Comment trouver son chemin sur internet ?

Le port ? C'est au bord de la mer, vous pouvez pas vous tromper !

Michaël PAULON

18 Mars 2021

Petits rappels

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

- Modèle OSI :

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

- Modèle OSI : les communications en réseau fonctionnent par couches encapsulées les unes dans les autres

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

- Modèle OSI : les communications en réseau fonctionnent par couches encapsulées les unes dans les autres
- Ipv4 / IPv6 :

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

- Modèle OSI : les communications en réseau fonctionnent par couches encapsulées les unes dans les autres
- Ipv4 / IPv6 :
  - IPv4 : 32 bits d'information : 192.168.1.10/24
  - IPV6 : 128 bits d'information : 2a01 :cb04 493 :6300 :131 :1932 :ad41 :54b4/64

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

- Modèle OSI : les communications en réseau fonctionnent par couches encapsulées les unes dans les autres
- Ipv4 / IPv6 :
  - IPv4 : 32 bits d'information : 192.168.1.10/24
  - IPV6 : 128 bits d'information : 2a01 :cb04 493 :6300 :131 :1932 :ad41 :54b4/64
- TCP :

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

- Modèle OSI : les communications en réseau fonctionnent par couches encapsulées les unes dans les autres
- Ipv4 / IPv6 :
  - IPv4 : 32 bits d'information : 192.168.1.10/24
  - IPV6 : 128 bits d'information : 2a01 :cb04 493 :6300 :131 :1932 :ad41 :54b4/64
- TCP : Protocole de couche 4 (Transport),

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

- Modèle OSI : les communications en réseau fonctionnent par couches encapsulées les unes dans les autres
- Ipv4 / IPv6 :
  - IPv4 : 32 bits d'information : 192.168.1.10/24
  - IPV6 : 128 bits d'information : 2a01 :cb04 493 :6300 :131 :1932 :ad41 :54b4/64
- TCP : Protocole de couche 4 (Transport), les deux parties font un handshake,

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

- Modèle OSI : les communications en réseau fonctionnent par couches encapsulées les unes dans les autres
- Ipv4 / IPv6 :
  - IPv4 : 32 bits d'information : 192.168.1.10/24
  - IPV6 : 128 bits d'information : 2a01 :cb04 493 :6300 :131 :1932 :ad41 :54b4/64
- TCP : Protocole de couche 4 (Transport), les deux parties font un handshake, vérification que les paquets sont bien arrivés,

Petits rappels

Ce séminaire ne rapellera pas forcément certaines bases de réseau, n'hésitez SURTOUT PAS à poser des questions si vous ne comprenez pas quelquechose.

- Modèle OSI : les communications en réseau fonctionnent par couches encapsulées les unes dans les autres
- Ipv4 / IPv6 :
  - IPv4 : 32 bits d'information : 192.168.1.10/24
  - IPV6 : 128 bits d'information : 2a01 :cb04 493 :6300 :131 :1932 :ad41 :54b4/64
- TCP : Protocole de couche 4 (Transport), les deux parties font un handshake, vérification que les paquets sont bien arrivés, garantie que les paquets sont dans l'ordre

Le routage

Hop-by-hop :

Le routage

Hop-by-hop :

- Si l'ip est dans le réseau local : on la contacte directement

Le routage

Hop-by-hop :

- Si l'ip est dans le réseau local : on la contacte directement
- sinon on regarde dans sa table de routage, on choisi le routeur en fonction des règles suivantes :
  - préfixe le plus précis
  - métrique la plus plus faible

Le routage

Hop-by-hop :

- Si l'ip est dans le réseau local : on la contacte directement
- sinon on regarde dans sa table de routage, on choisi le routeur en fonction des règles suivantes :
  - préfixe le plus précis
  - métrique la plus plus faible

On peut aussi implémenter des règles de policy-routing (matcher sur l'ip d'origine par exemple)

Pas d'info sur le chemin parcouru, pas de communication entre les routeurs, configuration majoritairement statique, possibilité de boucles ...

BGP ? Kékécé ?

Selon Wikipedia, BGP (Bordure Gateway Protocole) :

BGP ? Kékécé ?

Selon Wikipedia, BGP (Bordure Gateway Protocole) :

- est un protocole d'échange de routes (externe)

BGP ? Kékécé ?

Selon Wikipedia, BGP (Bordure Gateway Protocole) :

- est un protocole d'échange de routes (externe)
- a pour objectif principal d'échanger des informations de routage et d'accessibilité de réseaux entre AS

BGP ? Kékécé ?

Selon Wikipedia, BGP (Bordure Gateway Protocole) :

- est un protocole d'échange de routes (externe)
- a pour objectif principal d'échanger des informations de routage et d'accessibilité de réseaux entre AS
- circule sur TCP et est donc de la couche application

BGP ? Kékécé ?

Selon Wikipedia, BGP (Bordure Gateway Protocole) :

- est un protocole d'échange de routes (externe)
- a pour objectif principal d'échanger des informations de routage et d'accessibilité de réseaux entre AS
- circule sur TCP et est donc de la couche application
- base ses décisions de routage sur les chemins parcourus, les attributs des préfixes et un ensemble de règles de sélection définies par l'administrateur de l'AS

BGP ? Kékécé ?

Selon Wikipedia, BGP (Bordure Gateway Protocole) :

- est un protocole d'échange de routes (externe)
- a pour objectif principal d'échanger des informations de routage et d'accessibilité de réseaux entre AS
- circule sur TCP et est donc de la couche application
- base ses décisions de routage sur les chemins parcourus, les attributs des préfixes et un ensemble de règles de sélection définies par l'administrateur de l'AS
- est un protocole à vecteur de chemins

EBGP

BGP est utilisé pour organiser les routes entre les AS : External BGP

EBGP

BGP est utilisé pour organiser les routes entre les AS : External BGP

- Peering : chacun annonce ses propres routes à l'autres

EBGP

BGP est utilisé pour organiser les routes entre les AS : External BGP

- Peering : chacun annonce ses propres routes à l'autres
- Transit : le transitaire annonce des routes dont il n'est pas le destinataire final et le transité annonce ses propres routes

Principe

Il peut aussi être utilisé à l'interieur d'un AS : Internal BGP

- Routeurs de bordure qui font du EBGP avec l'exterieur
- Routeurs internes qui font du IBGP entre eux

Principe

Il peut aussi être utilisé à l'interieur d'un AS : Internal BGP

- Routeurs de bordure qui font du EBGP avec l'exterieur
- Routeurs internes qui font du IBGP entre eux

Problème : Les routeurs internes doivent être en full mesh : chacun parle à tous les autres.

Principe

Il peut aussi être utilisé à l'interieur d'un AS : Internal BGP

- Routeurs de bordure qui font du EBGP avec l'exterieur
- Routeurs internes qui font du IBGP entre eux

Problème : Les routeurs internes doivent être en full mesh : chacun parle à tous les autres.
Solutions :

- Route reflexion
- Confederation

Route reflexion

Deux type de routeurs :

Route reflexion

Deux type de routeurs :

- "Standard" (ou RR-client) : établi uniquement une session avec un RR et annonce ses propres routes

Route reflexion

Deux type de routeurs :

- "Standard" (ou RR-client) : établi uniquement une session avec un RR et annonce ses propres routes
- Route reflector (ou RR-server) :
  - si une route vient d'un non-client (par exemple un routeur EBGP ou un autre RR-server) : annonce uniquement aux clients
  - si une route vient d'un RR-client, annoncée à tous les autres peers(à l'exception du client qui a annoncé la route)

Confédération

On décompose l'AS en plusieurs AS "privés" (plages d'ASN 64512-65534 et 4200000000-4294967294)

Confédération

On décompose l'AS en plusieurs AS "privés" (plages d'ASN 64512-65534 et 4200000000-4294967294)

Il faut faire attention à ne pas annoncer les numéros d'AS privés en dehors de son AS.

Choisir la route

Le choix de la route à emprunter pour atteindre une destination se fait en fonction d'un ensemble de paramètres, par exemple :

Choisir la route

Le choix de la route à emprunter pour atteindre une destination se fait en fonction d'un ensemble de paramètres, par exemple :

- Next-hop : puis-je contacter le routeur voisin ?

Choisir la route

Le choix de la route à emprunter pour atteindre une destination se fait en fonction d'un ensemble de paramètres, par exemple :

- Next-hop : puis-je contacter le routeur voisin ?
- Weight : poid local pas propagé, permet de prioriser un voisin (le moins cher, le plus gros tuyau ...)

Choisir la route

Le choix de la route à emprunter pour atteindre une destination se fait en fonction d'un ensemble de paramètres, par exemple :

- Next-hop : puis-je contacter le routeur voisin ?
- Weight : poid local pas propagé, permet de prioriser un voisin (le moins cher, le plus gros tuyau ...)
- Self-originated : on privilégie ses propres routes

Choisir la route

Le choix de la route à emprunter pour atteindre une destination se fait en fonction d'un ensemble de paramètres, par exemple :

- Next-hop : puis-je contacter le routeur voisin ?
- Weight : poid local pas propagé, permet de prioriser un voisin (le moins cher, le plus gros tuyau ...)
- Self-originated : on privilégie ses propres routes
- AS-path : liste des AS parcourus, on préfère la plus courte (et permet d'éviter les boucles, on drop les routes où on est dans l'AS-path)

Choisir la route

Le choix de la route à emprunter pour atteindre une destination se fait en fonction d'un ensemble de paramètres, par exemple :

- Next-hop : puis-je contacter le routeur voisin ?
- Weight : poid local pas propagé, permet de prioriser un voisin (le moins cher, le plus gros tuyau ...)
- Self-originated : on privilégie ses propres routes
- AS-path : liste des AS parcourus, on préfère la plus courte (et permet d'éviter les boucles, on drop les routes où on est dans l'AS-path)
- MED : permet d'annoncer le routeur préféré pour contacter l'AS

Choisir la route

Le choix de la route à emprunter pour atteindre une destination se fait en fonction d'un ensemble de paramètres, par exemple :

- Next-hop : puis-je contacter le routeur voisin ?
- Weight : poid local pas propagé, permet de prioriser un voisin (le moins cher, le plus gros tuyau ...)
- Self-originated : on privilégie ses propres routes
- AS-path : liste des AS parcourus, on préfère la plus courte (et permet d'éviter les boucles, on drop les routes où on est dans l'AS-path)
- MED : permet d'annoncer le routeur préféré pour contacter l'AS
- Age : depuis quand la route est dans la table

Choisir la route

Le choix de la route à emprunter pour atteindre une destination se fait en fonction d'un ensemble de paramètres, par exemple :

- Next-hop : puis-je contacter le routeur voisin ?
- Weight : poid local pas propagé, permet de prioriser un voisin (le moins cher, le plus gros tuyau ...)
- Self-originated : on privilégie ses propres routes
- AS-path : liste des AS parcourus, on préfère la plus courte (et permet d'éviter les boucles, on drop les routes où on est dans l'AS-path)
- MED : permet d'annoncer le routeur préféré pour contacter l'AS
- Age : depuis quand la route est dans la table

En cas d'égalité sur les routes, on départage sur le Router-ID le plus faible puis sur l'ip du routeur la plus faible.

Multi-homing, RPKI et sécurité

Multi-homing : un AS a ses routes annoncées depuis plusieurs autres AS.

Multi-homing, RPKI et sécurité

Multi-homing : un AS a ses routes annoncées depuis plusieurs autres AS.

Comment vérifier qu'un peer a le droit d'annoncer une route ?

Multi-homing, RPKI et sécurité

Multi-homing : un AS a ses routes annoncées depuis plusieurs autres AS.

Comment vérifier qu'un peer a le droit d'annoncer une route ?

RPKI (Ressource Public Key Infrastructure) : certificat validé par l'IANA prouvant la possession de ressources par le LIR.
Permet de signer des ROA (Route Origination Authorizations) indiquant de quel AS peut venir quel préfixe.

Taille de la table et ASN 32bits

Ressources sous dimensionnées par rapport à la croissance d'internet.

Taille de la table et ASN 32bits

Ressources sous dimensionnées par rapport à la croissance d'internet.
En 2012, la RFC 6793 étend la taille des numéros d'AS de 16 à 32 bits.

Taille de la table et ASN 32bits

Ressources sous dimensionnées par rapport à la croissance d'internet.
En 2012, la RFC 6793 étend la taille des numéros d'AS de 16 à 32 bits.
En 2014, la full-table IPv4 a dépassé les 512k entrée, certains anciens routeurs encore utilisés n'étaient pas dimenssionnés pour plus de 512k entrées.

Taille de la table et ASN 32bits

Ressources sous dimensionnées par rapport à la croissance d'internet.
En 2012, la RFC 6793 étend la taille des numéros d'AS de 16 à 32 bits.
En 2014, la full-table IPv4 a dépassé les 512k entrée, certains anciens routeurs encore utilisés n'étaient pas dimenssionnés pour plus de 512k entrées.

Aujourd'hui une full table v4 fait 837k routes et une full table v6 107k.

Pakistan Telecom vs Youtube

article de presse

Verizon vs Cloudflare

article sur le blog de cloudflare

Merci beaucoup pour votre attention.
Des questions ?