جامعة سيدي محمد بن عبد الله بفاس
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH DE FES

كلية العلوم والتقنيات فاس
FACULTÉ DES SCIENCES ET TECHNIQUES DE FÈS

Projet de Fin d'Etudes

Licence Sciences et Techniques Génie informatique

Etude, Sécurisation et Implémentation du Protocole BGP

RADEEF

Lieu de stage : Régie Autonome de Distribution d'Eau et d'Electricité de Fès

Réalisé par :

Elamrani Abderrahmane

Zegaoui Mossaab

Encadré par :

Pr. BOUSHABA Abdelali

Mr. ELALAM Mohamed

Soutenu le 09/07/2021 devant le jury composé de :

Pr. BOUSHABA Abdelali

Pr. MAJDA Aicha

Pr. OUZARF Mohamed

Année Universitaire : 2020 / 2021

Remerciements

Tout d'abord, nous voudrions louer et remercier Dieu, le tout-puissant, qui nous a accordé d'innombrables bénédictions, connaissances et opportunités afin que nous ayons enfin pu accomplir ce travail.

Nous remercions grandement Monsieur le Directeur général Adjoint de la RADEEF Mr. MEZIANI Mohammed de nous avoir accordé le privilège de passer notre stage au sein de la régie pour une durée de deux mois.

Par la suite, nous remercions chaleureusement Pr. BOUSHABA Abdelali, notre encadrant académique pour sa disponibilité, sa bienveillance, son implication, et surtout ses précieuses recommandations qui nous été une aide inestimable.

Nos remerciements s'adressent également à notre encadrant de l'entreprise, Mr. Med El ALAM qui nous a encadré tout au long de stage, pour le partage de son expertise au quotidien et sans hésiter à aucun moment de consacrer une part de son temps précieux afin de nous aider dans la réalisation de ce travail.

Notre profond respect, et nos vifs remerciements aux autres membres du jury, Pr. MAJDA Aicha et Pr. OUZARF Mohamed de nous avoir honorés en acceptant d'évaluer et de juger ce modeste travail.

Nous tenons à exprimer notre profond sentiment de reconnaissance à toutes les personnes qui ont contribué, de près ou de loin, au bon déroulement de notre projet de fin d'études et qui ont favorisé sont aboutissement.

Dédicace

A nos chers parents, pour tout leur amour, leur tendresse, leurs prières et leur soutien au long de nos parcours universitaires. Aucune dédicace ne saurait être assez éloquente pour exprimer leurs efforts nuit et jour pour notre bien-être.

A nos professeurs qui ne cessent de nous encourager tout le temps et d'être une source d'admiration et de profond respect. Nous vous remercions pour vos efforts déployés afin de contribuer à notre formation.

Un grand merci à tous, votre soutien et votre encouragement nous donnent la force à continuer.

Résumé

En tant que protocole de routage interdomaine, le Border Gateway Protocol (BGP) est le ciment qui maintient ensemble les parties disparates d'Internet. Une limitation majeure de ce protocole est son incapacité à traiter de manière adéquate la sécurité, les récentes pannes et analyses de sécurité indiquent clairement que l'infrastructure de routage Internet est très vulnérable.

Dans ce PFE, nous focaliserons sur les vulnérabilités actuelles du système de routage interdomaine et à la fois aux efforts de recherche et de normalisation relatifs à la sécurité en BGP. Nous explorons les limites et les avantages des extensions de sécurité proposées pour ce protocole et la raison du manque d'implémentation globale de ces solutions, enfin nous réaliserons un scénario d'une implémentation du protocole BGP, ainsi qu'une configuration de sécurité d'une session BGP.

Abstract

As a cross-domain routing protocol, the Border Gateway Protocol (BGP) is the glue that holds disparate parts of the Internet together. A major limitation of this protocol is its inability to adequately handle security, recent failures and security scans have made it clear that the Internet routing infrastructure is very vulnerable.

In this PFE, we focus on the current vulnerabilities of the interdomain routing system and both research and standardization efforts related to security in BGP. We explore the limits and advantages of the security extensions proposed for this protocol and the reason for the lack of global implementation of these solutions, finally we will realize a scenario of implementation of the BGP protocol, as well as a security configuration of a BGP session.

Table des matières

Remerciements 2

Dédicace 3

Résumé 4

Abstract 4

Liste des figures 7

Liste des acronymes 9

Introduction générale 11

Chapitre 1 : Contexte Générale du Projet 12

1.1. Présentation générale de la RADEEF 13

1.2. Organigramme de l'organisme 14

1.3. Département Système d'Information 14

1.4. Plan à suivre 15

1.5. Diagramme de GANTT 15

Chapitre 2: Principe de Fonctionnement de BGP 17

2.1. Aperçu du protocole BGP 18

2.2. Initialisation d'une connexion BGP 19

2.3. Relation entre deux AS 20

2.4. Modes d'interconnexions BGP 21

2.4.1. Mode eBGP 22

2.4.2. Mode iBGP 23

2.5. Structure d'un message BGP 23

2.6. La métrique du protocole BGP 24

2.7. Algorithme de sélection de la meilleure route 26

2.8. Caractéristiques du BGP 27

Conclusion 31

Chapitre 3 : La sécurité en BGP 32

3.1. Problèmes de sécurité 33

3.1.1. Détournement de route BGP 33

3.1.2. Mauvaise configuration 34
3.1.3. Déni de Service 35
3.2. Solutions proposées 36
3.2.1. Techniques Cryptographies 36
3.2.2. Protection de la session BGP entre une paire de routeurs 37
3.2.3. Architecture de sécurité basée sur BGPSec 38
Conclusion 39
Chapitre 4 : Simulation d'une configuration de BGP 40
4.1. La modélisation par simulation 41
4.2. Implémentation de la topologie réalisé 42
4.3. Implémentation de la sécurité pour la topologie réalisé 45
Conclusion générale 47
Annexe 1 48
Annexe 2 54
Webographie 56

Liste des figures

Figure 1 : Organigramme de la RADEEF 14
Figure 2 : Organigramme du Département des Systèmes d'Information 15
Figure 3 : Tableau des taches du projet 16
Figure 4 : Diagramme de Gantt 16
Figure 5 : Propagation d'un préfixe IP sur l'Internet 19
Figure 6 : Diagramme de machine à états finis BGP 20
Figure 7 : relation de Peering en BGP 21
Figure 8 : Relation client/transitoire 21
Figure 9 : session eBGP direct 22
Figure 10 : Session eBGP multihop 22
Figure 11 : Session eBGP établies via un serveur de routes 23
Figure 12 : session iBGP avec les adresses loopback 23
Figure 13 : affichage de certains attributs de chemin BGP 26
Figure 14 : Processus de sélection de route BGP dans un routeur Cisco 27
Figure 15 : maillage complet dans iBGP 28
Figure 16 : iBGP avec réflecteur de route 29
Figure 17: filtrage d'annonce d'un préfixe 30
Figure 18 : diversité du routeur de bord 30
Figure 26 : nombre de détournement de préfixe dans 2020 33
Figure 27 : exemple de détournement de préfix. 34
Figure 28 : Comparaison des incidents BGP entre 2019 et 2020 36
Figure 29 : Le taux d'implémentation du PRKI 37
Figure 30 : Mécanisme de sécurité TTL 38
Figure 31 : Protection de chemin avec BGPSec 39
Figure 19 : topologie réalisé 42
Figure 20 : Ping du routeur C1 vers C4 43
Figure 21 : Ping du routeur C4 vers C1 43
Figure 22 : Message OPEN 44
Figure 23 : message KEEP ALIVE 44
Figure 24 : message UPDATE 45
Figure 25 : Message NOTIFICATION 45
Figure 32 : MD5 n'est pas activée dans un routeur BGP 45
Figure 33 : MD5 est activée uniquement d'un côté de la session BGP 46
Figure 34 : MD5 est activée dans les deux voisins BGP 46

Figure 35 : TTL Security n'est pas activée 46
Figure 36 : GTSM est activée 46

Liste des acronymes

OSI	Open System Interconnection
AFI	Address Family Identifier
AS	Autonomous System
ASBR	Autonomous System Border Router
BGP	Border Gateway Protocol
CPU	Central Processing Unit
DOS	Denial of Service
DDOS	Distributed Denial of Service
eBGP	external Border Gateway Protocol
iBGP	internal Border Gateway Protocol
EGP	Exterior Gateway Protocol
FIB	Forwarding Information Base
FSM	Finite State Machine
iBGP	internal Border Gateway Protocol
IXP	Internet eXchange Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IP	Internet Protocol
MD5	Message Digest version 5
OSI	Open System Interconnection
OSPF	Open Shortest Path First
RFC	Request For Comments

RIB	Routing Information Base
RIP	Routing Information Protocol
ROA	Route Origin Authorisations
RPKI	Ressource Public Key Infrastructure
TCP	Transmission Control Protocol
TTL	Time To live
GTSM	Generalized TTL Security Mechanism

Introduction générale

L’Internet se compose de nombreux sous-réseaux, qui sont connectés les uns aux autres. Ces sous-réseaux sont les systèmes autonomes (AS) qui composent l’Internet : chacun en héberge une partie. Afin d’échanger les routes d'un de ces AS à l'autre, le Border Gateway Protocol (BGP) est utilisé. Ce protocole souffre de plusieurs failles de sécurité, et leur exploitation peuvent rendre certaines parties d'Internet temporairement inaccessibles. Afin de lutter contre ces failles, plusieurs solutions de sécurité ont déjà été développées. Cependant, aucun de ceux-ci n’est déployé à grande échelle.

Dans ce travail nous listerons les différents risques de sécurité applicables aux interconnexions de réseau. Enfin, nous détaillerons les nouveaux mécanismes mis à disposition des opérateurs pour améliorer la sécurité de l’Internet à travers BGP, et pour lutter contre les menaces comme le détournement des paquets d’information.

Ce rapport est composé de 4 chapitres, dans le premier chapitre nous présentons le contexte général et la conduite du projet adoptée, le second chapitre est consacré aux généralités sur le routage interdomaine et particulièrement le protocole BGP, le chapitre 3 expose les menaces et les problèmes de sécurité de BGP, ainsi que quelques services de sécurité qui doivent être déployés pour prévenir une attaque réseau à travers ce protocole, le quatrième chapitre contient une analyse et une simulation d’un scénario d’implémentation de BGP.

Chapitre 1 : Contexte Générale du Projet

1.1. Présentation générale de la RADEEF

La Régie Autonome intercommunale de Distribution d'Eau et d'Electricité de la wilaya de Fès (RADEEF) est un établissement public à caractère industriel et commercial, doté de la personnalité morale et de l'autonomie financière, placé sous la tutelle du Ministère de l'Intérieur.

La RADEEF a été créé par délibération du conseil municipal de la ville de Fès en date du 30 avril et 29 août 1969 en vertu du Dahir n° 1.59.315 du 23 Juin 1960 relatif à l'Organisation communale, et ce après l'expiration du contrat de concession dont bénéficiait la Compagnie Fassie d'Electricité (CFE) au titre de la distribution de l'énergie électrique.

La dotation en capital de la Régie, à sa création, fut constituée par l'apport initial auquel se sont ajoutés la valeur des installations, du matériel et du stock remis par la ville ainsi que les fonds détenus pour le compte de celle-ci par l'ancien concessionnaire.

Par la suite, la RADEEF a été transformée en Régie Intercommunale suite à l'arrêté du Ministre de l'Intérieur n°3211 du 02-10-1985 portant autorisation de créer le nouveau syndicat des communes pour la gestion du Service de l'Eau potable dans 19 communes.

A compter du 1er Janvier 1996, la RADEEF a été chargée de la gestion du réseau d'assainissement liquide de la ville de Fès en vertu de l'arrêté du Ministre de l'Intérieur n° 2806-95 du 3 Juin 1996 approuvant les délibérations du conseil de la Communauté Urbaine de Fès et des conseils communaux relevant de cette communauté, lesquelles délibérations ont chargé la RADEEF de la gestion du réseau d'assainissement liquide de la ville de Fès.

Actuellement, la RADEEF assure la distribution de l'eau et de l'électricité ainsi que la gestion du réseau d'assainissement liquide l'intérieur de la ville de Fès et de la commune Ain Chkef. Elle est en outre chargée de la distribution de l'eau potable dans les communes urbaines de Sefrou et Bhalil ainsi que dans les communes rurales suivantes : Bir Tam-Tam, Ras Tabouda, Sidi Harazem, Ain Timgnai, Ouled Tayeb, Douar Ait Taleb et Douar Ait El Kadi [1].

1.2. Organigramme de l'organisme

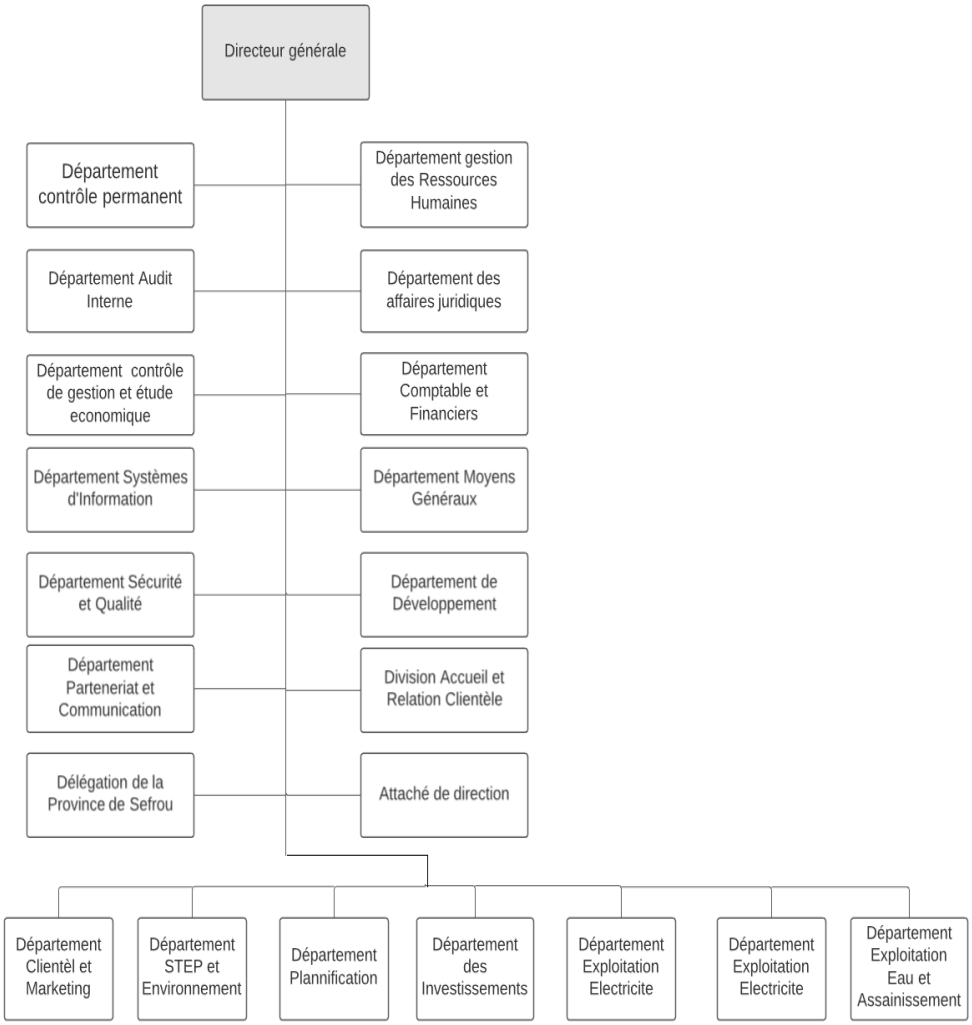


Figure 1 : Organigramme de la RADEEF

1.3. Département Système d'Information

Pour assurer la disponibilité et la maintenance de l'ensemble des systèmes d'informations, le département s'occupe de plusieurs missions :

- Gérer la division système d'information.
- Traduire les besoins exprimés par les utilisateurs en projets.
- Suivre l'activité des différents services de la division.
- Elaborer les plannings avec les différentes structures de la RADEEF.
- Organiser l'exploitation afin de satisfaire ces plannings.
- Piloter l'élaboration des dossiers d'appels d'offres relatifs à l'activité informatique.
- Mettre en place les contrats de maintenance matériels et logiciels et en assurer le suivi.
- Mettre en place un plan de formation des informations et le suivre.
- Reporting avec la direction.

Ce département est subdivisé en quatre divisions selon l'organigramme suivant :

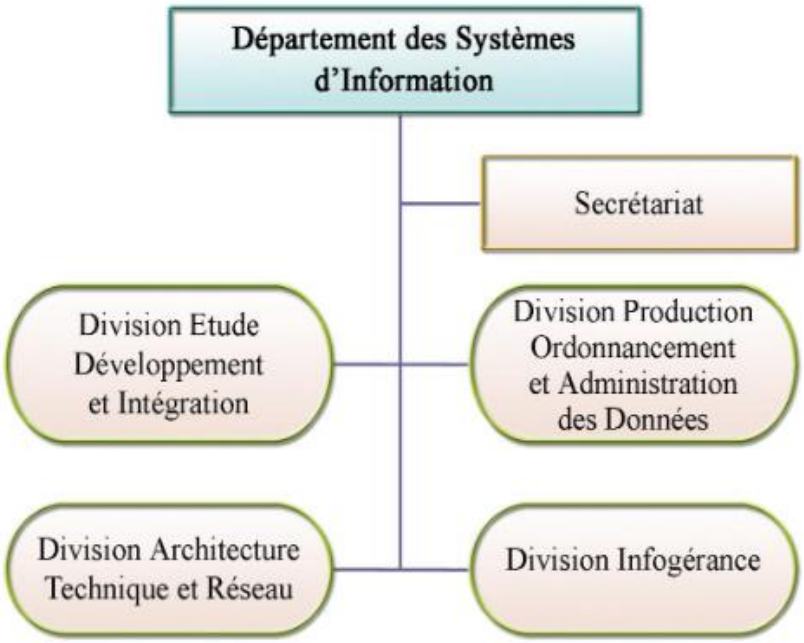


Figure 2 : Organigramme du Département des Systèmes d'Information

1.4. Plan à suivre

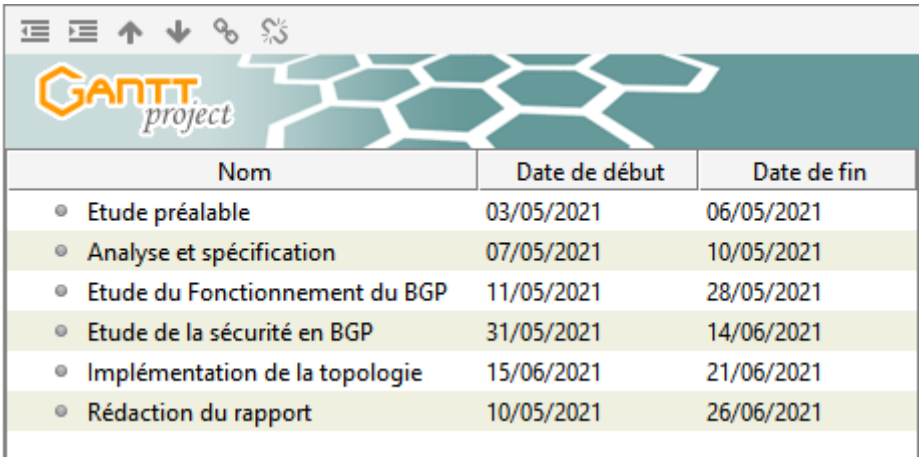
Dans ce PFE, nous présentons un aperçu détaillé sur le fonctionnement du protocole BGP, puis nous discutons les vulnérabilités de ce dernier, en plus des solutions proposées pour réduire les risques de ces failles, finalement nous réalisons une implémentation d'une configuration de BGP ainsi que celle de sa sécurité.

1.5. Diagramme de GANTT

La planification d'un projet consiste à prévoir le déroulement des tâches tout au long des phases, constituant son cycle de développement. Pour schématiser le planning du projet, le choix a été porté sur l'outil GanttProject, qui est l'un des outils de gestion de projet les plus efficaces pour l'ordonnancement d'un projet, il permet de vérifier d'un simple coup d'œil :

- Une présentation visuelle de l'ensemble de projet.
- Les échéanciers et délais de toutes les tâches.
- Les relations et les dépendances entre les différentes activités.
- Les phases du projet.

Le planning de réalisation de notre projet est comme suit :



Nom	Date de début	Date de fin
Etude préalable	03/05/2021	06/05/2021
Analyse et spécification	07/05/2021	10/05/2021
Etude du Fonctionnement du BGP	11/05/2021	28/05/2021
Etude de la sécurité en BGP	31/05/2021	14/06/2021
Implémentation de la topologie	15/06/2021	21/06/2021
Rédaction du rapport	10/05/2021	26/06/2021

Figure 3 : Tableau des taches du projet

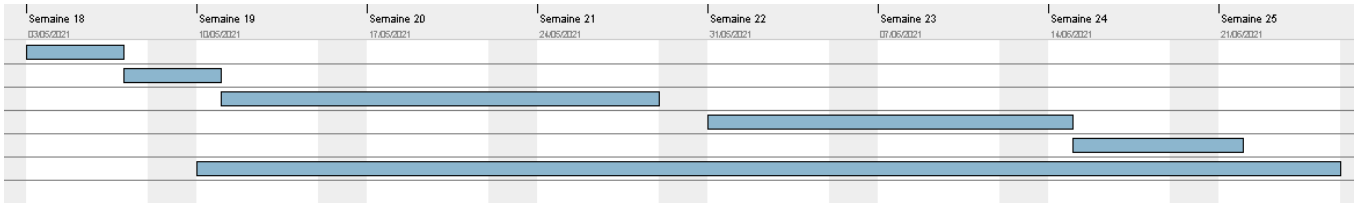


Figure 4 : Diagramme de Gantt

Chapitre 2 : Principe de Fonctionnement de BGP

Dans ce chapitre, nous présentons un aperçu détaillé sur le protocole BGP et certaines de ses caractéristiques, nous décrivons les différents états et messages échangées lors d'une initialisation d'une connexion BGP, puis nous expliquons l'algorithme de sélection de la meilleure route de ce protocole.

2.1. Aperçu du protocole BGP

Les protocoles de routages sont divisés en deux grandes catégories : protocoles de routage intérieur ou IGP (Interior Gateway Protocol) et protocoles de routage extérieur ou EGP (Exterior Gateway Protocol). Les IGP et les EGP ont des objectifs différents et recourent donc à des méthodes différentes, un IGP connaît l'ensemble de la topologie alors qu'un EGP cache toute information détaillée sur la topologie interne d'un AS (Autonomous System). Les IGPs comme RIP (Routing Information Protocol) et OSPF (Open Short Path First) sont efficaces pour les réseaux de taille modérée, mais ils ne sont pas capables de supporter le routage avec plusieurs milliers des nœuds et centaines de milliers de routes. Un EGP est d'intérêt double : les routeurs dans un AS l'utilisent pour appliquer une politique de routage interne, et les routeurs dans différents AS l'utilisent pour échanger les informations sur l'accessibilité des réseaux. Actuellement, le protocole BGP est le standard et l'unique protocole EGP pour le routage entre les AS. Une session BGP est établie entre deux routeurs IP, qui deviennent alors voisins BGP. Si ces deux routeurs font partie de différents AS, la session BGP est dite externe ou eBGP (external BGP), les routeurs initiant des sessions eBGP appelés routeurs de bord ou BR (Border Router), jouent le rôle des portes entrée/sortie pour leurs AS, on parle de routage inter-domaine. Ce protocole peut également être utilisé au sein d'un même AS, par exemple pour diffuser les routes apprises de l'Internet aux routeurs du réseau IP (figure 5): dans ce cas-là, la session est dite interne ou iBGP (internal BGP). BGP fait partit de la famille vecteurs-à distance, c'est-à-dire que les routes échangent des informations d'accessibilité sur leurs destinations en utilisant le prochain saut (*next_hop)* et une métrique de distance associé. BGP utilise TCP comme protocole de transport, qui lui permet une livraison fiable des mis à jour. Chaque route échangée entre des destinations réseaux est composée d'une part d'un préfixe (une adresse IP suivie par un slash et un nombre de bits utilisés pour la partie réseau), et d'autre part d'attribut de routes. Ces attributs et leur formalisme associé sont décrits en détail dans les paragraphes qui suivent [2].

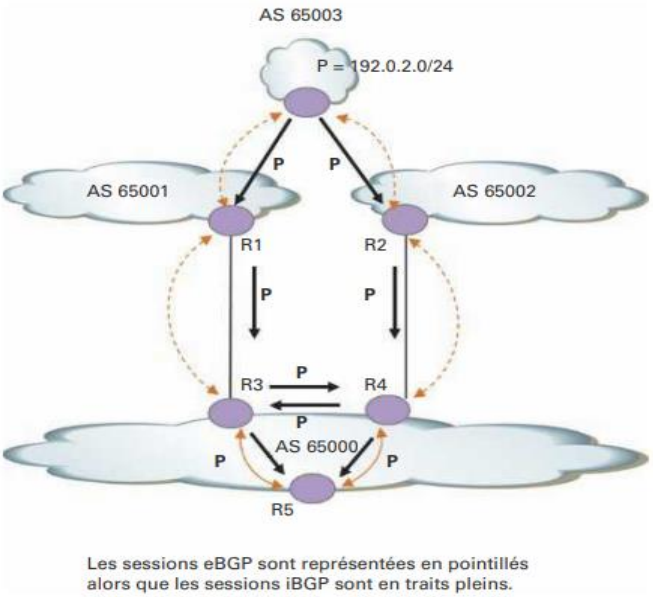


Figure 5 : Propagation d'un préfixe IP sur l'Internet

2.2. Initialisation d'une connexion BGP

Les voisins BGP passent par différents états finis avant qu'une connexion ne soit complètement établie. À chaque état, différents messages BGP sont envoyés dans les deux sens (figure 6) [3]. Ces états sont :

- Idle : c'est la première étape d'une connexion BGP. BGP attend un événement Start, qui est initié par un opérateur réseau (un administrateur établissant une session BGP via la configuration d'un routeur ou en réinitialisant une session déjà existante) ce qui provoque généralement un événement Start. Après l'événement Start, BGP initialise ses ressources, initie une connexion TCP et commence à attendre l'initialisation d'une connexion BGP par un voisin, BGP passe ensuite à l'état Connect. En cas d'erreur, BGP revient à l'état Idle.
- Connect : BGP initie la connexion TCP, si la négociation TCP à trois voies se termine, le processus de session BGP établi réinitialise le ConnectRetryTimer (la durée entre les tentatives d'établissement d'une connexion au voisin BGP tombé en panne) et envoie un message Open au voisin, puis passe à l'état OpenSent. Si le temporisateur ConnectRetry s'épuise avant la fin de cette étape, une nouvelle connexion TCP est tentée, le temporisateur ConnectRetry est réinitialisé et l'état passe à Actif. Si un autre résultat est reçu, l'état passe à Idle.
- Active : BGP démarre une nouvelle négociation TCP à trois voies. Si une connexion est établie, un message Open est envoyé et l'état passe à OpenSent. Si cette tentative

de connexion TCP échoue, l'état revient à l'état Connect et réinitialise le ConnectRetryTimer.

- OpenSent : BGP attend un message OPEN de son voisin (les deux messages OPEN sont vérifiés pour les erreurs), en cas d'erreurs (un mauvais numéro de version) le système envoie un message NOTIFICATION d'erreur et repasse à l'état Idle. S'il n'y a pas d'erreurs, BGP commence à envoyer des messages KEEPALIVE et l'état passe à OpenConfirm.
- OpenConfirm : BGP attend un message KEEPALIVE ou NOTIFICATION. À la réception du KEEPALIVE d'un voisin, l'état passe à Established. Si le *holdtimer* expire, un événement d'arrêt se produit ou un message de NOTIFICATION est reçu, l'état passe à Idle.
- Established : la session BGP est établie. Les voisins BGP échangent des routes via des messages UPDATE (les messages UPDATE et KEEPALIVE sont reçus), le *holdtimer* est réinitialisée. Si le *holdtimer* expire, une erreur est détectée et BGP remet le voisin à l'état idle.

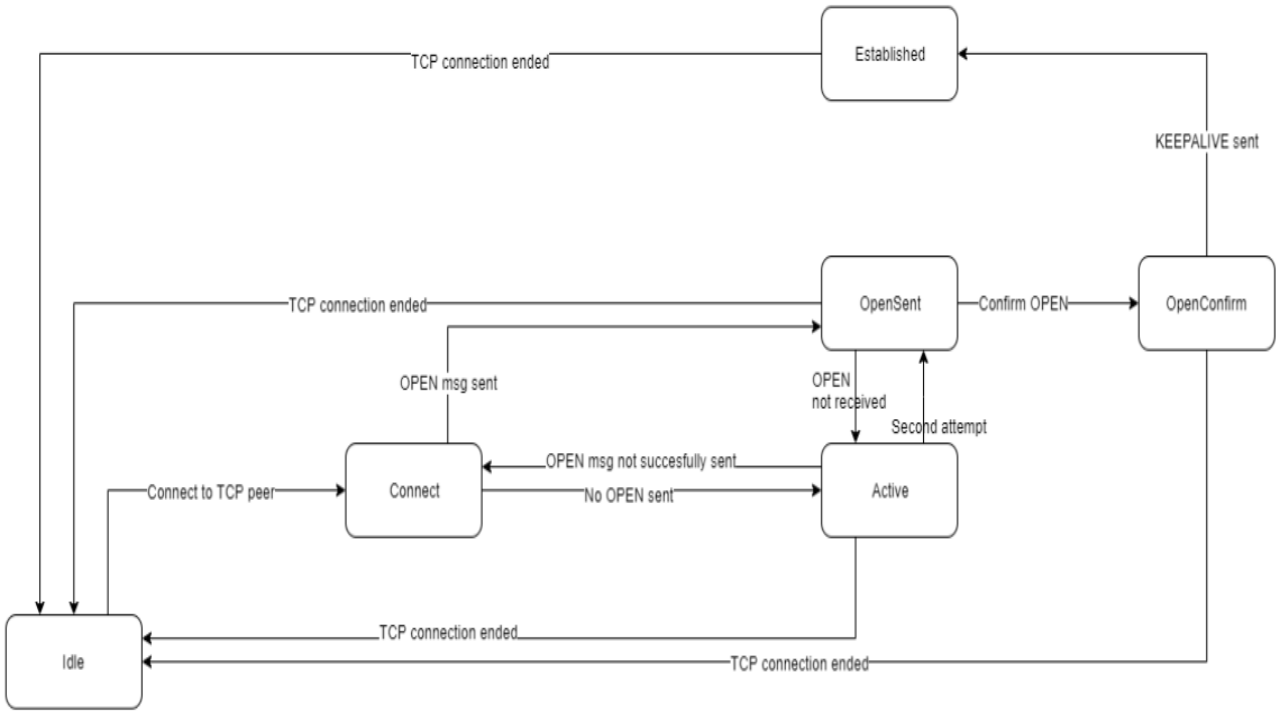


Figure 6 : Diagramme de machine à états finis BGP

2.3. Relation entre deux AS

Avant d'établir une relation de voisinage entre deux AS, un administrateur réseau devra spécifier l'un des différents types suivants [2].

➢ **La relation de Peering**

La relation de Peering est une connexion point à point entre des systèmes autonomes pairs (figure 7), on configure une session BGP sur chaque interface d'une liaison point à point de telle façon à ce que les sessions réalisées aux points de sortie du réseau avec les hôtes voisins en dehors d'AS. Un AS exporte uniquement les routes d'un pair vers ses clients et les routes d'un client vers un pair, cette relation est souvent sans règlement (gratuit).

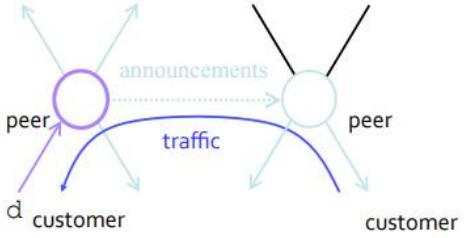


Figure 7 : relation de Peering en BGP

➢ **La relation client/transitoire**

Dans la relation client/transitoire, l'AS client attend de son transitaire de relayer l'ensemble de ses paquets de trafic vers le reste de l'internet. Pour ce faire le client annonce au transitaire via les sessions eBGP l'ensemble de ses propres routes, ainsi que celles des éventuels clients (figure 8). En contrepartie, le transitaire annonce au client l'ensemble des routes de l'Internet. Cette relation est en général fondée sur des bases contractuelles avec contrepartie financière, le client payant son fournisseur pour le service de transit.

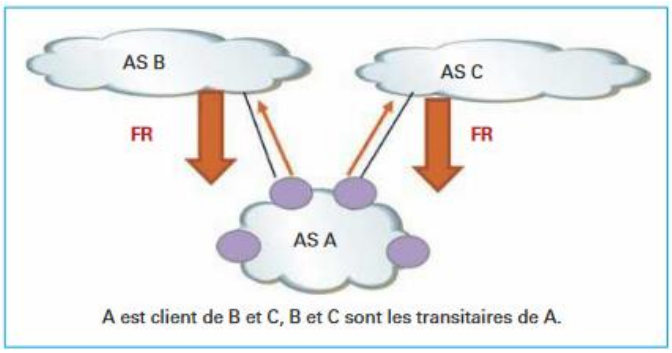


Figure 8 : Relation client/transitoire

2.4. Modes d'interconnexions BGP

Les systèmes interconnectés par une session eBGP sont administrés par deux entités différentes, ces interconnexions de réseau IP traduisant des modèles économiques bien précis entre les deux entités. Ce paragraphe s'attache également à décrire techniquement les formes classiques d'interconnexion les plus souvent rencontrées.

2.4.1. Mode eBGP

- **Session eBGP directe**

C'est la forme la plus traditionnelle d'établissement des sessions eBGP. En général, les deux routeurs sont directement connectés. L'interconnexion peut être réalisée par un câble ou à travers un équipement de transmission (figure 9) [4].

Figure 9 : session eBGP direct

- **Session eBGP multihop**

L'eBGP multihop permet une connexion voisine entre deux locuteurs eBGP (routeur parlant BGP) qui n'ont pas de connexion directe. La configuration de cette session doit alors préciser que la session est multihop, et contenir une information sur le nombre de sauts IP maximum que le paquet BGP traverse entre les deux points de montage.

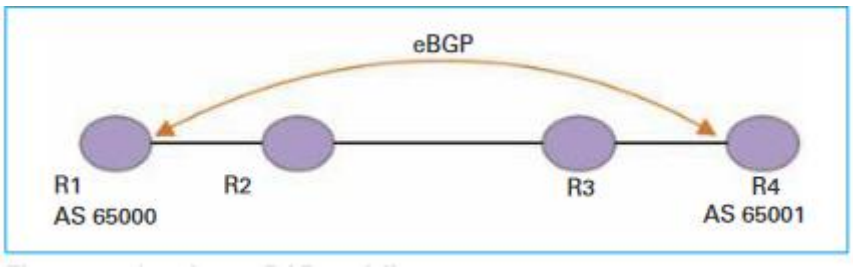


Figure 10 : Session eBGP multihop

- **Serveur de routes**

En général, les routes IP sont directement raccordées deux à deux. Mais, dans le cas d'un point d'échange, lorsque de nombreux opérateurs désirent se connecter ensemble, ces raccordements nécessiteraient de réaliser un maillage complet ou un full-mesh (chaque routeur BGP établit une relation de voisinage avec tous les autres routeurs BGP) de session eBGP, ce qui complexifierait l'architecture, Internet eXchange Point ou (IXP) peut alors offrir un serveur de routes, c'est-à-dire un équipement IP qui réalisera uniquement l'échange de routes entre les AS (figure 11). Au lieu de maintenir un voisinage eBGP individuel et direct avec tous les autres fournisseurs, un fournisseur d'accès Internet ou Internet Service Provider (SP) ne maintient qu'une seule connexion au serveur routeur exploité par l'IXP, ce qui réduit la complexité de la configuration sur chaque routeur frontière, les besoins en CPU et en

mémoire et évite la plupart des surcharges opérationnelles encourues par les accords de voisinage individualisés [2].

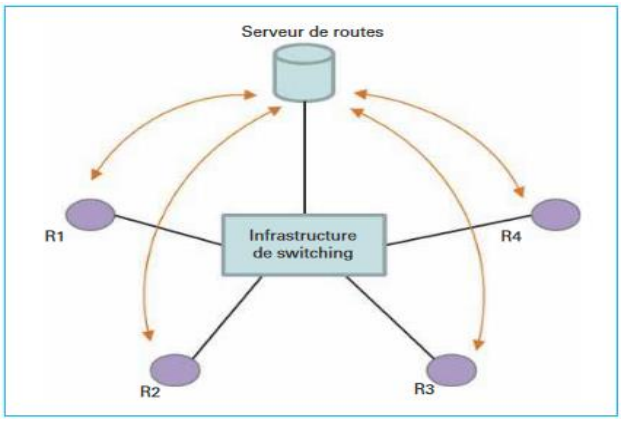


Figure 11 : Session eBGP établies via un serveur de routes

2.4.2. Mode iBGP

Les connexions iBGP sont généralement établies entre des adresses IP logiques, non associées à une interface physique particulière, des adresses loopback (figure 12) [5]. Classiquement, un protocole de routage interne dynamique (IGP) permet aux routeurs du réseau considéré de se joindre via leurs adresses loopback. Ainsi en cas de rupture d'un lien physique, la session iBGP reste active si un lien alternatif existe.

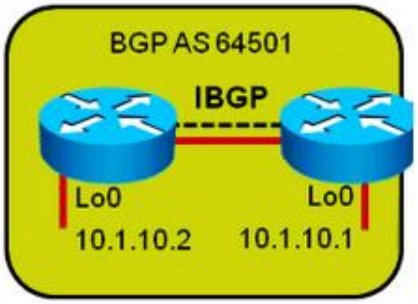


Figure 12 : session iBGP avec les adresses loopback

2.5. Structure d'un message BGP

La session BGP s'appuie sur la couche TCP, et plus précisément sur le port 179. Une fois la session TCP établie entre les deux routeurs voisins BGP, 5 types de messages BGP différents sont échangés.

- ✓ **Message OPEN :** Echangés à l'ouverture de la session pour identifier le voisin BGP, son numéro d'AS, et négocier certains paramètres optionnels de la session, comme l'annonce de :

- Les valeurs des timers à utiliser sur cette session (par exemple le *hold timer*, durée maximale entre la réception de deux messages, sur la session avant de déclarer celle-ci comme *down*).
- La capacité à échanger des numéros d'AS.

✓ **Message KEEPALIVE :** Echangés périodiquement si aucun autre message n'est transmis sur la session, afin qu'un routeur BGP soit capable de déterminer que son voisin est toujours disponible. Pour calculer l'intervalle de temps auquel il faut les émettre, le routeur récupère la valeur du paramètre *hold timer* contenu dans le message OPEN et le divise par 3. Lorsqu'un voisin ne reçoit aucun message sur une session pendant la totalité de la durée du *hold timer*, il détecte la perte de son voisin et clôt la session BGP.

✓ **Message NOTIFICATION :** Emis, lors de la clôture d'une session et spécifiant une condition d'erreur, il contient le code et le sous-code d'erreur pour fournir des précisions sur la nature d'erreur.

✓ **Message UPDATE :** Contenant les informations d'accessibilité réseau, à savoir les annonces de nouvelles routes ou parfois d'indisponibilité d'un réseau destination, les messages étant alors qualifiés de *withdrawal*, accompagnés de tous ses attributs de routes. Pour chaque session BGP qu'il maintient avec un voisin BGP, le routeur BGP construit une table de routage, contenant les informations de routages émises par ce voisin.

✓ **Message ROUTE-REFRESH :** Le message d'actualisation de routes est utilisé pour demander de manière dynamique à un annonceur de routes BGP de renvoyer les messages UPDATE.

2.6. La métrique du protocole BGP

La métrique BGP est relativement complexe, contrairement à OSPF qui n'utilise qu'un seul attribut, BGP utilise plus de 10. Lorsqu'un routeur BGP reçoit un préfixe BGP, il y aura de nombreux attributs de chemin (des informations associées à un routeur BGP, pour différentier les préfixes inclus dans un message UPDATE) qui lui seront associés, ce qui seront essentiels lorsqu'il s'agira pour BGP de choisir le meilleur chemin vers une destination. Ces attributs de chemin sont classifiés en quatre catégories principales [6].

➢ Catégories des attributs

Well-known Mandatory (WM) : Un attribut qui doit exister dans le paquet BGP UPDATE. Il doit être reconnu par toutes les implémentations BGP. Si un attribut connu est manquant,

une erreur NOTIFICATION est générée et la session est fermée. Ceci permet de s'assurer que toutes les implémentations BGP s'accordent sur un ensemble standard d'attributs.

Well-known discretionary (WD) : Un attribut qui est reconnu par toutes les implémentations BGP, mais qui peut ou non être envoyé dans le message UPDATE.

Optional transitive (OT) : Un attribut qui n'est pas besoin d'être compris par toutes les implémentations BGP, si un attribut facultatif n'est pas reconnu par l'implémentation BGP, cette implémentation recherche un indicateur transitif pour voir s'il est défini pour cet attribut particulier. Si l'indicateur est défini. L'implémentation BGP doit accepter l'attribut et le transmettre à d'autres locuteurs BGP.

Optional non transitive (ON) : Lorsqu'un attribut facultatif n'est pas reconnu et que l'indicateur transitif n'est pas défini, l'attribut doit être discrètement ignoré et non transmis à d'autres locuteurs BGP.

➢ Liste de quelques attributs de BGP

Origin : L'attribut origin indique l'origine d'un préfixe, et peut prendre trois valeurs : « i », « e » et « ? », « i » désigne les routes qui proviennent d'un IGP, généralement via la commande *network*, « e » désigne les routes appris par un EGP, maintenant le seul EGP est le BGP, « ? » (Incomplet) signifie que BGP n'est pas sûr de la manière exacte dont le préfixe a été injecté dans la topologie. Le scénario le plus courant ici est que le préfixe a été redistribué dans BGP à partir d'un autre protocole, généralement un IGP.

AS Path : L'AS Path est un attribut obligatoire qui est présent pour tous les préfixes échangés entre les voisins BGP. Lorsqu'un routeur BGP envoie un message UPDATE à un voisin d'un AS différent, il ajoute son propre numéro AS à l'avant (côté gauche) du chemin AS, le chemin AS répertorie tous les AS qui doivent être traversés pour atteindre l'emplacement d'où le préfixe auquel le chemin est attaché est annoncé.

Next_hop : L'attribut next_hop est l'adresse IP du prochain saut qui va être utilisée pour atteindre une certaine destination. Pour eBGP, le prochain saut est toujours l'adresse IP du voisin spécifié dans la commande *(neighbor)* [7].

Weight : Le poids est également l'un des attributs uniques, car sa valeur n'est pas transmise aux autres routeurs. Le poids est une valeur attribuée aux préfixes en tant que valeur localement significative, c'est est un nombre simple compris entre 0 et 65535, et plus la valeur de poids est élevée, plus la préférence pour ce chemin est élevée. Lorsque le préfixe est généré localement, il aura un poids de 32768. Sinon, le poids par défaut est 0 pour un préfixe.

Local_Pref : La préférence locale est une indication à l'AS sur le chemin qui est préféré pour sortir de l'AS, afin d'atteindre un certain réseau (un chemin avec une préférence locale plus élevée est plus préféré), la valeur par défaut de la préférence locale est 100. Contrairement à l'attribut de poids qui ne concerne que le routeur local, la préférence locale est un attribut qui est échangé entre les routeurs du même AS.

Un exemple des attributs de chemin pour le préfixe 100.100.100.0/24 reçu par le routeur TPA1 est illustré dans la figure 13.

```
TPA1#show ip bgp
BGP table version is 4, local router ID is 10.10.10.1
Status codes: s suppressed,d damped,h history,* valid,> best,i - internal,
r RIB-failure,S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 100.100.100.0/24 10.10.10.2               0             0 200 i
```

Figure 13 : affichage de certains attributs de chemin BGP

2.7. Algorithme de sélection de la meilleure route

Lorsque le protocole BGP reçoit plusieurs chemins vers une même destination, ces chemins sont stockés dans la table BGP, mais uniquement la meilleure route qui est installé dans la table de routage. BGP sélectionne la meilleure route en comparant les valeurs des attributs figurants dans une liste d'attributs du haut vers le bas (figure 14) [8]. Le premier attribut à comparer est le poids, le chemin avec la valeur du poids la plus élevée est choisie comme meilleur, si les deux chemins ont la même valeur, BGP compare le deuxième attribut, qui est la préférence locale, si encore une fois, les deux chemins ont la même valeur, BGP passe au troisième attribut, jusqu'à ce qu'il obtient un bris d'égalité, le dernier attribut à comparer dans la liste est l'adresse IP des deux voisins BGP, celui avec la valeur la plus élevée est choisie comme meilleur chemin. Finalement BGP prend la meilleure route et l'installe dans la table de routage.

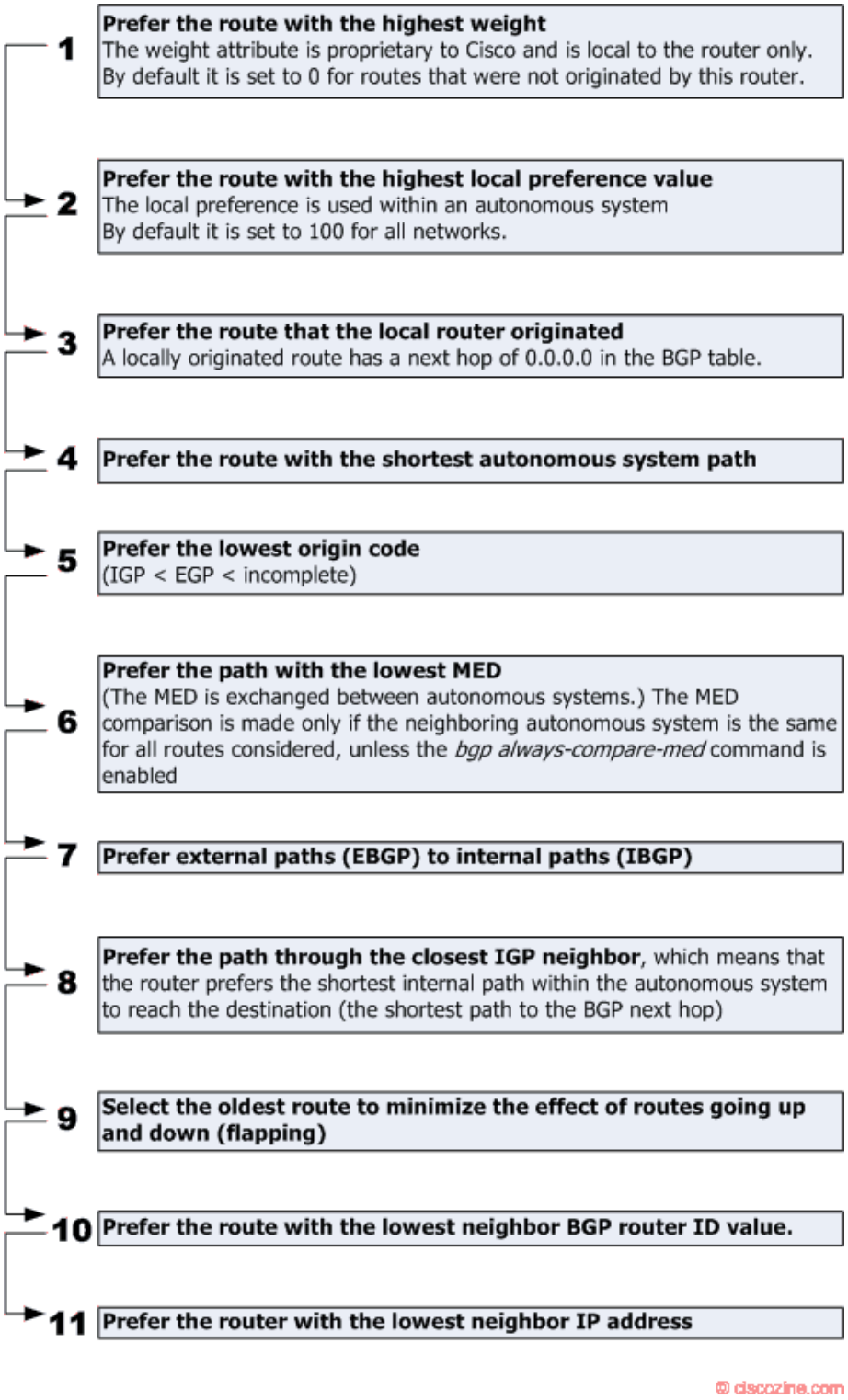


Figure 14 : Processus de sélection de route BGP dans un routeur Cisco

2.8. Caractéristiques du BGP

- **Scalabilité**

BGP a été conçu pour gérer des réseaux de grande taille comme Internet. Il peut transporter 200K-500K de préfixes sans surcharger un routeur avec des calculs lourds en raison du

changement dynamique des états de liaison. Sur Internet, le *flapping* (l'apparition et la disparition d'une route dans la table de routage) peut arriver très souvent. Un protocole de routage à état de lien (comme OSPF) n'est pas adapté pour gérer cette situation. Cependant, iBGP n'a pas de mécanisme de détection de boucle, alors une topologie de maillage complet doit être maintenue parmi les routeurs de bord, de sorte que chaque nœud interne doit établir des sessions iBGP avec tous autres les routeurs de bord pour garantir une visibilité complète. Le nombre de session nécessaire pour former cette maille complète entre n routeurs est $\frac{n\,(n-1)}{2}$ et chaque routeur doit gérer (n-1) session (figure 15) [9].

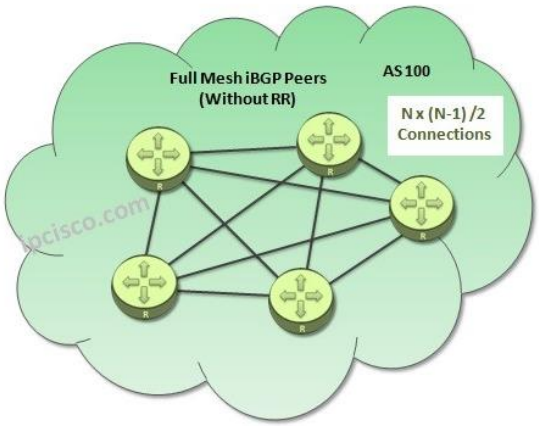


Figure 15 : maillage complet dans iBGP

Pour résoudre ce problème de mis en échelle, un AS peut employer une technique de scalabilité comme la réflexion de route (figure 16), cette technique permet de partager des informations de routage entre plusieurs routeurs sans avoir à envoyer exactement les mêmes informations à chacun des routeurs individuellement et sans introduire de boucles. Un réflecteur de route n'est plus limité par la restriction de re-publicité, ce qui lui permet de partager des routes avec d'autres voisins iBGP. Un routeur est configuré comme réflecteur de route ou RR (Route Reflector) et les autres routeurs sont connectés et envoient des mises à jour au RR uniquement.

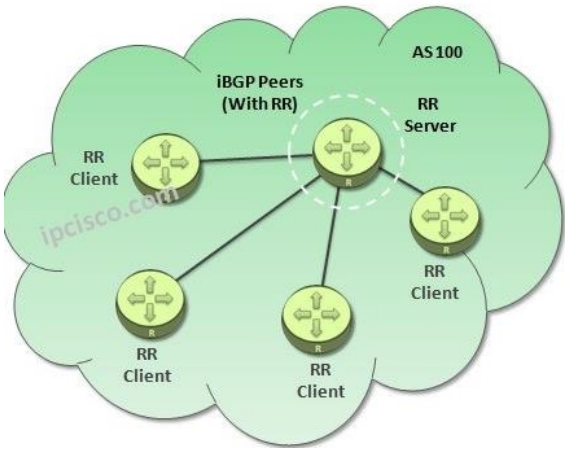


Figure 16 : iBGP avec réflecteur de route

➢ La performance

BGP est le protocole qui consomme le plus de ressources. Actuellement, le protocole BGP échange des dizaines de messages par seconde pour mettre à jour des centaines de routes dans la table de routage. De plus, le protocole peut atteindre des centaines de connexions TCP avec des routeurs voisins pour réaliser cet échange. Avec la croissance continue de l'Internet, ces nombres de connexions vont sûrement continuer à croître Cette croissance prévue de trafic du BGP risque de nuire aux autres protocoles qui s'exécutent sur la même interface de réseau et pourra par la suite produire une dégradation de la performance au niveau du même routeur.

➢ Filtrages des routes

Le filtrage des routes est une méthode pour identifier sélectivement les routes qui sont annoncés ou reçus des routeurs voisins et pour manipuler les flux de trafic, réduire l'utilisation de la mémoire et améliorer la sécurité. Par exemple, il est courant pour les SP de déployer des filtres de routage sur les locuteurs BGP auprès des clients pour s'assurer que seules les routes des clients sont autorisées sur le lien de voisinage, ce qui empêche le client de devenir accidentellement un AS de transit sur Internet [10].

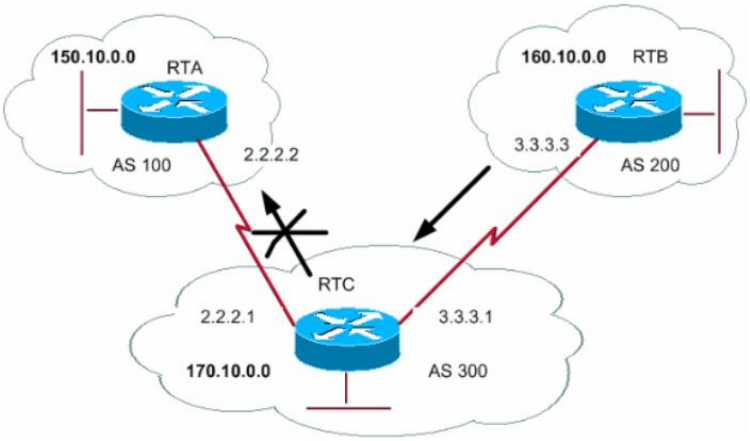


Figure 17: filtrage d'annonce d'un préfixe

Dans la figure 17, le routeur RTB initie le réseau 160.10.0.0 et envoie la mise à jour à RTC. Si RTC veut arrêter la propagation des mises à jour à AS 100, on doit définir une liste d'accès pour filtrer ces mises à jour pendant la communication avec RTA.

➢ Diversité de chemins

La conception BGP offre une flexibilité limitée en ce qui concerne la sélection de chemin. L'objectif principal du protocole est d'offrir au moins un chemin pour chaque destination, ce qui est suffisant dans des conditions normales. D'autre part, en cas de panne d'un lien ou d'un routeur, l'accessibilité est interrompue et le trafic peut être perdu en attendant la reprise après panne. Le nombre de routes disponibles pour atteindre une destination est suffisant pour assurer la redondance. Habituellement, un préfixe peut être atteint via plusieurs AS voisins. Les annonces de préfixe sont souvent cohérentes sur les liens vers le même AS voisin, ce qui signifie que les chemins annoncés sont similaires (figure 18), à l'exception de l'attribut *next_hop* qui désigne le routeur frontière précis envoyant le message BGP UPDATE. Ceci est quantifié par le terme next-hop-router diversity.

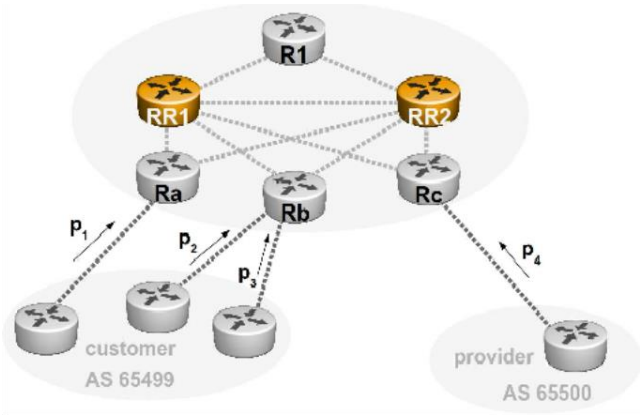


Figure 18 : diversité du routeur de bord

Dans la figure 18, le routeur Rb reçoit deux chemins P2 et P3 des voisins eBGP. Cependant BGP ne génère qu'un seul meilleur chemin que Rb peut propager dans le réseau interne.

Conclusion

Dans ce chapitre nous avons présenté un état de l'art sur le principe de fonctionnement de BGP, commençant par un aperçu détaillé du BGP, passant à l'initialisation d'une connexion BGP, suivie par examiner quelques attributs du BGP et leur rôle dans la sélection du meilleur chemin. D'autre part, on a cité d'autres caractéristiques spécifiques à ce protocole. Puisque le BGP n'effectue aucune validation des données, il est donc vulnérable aux attaques qui modifient les données envoyées. Dans le prochain chapitre, nous discuterons les attaques les plus courantes contre BGP et quelques solutions disponibles qui aident à empêcher ces attaques.

Chapitre 3 : La sécurité en BGP

3.1. Problèmes de sécurité

En raison de ses failles de sécurité permettant de nombreuses attaques possibles, plusieurs solutions ont été proposées pour améliorer la sécurité de BGP. Ces solutions de sécurité vont de solutions assez basiques qui se concentrent uniquement sur la défense contre une attaque (par exemple, le détournement de préfixe) à des solutions conçues pour résoudre la plupart des failles de sécurité dans BGP en même temps. Ce chapitre décrit en détail les attaques les plus fréquentes contre ce protocole, ainsi que certaines solutions proposées pour se protéger contre ces attaques.

3.1.1. Détournement de route BGP

Un détournement de route BGP se produit lorsqu'un AS intentionnellement ou par erreur prétend être l'origine d'un réseau qui a été attribué à un autre AS. En manipulant de manière malveillante les préfixes IP BGP, un attaquant peut rediriger le trafic afin d'intercepter ou de modifier le trafic. Cette attaque est possible car BGP n'exige aucune preuve de propriété d'un préfixe pour qu'un AS annonce qu'il possède un certain préfixe. Le détournement BGP au niveau Internet est effectué en configurant un routeur de périphérie pour annoncer les préfixes qui ne lui ont pas été attribués. Si l'annonce malveillante est plus spécifique que l'annonce légitime ou prétend offrir un chemin plus court, le trafic peut être dirigé vers le pirate de l'air IP. Les cas de détournement de préfixe sont plus fréquents qu'il n'y paraît à première vue. La figure 19 montre le nombre de détournements de préfixe du janvier à juillet 2020 [11].

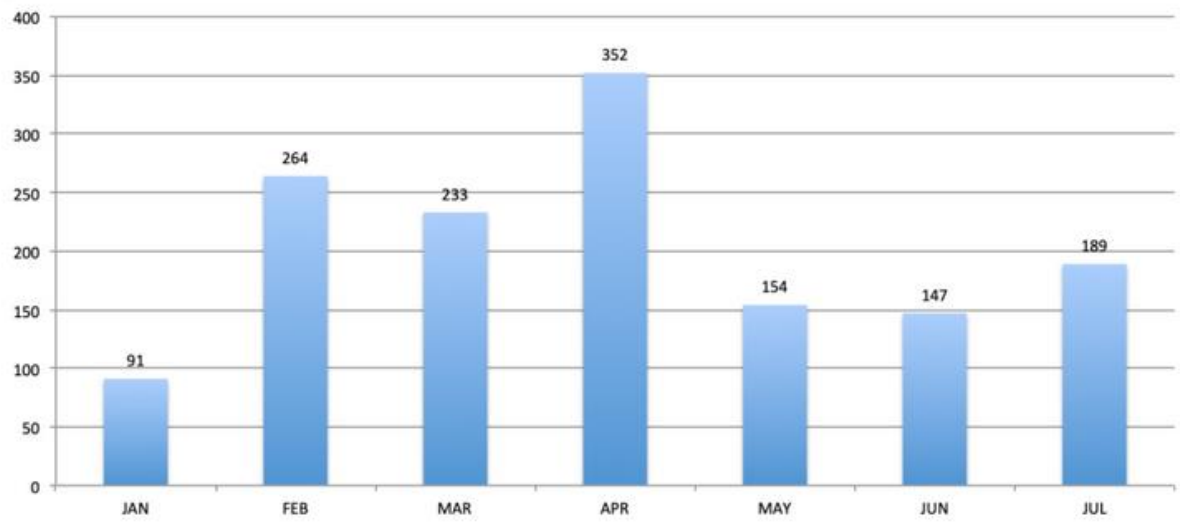


Figure 19 : nombre de détournement de préfixe dans 2020

Dans la figure 20, AS 2 et AS 3 sélectionneront une fausse route vers le préfixe 12.34.0.0/16, tandis que les autres AS sélectionneront la bonne route. Même si AS4 et AS 7 propage la route légitime vers AS 3, le nombre de sauts dans la route correcte sera supérieur au nombre

de sauts dans la route incorrecte déjà sélectionnée, ceci combiné sans authentifier quelle route est correcte ou quel AS possède réellement le préfixe mentionné, signifie que certains AS sélectionneront une mauvaise route vers un préfixe tandis que d'autres en sélectionneront une correcte [12].

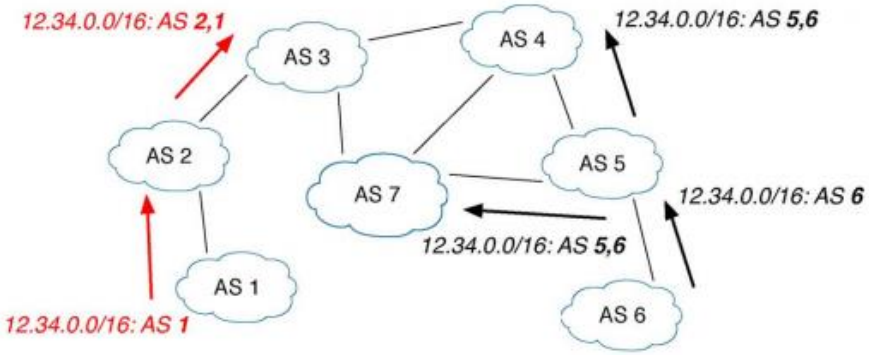


Figure 20 : exemple de détournement de préfix.

Une variante du détournement de préfixe est le détournement de sous-préfixe, qui peut être encore plus efficace qu'un détournement de préfixe ordinaire si une série de sous-préfixes est annoncée qui combinés constitue le préfixe d'origine. Un détournement de sous-préfixe implique qu'un AS prétend de posséder un préfixe qui est plus spécifique qu'un autre préfixe.

3.1.2. Mauvaise configuration

Une autre source de manque de fiabilité de BGP est la mauvaise configuration des routeurs qui parlent BGP. Une mauvaise configuration est une erreur de configuration qui entraîne la production ou la suppression involontaire de l'annonce de routage BGP. Elle conduit à la fois à un *slip* (erreurs involontaires) et à des erreurs (erreurs de conception) dans la terminologie des facteurs humains. Par exemple, un AS peut accidentellement filtrer une route censée autrement annoncer à un observateur distant, ce déni de service serait indiscernable d'un échec. De même, les mauvaises configurations de certains attributs de BGP ne seront généralement observables qu'entre les AS de participation [13]. Les impacts négatifs d'une mauvaise configuration comprennent :

Charge de routage : Diverses modifications augmentent la charge de routage en générant des mises à jour BGP inutiles. De nombreux routeurs parlant BGP sont déjà fortement chargés en raison de la croissance rapide d'Internet.

Perturbation de la connectivité : des erreurs de configuration peuvent perturber la connectivité, partiellement (partie du réseau) ou globalement.

Violation de la politique : par définition, les erreurs de configuration enfreignent la politique de l'AS, un préfixe peut être divulgué de manière incorrecte sur l'ensemble d'Internet, la route annoncée par erreur peut être choisie par rapport à une autre.

3.1.3. Déni de Service

La plupart des attaques ci-dessus peuvent être considérées comme des attaques par déni de service. Le trou noir d'une route, par exemple, provoque un déni de service pour ce préfixe, et la subversion du chemin peut également entraîner des retards ou des refus de service. Par exemple, une route suffisamment longue peut entraîner le dépassement de la durée de vie (TTL) d'un paquet. Dans le cas des deux pairs, un déni de service a également été envisagé par un attaquant distant utilisant des messages BGP erronés ou faux pour couper une connexion. Étant donné que BGP utilise TCP comme protocole de transport, il est également sujet aux attaques TCP. Ces attaques ne posent pas de vrais risques pour les routeurs individuels, mais deviennent encore plus conséquentes lorsque le cas distribué est considéré [14]. Cependant, ce n'est pas non plus une faiblesse exclusive au bon fonctionnement de BGP, et il existe déjà des contre-mesures DDoS (Distributed Denial of Service) dans le marché, comme CloudFlare [15]. Pourtant, ces contre-mesures ont tendance à ne pas traiter spécifiquement les attaques DDoS causées par l'envoi d'un trop grand nombre de messages BGP.

- **Fréquence des incidents BGP**

Les incidents BGP les plus fréquents sont le détournement de préfixe ou Route Misoriginations et les fuites de route BGP ou Route Leak (se produit lorsqu'une organisation annonce accidentellement à un SP qu'elle dispose d'une route vers une destination via un autre SP, qu'il s'agisse ou non d'un chemin souhaitable). Aujourd’hui les incidents de fuites en BGP ont diminué grâce à l’implémentation des filtres de préfixes IP par la plupart des AS (figure21) [16].

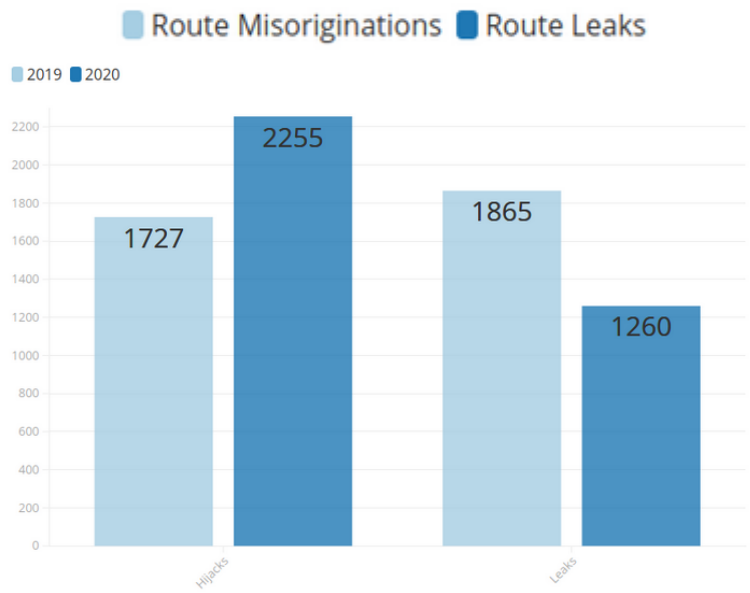


Figure 21 : Comparaison des incidents BGP entre 2019 et 2020

3.2. Solutions proposées

Plusieurs solutions ont été mises en œuvre avec des différents niveaux de protection. Dans cette section on va présenter les techniques cryptographiques utilisées pour améliorer la sécurité en BGP.

3.2.1. Techniques Cryptographies

Parmi les solutions proposées qui se basent sur la cryptographie, est l'infrastructure de ressources à clé publique ou (RPKI), son objectif principal est de fournir un mappage fiable des ensembles de préfixes aux AS. RPKI est un moyen de coupler une plage d'adresses IP à un numéro d'AS par le biais de signatures cryptographiques, décrites dans la RFC 6480 [17]. Les préfixes IP et les numéros AS sont les ressources, l'infrastructure à clé publique est gérée par les cinq registres Internet régionaux (RIR) qui donnent des adresses IP et des numéros AS (ASN), RPKI exploite le système d'infrastructure de certificat/clé publique qui est utilisé pour authentifier et crypter les sessions http, les e-mails, etc. Les RIR émettent ces certificats lorsqu'une ressource est distribuée, chaque RIR utilise un certificat racine auto-signé pour signer les certificats qu'ils délivrent. Les détenteurs de l'espace d'adressage génèrent à leur tour des autorisations d'origine de route, ou ROA (Routing Origin Authorisations) qui associent un préfixe d'adresse à un numéro d'AS, donnant à cet AS l'autorisation de créer le préfixe en question. Lorsque les AS reçoivent de nouvelles informations de routes, la seule chose qu'ils doivent vérifier est si oui ou non l'AS au début de la route est autorisé dans la RPKI à générer ce préfixe. Le titulaire de l'adresse IP signe le ROA avec la clé privée de son certificat (ROA contient également une longueur maximale de préfixe et une date

d'expiration). Par exemple, si AS 100 signe un ROA pour 193.0.0.0/21 avec une longueur de préfixe maximale de /22, alors il est autorisé à provenir 193.0.0.0/21, 193.0.0.0/22 mais pas 193.0.2.0/23. Les certificats et les ROA sont publiés dans des référentiels accessibles au public, où ils peuvent être téléchargés et utilisés pour gérer les listes des préfixes qui peuvent provenir d'un AS. La figure 22 nous montre le taux actuel d'implémentation du RPKI dans le monde, Valid signifie qu'il existe un ROA pour le trafic sous ce préfixe de destination, et les annonces BGP pour celui-ci sont annoncées par l'ASN correct, Unknown signifie qu'aucun ROA n'a été trouvé associé au trafic entrant, Invalid (incorrect numéro d'origine d'AS) signifie que la route choisie n'est pas générée par l'ASN spécifié dans le ROA [18].

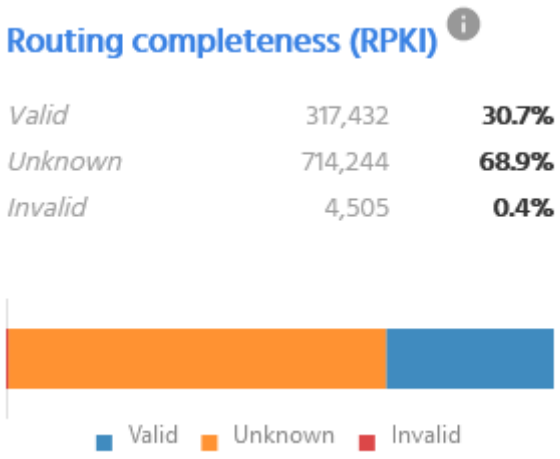


Figure 22 : Le taux d'implémentation du PRKI

3.2.2. Protection de la session BGP entre une paire de routeurs

La protection de la connexion entre deux routeurs parlant BGP repose à la fois sur la protection de la session TCP sous-jacente, et sur la mise en œuvre de défenses qui protègent la session BGP elle-même. Ci-dessous, nous décrivons deux méthodes de protection des communications par paires entre deux voisins BGP.

- **MD5 Intergity**

Le système de mot de passe MD5 est décrit dans la RFC 2385 [19], publiée en 1998. Le mécanisme calcule un hachage cryptographique MD5 sur le « pseudo-en-tête » TCP, qui comprend les adresses IP utilisées, le paquet BGP transporté dans le segment TCP et un mot de passe secret. Le hachage MD5 résultant est ensuite placé dans une option TCP dans l'en-tête TCP et le paquet est envoyé sur son chemin (le mot de passe n'est pas transmis.) L'autre côté effectue le même calcul MD5 et vérifie le résultat par rapport au hachage MD5 dans l'en-tête TCP. Si les deux hachages MD5 sont identiques, nous pouvons être sûrs de deux choses :

- L'expéditeur du paquet connaît également le mot de passe secret.

- Le segment TCP et son contenu n'ont pas été modifiés en transit

Ainsi, si un attaquant envoie des paquets de réinitialisation TCP falsifiés, le hachage MD5 sera manquant ou incorrect, de sorte que le routeur ignore simplement ces paquets et la session BGP ne sera pas affectée [23].

➢ Mécanisme de sécurité TTL généralisé

Le mécanisme de sécurité TTL généralisé ou GTSM (Generelazed TTL Security Mecanism) fournit une méthode pour protéger les pairs BGP contre les attaques à distance. Cette approche part du principe que dans la grande majorité des BGP sessions de voisinages, les deux pairs sont adjacents. L'attribut Time To Live (TTL), défini dans un paquet IP sera décrémenté de 1 à chaque saut. Les routeurs utilisant GTSM initialisent le TTL d'un paquet IP par la valeur maximale 255. Lorsqu'un locuteur BGP reçoit un paquet, il vérifie le la valeur de TTL, si cette valeur est inférieure à 254 (décrémentée d'un), le paquet est marqué ou rejeté tout simplement. Ceci empêche les attaques à distance provenant de plusieurs sauts, car ces paquets auront des TTL inférieurs à la valeur 254 (figure 23) [14].

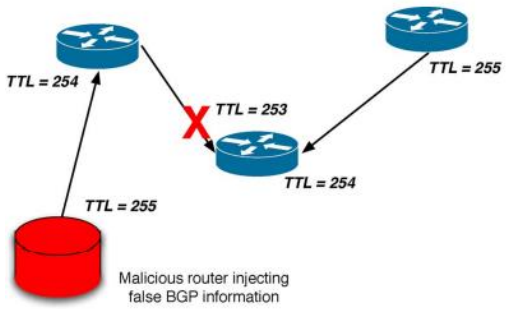


Figure 23 : Mécanisme de sécurité TTL

GTSM est simple, peu coûteux et généralement efficace contre attaquants non avertis. Cependant, l'efficacité de la solution pour atténuer les attaquants motivés est limitée.

3.2.3. Architecture de sécurité basée sur BGPSec

Les solutions précédentes utilisées par les SP pour sécuriser temporairement leur routage inter domaine, sont moins efficaces contre d'autres attaques. Cependant plusieurs architectures de sécurité ont été proposées pour améliorer la sécurité de BGP. Parmi ces solutions BGPSecurity ou (BGPSec), c'est une solution de sécurité qui a été proposée pour la première fois en 2011, lorsque le RPKI était sur le point d'être standardisé pour le compléter (11), elle a été normalisée en 2017 par l'IETF dans la RFC 8205 [20]. Parce que le RPKI ne fournit que l'authentification d'origine, BGPsec est destiné à s'assurer que l'AS-path est bien légitime, lorsque deux routeurs BGP négocient l'utilisation de BGPSec entre eux, ils remplacent

l'attribut AS_PATH dans les mises à jour BGP par un nouvel attribut BGPSec_Path, qui remplit la même fonction, mais désormais en toute sécurité. Avec chaque saut dans le chemin AS maintenant protégé par une signature, un routeur recevant un BGP UPDATE avec un attribut BGPSec_Path peut vérifier si le chemin AS est correct. Supposons que l'AS-path dans la figure 24 soit le suivant : 3 2 1. Le routeur de réception vérifie d'abord la signature de l'AS 1. La signature contient un « Subject Key Identifier » qui fait référence au certificat RPKI du routeur qui a créé la signature, c'est à dire que le routeur de réception utilise ce certificat pour vérifier la signature. Le routeur vérifie également qu'AS1 avait l'intention d'envoyer la mise à jour à AS2, il vérifie ensuite la signature qui a été générée à l'AS2 et s'il avait l'intention d'envoyer la mise à jour à 3, si la signature de l'AS 3 est également vérifiée, le chemin de l'AS est validé et les informations RPKI peuvent être utilisés pour lier les préfixes provenant de l'AS1 à ce chemin.

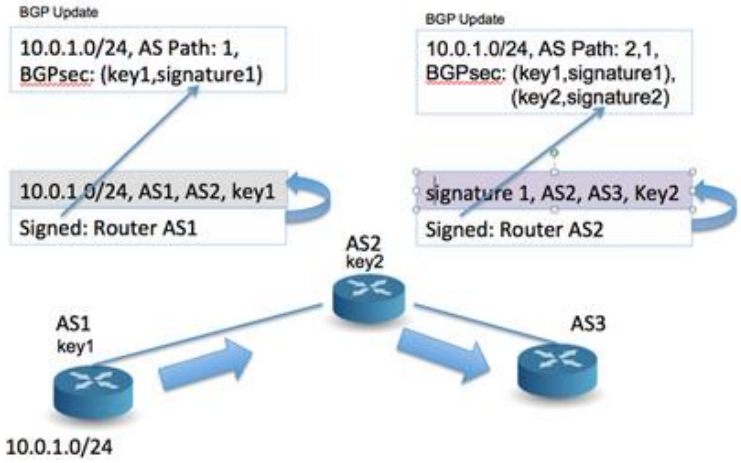


Figure 24 : Protection de chemin avec BGPSec

Cependant, pour que BGPSec fonctionne complètement, il doit y avoir un chemin ininterrompu de routeurs parlant BGPsec entre l'origine d'une mise à jour BGP, et la destination. Lorsqu'un routeur compatible BGPSec communique avec un routeur BGP standard (n'implémente pas BGPSec), il convertit l'attribut BGPSec_Path en un AS_Path standard, en supprimant toutes les informations de sécurité dans le processus.

Conclusion

Dans ce chapitre nous avons examinées les vulnérabilités du protocole BGP. En outre, nous avons différentiées entre les solutions existantes et proposées pour sécuriser ce protocole contre ces failles.

Chapitre 4 : Simulation d’une configuration de BGP

4.1. La modélisation par simulation

Une simulation est un modèle animé qui imite le fonctionnement d'un système existant ou proposé à l'aide d'un logiciel de simulation intuitif. La modélisation par simulation résout les problèmes du monde réel de manière sûre et efficace. Il fournit une méthode d'analyse importante qui est facilement vérifiée, communiquée et comprise en donnant un aperçu clair des systèmes complexes.

➢ Logiciel utilisé

Wireshark : Pour mieux analyser les performances du BGP lorsqu'il est implémenté dans un réseau, nous avons opté à utiliser Wireshark. Le Wireshark est un analyseur de paquets réseau où il peut capturer des données de paquets en direct à partir d'une interface réseau et les afficher avec toutes les informations de protocoles détaillées.

GNS 3 : GNS3 est un logiciel libre et open source qui est utilisé par des centaines de milliers d'ingénieurs réseau dans le monde pour émuler, configurer, tester et dépanner des réseaux virtuels et réels.

VMware Station : VMware Workstation Pro est un hyperviseur hébergé qui s'exécute sur les versions x64 des systèmes d'exploitation Windows et Linux, il permet aux utilisateurs de configurer plusieurs machines virtuelles (VM) sur une seule machine physique et de les utiliser simultanément avec la machine hôte. Chaque machine virtuelle peut exécuter son propre système d'exploitation.

➢ Matériels utilisés

Routeur : un périphérique qui connecte au moins deux réseaux ou sous-réseaux à commutation de paquets. Un routeur fonctionne sur la troisième couche du modèle OSI [2], et il est basé sur l'adresse IP d'une machine. Sa fonction principale est de gérer le trafic entre des réseaux en transférant les paquets de données vers leurs adresses IP prévues.

Switch : un appareil de haut débit qui reçoit les paquets de données entrants et les redirige vers leur destination sur un réseau local (LAN). Un commutateur dans un réseau local basé sur Ethernet lit les paquets/trames de données TCP/IP [22] entrantes contenant des informations de destination lorsqu'ils passent dans un ou plusieurs ports d'entrée. Les informations de destination dans les paquets sont utilisées pour déterminer quels ports de sortie seront utilisés pour envoyer les données vers leur destination prévue. Un commutateur fonctionne au niveau de la deuxième couche du modèle OSI.

Câble Fast Ethernet : Un câble Ethernet est un type courant de câble réseau utilisé avec les réseaux câblés. Les câbles Fast Ethernet connectent des périphériques tels que des PC, des routeurs et des commutateurs au sein d'un réseau local, implémentation de Fast Ethernet se fait au niveau de la couche physique, et son débit varie jusqu'à 100 Mbit/s.

4.2. Implémentation de la topologie réalisée

Pour étudier le fonctionnement du protocole BGP, une étude de cas a été mise en pratique (figure 25). Dans cette implémentation nous configurons une session eBGP dans les routeurs de bord de chaque AS, nous manipulons le trafic entrant et sortant de chaque AS, nous configurons une IGP à l'intérieur de chaque AS, nous configurons un maillage complet à l'intérieur d'AS 200 en utilisant le réflecteur de route. Enfin on test la connectivité entre toutes les AS.

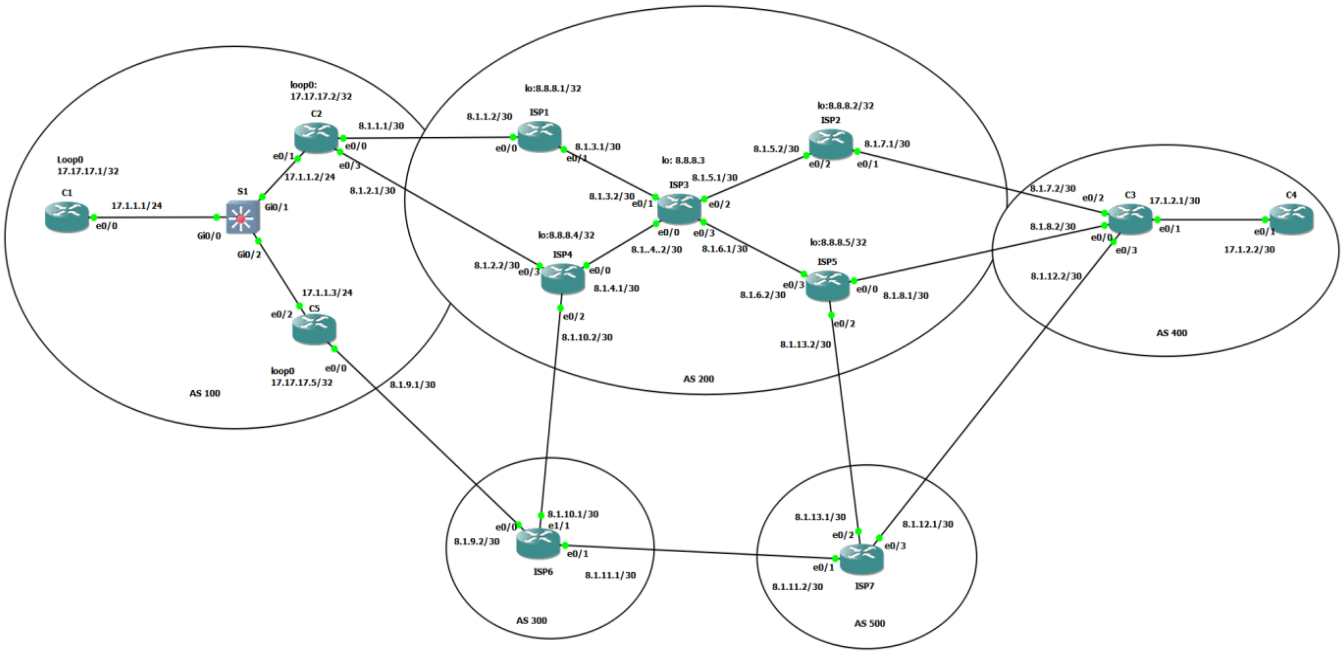


Figure 25 : topologie réalisée

Les tâches de cette implémentation sont comme suit :

- Configuration basique de toutes les machines.
- Configuration BGP sur C1 et d'un maillage complet en AS 200 en utilisant un réflecteur de route.
- Annonce d'une route par défaut vers C1 à partir de C2 et C5 en utilisant BGP.
- AS 100 devrait préférer envoyer le trafic hors-bande comme suit :
    - ISP 6 (primary) (figure 26), puis ISP1 (back-up) et ISP4 (secondary back-up).

- Le trafic vers AS 100 doit être envoyé depuis ISP6 en tant que principal.

- AS 200 doit préférer d'envoyer le trafic à travers ISP5 principalement avec ISP2 comme (primary back-up) et ISP7 (secondary back-up).
- Le trafic à AS 200 doit être envoyé depuis ISP5 comme principal périphérique entrant en utilisant l'attribut MED.

On fait un ping entre les AS clients, du routeur C1 au routeur C4 (figure 26). On remarque que la connectivité a été bien aboutie et le chemin configuré est bien respecté.

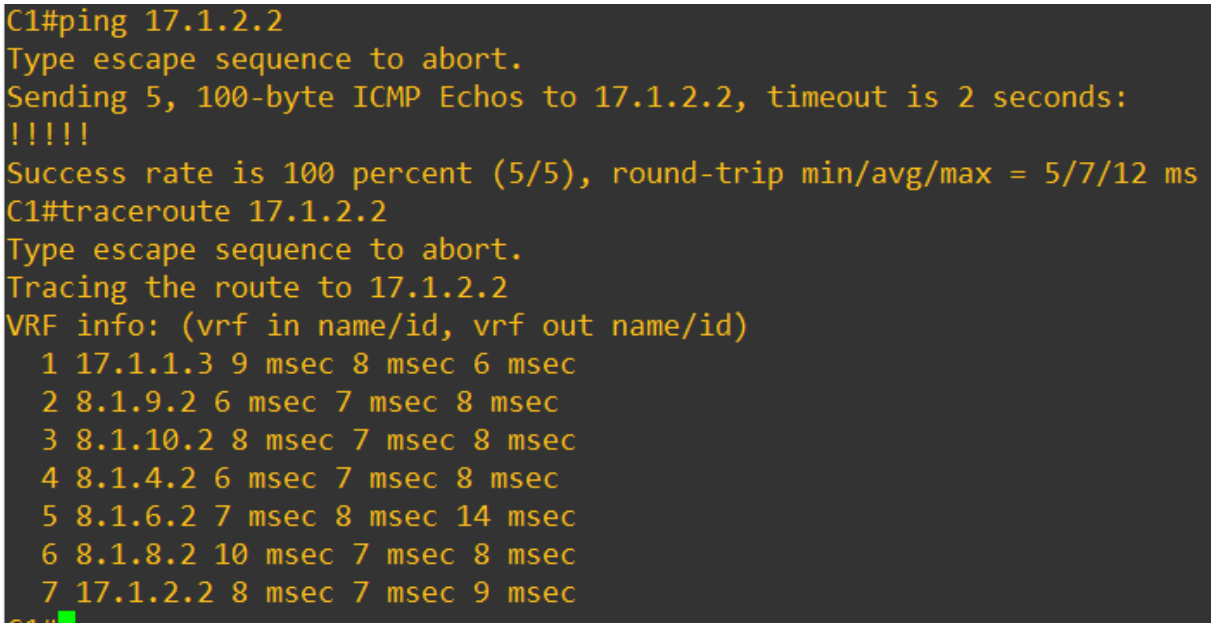


Figure 26 : Ping du routeur C1 vers C4

On fait un ping à l'inverse entre les AS clients du routeur C4 au routeur C1 (figure 27). Le ping est validé et le chemin parcouru est celui demandée.

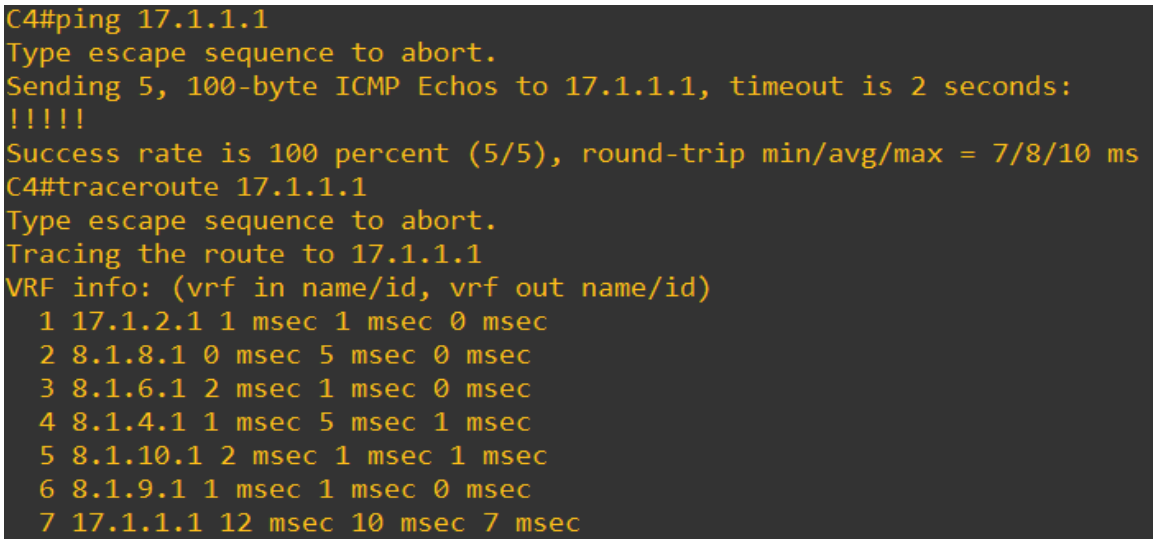


Figure 27 : Ping du routeur C4 vers C1

➢ Analyse des paquets BGP

Juste après la configuration de la relation de voisinage BGP entre les routeurs de bord C5 et ISP6, un message OPEN est échangé entre les deux routeurs pour établir une session BGP (figure 28).

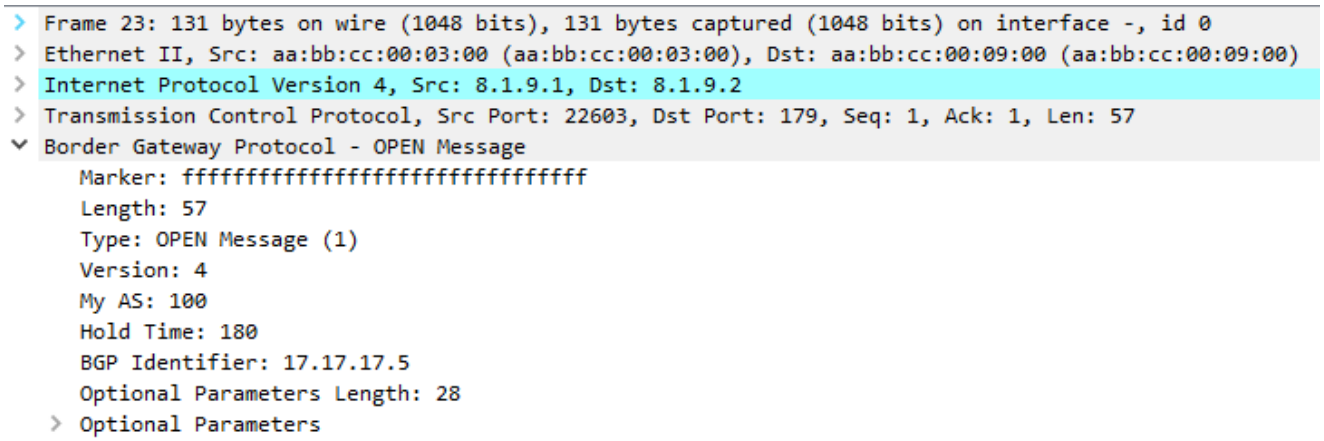


Figure 28 : Message OPEN

Ensuite, Un message KEEP ALIVE est échangé pour s'assurer que les deux voisins sont toujours en vie (figure 29).

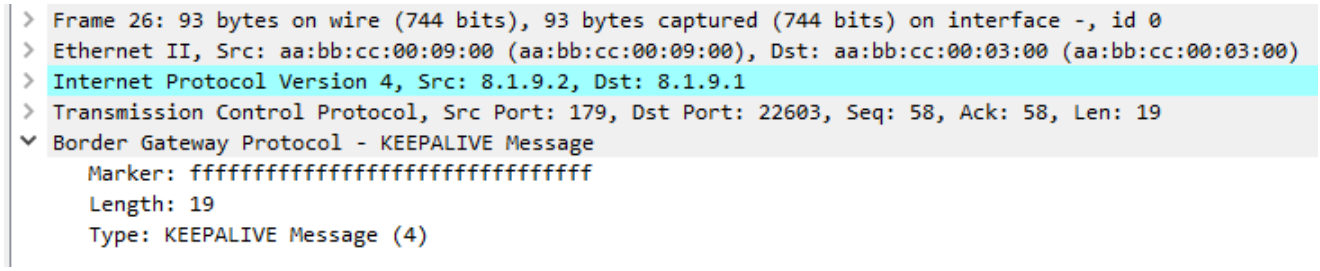


Figure 29 : message KEEP ALIVE

Une fois que la session BGP est établie, un message UPDATE (en spécifiant les différents attributs associés à chaque préfixe) est généré pour échanger les routes possibles, retirer les routes précédemment annoncées (figure 30).

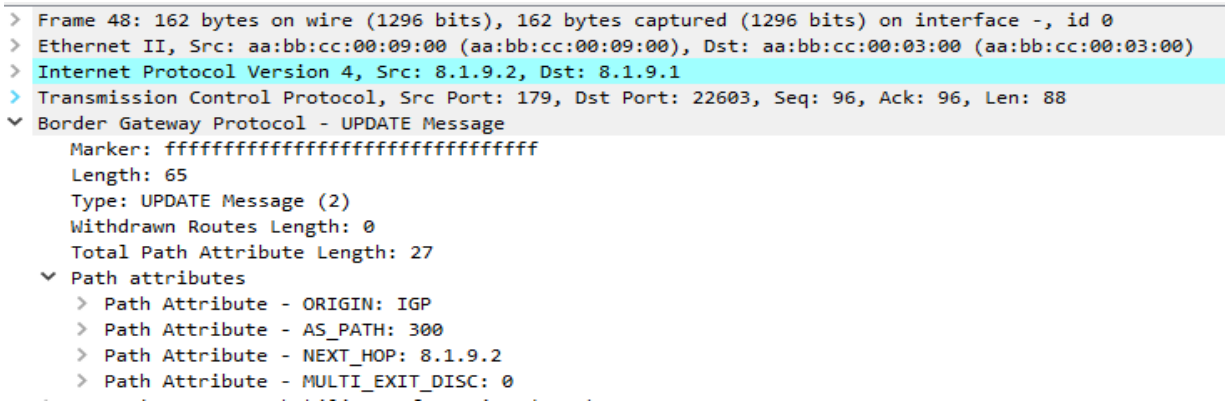


Figure 30 : message UPDATE

Lorsqu'on éteint le routeur C5, un message NOTIFICATION sera automatiquement généré et annoncera au voisin ISP6 que la session BGP entre les deux routeurs est terminée (figure 31).

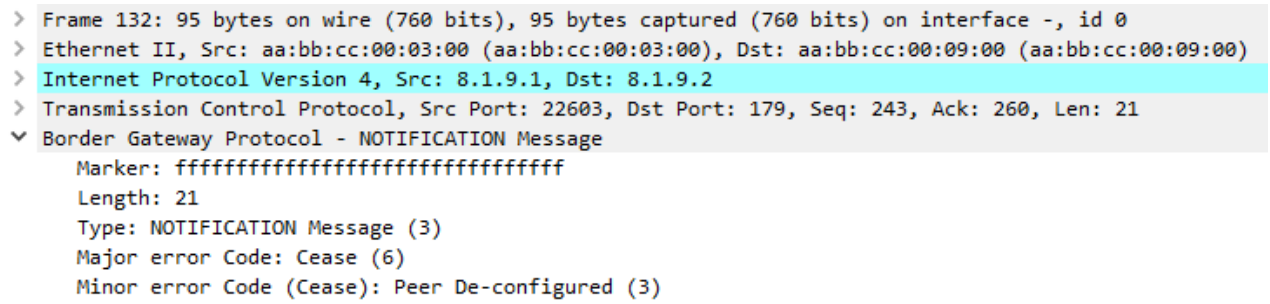


Figure 31 : Message NOTIFICATION

4.3. Implémentation de la sécurité pour la topologie réalisée

➢ MD5

L'authentification des voisins BGP étant une technique symétrique, elle doit être activée des deux côtés de la session d'appairage en même temps, l'authentification des voisins à l'aide de MD5 crée un hachage MD5 pour chaque paquet envoyé dans une session BGP.

Par défaut, l'option MD5 n'est pas activée dans un routeur BGP (figure 32).

Figure 32 : MD5 n'est pas activée dans un routeur BGP

Lorsqu'on configure le MD5 uniquement dans le routeur ISP6 (figure 33), une série de message de notification sera générée automatiquement indiquent que le routeur voisin C5 n'a pas encore configuré le MD5, dans ce moment la session BGP est dans l'état idle.

Figure 33 : MD5 est activée uniquement d'un côté de la session BGP

Une fois que les deux routeurs voisins ont configuré le même mot de passe MD5, l'option MD5 est activée dans les deux routeurs (figure 34), la session BGP devient établie et les deux voisins peuvent échanger les routes ente eux.

Figure 34 : MD5 est activée dans les deux voisins BGP

- **GTSM**

Puisque les deux voisins C5 et IPS6 ont une session eBGP direct, la valeur par défaut du TLL associé égale à 1(figure 35).

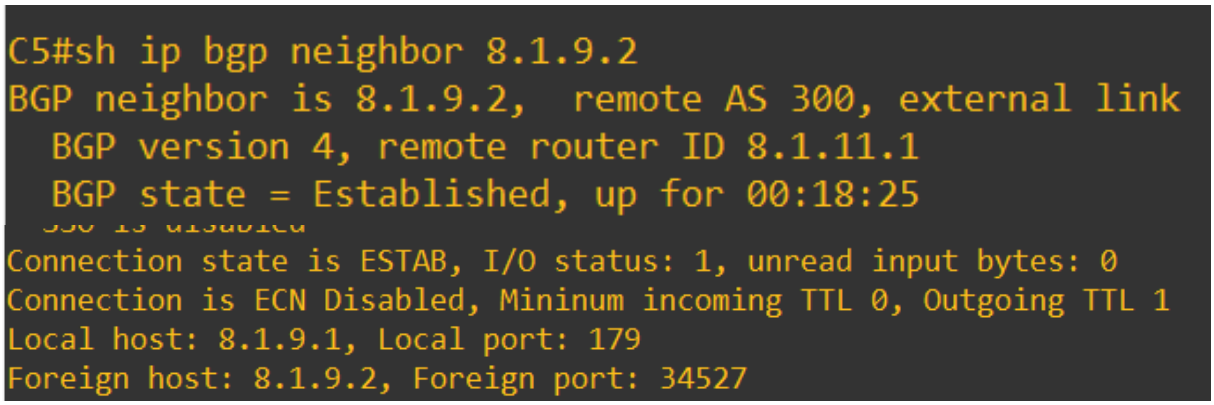


Figure 35 : TTL Security n'est pas activée

En activant l'option de GTSM dans les deux routeurs C5 et ISP6, ils négocient que la session BGP ne peut pas être de type multihop, mais plutôt directement connecté.

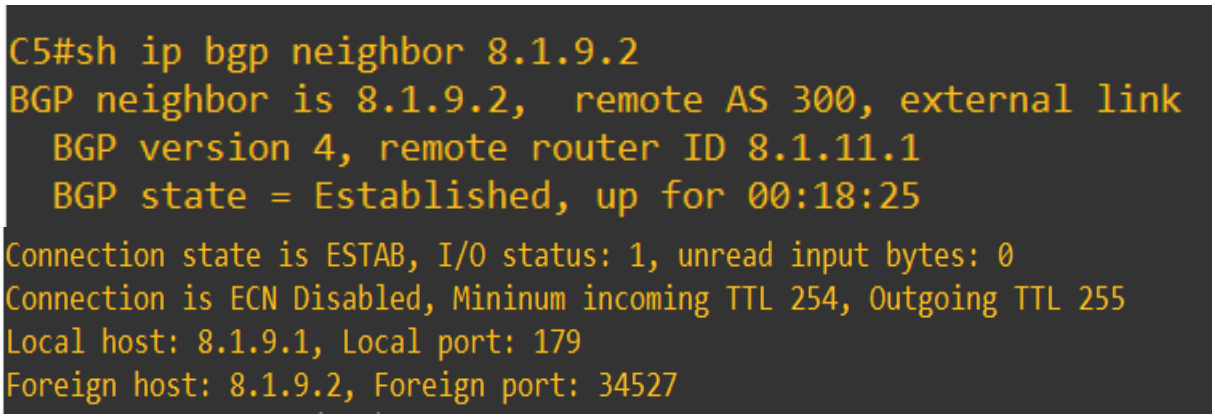


Figure 36 : GTSM est activée

Conclusion générale

Personne ne peut nier que le protocole BGP réussit à fournir un routage interdomaine stable et robuste, ainsi que le contrôle du trafic. Cependant, il est vulnérable aux interruptions et aux pannes de communication. Dans ce PFE, nous avons débuté le fonctionnement du protocole BGP par un aperçu détaillé de ce dernier, suivi par les différents états d'établissement d'une session BGP. De plus on a expliqué le processus utilisés par le BGP pour sélectionner le meilleur chemin. Enfin nous avons examiné les différentes menaces de sécurité contre ce protocole, en analysant certaines solutions proposées pour améliorer la sécurité en BGP. Néanmoins, le développement de la sécurité en BGP rendra l'Internet plus fiable et utile pour la communication entre les domaines de l'Internet.

Annexe 1

Configuration de la topologie (sans sécurité) :

- **Router C1**

C1#sh run

interface Loopback0

ip address 17.17.17.1 255.255.255.255

interface Ethernet0/0

ip address 17.1.1.1 255.255.255.0

router bgp 100

neighbor 17.17.17.2 remote-as 100

neighbor 17.17.17.2 update-source Loopback0

neighbor 17.17.17.5 remote-as 100

neighbor 17.17.17.5 update-source Loopback0

- **Router C5**

C5#sh run

interface Loopback0

ip address 17.17.17.5 255.255.255.255

interface Ethernet0/0

ip address 8.1.9.1 255.255.255.252

network 17.1.1.0 mask 255.255.255.0

neighbor 8.1.9.2 remote-as 300

neighbor 8.1.9.2 route-map set-local-pref in

neighbor 8.1.9.2 route-map onlypermitlocal out

neighbor 17.17.17.1 remote-as 100

neighbor 17.17.17.1 update-source Loopback0

neighbor 17.17.17.1 next-hop-self

neighbor 17.17.17.1 default-originate route-map set-default

neighbor 17.17.17.1 prefix-list default-route out

neighbor 17.17.17.2 remote-as 100

neighbor 17.17.17.2 update-source Loopback0

neighbor 17.17.17.2 next-hop-self

- **Router C2**

C2#sh run

interface Loopback0

ip address 17.17.17.2 255.255.255.255

interface Ethernet0/0

ip address 8.1.1.1 255.255.255.252

interface Ethernet0/1

ip address 17.1.1.2 255.255.255.0

network 17.1.1.0 mask 255.255.255.0

neighbor 8.1.1.2 remote-as 200

neighbor 8.1.1.2 route-map set-local-pref180 in

neighbor 8.1.1.2 route-map as-prepend out

neighbor 8.1.2.2 remote-as 200

neighbor 8.1.2.2 route-map set-local-pref150 in

neighbor 8.1.2.2 route-map as-prepend out

neighbor 17.17.17.1 remote-as 100

neighbor 17.17.17.1 update-source Loopback0

neighbor 17.17.17.1 next-hop-self

neighbor 17.17.17.1 default-originate

neighbor 17.17.17.1 prefix-list default-route out

neighbor 17.17.17.5 remote-as 100

neighbor 17.17.17.5 update-source Loopback0

neighbor 17.17.17.5 next-hop-self

- **Router C3**

C3#sh run

interface Ethernet0/0

ip address 8.1.8.2 255.255.255.252

interface Ethernet0/1

ip address 17.1.2.1 255.255.255.252

interface Ethernet0/2

ip address 8.1.7.2 255.255.255.252

interface Ethernet0/3

ip address 8.1.12.2 255.255.255.252

router bgp 400

network 17.1.2.0 mask 255.255.255.252

neighbor 8.1.7.1 remote-as 200

neighbor 8.1.7.1 weight 180

neighbor 8.1.7.1 route-map set-med-200 out

neighbor 8.1.8.1 remote-as 200

neighbor 8.1.8.1 weight 200

neighbor 8.1.8.1 route-map set-med-100 out

neighbor 8.1.12.1 remote-as 500

neighbor 8.1.12.1 weight 150

neighbor 8.1.12.1 route-map as-path-prepend out

- **ISP6**

ISP6#sh run

interface Ethernet0/0

ip address 8.1.9.2 255.255.255.252

interface Ethernet0/1

ip address 8.1.11.1 255.255.255.252

router bgp 300

network 8.1.9.0 mask 255.255.255.252

network 8.1.10.0 mask 255.255.255.252

network 8.1.11.0 mask 255.255.255.252

neighbor 8.1.9.1 remote-as 100

neighbor 8.1.10.2 remote-as 200

neighbor 8.1.11.2 remote-as 500

route-map set-default permit 10

set local-preference 200

- **ISP3**

ISP3#sh run

interface Loopback0

ip address 8.8.8.3 255.255.255.255

interface Ethernet0/0

ip address 8.1.4.2 255.255.255.252

```
interface Ethernet0/1
 ip address 8.1.3.2 255.255.255.252
interface Ethernet0/2
 ip address 8.1.5.1 255.255.255.252
interface Ethernet0/3
 ip address 8.1.6.1 255.255.255.252
router bgp 200
network 8.1.3.0 mask 255.255.255.252
 network 8.1.4.0 mask 255.255.255.252
 network 8.1.5.0 mask 255.255.255.252
 network 8.1.6.0 mask 255.255.255.252
 network 8.8.8.3 mask 255.255.255.255
 redistribute connected
 neighbor 8.8.8.1 remote-as 200
 neighbor 8.8.8.1 update-source Loopback0
 neighbor 8.8.8.1 route-reflector-client
 neighbor 8.8.8.2 remote-as 200
 neighbor 8.8.8.2 update-source Loopback0
 neighbor 8.8.8.2 route-reflector-client
 neighbor 8.8.8.4 remote-as 200
 neighbor 8.8.8.4 update-source Loopback0
 neighbor 8.8.8.4 route-reflector-client
 neighbor 8.8.8.5 remote-as 200
 neighbor 8.8.8.5 update-source Loopback0
```

```
neighbor 8.8.8.5 route-reflector-client
```

Annexe 2

Configuration de la sécurité en BGP

- ✓ **Configuration du MD5**

➢ Router C5

C5#sh run

router bgp 100

neighbor 8.1.9.2 password axcv123

➢ ISP6

ISP6#sh run

router bgp 300

neighbor 8.1.9.1 password axcv123

- ✓ **configuration du GTSM**

➢ ISP6

ISP6#sh run

router bgp 300

neighbor 8.1.10.2 ttl-security hops 1

➢ ISP4

ISP4#sh run

interface Loopback0

ip address 8.8.8.4 255.255.255.255

interface Ethernet0/0

ip address 8.1.4.1 255.255.255.252

interface Ethernet0/2

ip address 8.1.10.2 255.255.255.252

interface Ethernet0/3

```
 ip address 8.1.2.2 255.255.255.252
router bgp 200
network 8.1.2.0 mask 255.255.255.252
 network 8.1.4.0 mask 255.255.255.252
 network 8.1.10.0 mask 255.255.255.252
 network 8.8.8.4 mask 255.255.255.255
 neighbor 8.1.2.1 remote-as 100
 neighbor 8.1.10.1 remote-as 300
neighbor 8.1.10.1 ttl-security hops 1
 neighbor 8.8.8.3 remote-as 200
 neighbor 8.8.8.3 update-source Loopback0
```

Webographie

[1] Présentation de la RADEEF. http://www.radeef.ma/Accueil/Pr%C3%A9sentationetactivit%C3%A9s/Pr%C3%A9sentation/Pr%C3%A9sentationg%C3%A9n%C3%A9rale.aspx.

[2] Fonctionnement du BGP. https://www.techniques-ingenieur.fr/base-documentaire/technologies-de-l-information-th9 /reseau-internet-protocoles-multicast-routage-mpls-et-mobilite-42289210/protocole-de-routage-bgp-evolution-et-extensions-te7528/conclusion-te7528niv10005.html.

[3] Etats finis du BGP. https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=4.

[4] Session eBGP direct. https://www.cisco.com/c/fr_ca/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html#ebgpibgp.

[5] Session iBGP. https://www.exam4training.com/assuming-the-ibgp-session-within-as-64500-was-established-using-the-loopback-0-interface-between-the-two-routers-by-default-what-will-be-the-next-hop-of-the-routes-from-as-64501-when-the-routes-appe-2/.

[6] La métrique du BGP. https://www.networklab.fr/la-metrique-de-bgp/.

[7] Liste des attributs de BGP. http://www.ittc.ku.edu/EECS/EECS_800.ira/bgp_tutorial/14.html.

[8] BGP sélection du meilleur chemin. https://networklessons.com/bgp/bgp-attributes-and-path-selection.

[9] Réflecteur de route dans iBGP. https://ipcisco.com/lesson/bgp-route-reflector/.

[10] Filtrage de route en BGP .https://www.cisco.com/c/fr_ca/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html.

[11] Détournement de routes BGP. https://www.manrs.org/2020/09/what-is-bgp-prefix-hijacking-part-1/.

[12] Exemple de détournement de route. https://www.cise.ufl.edu/~butler/pubs/bgpsurvey.pdf.

[13] Misconfiguration dans BGP. https://conferences.sigcomm.org/sigcomm/2002/papers/bgpmisconfig.pdf.

[14] Attaque déni de service. https://www.researchgate.net/publication/224092573_A_Survey_of_BGP_Security_Issues_and_Solutions.

[15] CloudFlare. https://www.cloudflare.com.

[16] Incidents BGP. https://www.manrs.org/2021/02/bgp-rpki-and-manrs-2020-in-review/.

[17] Rfc6480, https://datatracker.ietf.org/doc/html/rfc6480.

[18] Taux d'implémentation de RPKI, https://observatory.manrs.org/#/overview.

[19] Rfc2385, https://datatracker.ietf.org/doc/html/rfc2385.

[20] Rfc8205, https://datatracker.ietf.org/doc/html/rfc8205.

[21] Modèle OSI, https://www.frameip.com/osi/.

[22] Modèle TCP/IP, https://www.frameip.com/tcpip/.

[23] BGP MD5 password, https://www.noction.com/blog/bgp-security-md5-password-gtsm.