VPN BGP-MPLS

VPN

Virtual **P**rivate **N**etworks

Objectifs des VPN

- interconnecter équipements à travers réseau tiers (FAI, …)
  - raisons économiques,
    - partage d' une infrastructure longue distance
    - coût du personnel et de la maintenance, …
  - mobilité (personnel à domicile, commerciaux, …)
- garder caractéristiques réseau privé
  - sécurité
  - Maîtrise/indépendance routage, adressage, gestion

Types de VPN

- 1) implanté par qui ?
  - équipement client (CPE : Customer Premise Equipment)
    - ex : tunnels IPsec, GRE, L2TP,
      - pas de multicast, transparent opérateur
      - configuration client : autant de tunnel que site ?
  - équipement opérateur
    - ex : VPN « RFC 2547 » (BGP-MPLS)
      - service offert par l' opérateur
- 2) implanté à quel niveau ?
  - niveau 3 (IP)
  - « niveau 2 » (ATM, Frame Relay)
  - niveau 2 sur niveau 3 (VPLS: trames sur IP)

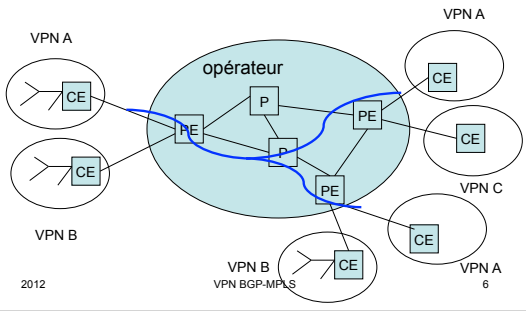
VPN type « RFC2547 »

- Service fourni par l'opérateur (PE)
- pas ou peu de configuration chez client
- transparence espace adressage client
- accès possible du VPN à Internet
- extensible
  - taille VPN
    - choix routage interne au VPN : étoile,mesh, …
  - nombre VPN
  - Multi-opérateurs ?

Termes/Modèle

- CE : Customer Equipment
  - routeur simple (routage intra par exemple)
- PE : Provider Equipment
  - routeur BGP/MPLS/RFC2547
- P : Equipement interne du Provider
  - routeur MPLS (LSR)
- VRF Virtual Routing and Forwarding
  - RIB et FIB « virtuelle » pour un VPN

Architecture



Principes

- PE
  - plusieurs tables de routage virtuelles (VRF)
  - 1 par VPN
- trafic des VPN entre PE encapsulé via MPLS
- informations de routage d'un VPN transmises via BGP
- 2 niveaux de label
  - fond de pile identifie VPN (ou VRF ou même route) : sémantique bout en bout
  - sommet de pile : LSP entre 2 PE

Routage : Extensions BGP

1) nouvelle famille d'adresse : VPN IPv4
   AFI=1 (IPv4), SAFI=128
   - Format : <RD> <Adresse IPv4>
   - **R**oute **D**istinguisher 8 octets
   - <type field> <value field> ex :
     - Type 0 <ASN> <Sous-numéro>
       ASN du provider, 2 octets
       sous numéro repère le VPN (géré par cet AS), 4 octets
     - Type 1 <IP address> <sous-numéro>
       IP adresse publique (4 octets)
       sous-numéro géré par propriétaire adresse (2 octets)

Routage : Extensions BGP

     - Type 2 <ASN> <Sous-numéro>
       idem type 0 mais ASN sur 4 octets
   - deux préfixes de 2 VPN différents
     - => RD différents (provider identique ou différent)
- => adresses IPv4 réutilisables (RD différents)
  Adresses privées 10.0.0.0/8, …
- Remarque : d'après le RFC 4364, les adresses des PE (next hop) doivent être encapsulées dans des adresses IP4 VPN avec RD = 0

Extensions BGP (2)

2) Nouvel attribut « label VPN » de type Label
3) Nouvel attribut « route target »
- de type « extended communities » (RFC 4360)
- une VRF a une liste d'import et d'export
- contrôle de la topologie du VPN
  - route marquée route Target RT1
    - = EC RT1
  - utilisée entre PE1 et PE2
  - <=> PE1 exporte RT1 et PE2 importe RT1

Topologie et Route Target

Topologie Mesh (maillage complet)
- une seule communauté
  - tout VRF importe et exporte cette communauté
  - équivalent Full Mesh iBGP
- + court chemin dans le réseau opérateur

Topologie et Route Target

Topologie Hub (étoile)
- 2 communautés HI et HO
  - Hub importe HI et exporte HO
  - Stubs importent HO et exportent HI
  - Entre 2 stubs, 1 saut via hub en plus
- permet de centraliser politique au Hub
  - redistribution entre sites du VPN, vers Internet

Exemple annonce

- Hypothèses
  - VPN V1 associé à RD1
  - VRF1 est un « stub » pour VPN V1
    - exporte vers HI, importe de HO
  - VRF2 est un « hub » pour VPN V1
    - exporte vers HO, importe de HI
  - VRF3 est un « stub » :
    - exporte vers HI, importe de HO

Exemple annonce

- PE1 (VRF1)
  - apprend préfixe P du VPN V1 (CE1) (via routage CE)
  - PE1 choisit label L1 (associé à VRF1 ou int)
  - PE1 annonce
    <RD1, P> <RT=HI> <L1>
    NRLI et 2 attributs : Route Target et label
- PE2(VRF2) accepte annonce
  - importe HI
  - place <RD1, P> dans sa table
  - annonce <RD1, P> <HO> <L2>

Annonce (suite)

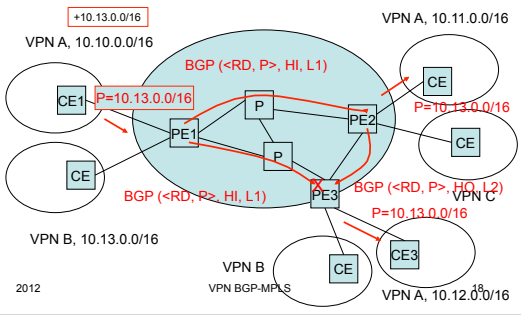
- PE3(VRF3>
  - refuse (ignore) 1ère annonce
    - car n' importe pas HI
  - accepte 2ème annonce
    - car importe HO
- Route de VRF3 vers P passe par VRF2 (hub)
  - utilisera LSP L2 vers VRF2 puis L1 vers VRF1

Label

- Choix du label : plusieurs possibilités
  1) un label par VRF Egress
     - => nécessite lookup (de P) à l'arrivée VRF
  2) un label par interface de sortie (~ FEC)
     évite tout lookup en réception
     sauf éventuellement pour link layer (ARP)
  3) un label par route (permet QoS)
  Remarque :
     un label par PE ne serait pas suffisant
     même adresse IP destination dans +sieurs VPN

Construction LSP

- VRF (PE2)
  - accepte <RD, P> <RT> <L> de PE1
  - LDP demande LSP vers PE1 (si aucun) :
    - Label Request FEC = PE1
    - nécessite route vers PE1 (/32)
  - un seul LSP vers PE pour
    - plusieurs préfixes même VRF
    - plusieurs VRF même PE



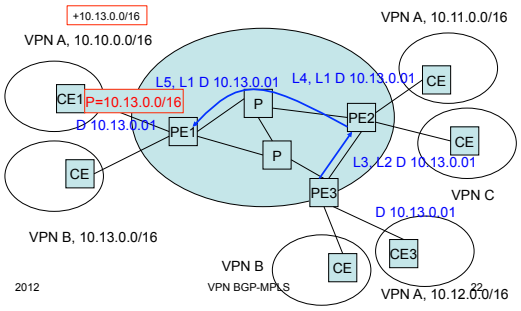
- +10.13.0.0/16

Données : Exemple (1)

– CE3 reçoit paquet pour 10.13.0.1
  – envoie à PE3 (ex : route par défaut vers VPN)
– PE3 reçoit paquet par interface IntA
  - VPN A => VRF3A
  - VRF3A : lookup 10.13.0.0/16 associé L2, PE2
    – PUSH L2, puis
    – PUSH L3 (label LSP) (MPLS « normal » FEC PE2)
    – émission

Données : Exemple (2)

– PE2 reçoit paquet, POP
  – L2 : vers VRF2A (POP de L2)
  – lookup table, PUSH L1, PUSH L4 (label LSP vers PE1)
– PE1 reçoit paquet, POP
  – L1 : vers VRF1 (et POP L1)
  – lookup table VRF1 : envoyé vers Int A (vers CE1)



Remarques

- Dans le réseau MPLS
  - une route /32 par PE (indépendant routes externes)
  - un LSP par PE (indépendant # VPN)
  - labels de fonds de pile
    - uniques pour un PE => pas de problème d'allocation
- => système extensible à grande échelle
- Création VPN
  - définir Route Distinguisher (provider) pour VPN
  - définir politique routage (Hub, mesh, …) et les RT

Remarques (2)

- Connexion nouveau site client
  - créer VRF si nouveau VPN et associer Int.
  - configurer politique import/extport
    - route-map sur les Route-Target
    - en général seulement sur 1 seul PE
  - configurer routage avec CE via interface
- Routage entre CE et PE
  - plusieurs possibilités
    - routes statiques (ex : pas de routeur CE)
    - IGP (ex OSPF) (une instance par VRF)
    - eBGP

Remarques (3)

- Extension multi-providers possible
- Fonctionnalités sur divers matériels
  - Cisco, Juniper, Alcatel, …
- Proposé par plusieurs providers

- Première version
  - RFC2547 (informationnel) mars 99
  - « RFC2547bis » publié comme RFC 4364 en février 2006

biblio

- RFC 2547 BGP/MPLS VPNs, mars 1999
  remplacé par
- RFC 4364 - BGP/MPLS IP Virtual Private Networks (VPNs), février 2006
- RFC 4360 BGP Extended Communities Attribute, février 2006
- RFC 2784 : encapsulation GRE mars 2000
- RFC 4023 GRE pour MPLS mars 2005