BGP

Border Gateway Protocol
BGP4

David LOPOI

RAPPEL

Adressage

Filtrage des adresses locales:
- **Ne pas transmettre**
- **Bloquer la réception**

RFC 1918

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

RFC 3927

- 169.254.0.0 /16

RAPPEL

Méthodes de filtrage

Prefix-list

- Ip prefix-list local seq 10 deny 10.0.0.0/8 le 32
- Ip prefix-list local seq 15 deny 192.168.0.0/12 le 32
- ……
- Ip prefix-list local seq n permit 0.0.0.0 le 32

routage vers null 0

- Ip route 10.0.0.0 255.0.0.0 null 0
- ……

David LOPOI

RAPPEL

Sécurisation de l'accès a vos router

- **Telnet**
- **Ssh**
- **Server radius**

David LOPOI

RAPPEL

Sécurisation de l'accès a vos router

Sécuriser l'accès Telnet

1. Créer une access-list pour autoriser des réseaux

Ex : access-list 101 permit ……

2. Applique aux accès line vty

```
Line vty 0 15
transport input telnet
```

David LOPOI

RAPPEL

Sécurisation de l'accès a vos router

utilisation de ssh

1. Créer un utilisater

```
Username toto password tata
```

2. Configurer le nom de domain

```
Ip domain-name lopoi.com
```

3. Activer la clé de cryptage

```
crypto key generate rsa
```

4. Configurer les accès line vty

```
Line vty 0 15
Transport input ssh
Login local
```

Nb: ssh –l « username » « cible » pour se connecter à partir d'un autre router

David LOPOI

RAPPEL

Sécurisation de l'accès a vos router

Utilisation d'un Server radius

1. Activer aaa authentication
   aaa new-model

2. Configurer la methode aaa d'authentification
aaa authentication login default none
aaa authentication login secure group radius
Radius-server host xxxx auth-port xx key xxx

3. Configurer les accès line vty
Line vty 0 15
Login authentication secure

David LOPOI

RAPPEL

Limitation de débit sur un lien

- **policy-map**
- **CAR**
- **Trafic shaping**

David LOPOI

RAPPEL

Limitation de débit sur un lien

policy-map

1. créer la policy-map
   policy-map client1
   class default-class
   police rate xxxx
   Conforme-action transmit
   Exced-action drop

2. Applique à l'interface
   service-policy input client

David LOPOI

RAPPEL

Sécurisation de l'accès a vos router

Utilisation d'un Server radius

1. Activer aaa authentication
   aaa new-model

2. Configurer la methode aaa d'authentification
   aaa authentication login default none
   aaa authentication login secure group radius
   Radius-server host xxxx auth-port xx key xxx

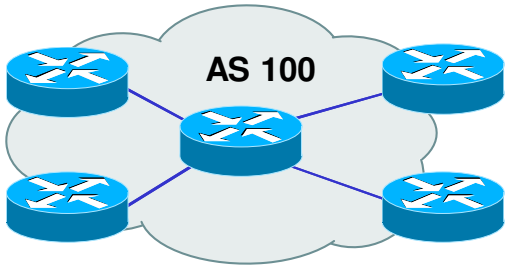
3. Configurer les accès line vty
   Line vty 0 15
   Login authentication secure

David LOPOI

BGP

Principes de base et vocabulaires

Système autonome (AS)

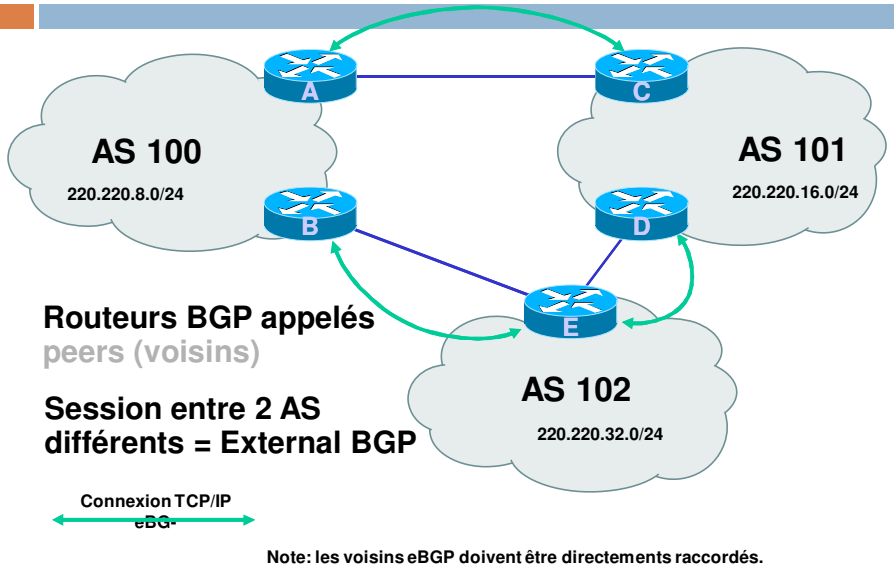


- Ensemble de réseaux partageant la même politique de routage
- Généralement sous une gestion administration unique
- Utilisation d'un IGP au sein d'un même AS

Système autonome (AS)...

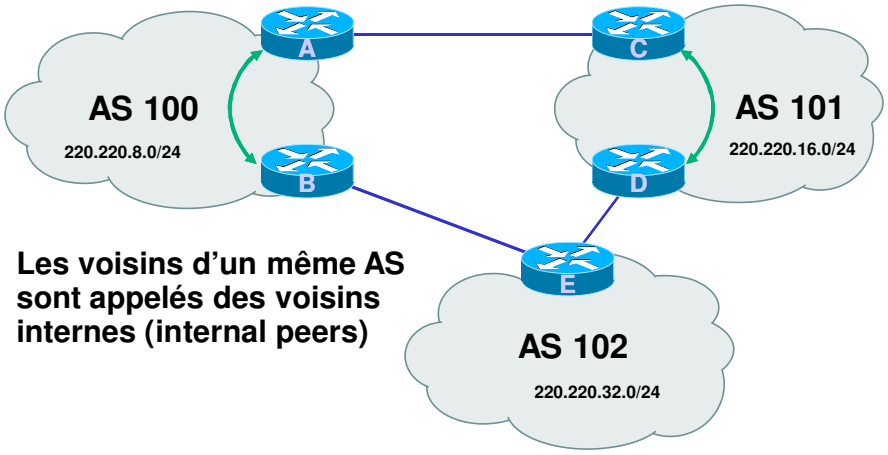
- Caractérisé par un numéro d'AS
- Il existe des numéros d'AS privés et publics
- 1-64511 & 64512-65535:
- **Utilisation**
  - Prestataire de services Internet
  - Clients raccordés à plusieurs prestataires
  - Quiconque souhaite établir une politique de routage spécifique

Sessions BGP - Externe



Note: les voisins eBGP doivent être directements raccordés.

Sessions BGP - Interne

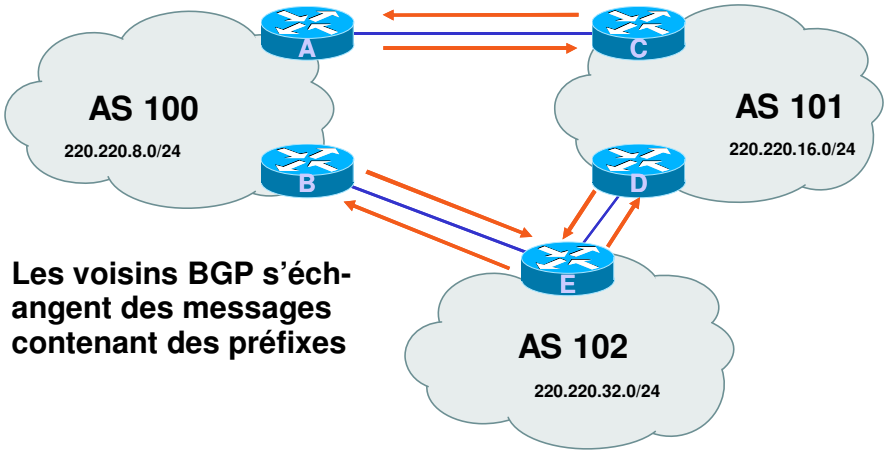


Les voisins d'un même AS sont appelés des voisins internes (internal peers)

Connexion TCP/IP iBGP

Note: les voisins iBGP peuvent ne pas être directement connectés.

Sessions BGP –Echange de routes



Les voisins BGP s'échangent des messages contenant des préfixes

Message de mise à jour BGP

BGP

Configurations de base

Commandes BGP de base(1)

Configuration

`router bgp` *<AS-number-local>*

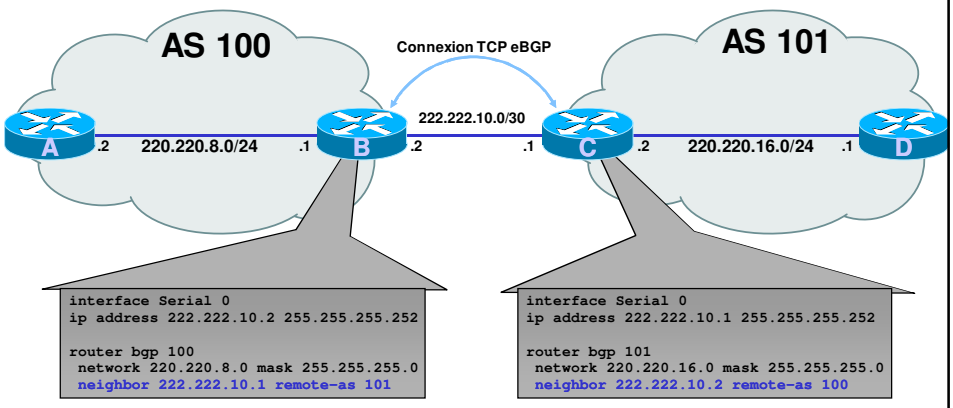
neighbor <ipv4 address> remote-as <as-number>

<as-number> = *<AS-number-local> pour les sessions IBGP*

<as-number> # *<AS-number-local> pour les sessions EBGP*

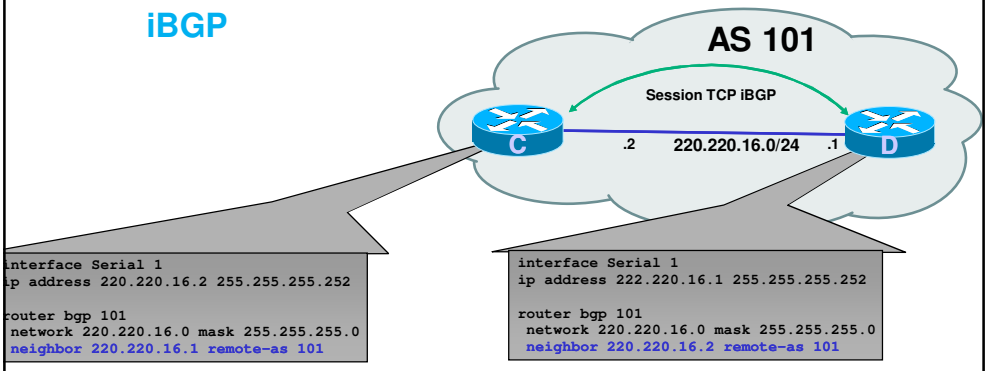
Configuration de sessions BGP

eBGP

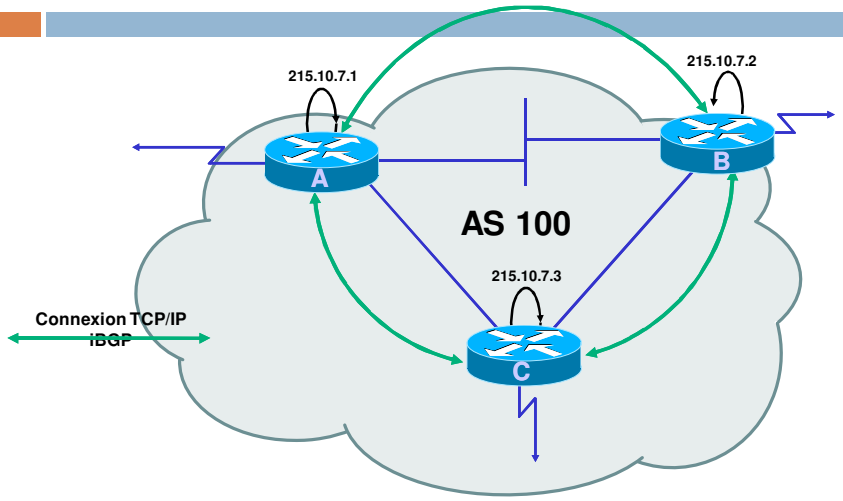


Configuration de sessions BGP

iBGP

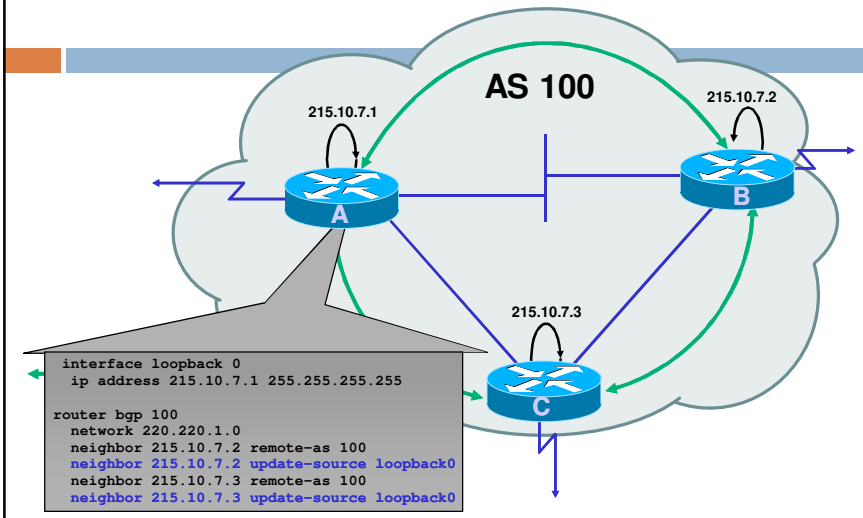


Configuration de sessions BGP

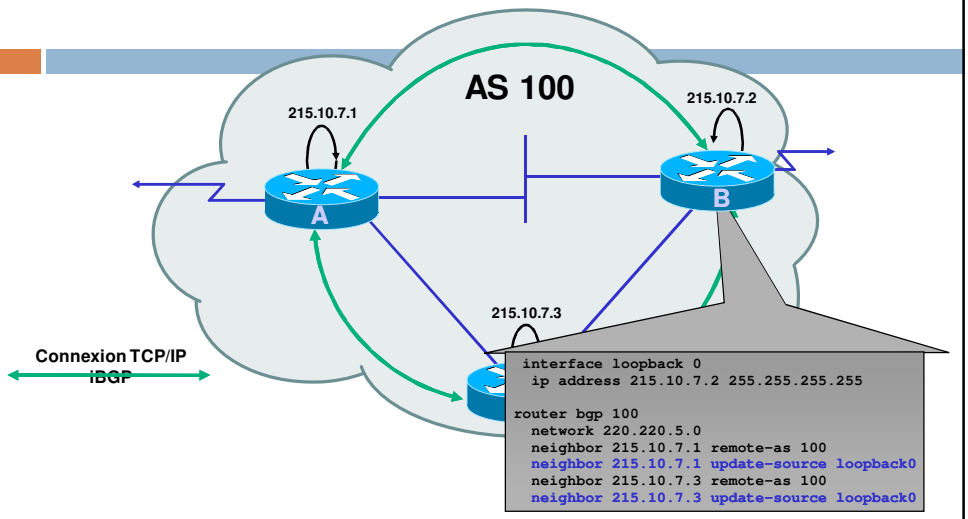


- *Il est recommandé d'utiliser des interfaces Loopback sur les routeurs comme extrêmités des sessions iBGP*

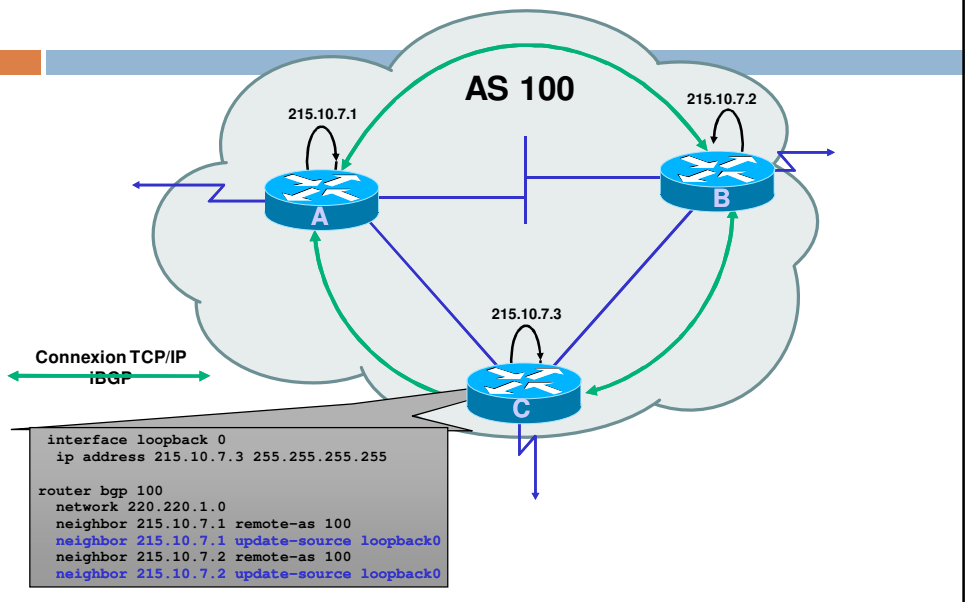
Configuration des sessions BGP



Configuration des sessions BGP



Configuration des sessions BGP



Commandes BGP de base(2)

Consultation d'information

```
show ip bgp  summary
show ip bgp neighbors
show  ip bgp
show ip bgp  neighbors xxxx advertise-routes
show ip bgp  neighbors xxxx routes
```

Liste des attributs de chemins BGP

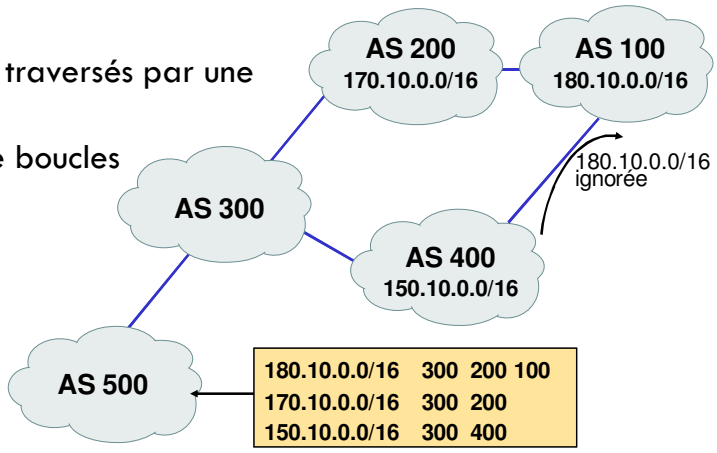
- Origine
- AS-path (chemin d'AS)
- Next-hop (prochain routeur)
- Multi-Exit Discriminator (MED)
- Local preference (préférence locale)
- BGP Community (communauté BGP)
- Autres...

AS-PATH (chemin d'AS)

- *Attribut mis à jour par le routeur envoyant un message BGP, en y ajoutant son propre numéro d'AS*
- Contient la liste des AS traversés par le message
- Permet de détecter des boucles de routage
  - Une mise à jour reçue est ignorée si elle contient son propre numéro d'AS

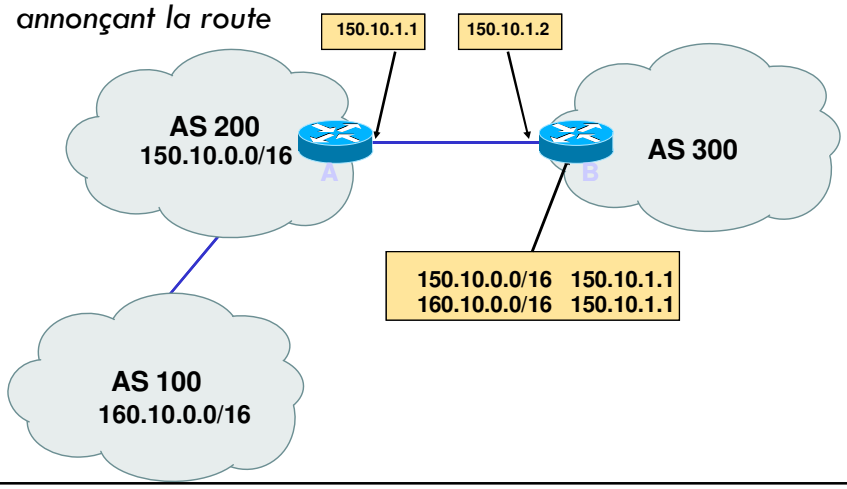
AS-Path (chemin d'AS)

- Liste des AS traversés par une route
- Détection de boucles



Next-Hop (prochain routeur)

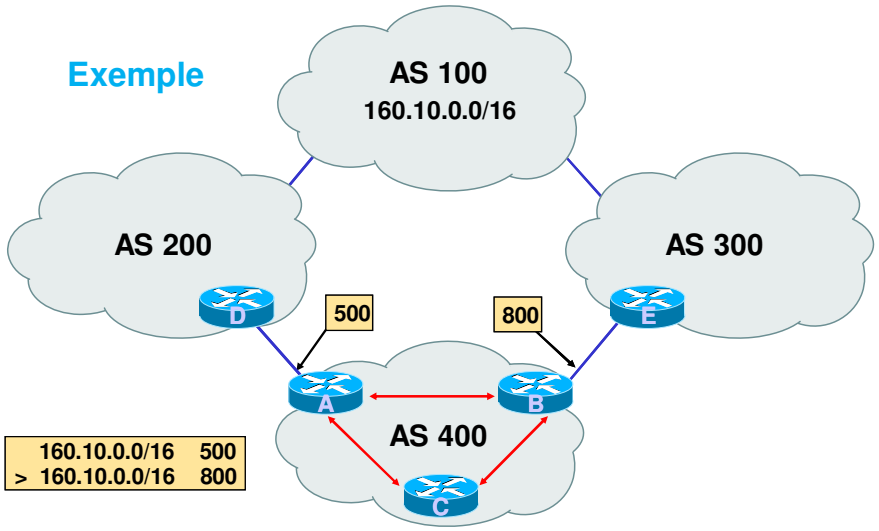
- *Adresse de l'interface annonçant la route*



Local Preference

- Paramètre local à un AS
- Permet de préférer une sortie à une autre
- Le chemin avec la préférence locale la plus élevée est sélectionné
- Obligatoire pour iBGP, non utilisé dans eBGP
- Valeur par défaut chez Cisco : 100

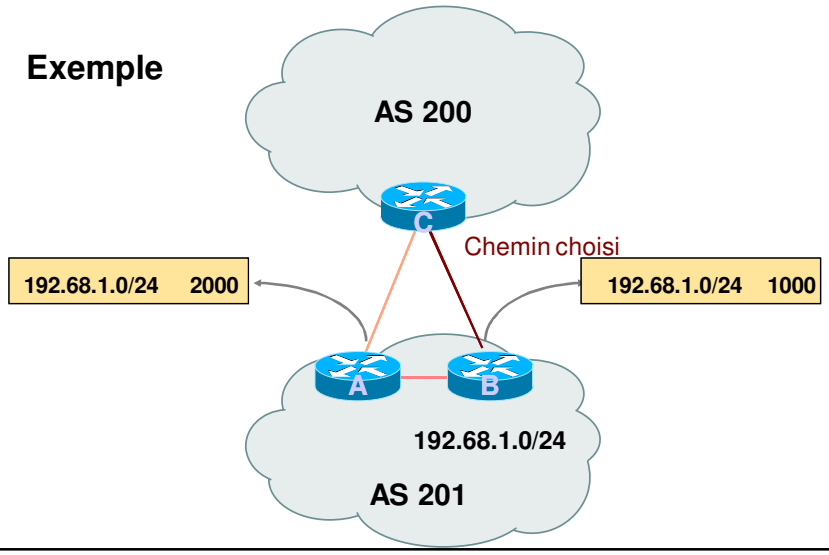
Local Preference



Multi-Exit Discriminator

- Attribut optionnel non transitif
- Permet de transporter des préférences relatives entre points de sortie
- Si les chemins viennent du même AS le MED peut être utilisé pour comparer les routes
- Le chemin avec le plus petit MED est sélectionné
- Le métrique IGP peut être choisi comme MED

Multi-Exit Discriminator (MED)



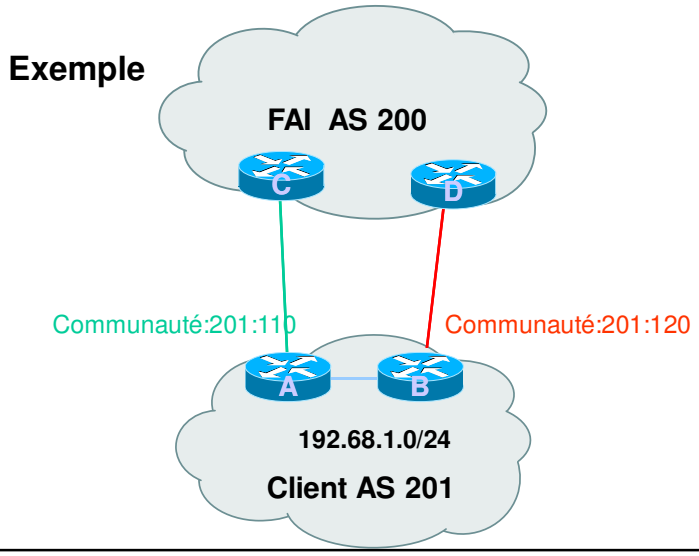
Origin (Origine de la route)

- Indique l'origine du préfixe
- Trois valeurs
  - IGP - préfixe obtenu avec une clause "network"
    - exemple : *network 35.0.0.0*
  - EGP - Redistribué par un EGP
  - Incomplete - Redistribué par un IGP
    - exemple : *redistribute ospf*
- IGP < EGP < INCOMPLETE

Communautés BGP

- Transitives, attribut facultatif
- Permettent de créer des groupes de destinations
- Chaque destination peut appartenir à plusieurs communautés
- Attribut très flexible, car il permet de faire des choix avec des critères inter ou intra-AS

Communautés BGP



Poids (Weight)

- Attribut spécifique Cisco utilisé lorsqu'il y a plus d'une route vers la même destination
- Attribut local à un routeur (non propagé ailleurs)
- Valeur par défaut 32768 pour les chemins dont l'origine est le routeur et 0 pour les autres
- Lorsqu'il y a plusieurs choix, on préferra la route dont le poids est le plus élevé.

Distance administrative

- NB: Les routes peuvent être apprises par plusieurs protocoles de routage
  - il faut les classifier pour faire un choix
- La route issue du protocole avec la plus faible distance est installée dans la table de routage
- Distances par défaut en BGP:
  - iBGP : 200
  - eBGP : 20
-

Configuration de base

Table de routage BGP

Ajout de préfixes dans la table BGP

Ajout de préfixes dans la table BGP

- **Deux grandes manière:**
  - - Utilisation de la commande "network"
- -Par redistribute (redistribuer les routes statiques ou Dynamique)

La command Network

- **`network`** <*ipaddress*> **`mask`** <*netmask*>
- *NB: Il faut que la route soit présente dans la table de routage du routeur pour qu'elle soit insérée dans la table* BGP

Redistribution

`Redistribute` *<protocol name>*

redistribute <protocole> signifie que toutes les routes du <protocole> seront transférés dans le protocole courant

- NB: L'origine de la route sera "*incomplete*", mais il est possible de le changer avec une "route-map"
- A utiliser avec prudence !

Utilisation de "redistribute"

- Attention avec les redistributions
  - redistribute <protocole> signifie que toutes les routes du <protocole> seront transférées dans le protocole courant
  - cette solution doit être contrôlée (volumétrie)
  - à éviter dans la mesure du possible
  - préférer l'utilisation de "route-maps" pour controler les routes redistribuée

Sélection de la meilleure route BGP (bestpath)

Critère de choix

- La route doit être synchronisée
  - C'est à dire être dans la table de routage
- Le "Next-hop" doit être joignable
  - Il se trouve dans la table de routage
- Prendre la valeur la plus élevée pour le poids (weight)
  - Critère spécifique Cisco et local au routeur
- Choisir la préférence locale la plus élevée
  - Appliqué pour l'ensemble des routeurs de l'AS
- La route est d'origine locale
  - Via une commande BGP "redistribute" ou "network"

Critère de choix

Choisir le plus court chemin d'AS
- en comptant le nombre d'AS dans l'attribut AS-Path

Prendre l'origine de valeur la plus faible
- IGP < EGP < INCOMPLETE

Choisir le plus petit MED
- pour des chemins en provenance d'un même AS

Préférer une route Externe sur une route Interne
- prendre la sortie la plus proche

Choisir le "next-hop" le plus proche
- Plus faible métrique IGP, donc plus proche de la sortie de l'AS

Plus petit "Router-ID"

Adresse IP du voisin la plus petite

Politique de routage - Liste de préfixes, Route Maps et Listes de distribution (distribute lists)

Politique de routage

- **Pourquoi ?**
  - Pour envoyer le trafic vers des routes choisies
  - Filtrage de préfixes en entrée et sortie
  - Pour forcer le respect des accords Client-ISP
- **Comment ?**
  - Filtrage basé sur les AS - filter list
  - Filtrage basé sur les préfixes - distribute list
  - Modification d'attributs BGP - route maps

Filtrage par - préfix-List

- **Router(config)# ip prefix-list list-name [seq**
- **seq-value] deny | permit network/len [*ge ge-value*] [le *le-value*]**

Filtrage par - préfix-List

- N'accepter la route par défaut
  - `ip prefix-list Exemple deny 0.0.0.0/0`
- Autoriser le préfixe 35.0.0.0/8
  - `ip prefix-list Exemple permit 35.0.0.0/8`
- Interdire le préfixe 172.16.0.0/12
  - `ip prefix-list Exemple deny 172.16.0.0/12`
- Dans 192/8 autoriser jusqu'au /24
  - `ip prefix-list Exemple permit 192.0.0.0/8 le 24`
    - Ceci autorisera toute route dans 192.0.0.0/8, sauf les /25, /26, /27, /28, /29, /30, /31 and /32

Filtrage par - préfix-List

- Dans 192/8 interdire /25 et au-delà
  - `ip prefix-list Exemple deny 192.0.0.0/8 ge 25`
    - Ceci interdit les préfixes de taille /25, /26, /27, /28, /29, /30, /31 and /32 dans le bloc 192.0.0.0/8
    - Très ressemblant au précédent exemple
- Dans 192/8 autoriser les préfixes entre /12 et /20
  - `ip prefix-list Exemple permit 192.0.0.0/8 ge 12 le 20`
    - Ceci interdit les préfixes de taille /8, /9, /10, /11, /21, /22 et au-delà dans le bloc 192.0.0.0/8
- Autoriser tous les préfixes
  - `ip prefix-list Exemple 0.0.0.0/0 le 32`

Filtrage par - préfix-List

- Exemple de configuration

```
router bgp 200
  network 215.7.0.0
  neighbor 220.200.1.1 remote-as 210
  neighbor 220.200.1.1 prefix-list PEER-IN in
  neighbor 220.200.1.1 prefix-list PEER-OUT out
!
ip prefix-list PEER-IN deny 218.10.0.0/16
ip prefix-list PEER-OUT permit 215.7.0.0/16
```

Tout accepter du voisin, sauf nos réseaux

Envoyer uniquement nos réseaux au voisin

Filtrage avec des expressions régulières

- L'expression régulière en BGP, est utilisé pour comparer l'attribut AS-Path
- Exemple : _3561$
- Grande fléxibilité qui permet de générer des expression complexes

Filtrage avec des expressions régulières

```
ip as-path access-list 1 permit 3561
ip as-path access-list 2 deny 35
ip as-path access-list 2 permit .*

router bgp 100
  neighbor 171.69.233.33 remote-as 33
  neighbor 171.69.233.33 filter-list 1 in
  neighbor 171.69.233.33 filter-list 2 out
```

Accepter les routes d'origine AS 3561. Tout le reste est rejeté en entrée ("deny" implicite).

Ne pas annoncer les routes de l'AS 35, mais tout le reste est envoyé (en sortie).

Route Maps

```
router bgp 300
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 route-map SETCOMMUNITY out
!
route-map SETCOMMUNITY permit 10
match ip address 1
match community 1
set community 300:100
!
access-list 1 permit 35.0.0.0
ip community-list 1 permit 100:200
```

Route-map : clauses match & set

Match Clauses

- AS-path
- Community
- IP address

Set Clauses

- AS-path prepend
- Community
- Local-Preference
- MED
- Origin
- Weight
- Autres...