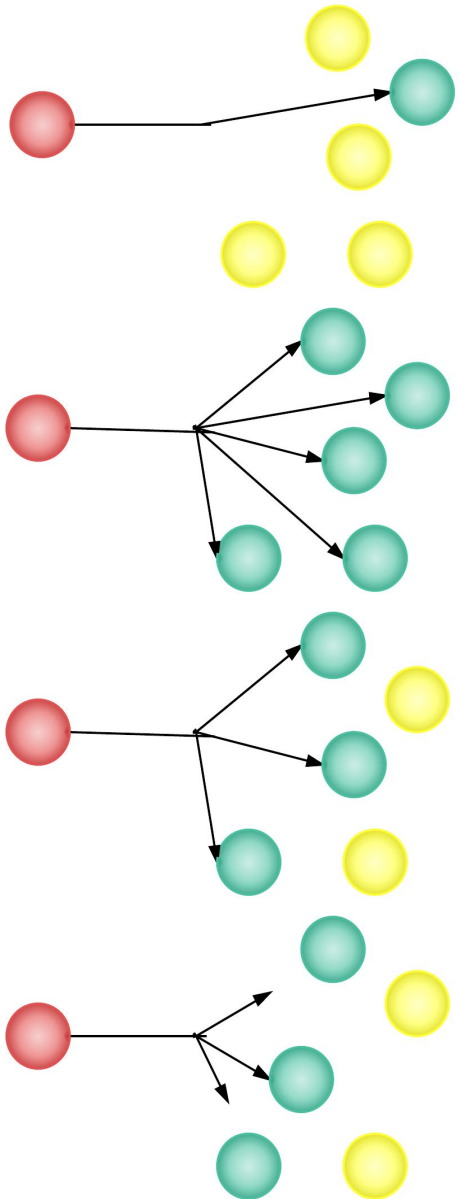
- La couche Internet est celle qui s'occupe d' adresser globalement les interfaces
- Elle détermine les meilleurs chemins à travers les inter-réseaux.

Elle utilise le protocole Internet (IP) qui est :

- **non fiable**
- **non connecté**

Modes de livraison

- Unicast : à destination d'une seule interface.
- Broadcast : à destination de toutes les interfaces
- Multicast : à destination d'un ensemble (un groupe) d'interfaces
- Anycast : à destination de l'interface la plus proche



Internet : rôles

Deux rôles sont définis en IP :

- Les **hôtes terminaux (noeuds)** qui disposent de une ou plusieurs interfaces attachées à un lien.
- Les **routeurs** qui disposent de plusieurs interfaces attachées à des liens et qui transfèrent le trafic qui ne leur est pas destiné. Ils prennent leurs décisions sur base de leur ***table de routage***.

Le routeur examine les en-têtes IP (au niveau des champs d'adresses) pour prendre ses décisions de routage. Il filtre (ne transfère pas) le broadcast.

Protocoles IPv4/IPv6

- Pour l'instant, la grande majorité des ressources Internet sont disponibles en IPv4.
- Un protocole Internet de nouvelle génération IPv6 est proposé et est déjà implémenté dans les réseaux des opérateurs, des grands fournisseurs de contenu.
- Etant donné que toutes les attributions d'adresse IPv4 sont épuisées, IPv6 doit être déployé.
- Etant donné que les hôtes terminaux ne peuvent utiliser que l'un ou l'autre des protocoles IP, on peut considérer que l'Internet IPv6 est un second Internet dont l' architecture va progressivement supplanter IPv4.
- Cette phase de transition peut durer jusqu'à 10 ans.

Adressage IP

L’adressage IP dispose des caractéristiques suivantes :

- C’est un identifiant logique (configuration administrative)
- Unicité : les adresses IP doivent être assignées à une seule interface.
- Organisation hiérarchique (par niveau) et géographique.

Internet : adressage IPv4 et IPv6

Les interfaces prennent une adresse IP :

- IPv4 : adresses codées sur 32 bits (4 octets) en notation décimale pointée. Par exemple : **195.238.2.21**
  La solution est largement épuisée aujourd'hui
- IPv6 : adresses codées sur 128 bits (8 mots de 16 bits) notée en hexadécimal. Par exemple : **200a:14d6:6f8:1:7256:81ff:febf:7c37**

Masque d'adresse

En IPv4 comme en IPv6, une adresse IP est toujours accompagnée de son masque.

Le masque d'une adresse IP détermine l'appartenance d' une adresse à un réseau IP.

Un masque est une suite homogène de bits à 1 et puis de bits à 0.

On peut l'écrire :

- en notation décimale (en IPv4, ancienne méthode)
- en notation CIDR qui reprend le nombre de bits à 1 dans le masque (en IPv4 et en IPv6)
  p. ex. /24 = 24 bits à 1 dans le masque.

Partie réseau ou préfixe

Par rapport à une adresse de référence les bits à 1 dans le masque correspondent à la partie que toutes les adresses IP partagent si elles sont dans le même réseau.

Soit l'adresse assignée 192.168.100.100/24 :

192.168.100.100

255.255.255.0

Toutes les adresses commençant par "192.168.100" appartiennent au même réseau, soit 192.168.1.1/24, 192.168.1.2/24, etc. jusque 192.168.1.255.

Partie hôte ou identifiant d'interface

Par rapport à une adresse de référence les bits à 0 dans le masque correspondent à la partie variable d'un réseau qui identifie les hôtes de manière unique.

Soit 192.168.100.100/24 :

`192.168.100.`**`100`**

`255.255.255.`**`0`**

Le nombre de bits à zéro dans le masque indique aussi le nombre d'adresses IP dans un réseau IP. Ici il y a 8 bits à zéro dans le masque, soit 2^8 (256) possibilités.

Première et dernière adresse IPv4

- En IPv4, la première adresse est réservée à l'identification du réseau (numéro de réseau).
- Également, la dernière adresse est réservée au mode de transmission broadcast (toutes adresses du réseau).
- Les adresses incluses entre la première et la dernière adresse peuvent être utilisées sur les interfaces

Adressage IPv6

- Le principe du masque IPv4 reste valable en IPv6. Mieux, par défaut, on utilisera un masque /64 qui divisent l'adresse en deux partie égales.
- La longueur de 128 bits des adresses IPv6 exigent une nouvelle notation en hexadécimal.
- La première adresse est assignable car on utilise une autre manière d'identifier le réseau.
  - soit l'adresse **200a:14d6:6f8:1**:7256:81ff:febf:7c37/64 fait partie du réseau **200a:14d6:6f8:1::/64**
- Le broadcast a disparu d'IPv6 comme mode de livraison et est remplacé par du Multicast (*Well-Know* ou *Solicited-Node*).

Adressage privé et adressage public en IPv4

A cause du manque d'adresse IPv4 la plupart des LANs sont adressés de manière privée dans les blocs : 10.0.0.0 /8, 172.16.0.0/12 et 192.168.0.0/16.

Ces adresses privées conformément à leur nature n'ont pas de destinations sur l'Internet.

Pour interconnecter un réseau privé à l'Internet public, on utilise un routeur NAT qui réalisera la traduction d'adresses privées en une ou plusieurs adresses publiques.

Expliqué de manière simple, les routeurs NAT altèrent les en-têtes en remplaçant les champs d'adresses contenant une IP privée par une IP publique.

Passerelle par défaut

- La passerelle par défaut est l'adresse IP dans le même réseau que l'hôte et qui permet de joindre d'autres réseaux, **soit l'adresse IP du routeur dans le LAN**.
- En IPv4, il faut la configurer manuellement ou l'attribuer par DHCP.
- En IPv6, elle est automatiquement annoncée par le routeur via des Router Advertisements (ND)
- Elle est nécessaire car ne pouvant connaître l'adresse physique du destinataire situé dans un autre réseau, le trafic est physiquement livré à la passerelle qui décidera du sort à réserver aux paquets.

Pare-feux

Les pare-feux ont pour objectif de filtrer les communications TCP/IP. Ils sont capables de tenir compte des sessions établies à partir d' une zone de confiance et d'empêcher tout trafic initié de l'Internet.

Quand ils sont placés dans le réseau (ailleurs que sur les hôtes), ils remplissent des tâches de routage. La plupart du temps cette fonction "pare-feu" est intégrée aux routeurs.

Activités

Outils de diagnostic en CLI :

- ipconfig
- ipconfig /all
- ipconfig /release
- ipconfig /renew
- ipconfig /flushdns
- netsh interface ipv6
- ping
- traceroute
- nslookup
- dig
- arp -a

5. Couche Accès au réseau

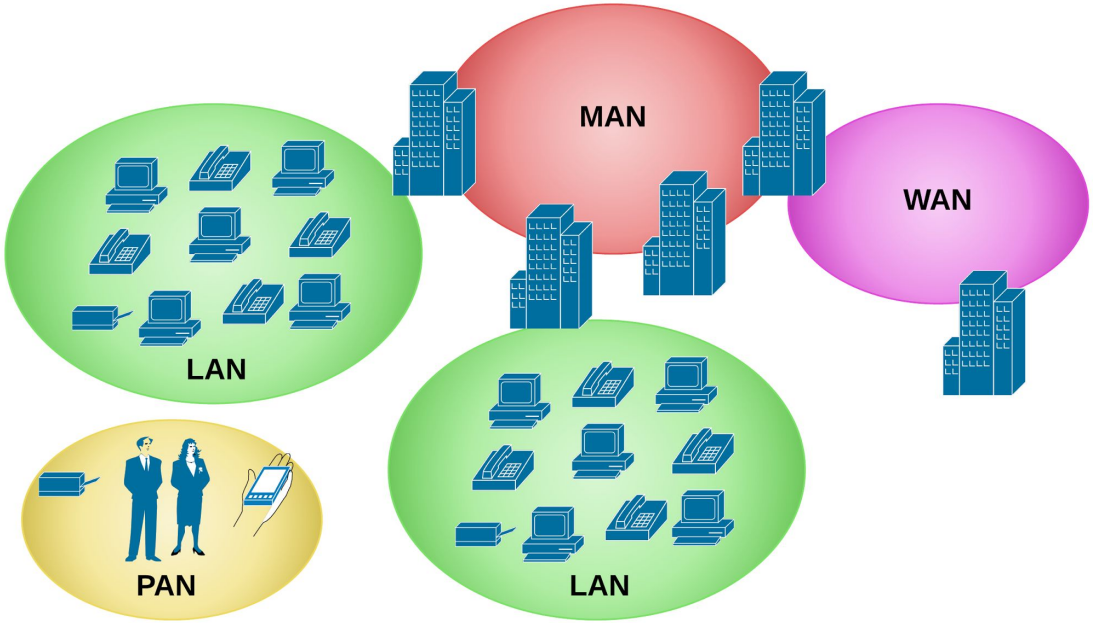
PAN, LAN, MAN, WAN, Ethernet, commutateurs

Accès au réseau

Le modèle TCP/IP (et l'IETF) ne s'occupent pas de la couche Accès Réseau sinon pour assurer l'interopérabilité avec ses protocoles.

- La couche AR fait le lien avec les protocoles de couches supérieures.
- Elle s'occupe de l'adressage physique.
- Elle s'occupe de la manière dont les interfaces placent des données sur un support (MAC).
- Elle définit des caractéristiques de bandes de fréquences, de bande passante, de qualité de câble, de connecteurs, etc.
- Elle fournit éventuellement des mécanismes de fiabilité au niveau local (physique).

LAN/MAN et WAN



La nature PAN, LAN, MAN, WAN est une manière de qualifier une technologie d'accès selon :

- la portée géographique
- et la vitesse.

- Une technologie LAN/MAN a une portée à l'échelle d'un bâtiment ou d'un campus et elle fournit un débit élévé.
- Une technologie WAN dispose d'une portée globale et elle est en général plus lente qu'une technologie LAN.

Technologies LAN/MAN/PAN

Le marché est dominé par les technologies LAN/MAN IEEE 802 :

- LAN/MAN : IEEE 802.3 Ethernet
- *W*LAN : IEEE 802.11 Wi-Fi
- *W*PAN : IEEE 802.15 Bluetooth, ZigBee
- *W*MAN : IEEE 802.16 WiMax

Technologies WAN

Les technologies WAN sont définies par l'ITU, l' ANSI ou d'autres organismes :

- xDSL
- DOCSIS
- 3G/LTE
- ISDN/RNIS
- Frame-Relay
- IP-MPLS
- ...

Introduction à la technologie LAN Ethernet

Ethernet est actuellement la technologie LAN L2 dominante :

- Diversité des supports : Cuivre (paire torsadée) et Fibre
- Interopérable (vers IP, vers les protocoles IEEE 802)
- Stabilité des infrastructures (supports) / Evolutivité de la technologie (services)
- Bon marché
- Facilité de déploiement
- Fiabilité assurée par l'infrastructure et par la commutation

Caractéristiques techniques d' Ethernet

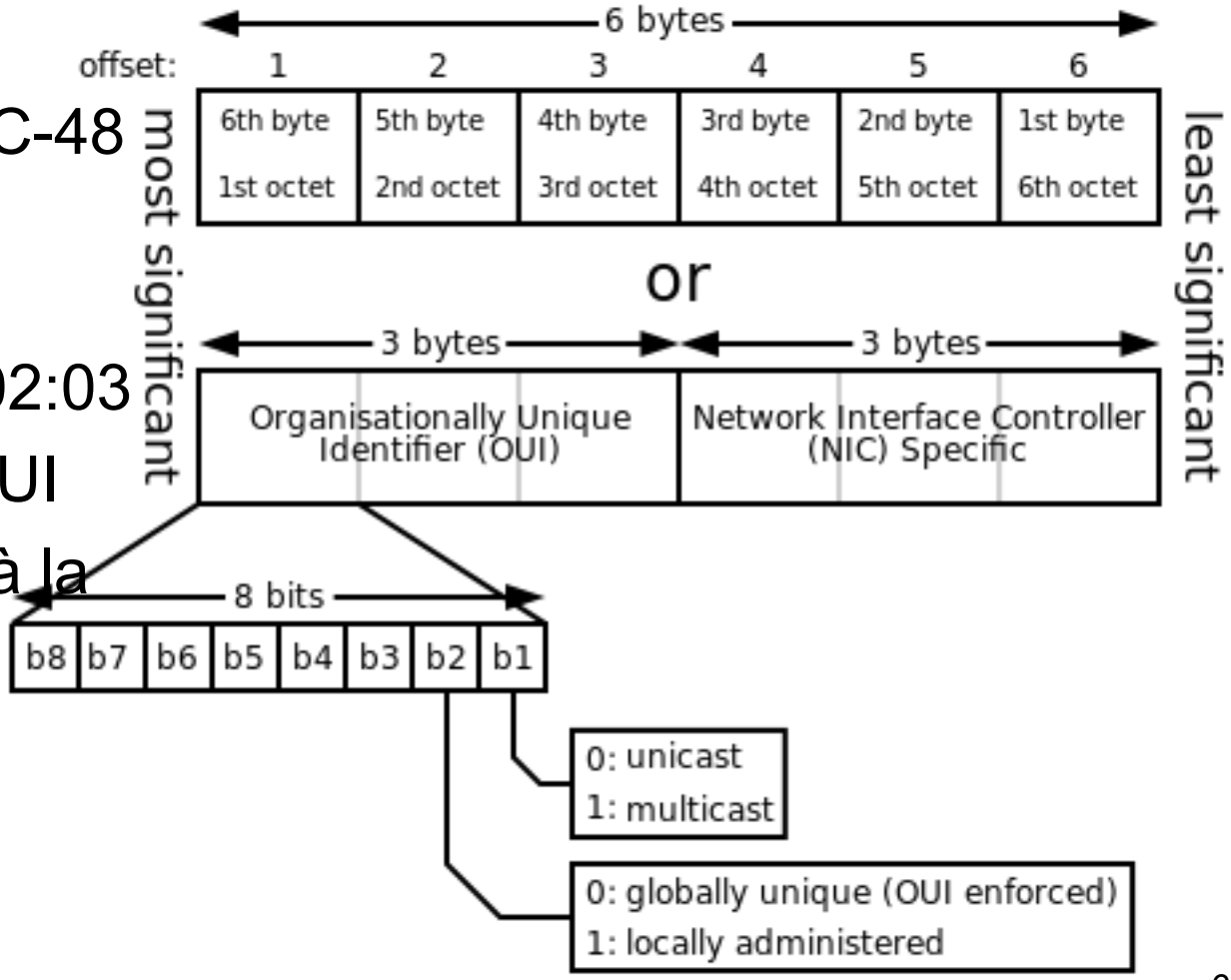
- Une technologie d'accès LAN et MAN
- Standardisé IEEE 802.3
- Aidé par IEEE 802.1 (Bridging) et IEEE 802.2 (LLC).
- de couche Liaison de données (L2) MAC : CSMA/CD
- et de couche Physique (L1)
- réputée non fiable (sans messages de fiabilité)
- non orientée connexion (pas d'établissement d'un canal préalable à la communication)

Adressage IEEE 802

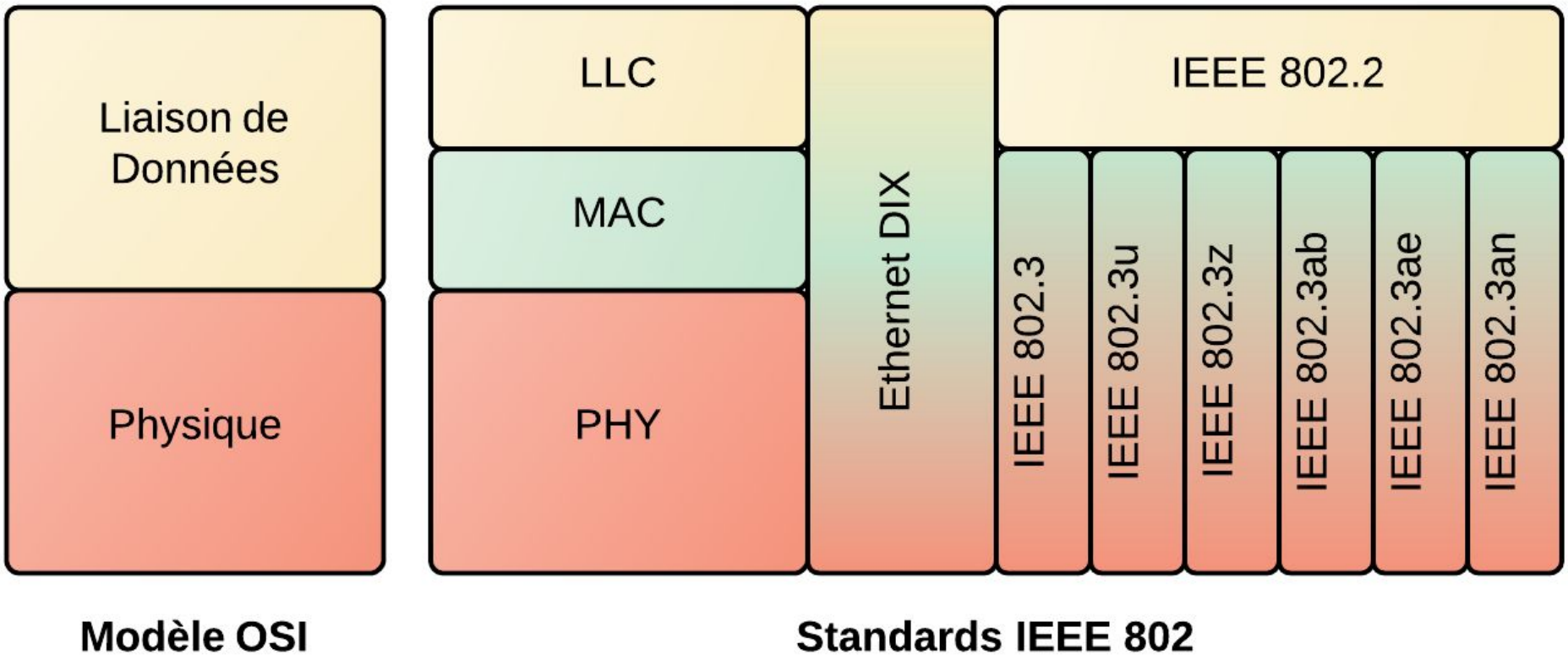
- L'adresse MAC IEEE 802 permet de distinguer les périphériques qui communiquent sur le réseau **local**
- Elle sert uniquement à livrer le trafic **localement**
- Elle est censée être unique
- Ce n’est pas un adressage hiérarchique et routable (comme IP)
- Est fondée dans les cartes réseau, mais peut être émulée.

Adressage de couche 2

- Adressage MAC-48 IEEE 802
- 48 bits
- AA:BB:CC:01:02:03
- 24 bits pour l'OUI
- 24 bits laissés à la discrétion des fabricants



Standard Ethernet/Modèle OSI



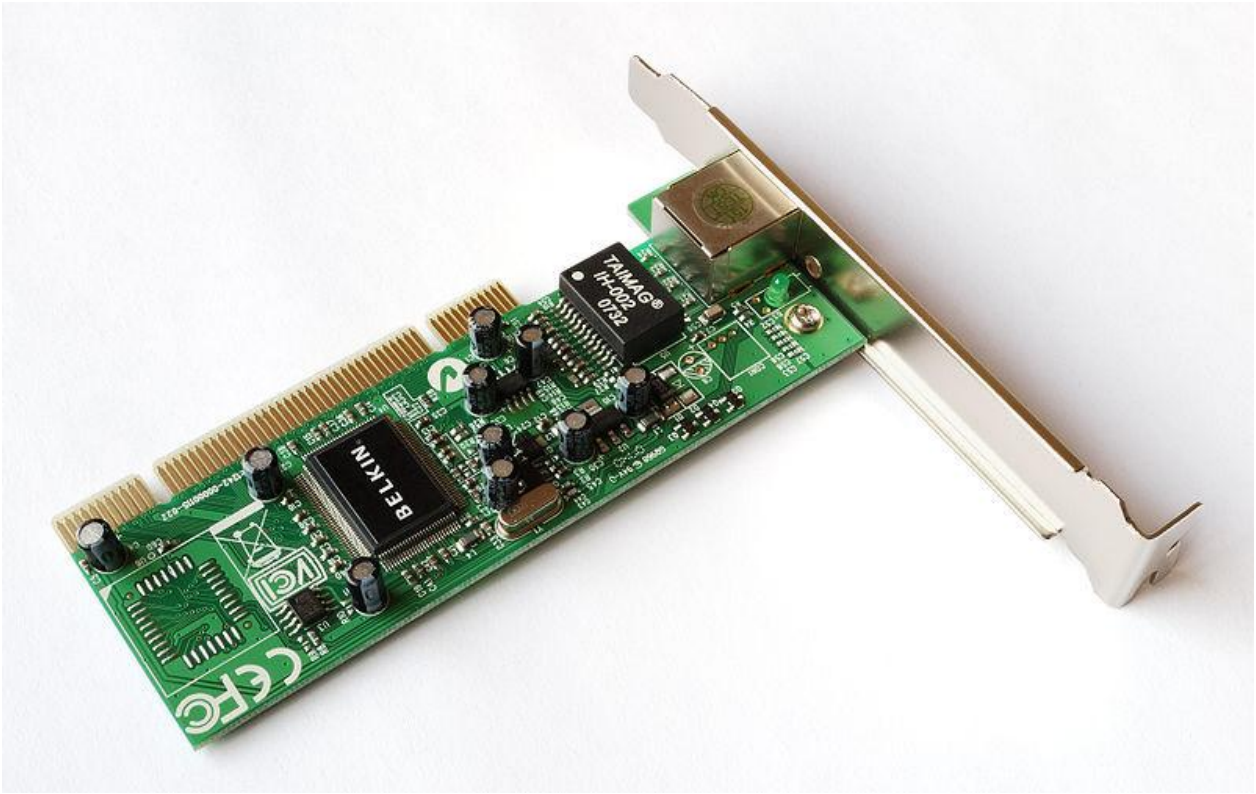
Le standard IEEE 802.3 couvre les deux basses couches du modèle OSI : PHY et MAC, soit la couche Accès Réseau

Synthèse des normes Ethernet

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	1000 Mbps	1000BASE-SX, 1000BASE-LX	IEEE 802.3z	Fibre, 550 m, 5 Km
Gigabit Ethernet	1000 Mbps	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

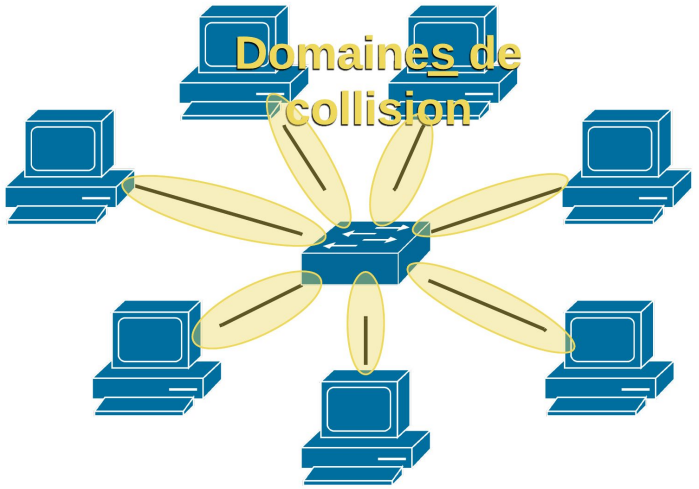
Network Interface Card

Une carte d'interface réseau (NIC) est un matériel de couche 1 et 2 (OSI). L'adresse MAC est fondée dans la puce de la carte.



Révolution de la commutation

- Les commutateurs ont révolutionné les LANs grâce à un **transfert rapide** et **dédié**, notamment grâce à des puces dédiées (ASIC).
- Les adresses MAC attachées à chaque port sont apprises dynamiquement et maintenue dans une table de commutation.
- Le commutateur **prend des décisions** en fonction des adresses MAC de destination qu'il connaît.



Topologie Physique	Topologie logique	Technologie
Etoile Hiérarchique Maillée	Commutée Segmentée	10/100/1000BASE-TX 1000BASE-SX/LX 10GBASE-T/SR/LR/LRM

Comportement d’un commutateur

Un commutateur constitue dynamiquement une table des adresses MAC attachées à ses ports en fonction du trafic qui lui parvient.

Cette table lui permet de transférer “aussi rapidement que le fil” le trafic *unicast* sur un port de sortie.

Un commutateur transfère par tous les ports sauf le port d’ origine :

- Le trafic inconnu.
- Le trafic de *broadcast*.
- Le trafic *multicast*.

6. Supports de transmission du signal

Cuivre, Fibre Optique, Air

Types de supports physiques

On peut coder le flux binaire en trois type d'ondes supportées par différents médias :

- **Ondes électriques** sur un support en cuivre :
  - xDSL : paire téléphonie
  - DOCSIS : câble coaxial
  - Ethernet : paire torsadée (8 fils)
- **Ondes lumineuse** :
  - sur de la fibre optique (Ethernet)
  - ou dans l'air (solutions propriétaires)
- **Ondes radio dans l'air** :
  - HSPA+/LTE, Wi-Fi, WiMax, Bluetooth, connexions satellite, ...

Connecteurs

En fonction des standards édictés, on trouvera plusieurs types de connecteurs.

L'usage d'un connecteur ne présume en rien de la technologie utilisée comme par exemple un connecteur RJ-45 peut connecter de :

- l'Ethernet
- du xDSL
- de l'ISDN
- un port console, ...

Connexion sur une console

- Console physique RS-232/USB
- Console virtuelle Telnet/SSH

Câblage et environnements bruités

1. Le câble cuivre ou FO et l'air transportent les données transmises. Mais ces supports exigent une **connectique** et un placement correct sans quoi le signal risque de se dégrader.
2. Tous les supports peuvent connaître des sources de **bruit** qui dégradent le signal.
3. Les supports ont aussi leurs caractéristiques en **vitesse** et en **portée**.

Cuivre

- Sensible aux **interférences électromagnétiques** : ascenseurs, néons, engins de puissance, etc.
- **Segments physiques limités** à quelques dizaines de mètres → répétition du signal.
- Relativement **bon marché**, **populaire**, **facile à déployer**.
- Format : Paire torsadée, coaxial

Fibre Optique

- La FO est insensible aux interférences électromagnétique et convient aux environnements industriels fortement bruités.
- Peut connaître des **interférences** dues à un mauvais placement du câble FO, une soudure mal réalisées, des connecteurs défectueux, etc.
- **Pas de limite** théorique sur la distance (plusieurs Km) et sur la vitesse (plusieurs Gb/s).
- En soi la FO n'est pas coûteuse. Par contre, le matériel de connexion et de déploiement est certainement plus coûteux (en compétences, en argent).
- Fibre monomode, fibre multimode

Air

- L'air a l'avantage de permettre des connexions au réseau de manière **non-mécanique**. On parle alors de technologies "sans fil".
- Toutefois, c'est un environnement fortement bruité qui peut être corrigé par :
  - des mécanismes de fiabilité protocolaires

    (réservation de ressources, accusés de réception, reprise sur erreur, etc.)
  - des mécanismes physiques comme MIMO.
- Leur portée dépend du **type d'onde** et de la **puissance** d'émission.

Hubs/concentrateurs/media partagé

- En tant que tel le support physique se contente de propager le signal.
- Soit le support est dédié à la communication de deux hôtes, soit le support est partagé entre plusieurs hôtes.
- Afin de distribuer le câble et regénérer le signal, la technologie Ethernet a connu à une époque des **hubs** ou des concentrateurs qui ont été progressivement remplacés par des **commutateurs**.

7. Interactions des protocoles

Routage, Pontage, Résolution de noms, résolution d'adresse, Attribution d'adresses et autres

Protocole de résolution de noms

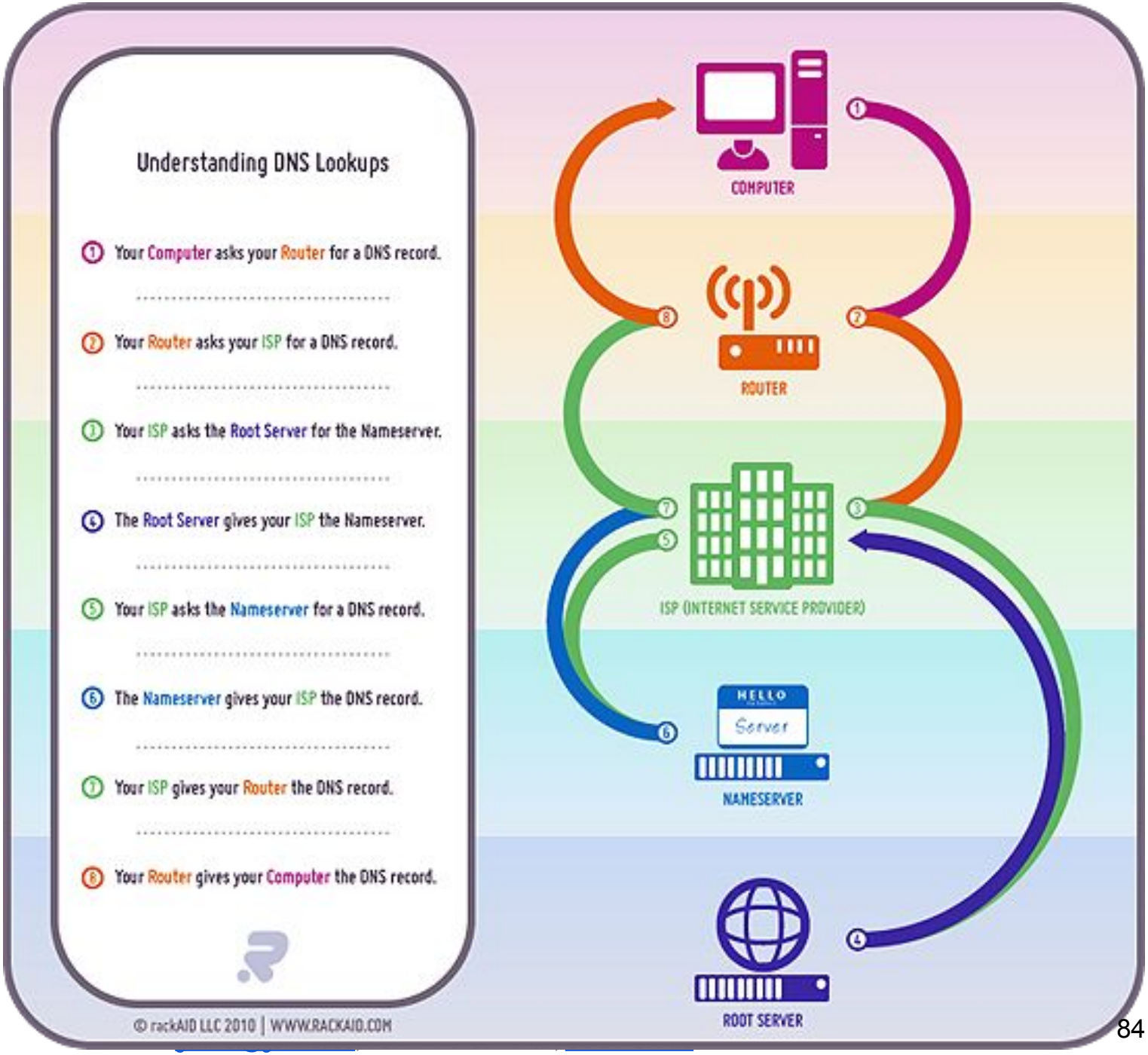
Au niveau protocolaire, seuls les adresses IP sont utilisées pour déterminer les partenaires d'une communication.

Mais dans l'usage courant d'Internet, on utilise des noms pour joindre des machines sur le réseau : c'est plus facile à manipuler que des adresses IP.

Le protocole et le système **DNS** permet de résoudre des noms en adresses IP.

DNS est une sorte de service mondial de correspondance entre des noms et des adresses IP. DNS utilise le port UDP 53.

DNS


Understanding DNS Lookups
1 Your Computer asks your Router for a DNS record.
2 Your Router asks your ISP for a DNS record.
3 Your ISP asks the Root Server for the Nameserver.
4 The Root Server gives your ISP the Nameserver.
5 Your ISP asks the Nameserver for a DNS record.
6 The Nameserver gives your ISP the DNS record.
7 Your ISP gives your Router the DNS record.
8 Your Router gives your Computer the DNS record.
© rackAID LLC 2010 | WWW.RACKAID.COM
COMPUTER
ROUTER
ISP (INTERNET SERVICE PROVIDER)
HELLO
Server
NAMESERVER
ROOT SERVER

Exemple d'interactions DNS/HTTP

Imaginons une station de travail adressée qui tente de joindre www.test.tf dans un navigateur web.

Quel sera le trafic généré par cette action de l'utilisateur ?

1. Résolution de nom
2. Connexion TCP
3. Echange HTTP
4. Fermeture de connexion TCP

Exemple de trafic DNS et HTTP

Trafic DNS

1. 192.168.88.189 -> 192.168.88.1 **DNS** 71 Standard **query 0xebb9** **A www.test.tf**
2. 192.168.88.189 -> 192.168.88.1 DNS 71 Standard query 0x1b6c AAAA www.test.tf
3. 192.168.88.1 -> 192.168.88.189 **DNS** 87 Standard **query response 0xebb9** **A 176.31.61.170**
4. 192.168.88.1 -> 192.168.88.189 DNS 71 Standard query response 0x1b6c

Établissement de session TCP

1. 192.168.88.189 -> 176.31.61.170 TCP 78 *60381→80* **[SYN]** **Seq=0**
2. 176.31.61.170 -> 192.168.88.189 TCP 74 *80→60381* **[SYN, ACK]** **Seq=0** **Ack=1**
3. 192.168.88.189 -> 176.31.61.170 TCP 66 *60381→80* **[ACK]** **Seq=1** **Ack=1**

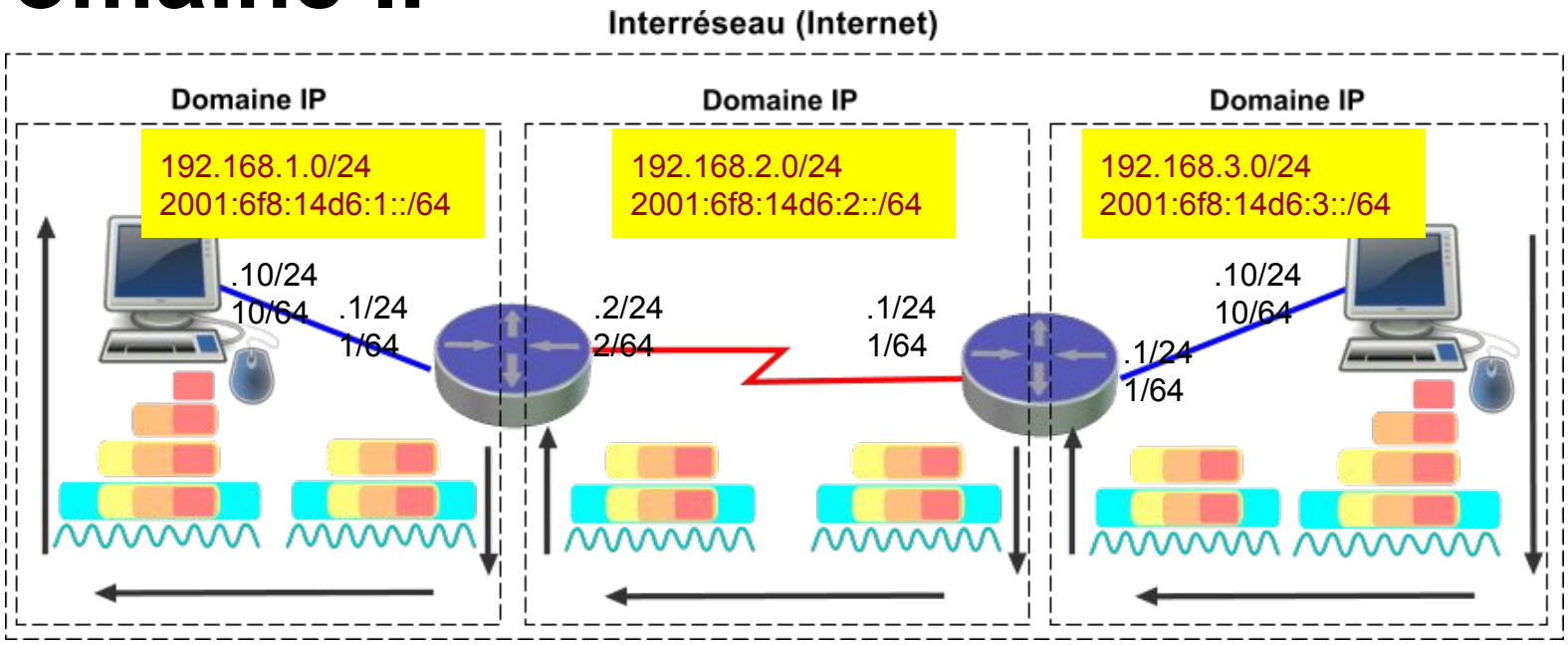
Requête et réponse HTTP

1. 192.168.88.189 -> 176.31.61.170 HTTP 207 GET / HTTP/1.1
2. 176.31.61.170 -> 192.168.88.189 TCP 66 80→60381 [ACK] **Seq=1** Ack=142
3. 176.31.61.170 -> 192.168.88.189 TCP 1506 [TCP segment of a reassembled PDU]
4. 176.31.61.170 -> 192.168.88.189 HTTP 1313 HTTP/1.1 200 OK (text/html)
5. 192.168.88.189 -> 176.31.61.170 TCP 66 60381→80 [ACK] Seq=142 Ack=2688

Fin de session TCP

1. 192.168.88.189 -> 176.31.61.170 TCP 66 60381→80 [FIN, ACK] **Seq=142** Ack=2688
2. 176.31.61.170 -> 192.168.88.189 TCP 66 80→60381 [FIN, ACK] **Seq=2688** **Ack=143**
3. 192.168.88.189 -> 176.31.61.170 TCP 66 60381→80 [ACK] Seq=**143** **Ack=2689**

Domaine IP

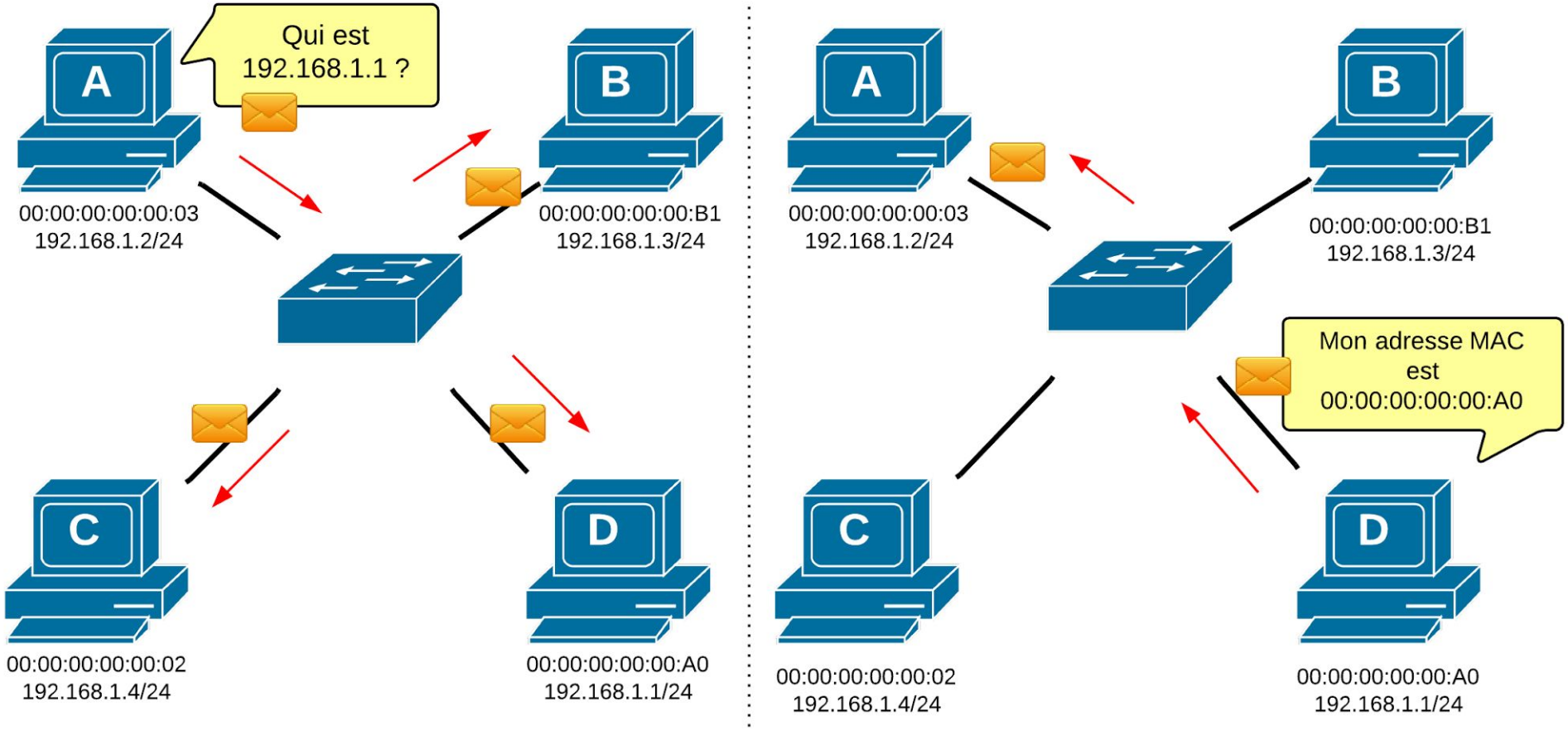


- Deux noeuds (hôtes, interfaces, cartes réseau, PC, smartphone, etc.) doivent appartenir au même réseau, au même domaine IP, pour communiquer directement entre eux.
- Quand les noeuds sont distants, ils ont besoin de livrer leur trafic à une passerelle, soit un routeur.
- D'une extrémité à l'autre, les adresses IP ne sont pas censées être modifiées (sauf NAT) par les routeurs. Par contre, le paquet est désencapsulé /ré-encapsulé différemment au niveau de la couche Accès au passage de chaque routeur.

Protocoles de résolution d'adresses et de découverte des hôtes

- Afin d'encapsuler un paquet IP dans une trame, l'hôte d' origine a besoin de connaître l'adresse physique (MAC) de la destination.
- En IPv4, c'est le protocole ARP (Address Resolution Protocol) qui remplit cette fonction. Les hôtes IPv4 maintiennnent une table appelée ***cache ARP***.
- En IPv6, c'est le protocole ND (Neighbor Discovery), sous-protocole IPv6, qui reprend cette fonction. Les hôtes IPv6 maintiennent une table appelée ***table de voisinage***.

ARP (Address Resolution Protocol)

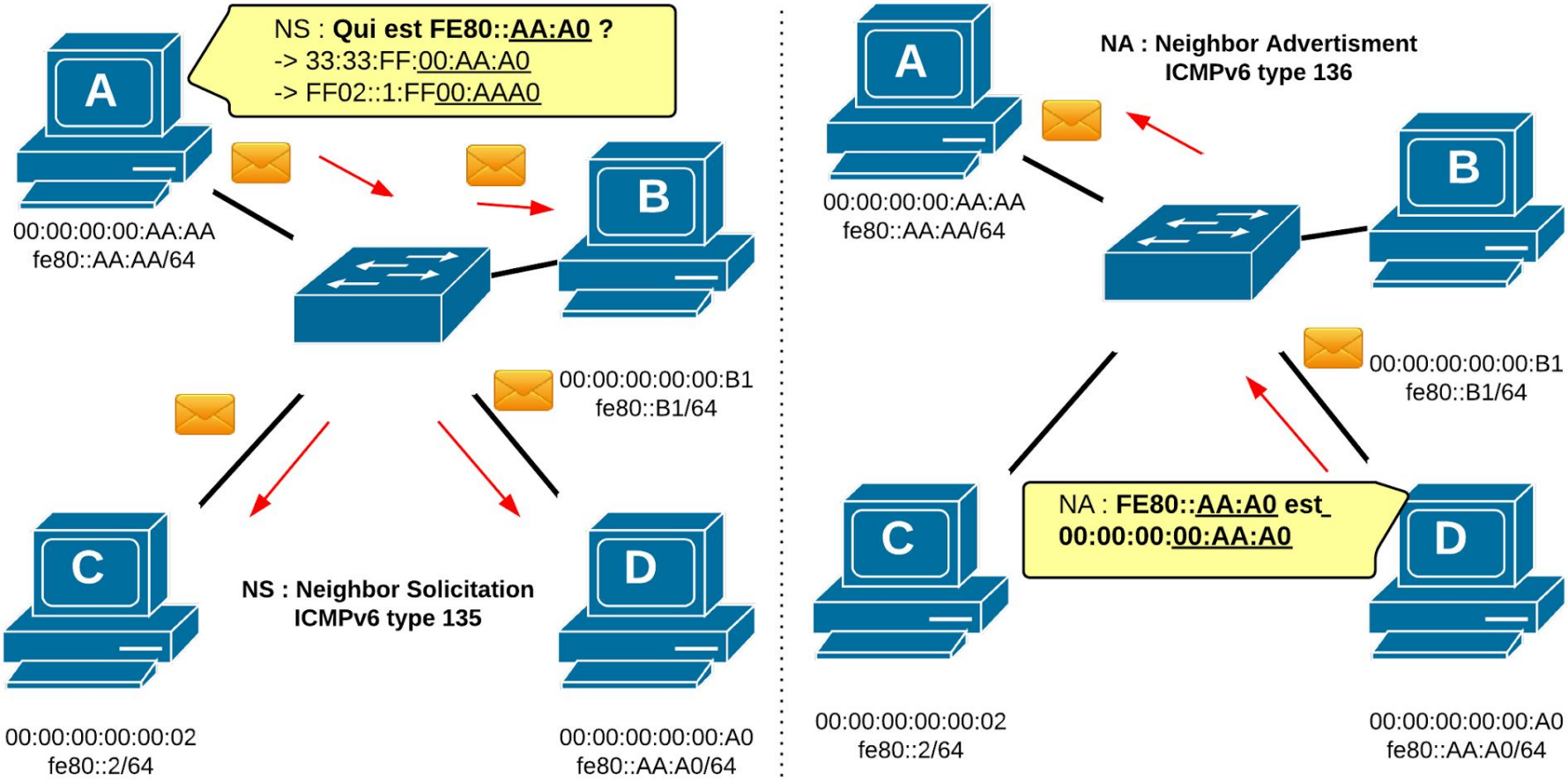


La requête ARP émane en **broadcast** et la réponse est envoyée en unicast.

ND (IPv6) aura un fonctionnement similaire en utilisant une adresse **multicast** spéciale en lieu et place du broadcast.

ND (Neighbor Discovery)

Découverte de voisin sollicitée



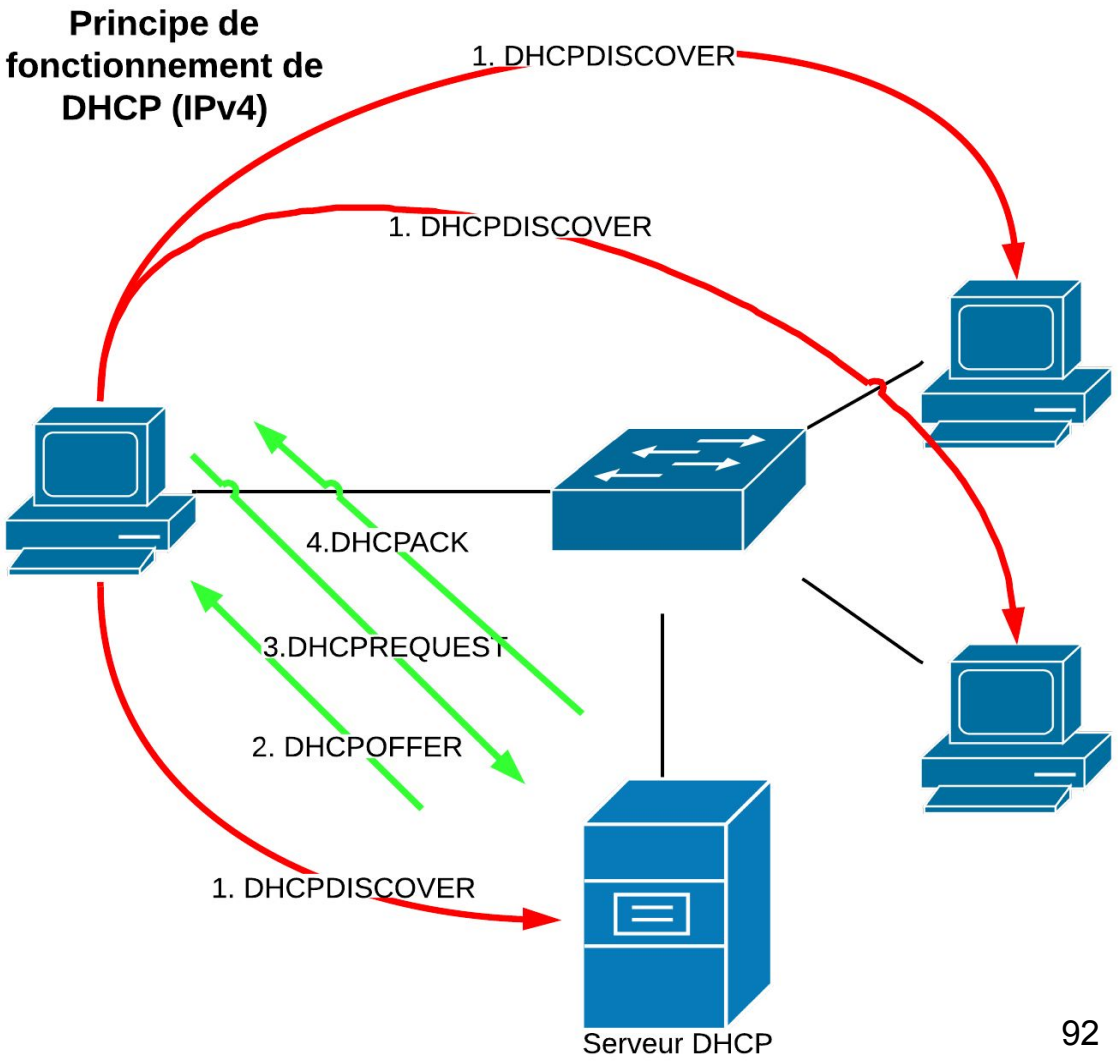
Protocoles d’attribution d’adresses

- Avant de pouvoir émettre du trafic TCP/IP, une interface doit disposer au minimum d’une adresse IP et de son masque et, éventuellement d’autres paramètres (passerelle par défaut, résolveur DNS, etc.).
- En IPv4, c’est **DHCP** qui permet d’attribuer ces paramètres à une interface qui le demande. DHCP maintient un état des adresses attribuées par un mécanisme de bail (à durée déterminée).
- En IPv6, le comportement par défaut est l’ **autoconfiguration** des interfaces mais la version actualisée de **DHCPv6** fournit un service géré des adresses.

DHCP (IPv4)

La procédure d'attribution d'adresses en DHCP (IPv4) consiste en l'échange de 4 messages.

Le premier message DHCP émane du client en **broadcast**, les autres sont échangés en unicast.



Méthodes de configuration IPv6

Dans un réseau IPv6, les routeurs sont automatiquement configuré pour envoyer des messages ICMPv6 Neighbor Discovery spéciaux : des Routeur Advertisement. Il faut aussi partie d'échanges sollicités (Router Solicitations).

Ces messages contiennent des informations sur la manière dont une interface du réseau doit se configurer :

- s'autoconfigurer ou pas avec le préfixe du réseau
- l'usage ou non de DHCPv6 en mode stateful ou stateless.

Interaction des protocoles

Avant qu'une interface puisse envoyer du trafic faut-il :

- qu'elle ait obtenu une adresse IP statique ou dynamique (**DHCP** en IPv4 ou **autoconfiguration/DHCPv6** en IPv6);
- qu'elle ait obtenu l'adresse du livraison physique de la destination locale ou de la passerelle par défaut si la destination n'est pas locale (**ARP** en IPv4 ou **ND** en IPv6);
- qu'elle ait résolu le nom de l'hôte destinataire en adresse IP (**DNS** sur IPv4 ou sur IPv6).

Autres protocoles de gestion

D'autres protocoles de gestion importants se rencontreront dans les réseaux TCP/IP, à titre d'exemples :

- ICMP qui permet en IPv4 et en IPv6 d'obtenir du diagnostic IP (ping et traceroute).
- NTP qui permet de synchroniser les horloges des hôtes sur le réseau.
- SNMP qui permet de collecter des informations sur le matériel à travers le réseau.
- SSH qui permet de monter une console distante à travers TCP/IP.
- ...

Protocoles de routage

Un système autonome (AS) est un ensemble de routeurs gérés par une autorité commune (d'une organisation).

Afin de remplir leurs tables de routage, les routeurs s'échange les informations sur les différents réseaux de destination grâce à des protocoles de routage intérieurs (au sein d'un AS)

- RIP
- OSPF
- IS-IS
- EIGRP

et extérieurs (entre AS) :

- BGP

Protocoles de pontage

Le comportement des commutateurs et les protocoles qui les accompagnent sont définis dans IEEE 802.1 (protocoles de pontage) :

- 802.1D-2004 : Bridging et Spanning-Tree
- 802.1Q-2011 : VLANs
- 802.1X-2010 : Port Based Network Access Control
- 802.1AB-2009 : LLDP protocole de voisinage
- 802.1AX-2008 : Agrégation de liens (initialement 802.3 ad-2000)

Leur portée concerne toute technologie IEEE 802.

8. Synthèse

Tableau de synthèse à remplir

Couches TCP/IP	Fonctions	Protocoles	PDU	Matériel	Adressage / identification	Diagnostic/ commandes
Application						
Transport						
Internet						
Liaison de données						
Physique						

Exercices Pratiques

Sur une station de travail Windows/Linux, sur un routeur et un commutateur :

1. Identifier les interfaces d'une machine et leurs différentes adresses IPv4, IPv6 et MAC.
2. Identifier les différentes tables de commutation, de routage et cache ARP.
3. Vérifier la résolution de noms et vider le cache DNS
4. Identifier les sessions TCP et UDP, tuer les processus associés.
5. Élaborer un diagnostic en couches avec des utilitaires communs.
6. Configurer les adresses IP des interfaces de manière statique, automatique et en client DHCP.

Suivi du document

25/01/2015 : ToDo

- Mise à jour IPv6, découverte de voisinage, SLAAC, ND, NS, RA/RS, NS/NA, NUD, DAD
- Routeurs et tables de routage

Quiz TCP/IP Fondamental

http://cisco.goffinet.org/quiz/quiz-tcp-ip-fondamental

Droits