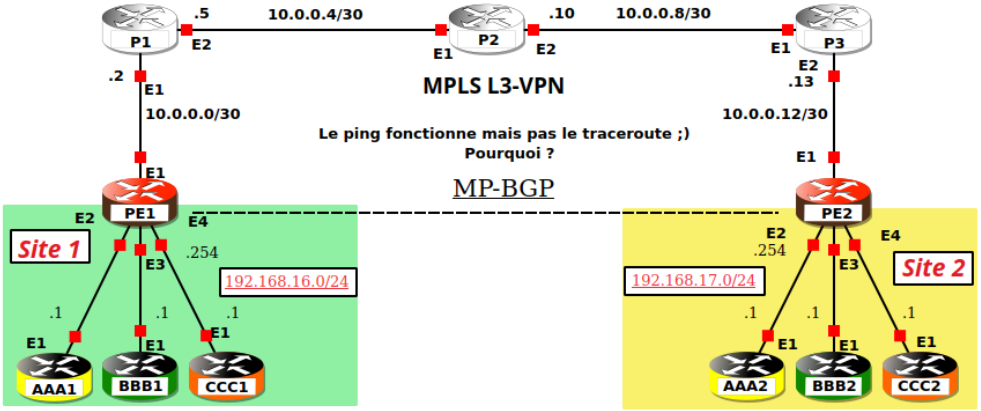
UNIVERSITÉ CAEN NORMANDIE

TP-L3VPN

20.03.2023

Tous en @IP privées ☺

Auteur : Pascal Fougeray



Source : Moi ☺

---

1 Introduction

Dans ce TP, je vous propose de voir comment des sites éloignés géographiquement en @IP privées peuvent communiquer au travers le WAN...

ou comment faire **que l'ISP économise les @IP publiques !**

2 La structure

Elle représente 3 entreprises nommées AAA, BBB et CCC. Oui je sais mais Casto, Leroy et Brico n'ont pas voulu me sponsoriser ☺

Les 3 routeurs de chaque côté sont des CE connectés à un PE d'une grande ville.

On a une entreprise qui a 2 sites. Il serait facile d'en ajouter un 3ième puis un 4ième etc ...

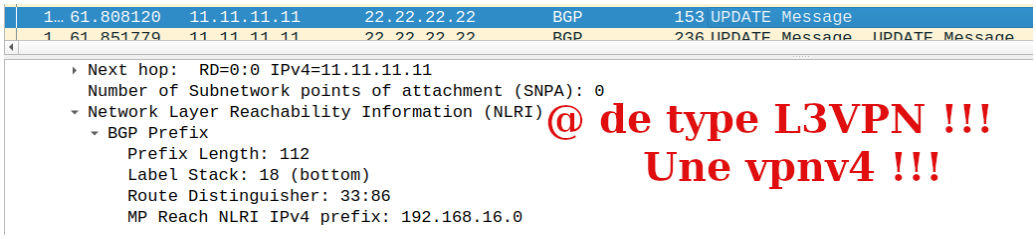
3 Les technologies utilisées

1. Le routage avec OSPF qui ne doit plus vous poser de souci. Nous n'avons qu'une seule aire, aucun intérêt de complexifier le système.
2. Le switching avec MPLS qui ne doit pas vous poser de souci non plus car on s'en moque, ça ne tombera pas au CT ! ! !
3. Le "routage" qui n'est pas un routage au sens de routes de type IP mais de routes de type L3VPN, des **VPN-IPv4**
4. Les VRF ou routeurs virtuels ayant chacun leur table de routage.

À la fin de ce TP vous devrez me donner un modèle logique de la structure physique utilisée durant ce TP.

4 TP

1. **Allumez** tous les routeurs.
2. **Mettez** une sonde wireshark entre **PE1** et **PE2** et **sélectionnez BGP**
3. **Expliquez** cette ligne de configuration sur les 2 PE
   Sur PE1
   /routing bgp peer add address-families=vpnv4 name=PE2 remote-address=22.22.22.22 remote-as=1664 update-source=lo0
   Sur PE2
   /routing bgp peer add address-families=vpnv4 name=PE1 remote-address=11.11.11.11 remote-as=1664 update-source=lo0
   Quel type d'@ s'échange en BGP les 2 PE ?
4. **Relevez** le *PATH Attribute - MP_REACH_NLRI*. Que contient-il ?



5. Pourquoi un ***ip route print*** sur P1 et/ou P2 et/ou P3 ne renvoie aucune route de type 192.168.16.0/24 ou 192.168.17.0/24 ?

```
[admin@P2] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADo  1.1.1.1/32                         10.0.0.5                110
 1 ADC  2.2.2.2/32         2.2.2.2         lo0                       0
 2 ADo  3.3.3.3/32                         10.0.0.10               110
 3 ADo  10.0.0.0/30                        10.0.0.5                110
 4 ADC  10.0.0.4/30        10.0.0.6        ether1                    0
 5 ADC  10.0.0.8/30        10.0.0.9        ether2                    0
 6 ADo  10.0.0.12/30                       10.0.0.10               110
 7 ADo  11.11.11.11/32                     10.0.0.5                110
 8 ADo  22.22.22.22/32                     10.0.0.10               110
[admin@P2] >
```

   Réponse les routeurs P1, P2 et P3 ne font pas ici du routage quand le paquet vient des CE pour aller aux autres C2. Ils font du switching de label

6. **Relevez** les @IP des interfaces E2, E3 et E4 des 2 PE. Pourquoi est-ce cela ?
   Réponse : on a 3 VRF, 3 routeurs virtuels avec chacun sa table de routage

7. Comment PE1 peut pinguer un CE, sachant qu'ils ont tous la même @IP privée !
   Si vous lancez la commande ***ping 192.168.16.1*** sur PE1

```
[admin@PE1] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADC  192.168.16.0/24    192.168.16.254  ether3                    0
 1 ADb  192.168.17.0/24                    22.22.22.22             200
 2 ADC  192.168.16.0/24    192.168.16.254  ether4                    0
 3 ADb  192.168.17.0/24                    22.22.22.22             200
 4 ADC  192.168.16.0/24    192.168.16.254  ether2                    0
 5 ADb  192.168.17.0/24                    22.22.22.22             200
 6 ADo  1.1.1.1/32                         10.0.0.2                110
 7 ADo  2.2.2.2/32                         10.0.0.2                110
 8 ADo  3.3.3.3/32                         10.0.0.2                110
 9 ADC  10.0.0.0/30        10.0.0.1        ether1                    0
10 ADo  10.0.0.4/30                        10.0.0.2                110
11 ADo  10.0.0.8/30                        10.0.0.2                110
12 ADo  10.0.0.12/30                       10.0.0.2                110
13 ADC  11.11.11.11/32    11.11.11.11     lo0                       0
14 ADo  22.22.22.22/32                     10.0.0.2                110
[admin@PE1] >
```

```
[admin@PE2] > /ip route print
Flags:   - disabled,   - active,   - dynamic,
  - connect,   - static,   - rip,   - bgp,   - ospf,   - mme,
  - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADb  192.168.16.0/24                    11.11.11.11             200
 1 ADC  192.168.17.0/24    192.168.17.254  ether3                    0
 2 ADb  192.168.16.0/24                    11.11.11.11             200
 3 ADC  192.168.17.0/24    192.168.17.254  ether4                    0
 4 ADb  192.168.16.0/24                    11.11.11.11             200
 5 ADC  192.168.17.0/24    192.168.17.254  ether2                    0
 6 ADo  1.1.1.1/32                         10.0.0.13               110
 7 ADo  2.2.2.2/32                         10.0.0.13               110
 8 ADo  3.3.3.3/32                         10.0.0.13               110
 9 ADo  10.0.0.0/30                        10.0.0.13               110
10 ADo  10.0.0.4/30                        10.0.0.13               110
11 ADo  10.0.0.8/30                        10.0.0.13               110
12 ADC  10.0.0.12/30      10.0.0.14       ether1                    0
13 ADo  11.11.11.11/32                    10.0.0.13               110
14 ADC  22.22.22.22/32    22.22.22.22     lo0                       0
[admin@PE2] >
```

```
[admin@PE1] > ping 192.168.16.1

    0                                                    no route to host
    1                                                    no route to host
    sent=2 received=0 packet-loss=100%

[admin@PE1] > ping 192.168.16.1
arp-ping  do-not-fragment  interface  routing-table  src-address
count     dscp             interval   size           ttl
[admin@PE1] > ping 192.168.16.1 routing-table=
AAA  BBB  CCC  main
[admin@PE1] > ping 192.168.16.1 routing-table=AAA

    0 192.168.16.1                              56  64 7ms
    1 192.168.16.1                              56  64 4ms
    sent=2 received=2 packet-loss=0% min-rtt=4ms avg-rtt=5ms max-rtt=7ms
```

Il faut lui indiquer de quelle vrf ! `[admin@PE1] > ping 192.168.16.1`

ping 192.168.16.1 routing-table=AAA

8. **Conclusion**, les routeurs PE ont 4 tables de routage : La principale et les 3 VRF AAA, BBB et CCC !

4.1 L3 - VPN !

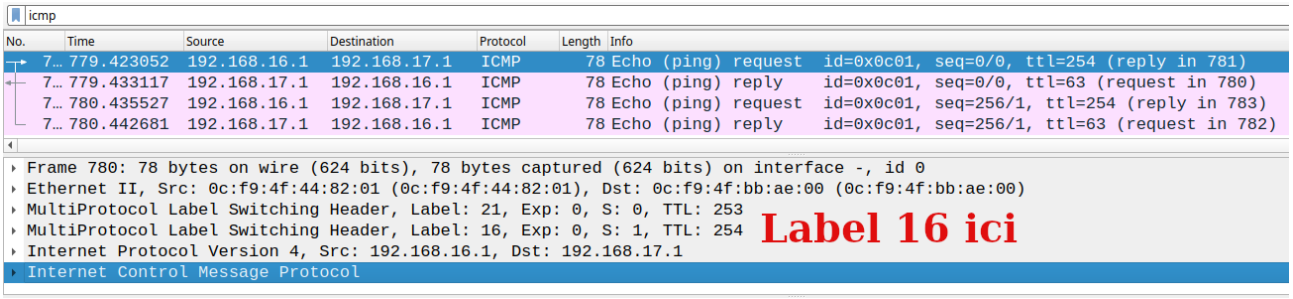
1. **Loguez** vous sur AAA1 ou BBB1 ou CCC1
2. **Mettez** 3 sondes wireshark entre PE2 et les 3 CE et **sélectionnez** le protocole du ping
3. **Faites** un ping 192.168.17.1 et regardez ce que vous obtenez sur les 3 wireshark
4. Est-ce logique ?
   On a bien 3 VPN ?
   AAA1 ne peut communiquer qu'avec AAA2
5. Comment cela fonctionne ? **Cela ne sera pas demandé au CT.**
6. Pour ceux qui veulent savoir, la commande ***mpls forwarding-table print*** sur PE1 et PE2
   Donne **la correspondance des labels et des @IP de réseau de destination**

```
[admin@PE1] > /mpls forwarding-table print
Flags:   - hw-offload,   - ldp,   - vpls,   - traffic-eng

 0    expl-null
 1    16                                  192.168.16.0/24@AAA
 2    17                                  192.168.16.0/24@BBB
 3    18                                  192.168.16.0/24@CCC
 4    19              19                  10.0.0.12/30                ether1
 5    20              16                  2.2.2.2/32                  ether1
 6    21              20                  22.22.22.22/32              ether1
 7    22                                  10.0.0.4/30                 ether1
 8    23                                  1.1.1.1/32                  ether1
 9    24              17                  10.0.0.8/30                 ether1
10    25              18                  3.3.3.3/32                  ether1
[admin@PE1] >
```

```
[admin@PE2] > mpls forwarding-table print
Flags:   - hw-offload,   - ldp,   - vpls,   - traffic-eng

 0    expl-null
 1    16                                  192.168.17.0/24@AAA
 2    17                                  192.168.17.0/24@BBB
 3    18                                  192.168.17.0/24@CCC
 4    19                                  10.0.0.8/30                 ether1
 5    20              16                  10.0.0.0/30                 ether1
 6    21              17                  2.2.2.2/32                  ether1
 7    22              19                  10.0.0.4/30                 ether1
 8    23              20                  1.1.1.1/32                  ether1
 9    24                                  3.3.3.3/32                  ether1
10    25              21                  11.11.11.11/32              ether1
[admin@PE2] >
```

PE2 dit à PE1 pour aller en 192.168.17.0/24@AAA tu me mets le label 16

D'où la capture wireshark suivante :



Et réciproquement **PE1 dit à PE2 pour aller en 192.168.16.0/24@AAA tu me mets le label 16**

— Puisque la structure est symétrique
— Si c'était BBB1 qui avait fait un ping on aurait le label 17
— Si c'était CCC1 qui avait fait un ping on aurait le label 18

7. **Conclusion on a ici 3 VPN que P1, P2 et P3 ne voient pas ! ! !**

5 Conclusion

1. **Dessinez** le modèle logique de la structure physique de PE1 à PE2.
2. **Concluez**