Cours 3 : Border Gateway Protocol (BGP)

R302 : Réseaux opérateurs

IUT R&T 2e année

Fatma Essaghaier

Introduction

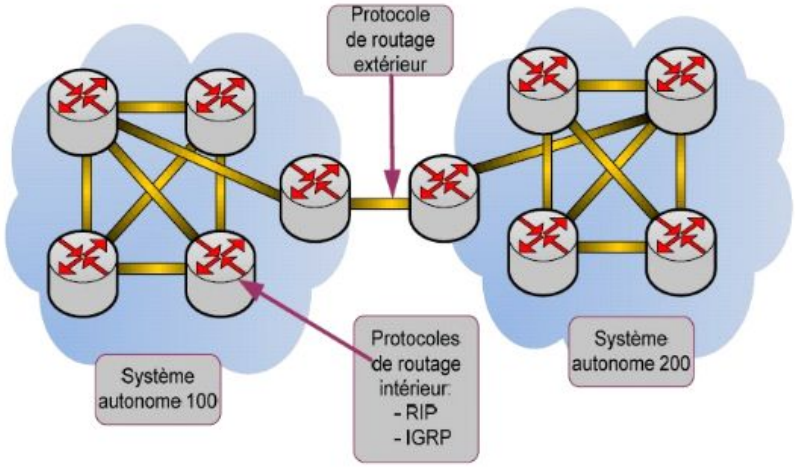
- Il existe 2 types de protocole de routage :
  - Les IGP (Interior Gateway Protocol) assurent le routage au sein des AS (Autonomous System). Par exemple : RIP, EIGRP, OSPF.
  - Les EGP (Exterior Gateway Protocol) assurent le routage entre les AS.

- BGP est un protocole de routage EGP, utilisé principalement sur Internet.

- Il permet d'établir des connexions entre les différents systèmes autonomes (AS) qui composent l'architecture du réseau.

Système autonome (AS / SA)

- Ensemble de réseaux partageant la même politique de routage (même IGP)
- Généralement sous une gestion administration unique.
-
- Chaque AS est identifié par un **numéro d'AS** unique, attribué par des organisations comme l'IANA (Internet Assigned Numbers Authority) ou les RIR (Regional Internet Registries).



- Pierre angulaire d'Internet, permet de structurer et de réguler le routage à grande échelle.

Définition BGP

- BGP est utilisé pour échanger des routes entre des routeurs de différents AS (eBGP) ou à l'intérieur d'un même AS (iBGP).
  - conçu pour fonctionner à l'échelle d'Internet (milliers de routes)
  - respecte les politiques de routage locales des AS.
- BGP est du type Path Vector. C'est un dérivé du type vecteur de distance.
  - Chaque routeur BGP stocke non seulement les routes mais aussi les chemins (liste des AS traversés) pour atteindre une destination.
  - La métrique utilisée est très complexe avec 'une liste d'attributs associés à la route.
- BGP est un protocole de couche application (pour remplir la table de routage).
- Repose sur des sessions TCP (utilise le port 179) pour garantir la fiabilité des échanges.
- Permet des politiques de routage flexibles et un contrôle total des décisions: l'admin peut choisir quelles routes accepter, annoncer ou prioriser.

fonctions de base BGP

- Authentification des routeurs et acceptation de communication
- Transmettre des message d'accessibilité positive ou négative
- Vérifier pour chaque routeur si son homologue, et la connexion réseau qui les réunit pour dialoguer, est fonctionnelle

iut Bethune réseaux & télécoms informatiques

MESSAGES BGP

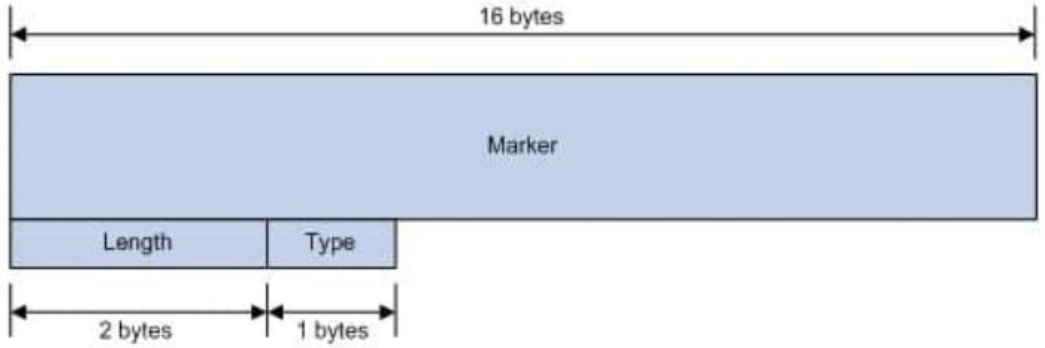
Les messages BGP

- Cinq types de messages principaux
- Chaque msg a une fonction spécifique et joue un rôle crucial dans la gestion des sessions et l'échange des informations de routage entre routeurs.
- Ces messages permettent de garantir la stabilité et l'efficacité des communications inter-systèmes autonomes (AS).

Type de message	Fonction	Rôle
OPEN	Établir une session BGP et négocier les paramètres	Permet l'identification des routeurs et la configuration des paramètres de session comme la version et le Hold Time.
UPDATE	Envoyer ou retirer des routes	Garantit que les informations de routage sont toujours à jour.
KEEPALIVE	Maintenir la session BGP active	Vérifie la validité continue de la session BGP.
NOTIFICATION	Signaler une erreur et fermer la session	Interrompt la session en cas de détection d'une erreur grave.
ROUTE-REFRESH	Demander l'actualisation des informations de routage	Permet de rafraîchir les routes sans redémarrer la session.

En tête des messages BGP

- Tous les msg BGP commencent par un en-tête de taille fixe.
- L'entête contient trois champs principaux : **Marqueur**, **Longueur**, et **Type**.



- Marqueur -16 octets: sert à l'authentification, délimitation et à la compatibilité avec les anciennes versions de BGP.
- Longueur - 2 octets : indique la longueur totale du msg (min 19 octets, max 4096 octets)
- Type -1 octet : identifie le type de message BGP (OPEN, UPDATE, etc.)

Message OPEN

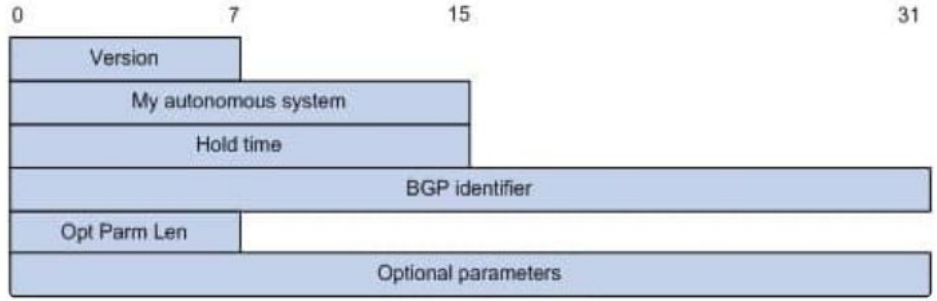
- **Établissement d'une session** : Dès qu'une connexion TCP est établie entre deux routeurs BGP, un message OPEN est envoyé par chaque routeur pour initier la session.

- **Vérification des paramètres** : Les routeurs échangent des informations importantes telles que le numéro d'AS et l'identifiant BGP pour s'assurer qu'ils sont compatibles.

- Une fois que le message OPEN a été échangé avec succès, la session BGP est considérée comme établie, et les messages KEEPALIVE et UPDATE peuvent être échangés pour maintenir la session et partager des routes.

Message OPEN

Le msg OPEN contient les champs suivants:



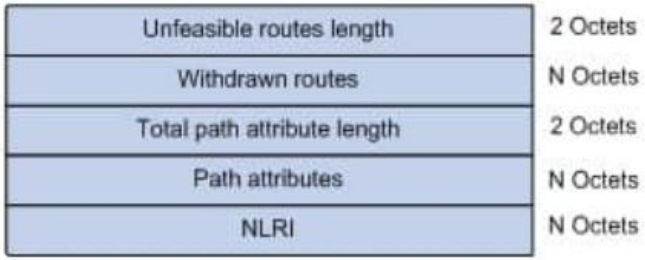
- Version -1 octet: la version du protocole utilisé par le routeur (actuellement BGP-4)
- My Autonomous System (AS) - 2 octets: le numéro de l'AS (système autonome) du routeur émetteur.
- Hold Time - 2 octets: la durée maximale (en sec) d'attente sans message KEEPALIVE ou UPDATE, sinon la session est considérée inactive. La valeur recommandée est de 180 secondes. (Si 0,pas de messages KEEPALIVE.)
- BGP Identifier - 4 octets: Adresse IP identifiant le routeur BGP. Généralement, c'est l'IP la plus élevée du routeur.
- Optional Parameters Length -1 octet : la longueur totale (en octets) des paramètres optionnels (0, si aucun).
- Optional Parameters - n octets: Paramètres optionnels, tels que le support de IPv6.

Message UPDATE

- Le message **UPDATE** est l'un des messages les plus importants du protocole BGP.
- Utilisé pour transmettre les informations de routage entre les routeurs BGP.
- Il permet à un routeur d'annoncer des routes nouvellement disponibles ou de retirer des routes qui ne sont plus accessibles.
- Ce message est crucial pour assurer que les tables de routage restent à jour dans les systèmes autonomes (AS).

Message UPDATE

Le message **UPDATE** est structuré en plusieurs champs, chacun jouant un rôle spécifique dans la MAJ des routes :



1. **Unfeasible Routes Length** – 2 octet : longueur totale des routes retirées en octets (0,si aucun)

2. **Withdrawn Routes** – n octets: la liste des préfixes IP des routes retirées. Chaque route retirée est représentée sous la forme d'un préfixe IP et d'une longueur de préfixe.
   Il est utilisé lorsque des routes ne sont plus accessibles et doivent être retirées des tables de routage.

3. **Total Path Attribute Length** – 2 octets : la longueur totale des attributs de chemin en octets (0,si aucun)

4. **Path Attributes** – n octets: liste des attributs associés aux routes annoncées. Les attributs de chemin sont des informations supplémentaires qui décrivent les routes et permettent de gérer le routage de manière efficace.
   Quelques attributs clés sont :
   - **AS_PATH** : Liste des systèmes autonomes traversés par la route.
   - **NEXT_HOP** : Adresse IP du prochain saut pour atteindre la destination.
   - **LOCAL_PREF** : Préférence locale indiquant la priorité des routes à l'intérieur d'un AS.

5. **Network Layer Reachability Information (NLRI)** – variable : la liste des préfixes IP des routes annoncées. Chaque route annoncée est représentée sous la forme d'un préfixe IP et d'une longueur de préfixe.

Message UPDATE

- **Annonce de nouvelles routes** : Lorsqu'un routeur apprend de nouvelles routes ou que des routes changent, il envoie un message UPDATE pour informer les autres routeurs de ces changements. Les informations de routage sont décrites par des attributs de chemin, tels que l'AS_PATH, qui identifient les routes empruntées.

- **Retrait de routes** : Si des routes ne sont plus accessibles, le routeur envoie un message UPDATE avec la liste des routes retirées dans le champ **Withdrawn Routes**. Cela permet de garantir que les autres routeurs mettent à jour leurs tables de routage en supprimant les routes obsolètes.

- **Gestion des attributs de chemin** : Les attributs de chemin (comme AS_PATH et NEXT_HOP) sont essentiels pour éviter les boucles de routage et pour déterminer le meilleur chemin à emprunter. Ces informations permettent de s'assurer que le routage reste stable et efficace.

Message KEEPALIVE

- Le message **KEEPALIVE** est utilisé pour maintenir la session BGP active entre deux routeurs.
- Vérifier que la connexion BGP reste active et en bon état.
- Envoyé périodiquement à intervalles réguliers, toutes les 30 sec par défaut.
- Contrairement à d'autres messages BGP comme **OPEN** ou **UPDATE**, le message KEEPALIVE ne transporte aucune information de routage.
- Le message **KEEPALIVE** ne contient que l'en-tête BGP standard, sans aucun champ supplémentaire. Sa longueur totale est donc de 19 octets.

Champ	Taille	Description
Marqueur	16 octets	Champ rempli de bits "1" (0xFFFF), utilisé à des fins d'authentification et de compatibilité.
Longueur	2 octets	Indique la taille totale du message (toujours 19 octets pour KEEPALIVE).
Type	1 octet	Le type de message est 4, correspondant au message KEEPALIVE.

Message KEEPALIVE

Fonctionnement du message KEEPALIVE :

1. **Maintien de la session BGP** : Le message **KEEPALIVE** est envoyé régulièrement par chaque routeur BGP pour s'assurer que la session reste active. Si l'un des routeurs ne reçoit pas de message **KEEPALIVE** dans un délai défini (généralement le temps de maintien "Hold Time" négocié lors du message OPEN), la session BGP est considérée comme expirée et est fermée.
2. **Périodicité des messages** : Par défaut, un message **KEEPALIVE** est envoyé toutes les 30 secondes. Cependant, cette valeur peut varier en fonction de la configuration des routeurs et du Hold Time négocié dans le message OPEN. Si le Hold Time est configuré à 0, cela signifie que les messages **KEEPALIVE** ne seront pas utilisés, et seules les mises à jour de routage permettront de maintenir la session.
3. **Absence de données de routage** : Le message **KEEPALIVE** ne transporte aucune information concernant les routes ou les mises à jour de routage. Il se limite à l'en-tête BGP de 19 octets.

Rôle du message KEEPALIVE :

- **Vérification de la session** : Il permet de garantir que la session BGP est toujours en cours entre deux routeurs. Si un routeur cesse d'envoyer des messages **KEEPALIVE**, cela indique une défaillance de la session.
- **Surveillance de l'activité** : En absence de messages **KEEPALIVE** ou **UPDATE**, la session est automatiquement fermée une fois que le Hold Time est expiré.

Message NOTIFICATION

- Le message **NOTIFICATION** est utilisé pour signaler une erreur critique ou une anomalie détectée au sein d'une session BGP. Il est essentiel pour assurer l'intégrité et la stabilité des sessions BGP, en permettant :

  - **Signalisation d'erreur** : Dès qu'un routeur détecte une anomalie dans la session BGP (comme une incompatibilité de version ou un attribut de routage incorrect), il envoie un message NOTIFICATION à son pair BGP. Ce message signale le problème rencontré afin que l'autre routeur en soit informé.

  - **Fermeture immédiate de la session** : Une fois le message NOTIFICATION envoyé, la session BGP entre les deux routeurs est immédiatement fermée. Cela permet d'éviter que des informations de routage incorrectes soient échangées ou propagées sur le réseau.

  - **Aide au diagnostic** : Le champ Data peut contenir des informations supplémentaires pour aider à diagnostiquer l'erreur. Par exemple, il peut inclure une copie des données erronées reçues, facilitant ainsi le dépannage.

Message NOTIFICATION

Le message **NOTIFICATION** est structuré avec les champs suivants :

- Error Code – 1 octet : Type d'erreur détectée. Chaque type d'erreur correspond à un numéro spécifique.

  Exemples d'erreur :

  1 : Erreur de synchronisation
  2 : Erreur de version de BGP
  3 : Erreur de configuration ou d'attributs

- Error Subcode – 1 octet: Détail supplémentaire sur la nature exacte de l'erreur.

  Exemples de sous-codes d'erreur :

  - Error Code 1 (Erreur de synchronisation) : 1 : Message BGP non synchronisé.
  - Error Code 2 (Erreur de version BGP) : 2 : Version BGP incompatible.

- Data – (n octets) : Informations additionnelles pour diagnostiquer l'erreur.

Message REFRESH

- Le message **ROUTE-REFRESH** permet à un routeur BGP de demander à un pair de renvoyer les informations de routage pour une famille d'adresses spécifique, sans avoir à redémarrer la session BGP.

- Ce message est utilisé dans des environnements où le routage est basé sur plusieurs familles d'adresses, telles que **IPv4** et **IPv6**, et permet d'actualiser les informations de routage de manière ciblée.

- Le message **ROUTE-REFRESH** contient des champs spécifiques permettant de définir la famille d'adresses pour laquelle le rafraîchissement des informations de routage est demandé :

    1. **AFI (Address Family Identifier)** – 2 octets : identifie la famille d'adresses concernée par la demande de rafraîchissement. Par exemple : (**1** pour IPv4 ou **2** pour IPv6)

    2. **Reserved** – 1 octet, champs réservé toujours égal à 0.

    3. **SAFI (Subsequent Address Family Identifier)** – 1 octet Précise la sous-famille d'adresses concernée. Par exemple: **1** : Unicast, **2** : Multicast)

Message REFRESH

Fonctionnement du message ROUTE-REFRESH

1. **Rafraîchissement des routes** : Lorsqu'un routeur BGP souhaite obtenir les informations de routage actualisées pour une famille d'adresses spécifique (par exemple, pour IPv4 unicast), il envoie un message **ROUTE-REFRESH** à son pair BGP. Ce dernier répond en envoyant à nouveau toutes les routes pertinentes pour cette famille d'adresses.

2. **Éviter la réinitialisation de la session** : Le message **ROUTE-REFRESH** est utile car il permet de demander un rafraîchissement des routes sans avoir besoin de redémarrer la session BGP. Cela améliore la flexibilité et la continuité des opérations de routage.

3. **Rafraîchissement ciblé** : Le message permet de rafraîchir les routes pour une **famille d'adresses** spécifique. Par exemple, si un routeur gère à la fois des adresses **IPv4** et **IPv6**, il peut choisir de rafraîchir les routes uniquement pour **IPv6** sans affecter celles d'**IPv4**.

iut Bethune réseaux & télécoms informatiques

TABLES DE ROUTAGES BGP

Tables de routage BGP

- Les **tables de routage BGP** sont des éléments essentiels dans le fonctionnement du protocole BGP (Border Gateway Protocol).

- Le rôle des tables de routage BGP est d'optimiser le chemin des paquets en fonction des informations de routage reçues et des politiques de routage configurées.

- Elles stockent et gèrent les informations de routage échangées entre routeurs BGP au sein de systèmes autonomes (AS).
  En entrée : table Adj-RIB-in En sortie : table Adj-RIB-out En interne : table Loc-RIB

- Principales tables associées à BGP :

Table	Rôle principal
Adj-RIB-In	Stocke toutes les routes reçues des pairs BGP avant filtrage.
Loc-RIB	Contient les routes optimales sélectionnées après application des politiques de routage.
Adj-RIB-Out	Contient les routes prêtes à être annoncées aux autres pairs BGP.
RIB (Table IP)	Stocke les routes finales utilisées pour le routage des paquets.

Table Adj-RIB-In

- La table BGP de session **Adj-RIB-In** (Adjacency Routing Information Base - In) stocke les informations de routage reçues d'autres routeurs BGP (peers).

- Elle contient toutes les routes annoncées par les pairs BGP, externes (eBGP) ou internes (iBGP).

- **Filtrage initial** : Avant d'ajouter une route dans cette table, des vérifications de base sont effectuées (telles que la validation de l'AS_PATH et du NEXT_HOP).

- Les politiques de filtrage ou d'acceptation sont appliquées ici pour déterminer si les routes seront conservées ou non.

Table Loc-RIB

- La table de sélection de route **Loc-RIB** (Local Routing Information Base) est la table principale utilisée par BGP pour stocker les routes sélectionnées.

- Elle contient les routes optimales choisies après application des politiques de routage et de sélection de chemins.

- Stocke les meilleures routes pour chaque destination après avoir comparé les routes dans la table Adj-RIB-In. Le routage réel est effectué à partir de cette table.

- **Sélection des routes** : BGP applique ses critères de sélection (comme AS_PATH, LOCAL_PREF, et MED) pour déterminer la meilleure route vers chaque destination.

- **Mise à jour continue** : Cette table est mise à jour en fonction des changements dans le réseau (par exemple, lorsque de nouvelles routes sont annoncées ou que des routes sont retirées).

Table Adj-RIB-Out

- La table d'exportation **Adj-RIB-Out** stocke les routes sélectionnées par le routeur BGP qui seront envoyées à ses pairs.
- Cette table ne contient que les routes que le routeur a décidé d'annoncer.
- Stocke les routes que le routeur BGP va annoncer à ses pairs BGP (soit iBGP, soit eBGP).
- **Application des politiques d'exportation** : Avant d'ajouter une route dans cette table, les politiques d'exportation (comme les filtres de routes) sont appliquées pour décider si une route doit être annoncée à un pair.
- **Annonce des routes** : Les routes dans cette table sont envoyées aux voisins BGP via des messages **UPDATE**.

Table RIB

- La table de routage IP **RIB** (Routing Information Base) n'est pas exclusive à BGP, mais elle contient les routes finales utilisées par le routeur pour le transfert des paquets.

- Les routes de la **Loc-RIB** qui sont sélectionnées comme les meilleures routes sont installées dans la table de routage IP du routeur (RIB).

- Stocke les routes optimales de plusieurs protocoles de routage (BGP, OSPF, RIP, etc.).

- **Routes finales** : Les routes de la table **Loc-RIB** qui sont jugées les meilleures sont transférées ici et utilisées pour router les paquets sur le réseau.

- **Priorisation** : Si plusieurs protocoles de routage (comme BGP et OSPF) fournissent des routes vers la même destination, des critères de priorisation sont appliqués pour déterminer quelle route utiliser.

iut Bethune réseaux & télécoms informatiques

ATTRIBUTS DE CHEMIN BGP

Critères de sélection des routes BGP

- Les **attributs de chemin BGP** jouent un rôle crucial dans la sélection des routes et le contrôle du routage dans BGP.

- Ils permettent à un routeur de choisir le meilleur chemin vers une destination en fonction de plusieurs critères, tout en évitant les boucles et en appliquant des politiques de routage.

- BGP applique plusieurs critères pour sélectionner la meilleure route à installer dans la table **Loc-RIB** et la table de routage IP (RIB).

Critères de sélection des routes BGP

1. **LOCAL_PREF (Préférence locale)** : est un attribut utilisé à l'intérieur d'un même AS pour indiquer la priorité d'une route. Plus la valeur de **LOCAL_PREF** est élevée, plus la route est préférée.

    a. Il est utilisé pour **préférer certaines routes** dans un AS par rapport à d'autres.
    b. Contrairement à **AS_PATH**, cet attribut n'est pas propagé en dehors de l'AS. Il est principalement utilisé pour définir des **politiques de routage internes**.

2. **AS_PATH (Chemin d'AS)** : contient la liste des systèmes autonomes (AS) que le paquet doit traverser pour atteindre une destination donnée. À chaque fois qu'une route est propagée à un nouveau système autonome, son numéro d'AS est ajouté à l'AS_PATH.

    a. Permet de tracer le chemin parcouru par une route à travers plusieurs AS.
    b. Utilisé pour éviter les **boucles de routage** : un AS ne peut pas réannoncer une route où il est déjà présent dans l'AS_PATH.
    c. **Sélection du meilleur chemin** : BGP préfère les chemins avec un **AS_PATH** plus court (moins d'AS traversés).

Critères de sélection des routes BGP

3. **MED** (Multi-Exit Discriminator) est utilisé pour influencer le choix du point d'entrée lorsqu'un AS est accessible via plusieurs points d'entrée (multiple links). Une valeur plus faible de **MED** est préférée.

    a. Permet à un AS de spécifier à un autre AS quel point d'entrée utiliser de préférence pour atteindre certaines destinations.
    b. Utilisé pour ajuster les préférences sur les points d'interconnexion entre deux AS.
    c. Contrairement à **LOCAL_PREF**, il est utilisé pour influencer le routage **inter-AS**.

4. NEXT_HOP : L'attribut **NEXT_HOP** indique l'adresse IP du prochain routeur (ou prochain saut) à travers lequel les paquets doivent passer pour atteindre la destination. C'est l'adresse du routeur de bord (border router) du système autonome voisin.

    a. Spécifie le routeur vers lequel les paquets doivent être envoyés pour atteindre la destination.
    b. Lors de la sélection de routes, si le NEXT_HOP n'est pas accessible, la route est ignorée.

Critères de sélection des routes BGP

5. WEIGHT (Poids): L'attribut **WEIGHT** est un attribut propriétaire de Cisco, utilisé uniquement au sein d'un routeur. Il détermine la préférence d'une route par rapport à une autre, et plus la valeur de **WEIGHT** est élevée, plus la route est prioritaire.

a. Utilisé pour la **sélection locale** des routes au sein d'un routeur BGP.
b. Cet attribut n'est pas propagé aux autres routeurs et n'a pas d'impact sur les décisions de routage d'autres routeurs.

6. ORIGIN: L'attribut **ORIGIN** spécifie l'origine de la route, c'est-à-dire la manière dont la route a été introduite dans BGP. Cet attribut aide BGP à **déterminer la confiance** que le protocole doit accorder à une route en fonction de son origine. Il peut avoir trois valeurs :

a. **IGP** (Interior Gateway Protocol) : La route a été apprise via un IGP comme OSPF ou RIP.
b. **EGP** (Exterior Gateway Protocol) : La route a été apprise via un ancien protocole comme EGP.
c. **INCOMPLETE** : La route a été apprise par d'autres moyens (comme la redistribution d'une route statique dans BGP).

Critères de sélection des routes BGP

7. COMMUNITY: est un attribut utilisé pour regrouper des routes et appliquer des politiques de routage communes à un ensemble de routes. Il s'agit d'un identifiant qui peut être partagé entre plusieurs routes afin de simplifier la gestion des politiques.

a. Il permet de **classer les routes** selon des groupes pour appliquer des règles uniformes sur ces routes.
b. Les administrateurs réseau peuvent utiliser les **COMMUNITY** pour faciliter l'application de filtres ou de règles de routage spécifiques à un groupe de routes.

Politique de routage

BGP n'a pas de métrique unique (pour déterminer le meilleur chemin d'AS vers un réseau), mais un ensemble d'attributs de chemin PA hiérarchisés

BGP applique les critères suivants, dans cet ordre, pour choisir la meilleure route :

1. **Weight** : La route avec le **Weight** le plus élevé est préférée (Cisco uniquement, local au routeur).
2. **LOCAL_PREF** : La route avec la valeur de **LOCAL_PREF** la plus élevée est préférée (utilisée au sein d'un AS).
3. **AS_PATH** : La route avec le **chemin AS_PATH** le plus court (moins d'AS traversés) est préférée.
4. **Origin** : La route avec l'origine la plus fiable (IGP > EGP > INCOMPLETE) est préférée.
5. **MED (Multi Exit Discriminator)** : Si plusieurs routes mènent au même AS, la route avec le **MED** le plus bas est préférée.
6. **eBGP sur iBGP** : Si deux routes sont équivalentes, BGP préfère une route apprise via eBGP plutôt que via iBGP.
7. **Router ID** : Si toutes les autres valeurs sont identiques, BGP préfère la route avec le **Router ID** le plus bas.

PROCESSUS DE FONCTIONNEMENT BGP

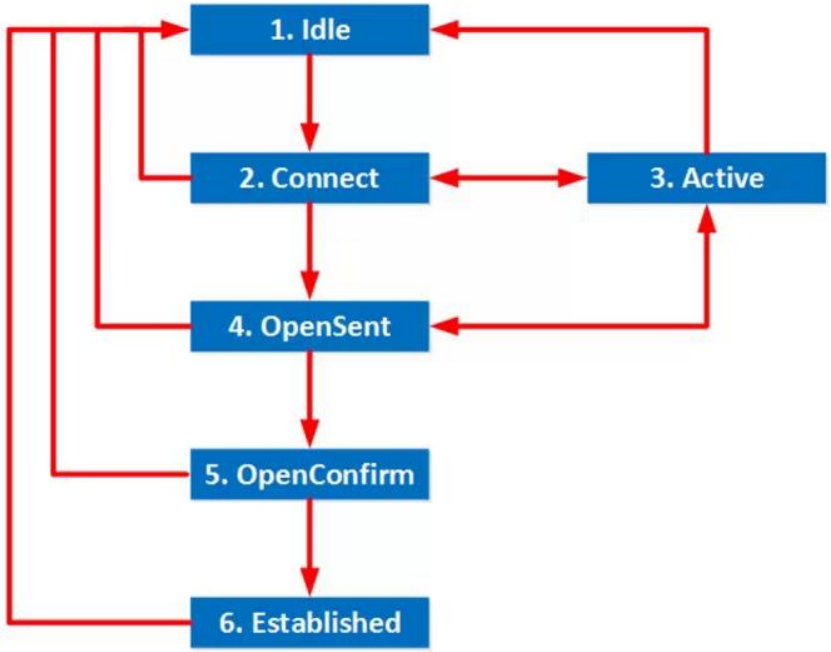
Processus BGP

- Lorsqu'une session BGP est établie entre deux routeurs BGP (appelés **voisins** ou **pairs**), ils passent par plusieurs **états** avant de pouvoir échanger des informations de routage.

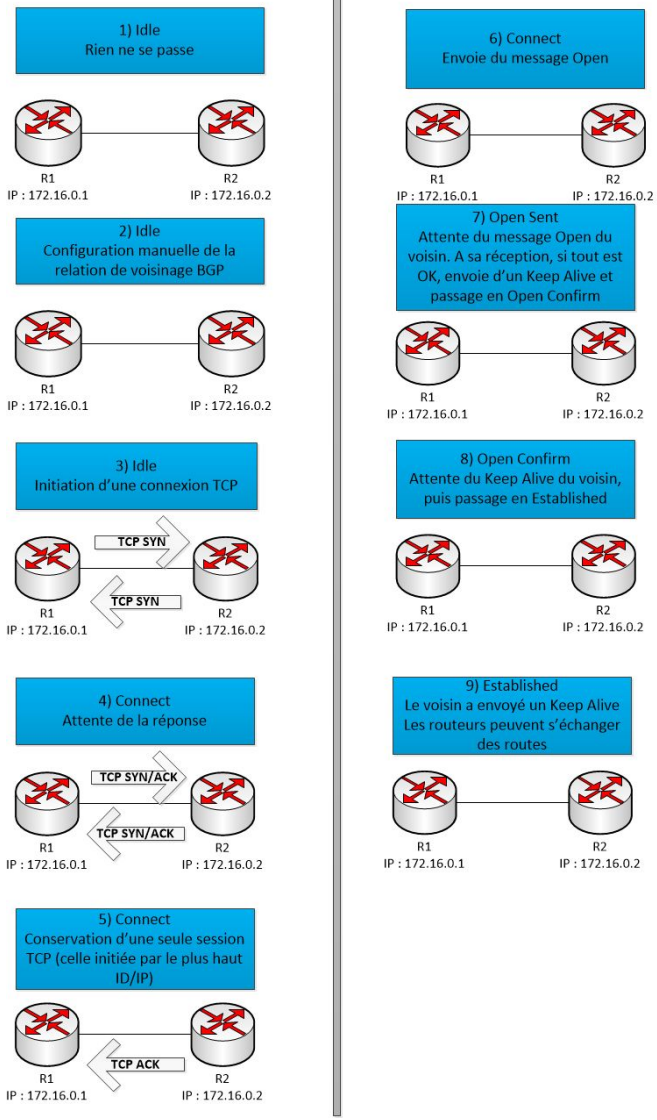
- Le protocole BGP est basé sur des sessions TCP, et ces états reflètent les différentes étapes d'établissement et de maintien de la connexion entre les routeurs voisins.

État	Description	Actions	Transition
Idle	Attente pour initier une connexion TCP.	Le routeur initialise les ressources.	Passe à **Connect** après une tentative de connexion TCP réussie.
Connect	Tentative d'établissement de connexion TCP avec le pair BGP.	Envoie un message **OPEN** si la connexion est établie.	Passe à **OpenSent** si la connexion TCP est réussie.
Active	Tentative active de rétablir la connexion TCP.	Nouvelle tentative d'initiation d'une connexion TCP avec le pair.	Passe à **OpenSent** si la connexion TCP est établie, ou retourne à **Idle**.
OpenSent	Envoi du message **OPEN** au pair BGP.	Attente de la réponse **OPEN** du pair BGP.	Passe à **OpenConfirm** si la réponse **OPEN** est reçue.
OpenConfirm	Attente de la réception d'un message **KEEPALIVE** pour confirmer l'établissement de la session.	Vérifie la réception du message **KEEPALIVE**.	Passe à **Established** si le message **KEEPALIVE** est reçu correctement.
Established	Session BGP active, échange de messages de routage via **UPDATE**.	Envoi et réception de messages **UPDATE** et **KEEPALIVE** pour maintenir la session active.	Reste dans cet état jusqu'à la détection d'une erreur ou la fermeture.

Processus BGP



Différents états du processus BGP



iut Bethune réseaux & télécoms informatiques

FILTRAGE DES ROUTES BGP

Politiques de filtrage des routes

- Les politiques de filtrage permettent de **limiter les routes acceptées** ou **annoncées** par un routeur BGP à un autre.

- Cela peut être fait pour des raisons de sécurité, pour éviter l'annonce de routes indésirables ou pour appliquer des politiques d'entreprise spécifiques.

- Une politique de filtrage peut influencer:
  - Le traitement des routes reçues
  - Le traitement des routes annoncées
  - L’interaction avec les IGP de l’AS

Type de filtrage:

1. **Filtrage à l'importation** (Ingress Filtering)
    - **Description** : Les routes **importées** par un routeur depuis ses voisins (routes reçues) peuvent être filtrées avant d'être installées dans la table de routage.
    - **Rôle** : Permet de décider quelles routes BGP sont acceptées pour entrer dans le réseau, en fonction de critères tels que les préfixes IP ou les attributs BGP (comme AS_PATH).
    - **Exemple d'utilisation** : Ne pas accepter de routes provenant d'un certain AS.
2. **Filtrage à l'exportation** (Egress Filtering)
    - **Description** : Les routes **exportées** par un routeur à ses voisins peuvent également être filtrées. Cela empêche l'annonce de certaines routes à des pairs BGP.
    - **Rôle** : Contrôle quelles routes BGP seront propagées à d'autres réseaux.
    - **Exemple d'utilisation** : Ne pas annoncer les routes internes d'une organisation à un fournisseur d'accès internet (FAI).

Méthodes de filtrage :

- **Access-lists** : Utilisées pour filtrer les routes BGP en fonction de leur préfixe IP.
- **Prefix-lists** : Plus efficaces qu'Access-lists, elles permettent de filtrer les routes en fonction des plages de préfixes IP.
- **Route-maps** : Méthode avancée permettant de filtrer des routes selon plusieurs critères, comme les attributs BGP (AS_PATH, NEXT_HOP, etc.) et de modifier les attributs des routes.

Politiques de filtrage des routes

Exemples pratiques de politiques de filtrage et de contrôle de routage :

1. **Restreindre les routes internes** : Un administrateur peut créer une règle dans une **route-map** pour que certaines routes internes ne soient pas annoncées à un pair eBGP externe. Cela permet de protéger le réseau interne.

2. **Influencer le chemin des paquets** : En manipulant les valeurs de **LOCAL_PREF**, un administrateur peut forcer tout le trafic sortant à emprunter un lien spécifique dans un réseau multi-lien.

3. **Éviter les boucles de routage** : En utilisant **AS_PATH Prepending**, un AS peut rendre certaines routes moins attrayantes pour les voisins, évitant ainsi que ces routes ne soient choisies par inadvertance.

iut Bethune réseaux informatiques & télécoms

RÈGLES BGP

Règles BGP

1. Synchronisation BGP

La règle de **synchronisation** stipule que BGP ne doit annoncer une route à ses pairs eBGP (externes) que si cette route est connue et présente dans la table de routage interne (via un IGP tel qu'OSPF ou RIP). Autrement dit, la route doit être synchrone avec l'IGP avant d'être propagée à l'extérieur.

Objectif :

- Cette règle a été conçue pour éviter les **boucles de routage** et garantir que les routes annoncées par BGP sont réellement utilisables à l'intérieur de l'AS.

Fonctionnement :

- Si un routeur BGP apprend une route via un autre AS, il attend que cette route soit propagée à travers son propre AS (via un protocole IGP) avant de la réannoncer à d'autres systèmes autonomes. Cela garantit que la route est accessible par l'ensemble du réseau interne avant qu'elle ne soit annoncée à l'extérieur.

Limites et solutions :

- Dans les réseaux modernes, cette règle n'est souvent **pas appliquée** car elle ralentit la convergence du réseau BGP. La plupart des administrateurs réseau désactivent la synchronisation lorsque tout le réseau interne repose sur BGP et que la redondance est assurée par des mécanismes de BGP.
- La synchronisation est généralement désactivée avec la commande suivante sur les routeurs Cisco : `no synchronization`.

2. Split Horizon BGP

La règle de **Split Horizon** vise à prévenir les **boucles de routage**. Elle stipule que BGP ne doit pas réannoncer une route reçue via un peer iBGP (membre du même AS) à un autre peer iBGP.

Objectif :

- Empêcher la réannonce des routes iBGP pour éviter les boucles de routage internes.

Fonctionnement :

- Lorsqu'un routeur iBGP apprend une route d'un autre routeur iBGP, il ne la propage pas aux autres routeurs iBGP au sein du même AS. Cela signifie que tous les routeurs BGP internes doivent être connectés en **full mesh** (chaque routeur iBGP doit être connecté à tous les autres routeurs iBGP).

Limites et solutions :

- La règle de Split Horizon peut poser des problèmes de scalabilité dans de grands réseaux, où il devient difficile d'établir un maillage complet entre tous les routeurs iBGP.
- Pour contourner cette règle et améliorer la scalabilité, on peut utiliser des solutions comme :
  - **Route Reflectors (RR)** : Un Route Reflector peut réannoncer des routes iBGP à d'autres routeurs iBGP.
  - **Confédérations BGP** : Permettent de diviser un grand AS en plusieurs petits sous-AS tout en appliquant des règles de routage internes comme si chaque sous-AS faisait partie d'un seul AS.

3. Règle de Next-Hop BGP

La règle du **Next-Hop** en BGP concerne la manière dont l'adresse **NEXT_HOP** est mise à jour lors de la propagation des routes à travers plusieurs routeurs.

Fonctionnement :

- Lorsque BGP annonce une route à un pair eBGP (externe), il met à jour l'adresse **NEXT_HOP** pour que celle-ci pointe vers le routeur qui effectue l'annonce.
- Cependant, lorsqu'un routeur iBGP annonce une route à un autre routeur iBGP, il **ne modifie pas** l'adresse **NEXT_HOP**. Ainsi, les routeurs iBGP doivent connaître l'accessibilité du **NEXT_HOP** pour valider la route.

Limites et solutions :

- Si le routeur iBGP ne peut pas accéder à l'adresse NEXT_HOP, la route sera considérée comme inaccessible. Pour résoudre ce problème, des mécanismes comme **IGP** sont utilisés pour propager les informations de **NEXT_HOP** à travers le réseau.

4. Règle de Full Mesh iBGP

La règle de **Full Mesh** stipule que tous les routeurs iBGP d'un AS doivent être connectés les uns aux autres pour qu'ils puissent échanger des informations de routage sans rencontrer de problèmes.

Fonctionnement :

- En raison de la règle de Split Horizon, les routeurs iBGP ne peuvent pas réannoncer les routes qu'ils apprennent d'autres routeurs iBGP. Pour garantir que toutes les routes sont propagées à travers l'AS, chaque routeur iBGP doit établir une session avec tous les autres routeurs iBGP.

Limites et solutions :

- Le principal inconvénient du maillage complet (Full Mesh) est qu'il ne passe pas à l'échelle pour les grands réseaux. Plus le nombre de routeurs dans l'AS augmente, plus le nombre de connexions à établir devient exponentiel.

- Solutions :
  - **Route Reflectors (RR)** : Permettent de réduire la complexité du maillage en centralisant les annonces de routes.
  - **Confédérations BGP** : Fractionnent l'AS en sous-AS plus petits pour améliorer la gestion des routes et limiter le nombre de connexions.

iut Bethune réseaux informatiques & télécoms

CONFIGURATION BGP

Commandes clé

1. **Activer BGP** : `router bgp 65001`
2. **Configurer un voisin** : `neighbor <IP_address> remote-as <AS_number>`
3. **Annoncer des réseaux** : `network <network> mask <subnet_mask>`
4. **(Optionnel) Configurer des route-maps** : `route-map <name> permit 10`
5. **Vérifier l'état de BGP** : `show ip bgp summary`