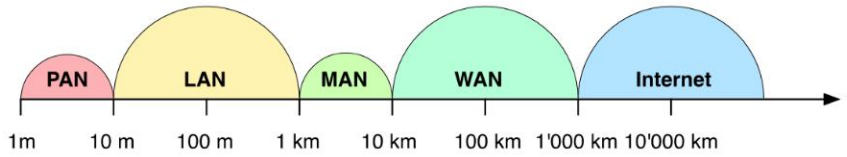
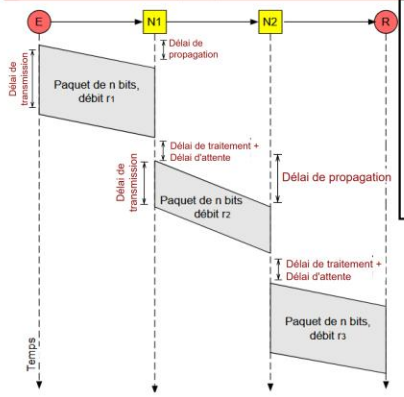
Paramètre	S	Exemple	Unités
Délai	t	Délai aller-retour Délais de transmission	1 s 1 ms = 1/1000 s = 10^{-3} s 1 µs = 1/1000 ms = 10^{-6} s
Vitesse	v	Vitesse de propagation	1 m/s 1 km/s = 1000 m/s = 10^{3} m/s
Longueur de données	l	Taille d'un paquet Taille d'un fichier	1 B 1 KiB = 1024 B = 2^{10} B 1 MiB = 1024 KiB = 2^{20} B 1 GiB = 1024 MiB = 2^{30} B 1 TiB = 1024 GiB = 2^{40} B
Débit binaire	r	Débit de transmission	1 b/s 1 kb/s = 1000 b/s = 10^{3} b/s 1 Mb/s = 1000 kb/s = 10^{6} b/s 1 Gb/s = 1000 Mb/s = 10^{9} b/s
Taux de perte	p	Taux de perte de paquets	Pas d'unité 1% = 0.01 = 1/100 = 10^{-2}



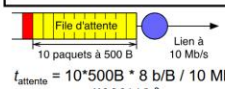


Délai

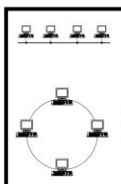
Transmision : n/r
n : longueur du paquet
r: débit binnaire du lien

Propagation : L/V
L : longueur du lien
V : vitesse de propagation

Attente : SNi/r
SNi : somme de la taille de tous les paquets devant le paquet considéré
r : debit binaire du lien



$t_{attente}$ = 10*500B * 8 b/B / 10 Mb/s
= 4'000*10^{-6} s
= 4 ms



1 trans à la fois
- USB

Bien contre les pannes
- optique net

1 node central qui retransmet tous
- LAN

Le mieux pour les pan
- WAN

HUB ( ) :
Juste transmet les bits sur toutes les sorties

Switch Ethernet ( ) :
Interconnect les équipement

Dois pouvoir fonctionner sans aucun config

Utilise un table de filtrage (table CAM) pour envoyer les trame uniquement au destinataire

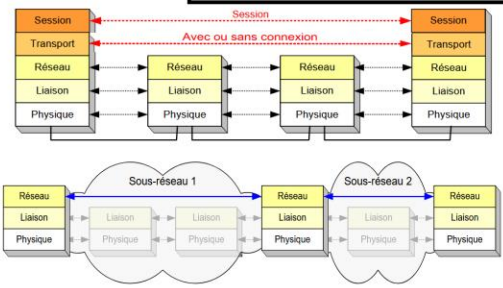
TABLE CAM :
En gros, au debut c'est vide, Quand il reçoit une trame (de M1), si il connais pas le destinataire(M2), il envoye en broadcast et si il connaisais pas la source(M1), il l'ajoute à la table.
Quand M2 lui repond, bah il connais M1 donc il peut directe lui envoyer + maintenant il connais M2

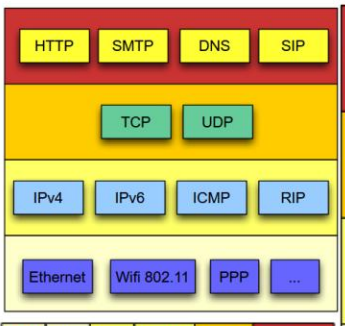
Routeur ( ) :
-Route les paquets
-Implémente le protocle IP
-Interconnect les reseaux mais les sépare aussi

Commutation :
Circuits : phone | continue
Paquets : IT | segmenter

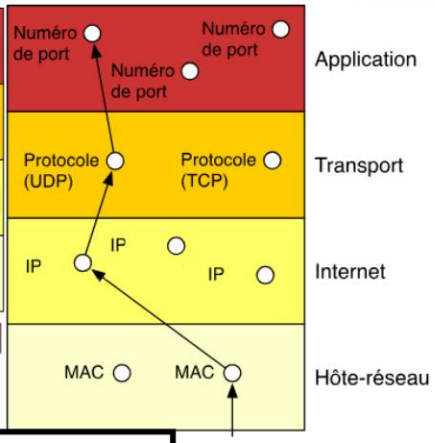
ISO

Application	**Protocoles des applications**	**- Point d'accés au serivces Exemple : HTTP, SMTP**
Présentation	**Syntaxe des données transmises**	**- gère la syntaxe de transfert (ASCII ou Unicode) - Dilalogue et chiffrement des données**
Session	**Permet aux utilisateurs des terminaux d'établir des « sessions » entre eux**	**- "dialogues" (échange bidirectionnels) - Retablie lors d'interruption de session Exemple : transfert d'un fichier très long**
Transport	**Transmission de bout en bout, entre les terminaux**	**- Découper les données pour les couches suppérieurs - Optimise le transport des données - Service fiable (tous les paquets sont bien arrivé) et non fiable (skip les paquets perdus)**
Réseau	**Sous-réseau, Routage, Adressage**	
Liaison	**Simuler une liaison parfaite, sans erreur, pour les lvl supp**	**- Découpe les séquence de bits en packet (trames) - Check les frontier des trames - Corrige les erreur de transmision - Gère la vitesse du flux**
Physique	**Transmission de bits de façon brute +3 -> +25 volt = 0 -3 -> -25 volt = 1**	





Type, Proto = Id du lvl supp

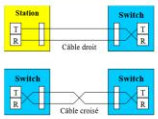


Ethernet

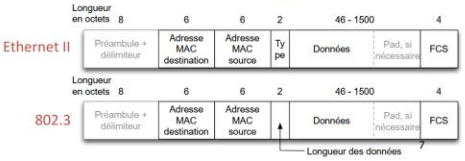
Type	Débit	Support principal	Remarque
FastEthernet	100 Mb/s	Câble UTP électrique	En train de disparaître
Gigabit-Ethernet	1 Gb/s	Câble UTP électrique (ou fibre optique)	Le plus courant actuellement
10/25/50/... Gigabit-Ethernet	10/25/50/... Gb/s	Fibre optique	Utilisé dans les centres de calcul

UTP (Unshielded Twisted Pair)

- 4 paires torsadées non blindées|(10 et 100)Mb/s (2 paire utiliser)
- longueur max : 100m



- Il existe deux formats incompatibles
  - Presque toutes le cartes réseau envoie le format Ethernet II
  - Mais elles comprennent aussi le format 802.3



Préambule : 7 octets (10101010)+ 1 last (10101011) | sychoniser horloge pour garantire une bonne réception

Addr MAC : Addr MAC

Type : indique le protocole de la couch supp | IPv4 : 0x0800, IPv6 : 0x86DD, ARP : 0x0806

Données : min 46 et max 1500 octets | si plus court que 46 → remplissage (pad) est ajoutées

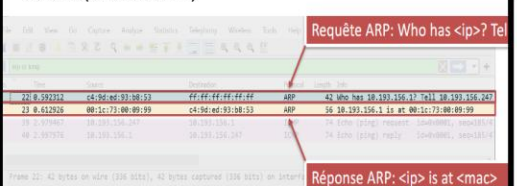
Somme de contrôle (FCS) : la trame se termine par FCS de 32 bits | crée avec l'algo CRC-32 | les recepteurs et les switches intermediaires la verifient | ETHERNET NE PREND PAS LES TRAMES ERRONÉES

ARP (Address Resolution Protocol)

- Trouve l'Addr MAC à qui correspond une Addr IP
- use in LAN

Fonctionement

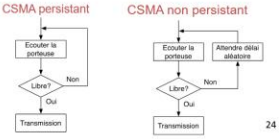
- ARP utilise un cache avec les correspondances (IP : MAC)
- Requête ARP en broadcast si l'addr IP n'est pas dans le cache
- La machine concernée répond avec son MAC
- Les entrées du cache sont éliminées si elles ne sont pas rafraîchies(toutes les 20 min)



Ethernet est un médium partagé

- Une seul transimission est possible à chaque instant
- Pour géré quand 2 Machin envoye en meme temps, il y a le protocol CSMA :

- *Carrier Sense* : écouter si le canal est libre avant de transmettre
- *Multiple Access* : partage du même canal de transmission



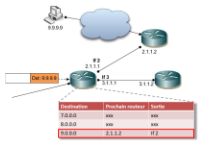
Routage

Acheminement (forwarding) :
- fonctionalité de IP
- IP utilse la table de routage pour savoir où sauter
- Exec pour chaque paquet

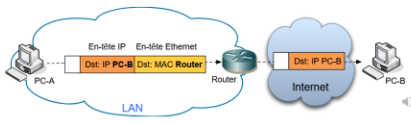
Fonctionement :
Le routeur à une table de routage

Réseau de destination	Prochain routeur	Interface de sortie
123.0.0.0	216.1.2.3	Interface 1

- cherche si il a le reseaux du destinataire dans ça table
- si non, utilise la route par defaut, si il y a
- si non, skip



Remise indirecte :
- le destination se trouve pas dans le réseau
- Le routeur construit une trame avec comme Addr MAC destinataire celle du prochain nœud



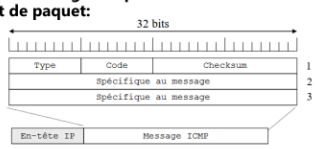
Remise directe :
- le destination se trouve dans le réseau
- Le routeur construit une trame avec comme Addr MAC destinataire celle du destinataire final

Routage (routing) :
- fonctionalité des protocoles routage, comme RIP
- Table de routage avec route optimale
- Exec regulièrement pour update la table

- Statique ou dynamique

Mask / Destination	Prochain routeur	Sortie
1.0.0.0/8	Directement connecté	If 1
150.1.0.0/16	Directement connecté	If 2
200.1.1.0/24	Directement connecté	If 3
Route par defaut→ 0.0.0.0/0	1.1.1.1	If 0

ICMP (Internet Control Message Protocol) :
- communique des problèmes
- effectue des diagnostiques
- Format de paquet:



Type	Message	Description
0 et 8	Echo request et reply	Ping
3	Destination Unreachable Code 0: network unreachable Code 1: host unreachable	Problème de routage
5	Redirect	Le routeur indique à la source qu'il y a un meilleur chemin
11	Time exceeded	TTL d'un datagramme est arrivé à 0

RIP (Routing Information Protocol) :
– Protocole de routage simple

– Utilisé dans de petits réseaux

– Utilise le nombre de sauts comme métrique pour calculer le plus
court chemin

- Limitations : Max 15 sauts et update des routes peut être lent des fois >:[

Fonctionement :
- Chaque routeur maintient une table de routage
- Chaque routeur envoie regulièrement ça table de routage à tous ses voisins
- chaque routeur utilise les tables reçues pour calculer ses routes

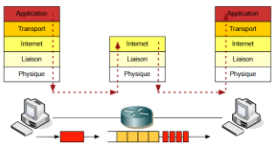
Protocole IP

Offre :
1) Transmission sans connexion :
- pas besoins de connexion avant envoie de donné
- Un paquet (datagramme) contient toutes les info pour son traitement

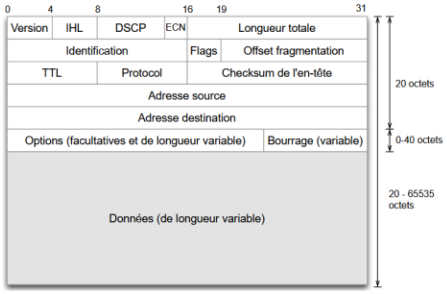
2) Service non fiable (Best effort) :
- Essaie de transmettre au mieux les paquets, pas garantie
- les paquets peuvent être perdu / arriver en désordre / retard

3) Fragementation / reassemblage :
- une source ne connais nit le chemin, nit la tech, juste la taille de paquet max

- un routeur intermédiaire peut framenter un datagramme



Format des datagramme :



- Version (4 bits) : IPv4 ou IPv6

- IHL (Internet Header Lenght) (4 bits) : taille du header, obligatoire à cause des options, en mult de 4 octets (HLT = 5 → 20 octets) une entête à une longeur entre 20 et 60 octets

- DSCP (6 bits) : Raremet utilisé, definit une qualité de service
Ex : service avec débitgaranti

- ECN (Explicit congestion notification) (2 bits) : permette de signaler une source trop soliciter

- Longueur total (16 bits) : taille total du datagramme (en octets)
Max = 65'535 octets

- Identification (16 bits) : ID unique au datagrame

- Flags (3 bits) : DF (Dont fragment) | MF (More fragments) = 0 pour le dernier fragment, sinon 1

- Offset de fragmentation (12 bit) : position du fragment dans le datagrame (en mutl de 8 octets)

- TTL (Time to live) (8 bits) : permette d'eliminer des paquets pris dans une boucle de routage, c'est le nombre de sauts avant la morts en gros

- Protocole (8 bits) : protocle de la couche supp

-checksum de l'en-tête (16 bits) : check sum verifier par les routeur et ça change à chaque saut

- Option (variable) : rarement utiliser, definit une options de routage ou de securité

- Bourrage(variable) : Taille du header dois être un mult de 4octets, donc il faut compléter

Fragmentation :
- à partire de (Ethernet : 1500 octets | WLAN : 7981 octets) on fragment

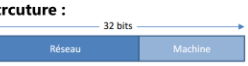
Algorithme de Bellman-Ford distribué :
Calculer la meilleur roue ver un réseau x :
1) Routeur choisit la route la plus courte ver X parmi celles annoncées par les voisins

2) Il incrémente la distance de la route de 1 pour tenir compte de ladistance entre lui et le voisin

Addr IP

Format : 32bits (4 octes)
EX : 193.10.4.3

Strcuture :



2 partie :
- ID Network | donné par un autorité (EX : IPS)
- ID Host | donné par des entreprise, organisation ou user

Class :

Classe	Préfixe réseau	Suffixe machine	Plage d'adresses	Exemple	Commentaire
A	8 bits	24 bits	1.0.0.0 – 127.255.255.255	85.218.0.70	126 réseaux, 16 Mio hôtes
B	16 bits	16 bits	128.0.0.0 – 191.255.255.255	128.178.50.12	16k réseaux, 64k hôtes
C	24 bits	8 bits	192.0.0.0 – 223.255.255.255	193.134.220.23	2 Mio réseaux, 254 hôtes
D			224.0.0.0 – 239.255.255.255	224.0.0.2	Adresses multicast, par exemple « Tous les routeurs »

ADDR SPECIAL :
- Loopback : 127.x.y.z

- Boradcast local : 255.255.255.255

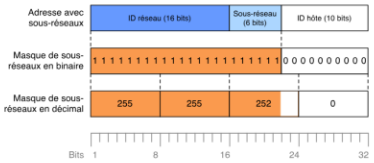
- Addr du réseau : prefixe network + tous les bits à 0
Ex : 132.2.0.0

- Addr broadcast réseau : prefixe network + tous les bits à 1
Ex : 132.2.255.255

Problème de class fixes :
- Gaspillage d'Addr : si besoin de 2 Machine → class C → no nice

- Gestion difficile : on pourrais vouloir subdiviser les Addr par secteur

Mask :



Subdiv class B en 2^6 (64) sous-réseaux, chacun avec 2^10 (1024) machines
Première addr est l'addr du sous-réseau et la dernière Addr est un broadcast
Mask exemple : 255.255.252.0 (bits à 0 = libre pour l'ID)

Calculs de Mask :
EX donné : network B
min 10 sous-réseaux | max 600 machine par sous-réseau

1) definire le mask : on veut crée n sous-réseaux avec au min x machines par sous-réseaux

2) definire l'Addr d'un sous-réseau : Addr IP est x, mask est m. Quelles Addr IP en fait partie ?

Class B → 16 bits disponible pour le sous-réseau et ID hôte

10 sous-réseau → (8<10<16) → 4 bits → 16 sous-réseaux

600 machines → (512<600<1024) →10 bits → 1024 machines

2 bits qui reste, faut les ajouter sois au sous-réseaux, sois au machines sois au 2

Notation CIDR (Classless Interdomain Routing) :
- Ex : 200.123.230.23/21 -> 21 premier bits du mask sont à 1 (255.255.248.0)

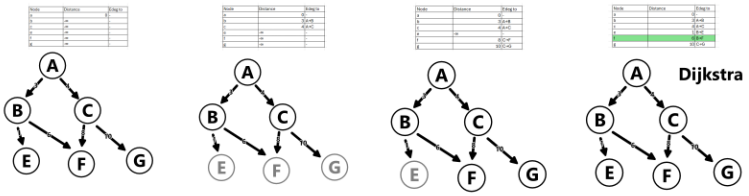
Addr privé :
Addr interne à un réseau → pour l'extérieux une Addr public temp est attribuer

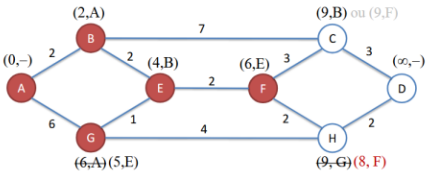
Adresses			Commentaire
10.0.0.0	–	10.255.255.255	1 réseau classe A
172.16.0.0	–	172.31.255.255	16 réseaux classe B
192.168.0.0	–	192.168.255.255	256 réseaux classe C

NAT (Network Address Transaltion) :
Traduit un Addr privée en public

2 type :
- NAT simple : pool d'Addr public → les Addr sont allouée temp donc connection limiter par le nombre d'Addr disponible

- NAPT : une seul Addr public, utilise le port TCP/UDP pour determiner quel la source/destinaton | Ex: privé → NATP → [public|port : 5001]





c'est pareille qu'en algo, mais à la place de stocker la distance par rapport à la node, on stocke la distance totale

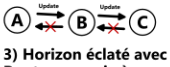
Propagation :
bonnes nouvelles → meilleure route se propage rapidement

Mauvaises nouvelles → si il y a une panne, les routes s'update lentement ver ∞

Heuristiques :
pour accélérer la convergence

1) definir une distance max (au de la de n → ∞)

2) Horizon éclaté (Split horizon)
En gros, on renvoie pas la table à un routeur qui nous a permis d'update



3) Horizon éclaté avec retour empoisonné
Routeur envoie à ses voisiins qu'une route est en pane avec un distance ∞

Addr MAC

Format : 48bits (6 octes)
EX : C8:2A:14:25:CD:BF

Structure :
3 premier octes : ID du constructeur
- 00:00:0C:xx:xx:xx Cisco
- 00:02:B3:xx:xx:xx Intel

3 dernier octets : ID de la cart (généré à la création)

ADDR SPECIAL :
- FF:FF:FF:FF:FF:FF = Broadcast

Architecture d'internet

- Les machine sont connectés à Internet par un ISP (Internet Service Provider)

- il y a des IPS de tier 2 (internationales) et tier 1 (intercontinentale)
- les IPS utilise principalement la fibre lobgue distance (débits : 100 Gb/s)

Perring
- connection entre les IPS, petit → grand = paye | meme taille = free
- ils utilisent pour ça un IXP (Internet Exchange Points)
IXP : des grands salles de routeurs dedier

Tech utiliser :
– xDSL (ADSL, VDSL, typiquement 1 – 20 Mb/s)
– Modem câble (typiquement 1 – 100 Mb/s)
– Accès mobile (3G ou LTE, typiquement 1 Mb/s – 100 Mb/s)
– Fibre optique avec Ethernet (typiquement 100 Mb/s – 1 Gb/s)

Objectifs de sécurité (CIA)

3

Routage par état de lien

Famille de protocoles qui vise à corriger les problème des méthodes par vecteur de distance.

Fonctionement :
routeur effectue regulièrement
1) Decouvrire ses voisins
2) Determiner la distance
3) Construire un paquet avec l'info recupérer
4) Envoyer ce paquet à tous les autre routeurs du sous-réseau
5) Calculer le plus court chemin

Paquet LSP (link state packet) :
- Les LSP sont envoyer en braodcast
- Un LSP à une durée de vie limiter
- La reception d'un LSP envoie un accusé de réception

Caractéristique	Vecteur de distance	Etat de lien
Information envoyée	Vecteurs de distance: **état du réseau global**, vu par le routeur	Envoi des états de lien: **état des liens locaux**, vus par le routeur
Destinataires de l'information	Uniquement les **voisins directs**	Tous les nœuds du réseau, par inondation
Méthode de calcul	Bellman-Ford **calcul partiel** pour compléter le calcul effectué par les voisins	Dijkstra **calcul complet** sur la base des informations reçues de tous les autres nœuds
Avantages	Protocole simple	Convergence rapide et fiable
Inconvénients	Convergence peut être lente Vecteurs de distance peuvent être volumineux	Envoi des message par inondation est complexe

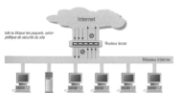
Firewall

Filtre les paquets entrant et sortant pour securisé le réseau
protege pas contre : user, connection qui passe par lui, virus/vers

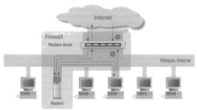
Refus par défaut	Permission par défaut
« Ce qui n'est pas expressément autorisé est interdit » • Choix évident du point de vue de l'administrateur • Difficile à comprendre pour les utilisateurs	*« Ce qui n'est pas expressément interdit est autorisé »* • Suppose que les utilisateurs connaissent les dangers • Vouée à l'échec • Course contre les nouveaux services, les nouvelles failles, les nouvelles idées des utilisateurs

Types d'équipements :
1) routeur écrand / firewall : flitre les paquet
2) proxy : Retransmet les requêtes des clients vers le vrai serveur
3) Machine bastion : server exposer ver l'exterieur (genre server web)

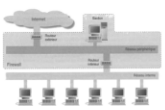
Architecture :
Routeur écran simple
• Simple à mettre en place
• Niveau de sécurité basic
• Pas de défense enprofondeur (une seulebarrière à franchir)
• Pas de sécurité applicative



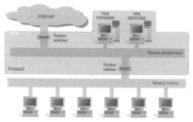
Routeur écran avec bastion
• Bon niveau de sécurité (réseau et applicative)
• Le bastion se trouve sur le réseau interne
• Le routeur écran est l'unique point de défense



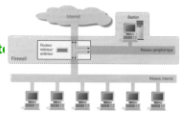
Sous-réseau à écran (DMZ) (demilitarized zone)
• Solution bien sécurisée
• Solution standard dans les réseauxd'entreprise
• Solution coûteuse



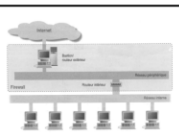
Plusieurs bastions
• Performances améliorées
• Différents niveaux de sécurité
• Solution coûteuse



(Variant) fusionner routeurs externe et interne
↑ Ne diminue que peu lasécurité
• Le routeur est le seulélément de défense



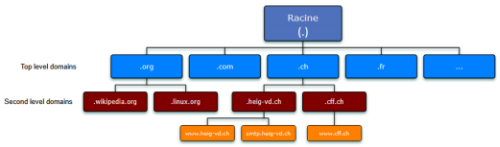
(Variant) fusionner routeur externe et bastion
↑ Ne diminue que peu lasécurité



NE PAS fusionner bastion et routeur interne
Rend inutile le réseaupériphérique
– Si le bastion est infiltré,l'agresseur a accès autrafic LAN

DNS

Max 253 caractères et Max 63 carctères par label



RR (Resource Record) :
Chaque nodes DNS peut être associer une ensemble de ressources (d'hab c'est juste un IP)

Nom de domaine	Durée de vie	Classe	Type	Valeur

- Durée de vie : durée en secondes, exemple 86'400 = 1 jours
- Type : Type de l'enregistrement

Type	Signification	Valeur
A	Adresse IPv4	Par exemple 193.134.220.23
AAAA	Adresse IPv6	Par exemple 2a00:1450:4002:803::1017
CNAME	Nom canonique	Nom canonique d'un serveur pour un alias donné. Par exemple gmail-smtp-msa.l.google.com pour smtp.gmail.com
MX	Serveur de messagerie	Nom canonique du serveur de messagerie pour ce domaine Par exemple mailcl1.heig-vd.ch pour heig-vd.ch
NS	Serveur de noms	Nom du serveur DNS responsable pour un domaine. Par exemple dnsext02.heig-vd.ch pour heig-vd.ch
TXT	Texte	Texte ASCII arbitraire
PTR	Pointeur	Nom de domaine pour une adresse IP. Pour la résolution inverse. Par exemple www.heig-vd.ch pour 23.220.134.193.in-addr.arpa
SOA	Description de la zone	Serveur principal, courriel de contact et d'autres informations concernant la zone de ce domaine

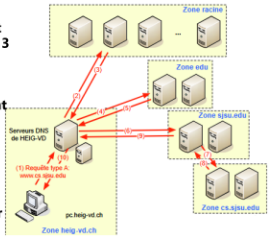
Zone DNS :
Une zone est une partie de l'arborescence pour laquelle un server a la responsabilité admin

Une zone peux sous-zons en déléguant

Requêtes DNS :
1) Recherche du nom de domaine x

2) Le serveur DNS (HEIG) ne connait pas x → envoie la requête à un des 13 serveurs racine

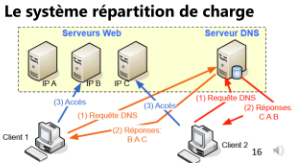
3/4) Recherche itéerative :
le serveur racine repond directement en indiquant le serveur DNS officiel de la zone x
/
recherches récursives
En gros, la diff c'est que quand le server DNS ne connais pas la reponces, en iterative, il vas envoyer une reponces pour dire "vas voir là bas" alors quand recursive, il envoie lui meme la query et après renvoie la reponce lui meme à la machine



7) la requet arrive à un server qui connais la reponse et la renvoie (7→8→9→10)

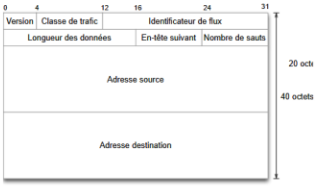
Cache DNS :
Les serveur on un cache pour garder les reponces précédent afin de repondre plus vite au prochain demande
- il vas juste dire spécifier que la réponce n'est pas "officielle" si il utilise le cache

Round-robin :
Le système répartition de charge



16

En-tête :



-Classe de trafic (8 bit) : services différenciés

-Identificateur de flux (20 bit) : Permettra à l'avenir le traitement plus efficace de flux de paquets

-Longueur des données (16 bit) : Max 65'535 / option "Jumbogrammes" pour plus de data

-En tete suivant (8 bits) : ID du type d'en-tête suivant

- Nombre de sauts : TTL

IPv6

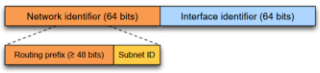
1) sur 128 bits
2) En-tête simplifier
3) PAS de fragmentation par les routeurs
4) Extensibilité par l'en-tête
5) Nouvelles fonctionnalités
– Autoconfiguration d'adresses des machines (sans DHCP)
– Découverte de la MTU le long d'une route
6) ARP, ICMP, IGMP remplacés par ICMPv6

Format :
8 groupes de 4 chiffres hexa
exemple : 2001:AB75:4345:4A45:AF3F:3255:F431:A44B

Simplification :
- les premiers 0 d'un group peuvent être skip (A12 → 0A12)
- plusieur groupes de 0 peuvent être skip par "::"
EX : 2010:0:0:0:0:800:200C:2342 → 2010::800:200C:2342
0:0:0:0:0:0:0:1 → ::1

Structure :
Prefix network : 64 bits
ID machine : 64 bits

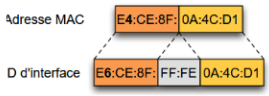
Le prefix network peux contenire le sous-réseaux



Exemple :
2001:123:12:1AA0:1:2:3:4
2001:123:12:: /48 | Prefix
...1AA0... (16 bits) | sous-réseau
::1:2:3:4 (64 bits) | ID machine

Prefix :
globale : 2000:: - 3FFF:
local : FE80::/64

Auto-config de l'ID :
Méthode EUI-64 modifiée
- prendre l'Addr MAC d'une interface
- ajouter FFFE au mid
- flip le 2ème bit de poids faible du premier octet



Autre Addr :

Adresse	Explication
::1	**Adresse de rebouclage (loopback)** Similaire à 127.0.0.1 en IPv4
::	**Adresse non spécifiée** Similaire à 0.0.0.0 en IPv4. Utilisée si l'adresse n'est pas encore connue.
FF00::/8	**Adresses multicast** Par exemple FF02::1 → tous les nœuds du 'lien' (=LAN). L'adresse FF02::1 correspond à 255.255.255.255 en IPv4.
FC00::/7	**Adresse locale unique** Similaire aux adresses privées. Pour la communication à l'intérieure d'une organisation (non routable sur Internet).
Comme unicast globale	**Adresse anycast** Une adresse globale peut être assignée à plusieurs interfaces/machines. Le routage normal fait qu'un paquet avec une adresse anycast comme destination est routé vers l'interface la plus proche.

Nouvelle fonctionnalité :

Découvert de voisins :
Remplace le protocole ARP avec ICMPv6

- Message "get neightbord" | boardcast qui l'IPv6 chercher

- Message "annonce neightbord" | repond au premier message

Fragmentation :
Min 1280 oct

Algorithme
- Partie non fragmentable: en-tête de base et l'option hop-by-hop
- Le reste peut être fragmenté
- Chaque fragment comprend
  - La partie non fragmentable complète
  - L'en-tête de fragmentation
  - Une partie du datagramme