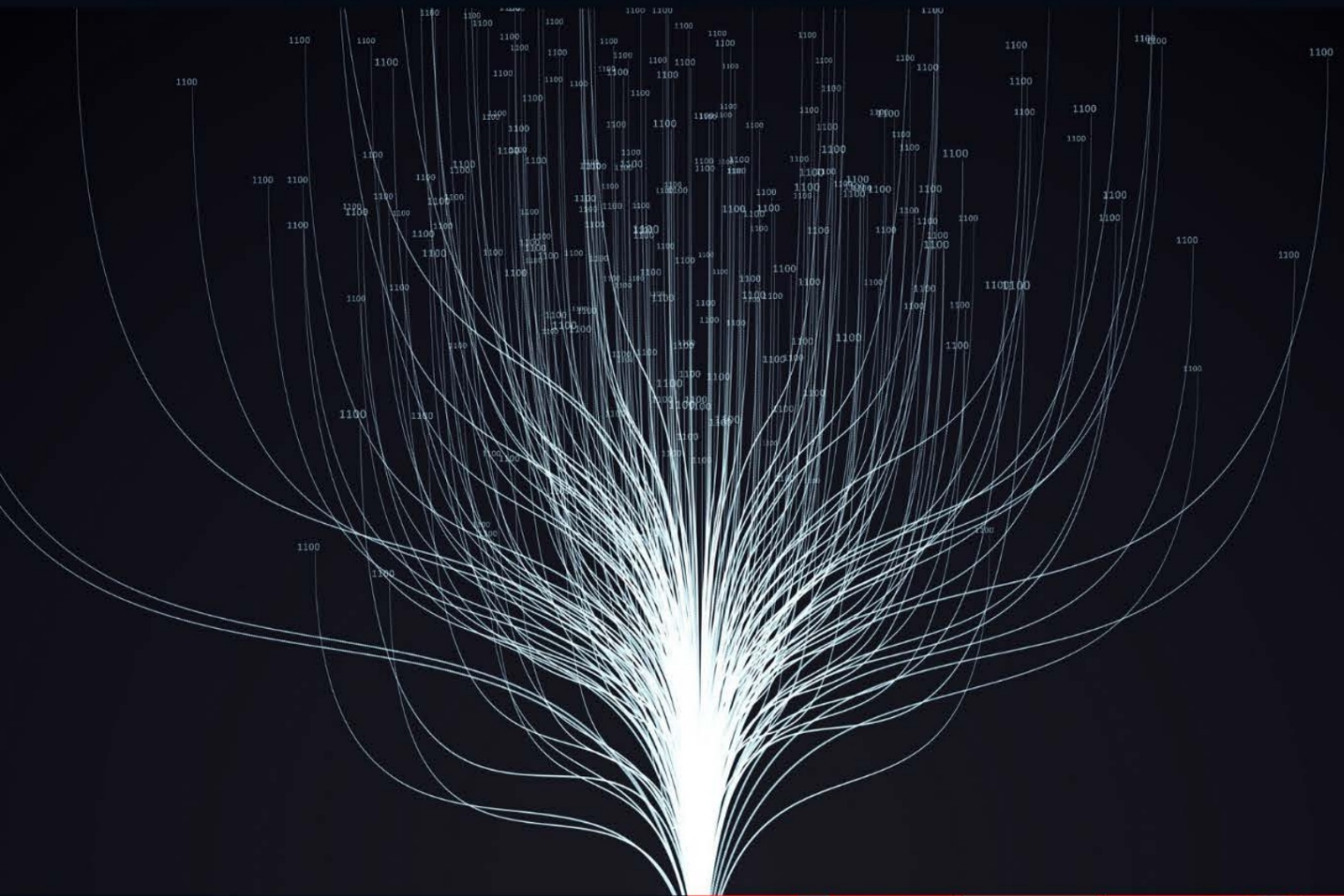


Du routage à la sécurisation



Routage inter-AS avec BGP l'indispensable des ingénieurs réseau

BGP pour les fournisseurs de services Internet

- Principes de base du routage
- Principes de base de BGP
- Attributs BGP
- Sélection du chemin BGP
- Politique BGP •
- Capacités BGP • Mise à
- l'échelle de BGP

Notions de base sur le routage

Terminologie et concepts

Concepts de routage

reseauenclair.com

- IPv4
- Routage •

Transfert

- Quelques définitions
- Options de politique
- Protocoles de routage

IPv4

- Internet utilise IPv4

les adresses ont une longueur de

32 bits allant de 1.0.0.0 à 223.255.255.255

0.0.0.0 à 0.255.255.255 et 224.0.0.0 à 255.255.255.255

ont des utilisations « spéciales »

- L'adresse IPv4 comporte une partie réseau et une partie hôte

Format d'adresse IPv4

- Adresse et masque de sous-réseau

écrit comme

12.34.56.78 255.255.255.0 ou

12.34.56.78/24

le masque représente le nombre de bits réseau dans l'adresse
32 bits

les bits restants sont les bits hôtes

À quoi sert un routeur ?

reseauenclair.com



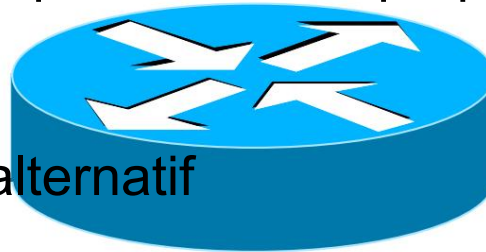
Une journée dans la vie d'un routeur

reseauenclair.com

trouver le chemin

paquet en avant, paquet en avant, paquet en avant, paquet
en avant...

trouver un chemin alternatif



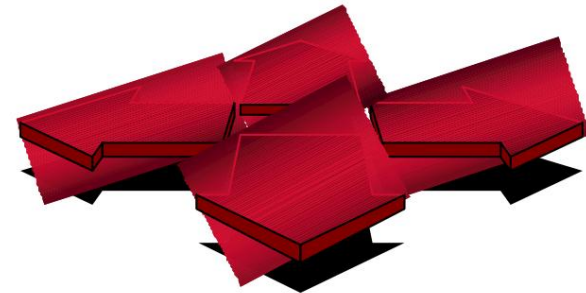
paquet en avant, paquet en avant, paquet en avant, paquet
en avant...

répéter jusqu'à ce que l'alimentation soit éteinte

Routage versus transfert

reseauenclair.com

- Routage = construire des cartes et donner des directions
- Transfert = déplacement de paquets entre les interfaces selon les « directions »



Routage IP – trouver le chemin

reseauenclair.com

- Chemin dérivé des informations reçues d'un protocole de routage
- Plusieurs chemins alternatifs peuvent exister
meilleur prochain saut stocké dans la table [de transfert](#)
- Les décisions sont mises à jour périodiquement ou en fonction des changements de topologie (pilotés par les événements)
- Les décisions sont fondées sur :
topologie, politiques et métriques (nombre de sauts, filtrage, délai, bande passante, etc.)

Recherche d'itinéraire IP

reseauenclair.com

- Basé sur le paquet IP de destination
- routage « correspondance la plus longue »

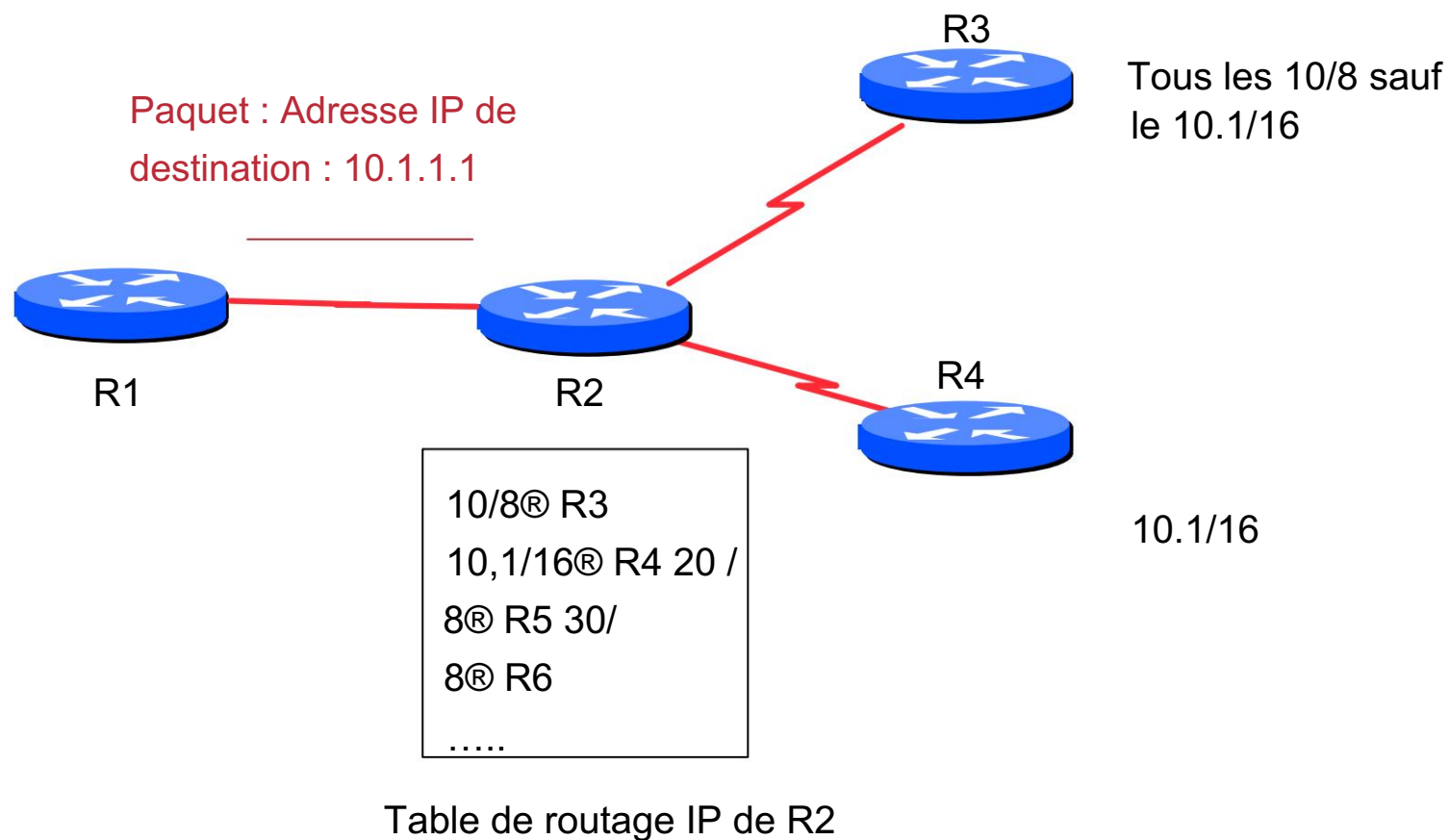
préfixe plus spécifique préféré au préfixe moins spécifique

exemple : un paquet avec la destination 10.1.1.1/32 est envoyé au routeur annonçant 10.1/16 plutôt qu'au routeur annonçant 10/8.

Recherche d'itinéraire IP

reseauenclair.com

- Basé sur le paquet IP de destination



Recherche d'itinéraire IP : routage de correspondance la plus longue

reseauencclair.com

- Basé sur le paquet IP de destination

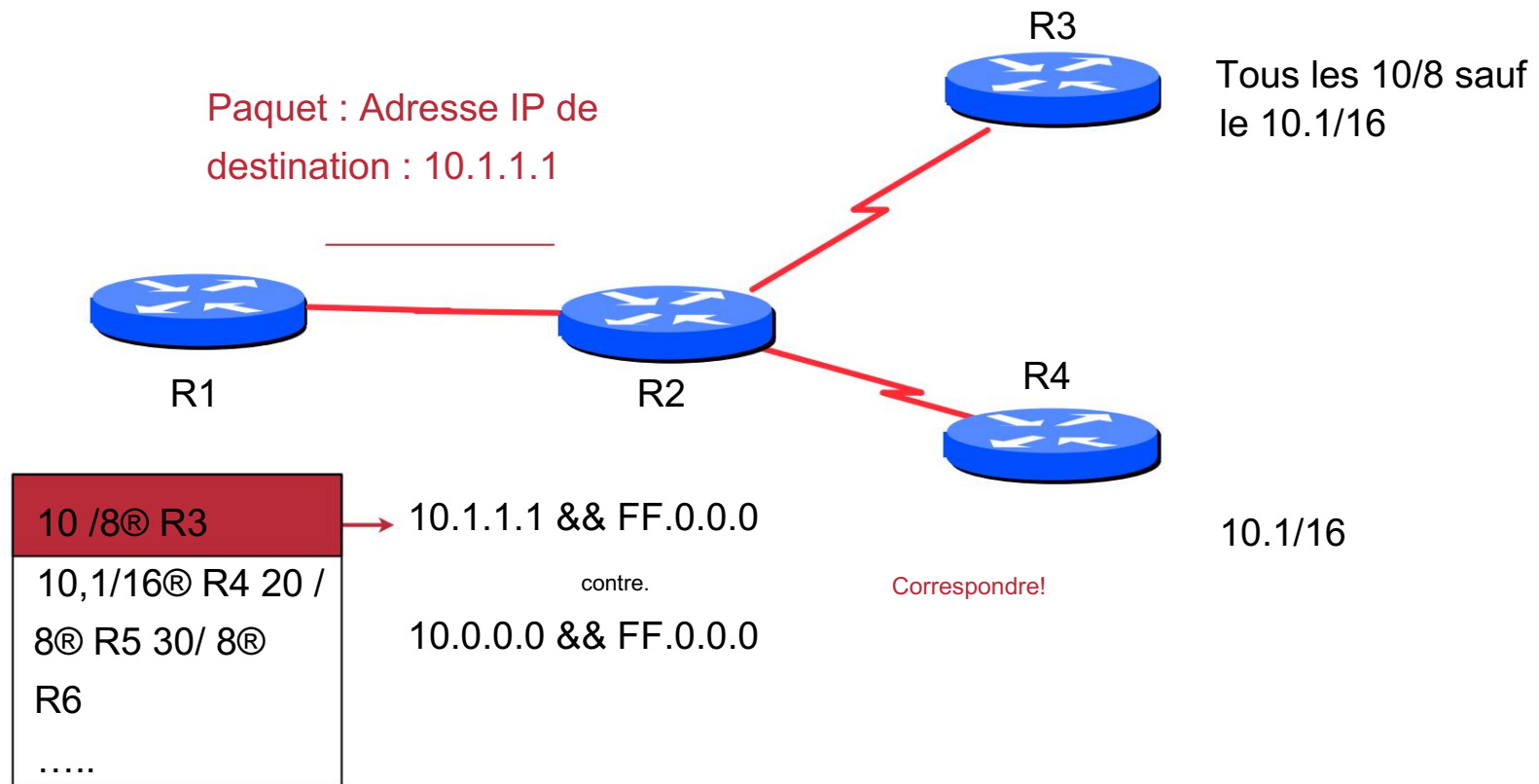


Table de routage IP de R2

Recherche d'itinéraire IP : routage de correspondance la plus longue

reseauenclair.com

- Basé sur le paquet IP de destination

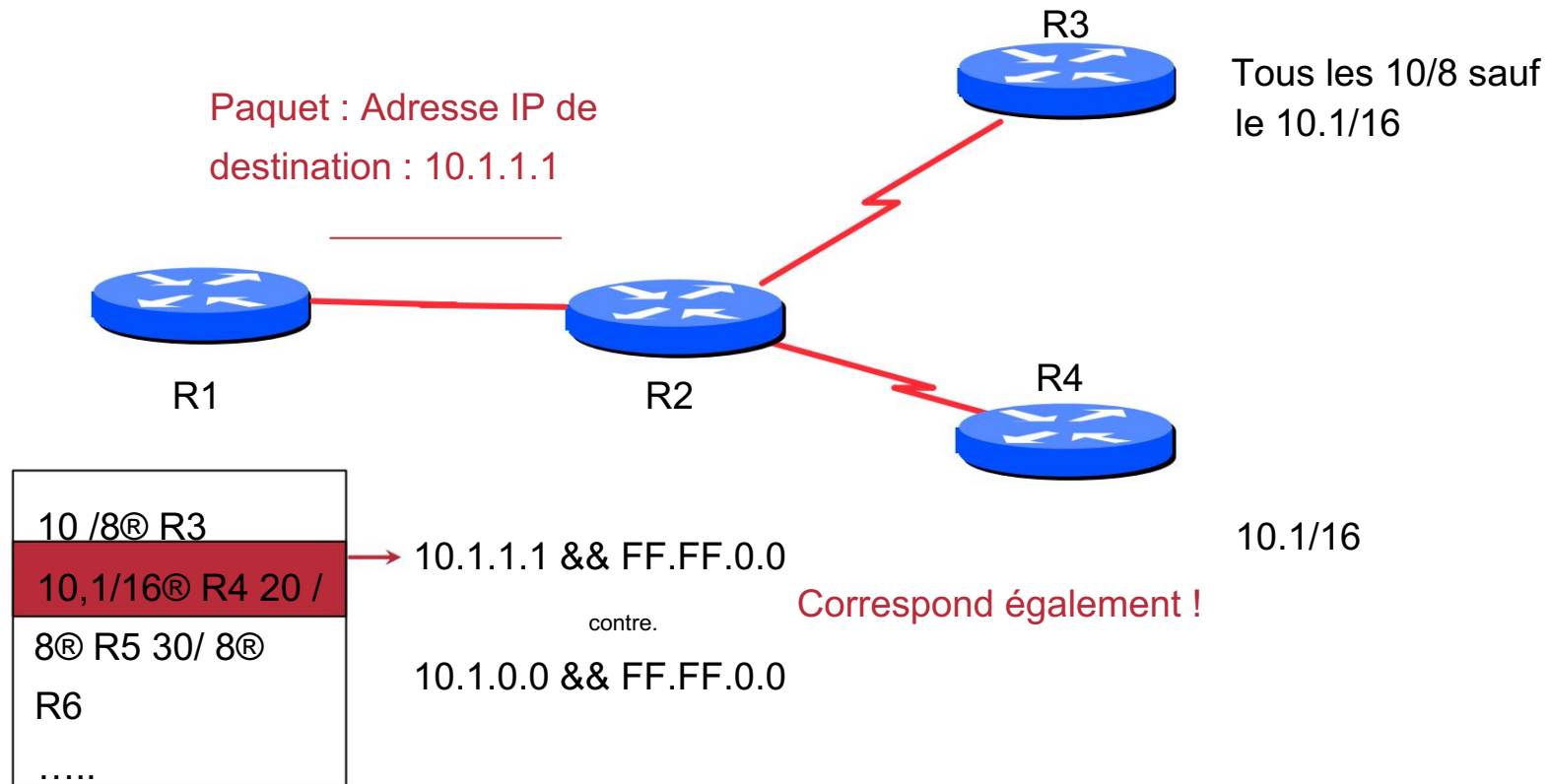


Table de routage IP de R2

Recherche d'itinéraire IP : routage de correspondance la plus longue

reseauenclair.com

- Basé sur le paquet IP de destination

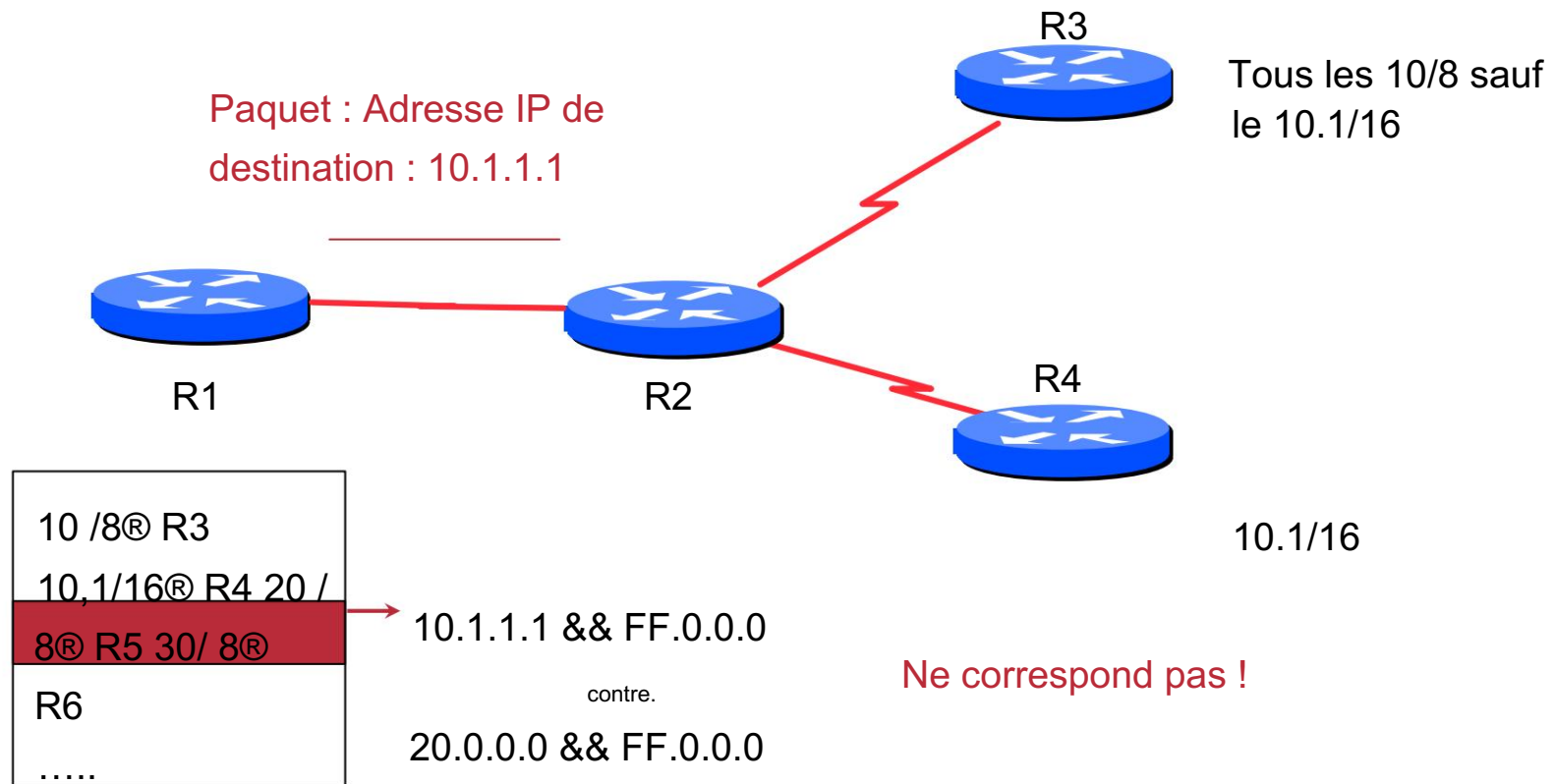


Table de routage IP de R2

Recherche d'itinéraire IP : routage de correspondance la plus longue

reseauencclair.com

- Basé sur le paquet IP de destination

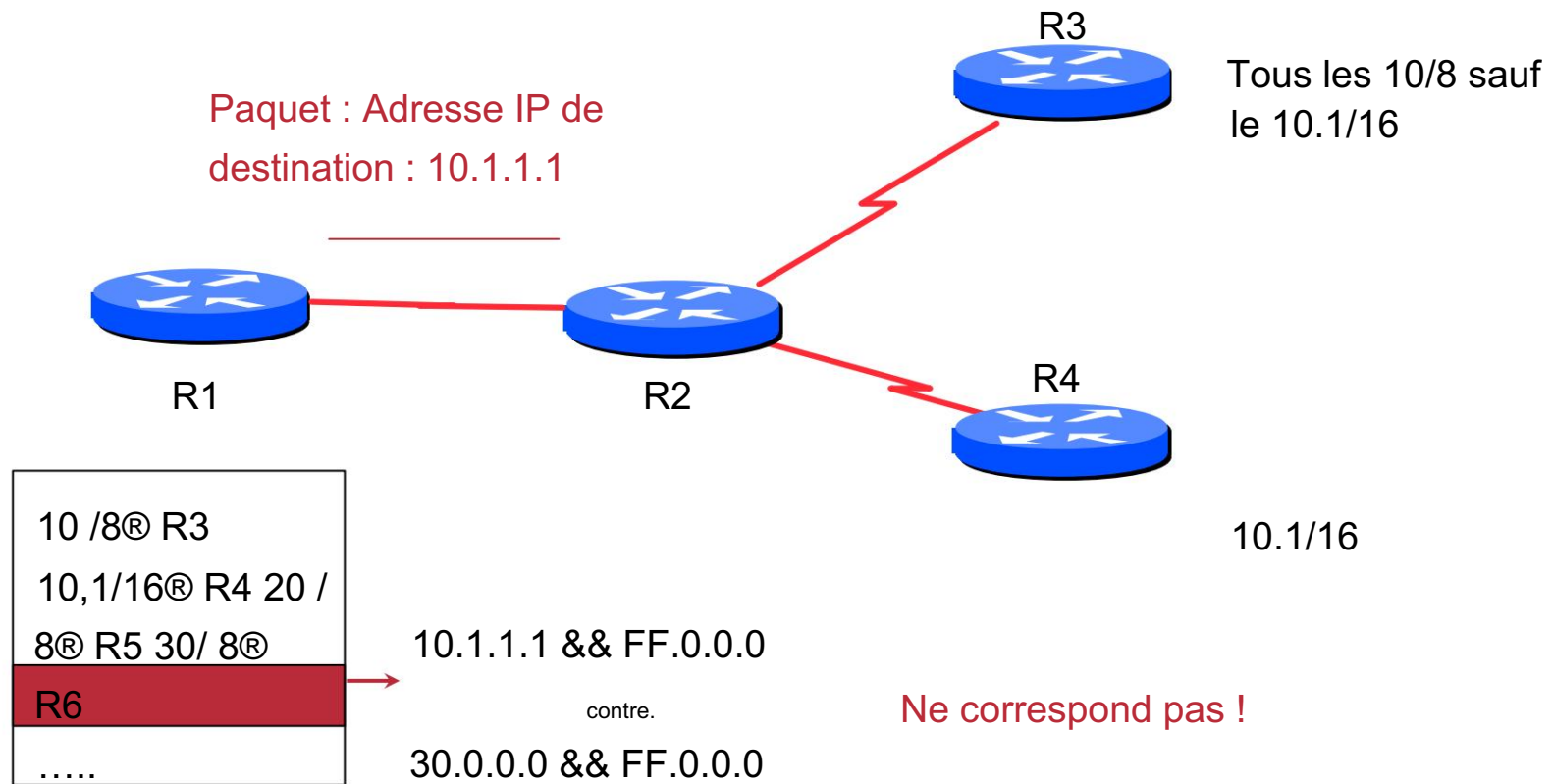


Table de routage IP de R2

Recherche d'itinéraire IP : routage de correspondance la plus longue

reseauenclair.com

- Basé sur le paquet IP de destination

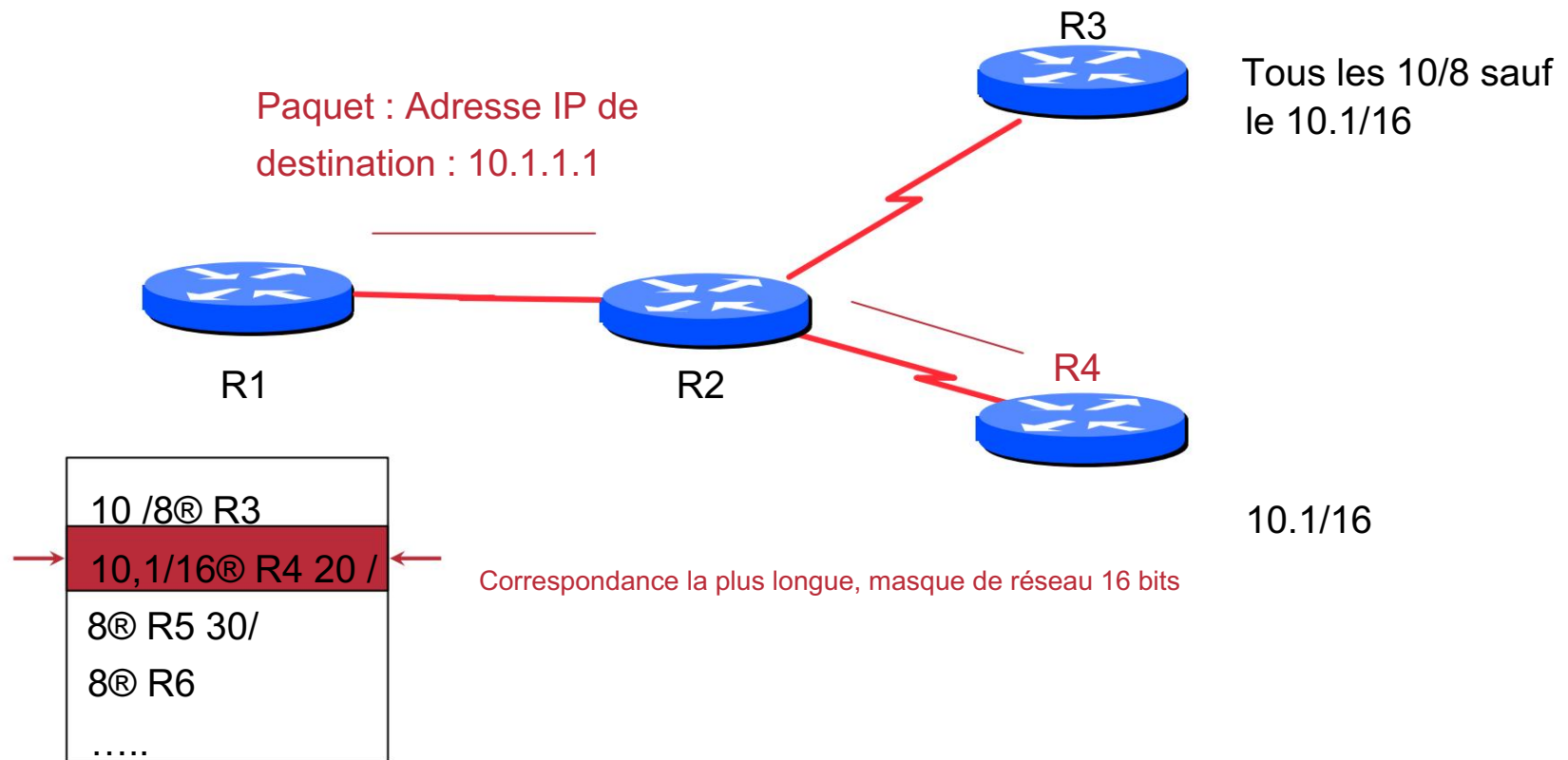


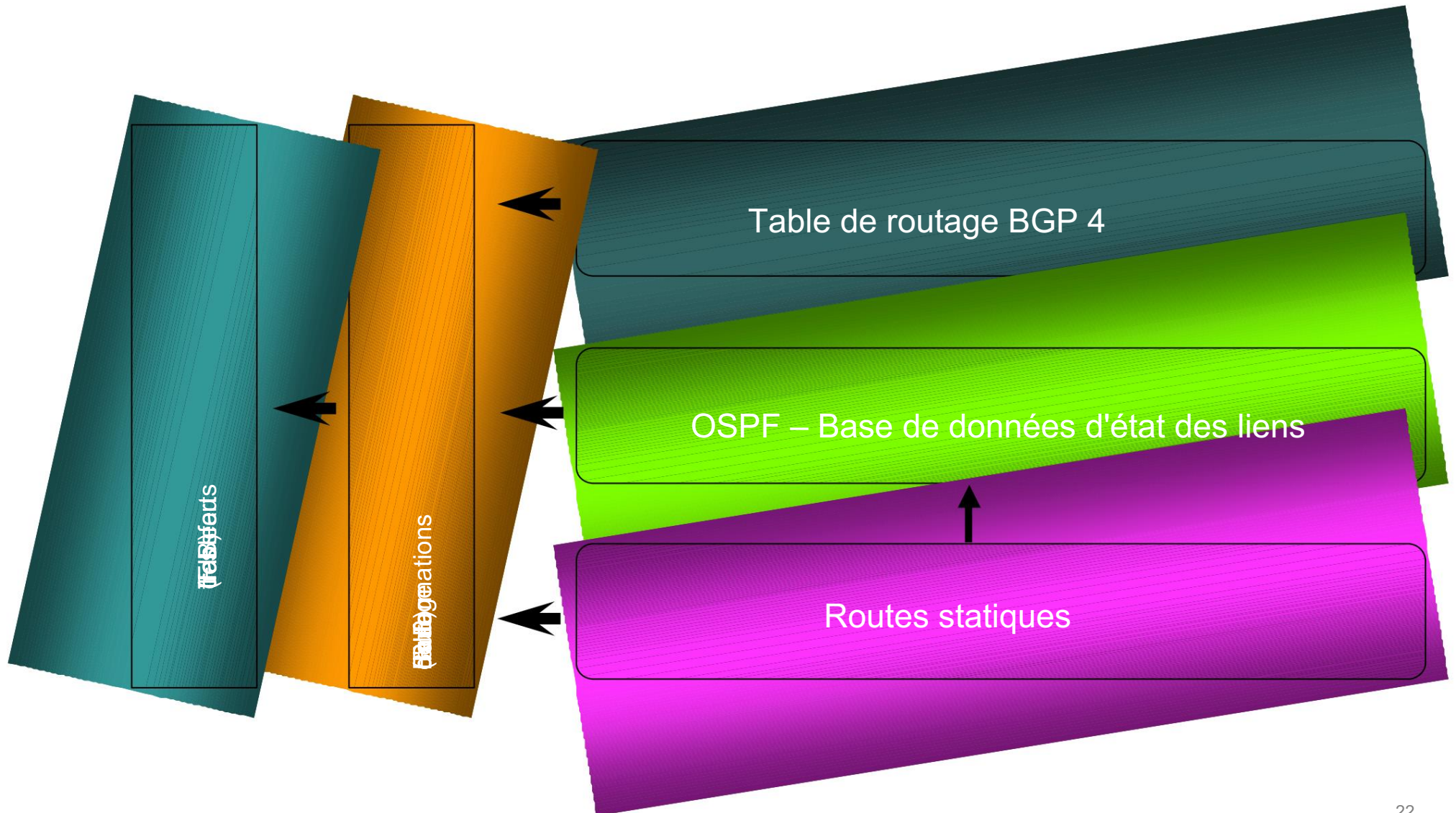
Table de routage IP de R2

Redirection IP

- Le routeur décide sur quelle interface un paquet est envoyé à
- Table de transfert remplie par le processus de routage
- Décisions de transmission :
 - adresse de destination
 - classe de service (file d'attente équitable, priorité, autres)
 - exigences locales (filtrage des paquets)
- Peut être facilité par du matériel spécial

Les tables de routage alimentent le Table de transfert

reseauenclair.com



Routage explicite ou par défaut

reseauenclair.com

- Défaut:

simple, bon marché (cycles, mémoire, bande passante)

faible granularité (jeux métriques)

- Explicite (zone franche par défaut)

frais généraux élevés, complexe, coût élevé, granularité élevée

- Hybrid

minimiser les frais généraux

fournir une granularité utile nécessite

certaines connaissances en filtrage

Trafic de sortie

reseauenclair.com

- Comment les paquets quittent votre réseau • Le trafic de sortie dépend de : la disponibilité de l'itinéraire (ce que les autres vous envoient) l'acceptation de l'itinéraire (ce que vous acceptez des autres) la politique et le réglage (ce que vous faites avec les itinéraires des autres)
- Accords de peering et de transit

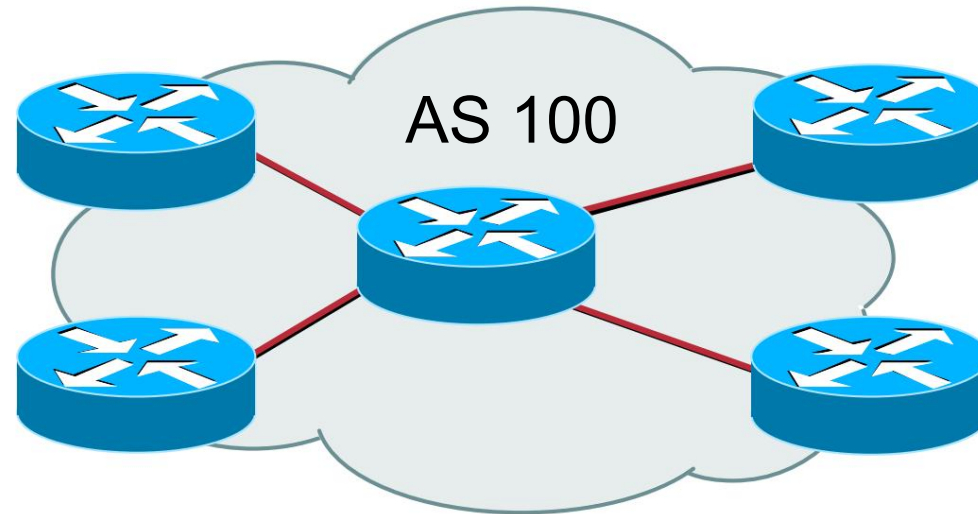
Trafic entrant

reseauencclair.com

- Comment les paquets parviennent à votre réseau et à celui de vos clients
- Le trafic entrant dépend de :
 - quelles informations vous envoyez et à qui
 - en fonction de votre adressage et de vos AS
 - basé sur la politique des autres (ce qu'ils acceptent de vous et ce qu'ils en font)

Systeme autonome (AS)

reseauenclair.com



- Collection de réseaux avec la même politique de routage
- Protocole de routage unique
- Généralement sous une seule propriété, fiducie et contrôle administratif

Définition des termes

reseauenclair.com

- Voisins

AS qui échangent directement des informations de routage

Routeurs qui échangent des informations de routage

- Annoncer

envoyer des informations de routage à un voisin

- Accepter

recevoir et utiliser les informations de routage envoyées par un voisin

- Originaire

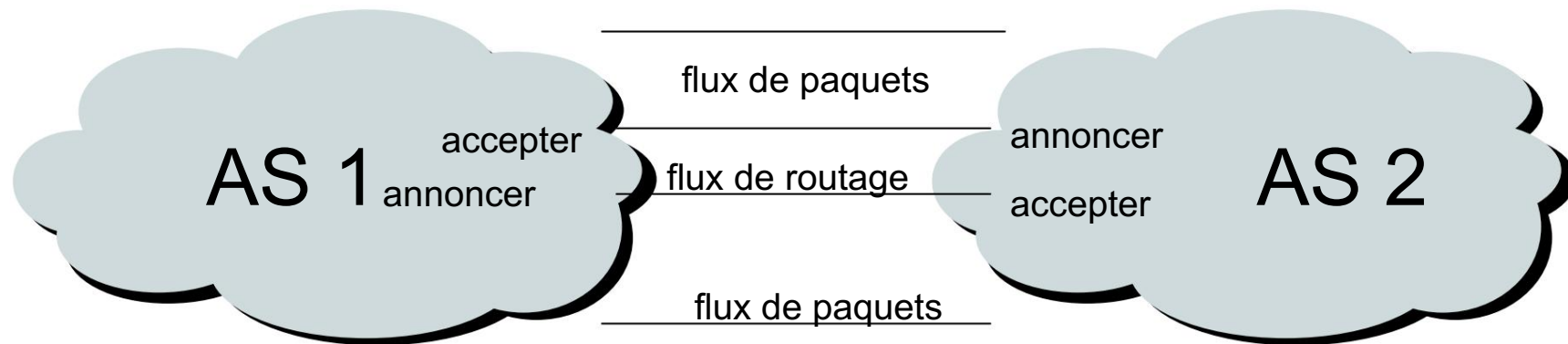
insérer des informations de routage dans des annonces externes (généralement à la suite de l'IGP)

- Pairs

routeurs dans les AS voisins ou au sein d'un même AS qui échangent des informations de routage et de politique

Flux de routage et flux de paquets

reseauenclair.com



Pour que les réseaux AS1 et AS2 communiquent :

AS1 doit annoncer à AS2

AS2 doit accepter d'AS1

AS2 doit annoncer à AS1

AS1 doit accepter d'AS2

Flux de routage et flux de trafic

reseauencclair.com

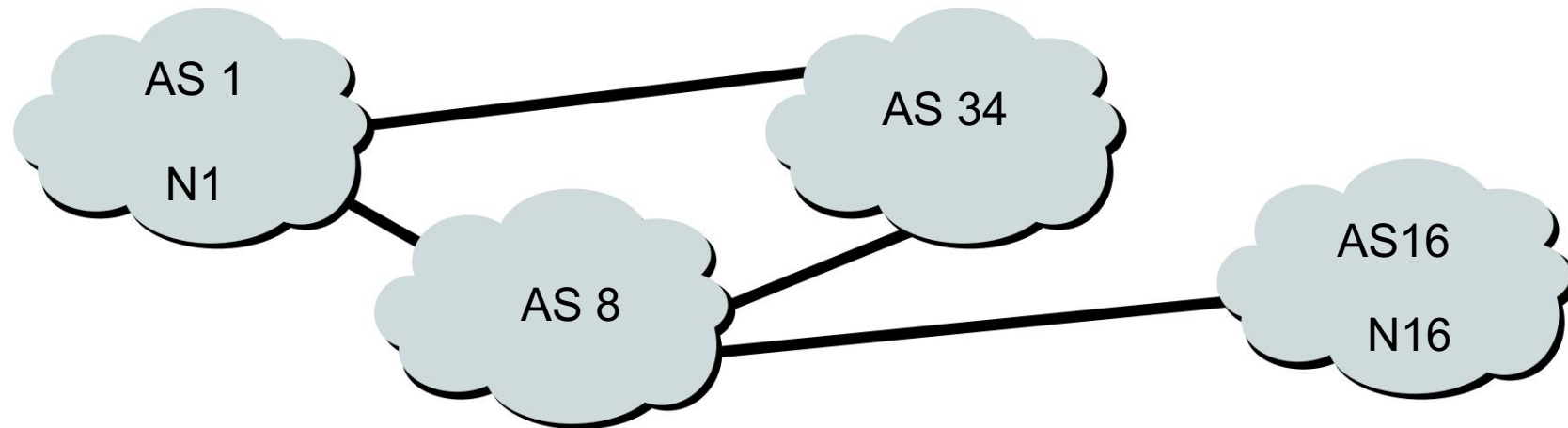
- Le flux de circulation est toujours en sens inverse direction du flux de routage information

Le filtrage des informations de routage sortantes inhibe le flux de trafic entrant

Le filtrage des informations de routage entrantes inhibe le flux de trafic sortant

Flux de routage/Flux de paquets : Avec plusieurs AS

reseauenclair.com



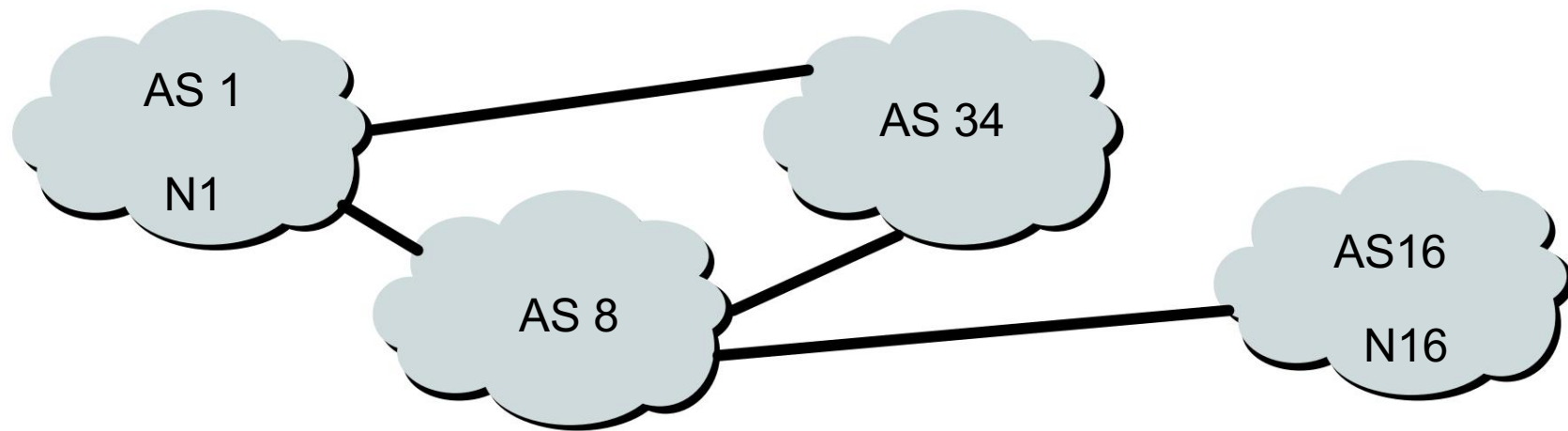
Pour que le réseau N1 dans AS1 envoie du trafic au réseau N16 dans AS16 :

- AS16 doit émettre et annoncer N16 à AS8.
- AS8 doit accepter N16 de AS16.
- AS8 doit annoncer N16 à AS1 ou AS34.
- AS1 doit accepter N16 d'AS8 ou AS34.

Pour le flux de paquets bidirectionnel, des politiques similaires doivent exister pour N1.

Flux de routage/Flux de paquets : Avec plusieurs AS

reseauenclair.com



À mesure que plusieurs chemins entre les sites sont mis en œuvre, il est facile de comprendre à quel point les politiques peuvent devenir assez complexes.

Politique de routage

reseauenclair.com

- Utilisé pour contrôler le flux de trafic entrant et sortant d'un FAI réseau
- Le FAI prend des décisions sur les informations de routage à accepter et à rejeter de ses voisins

Itinéraires individuels

Routes générées par des AS spécifiques

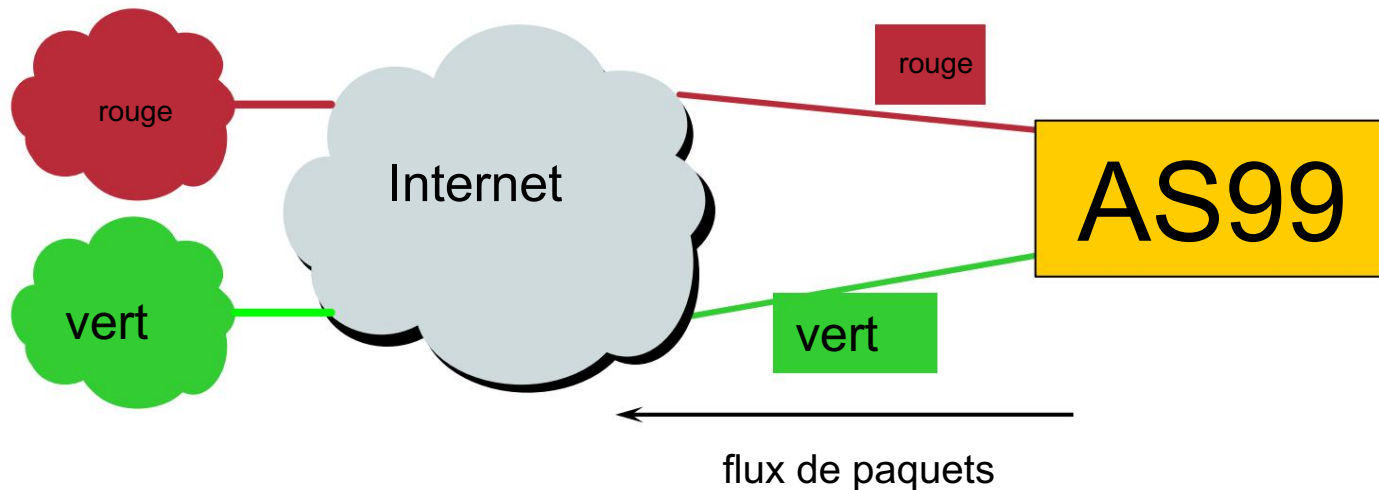
Routes traversant des AS spécifiques

Itinéraires appartenant à d'autres groupements

Des groupements que vous définissez comme bon vous semble

Limitations de la politique de routage

reseauenclair.com



- AS99 utilise un lien rouge pour le trafic vers l'AS rouge et le lien vert pour le trafic restant
- Pour mettre

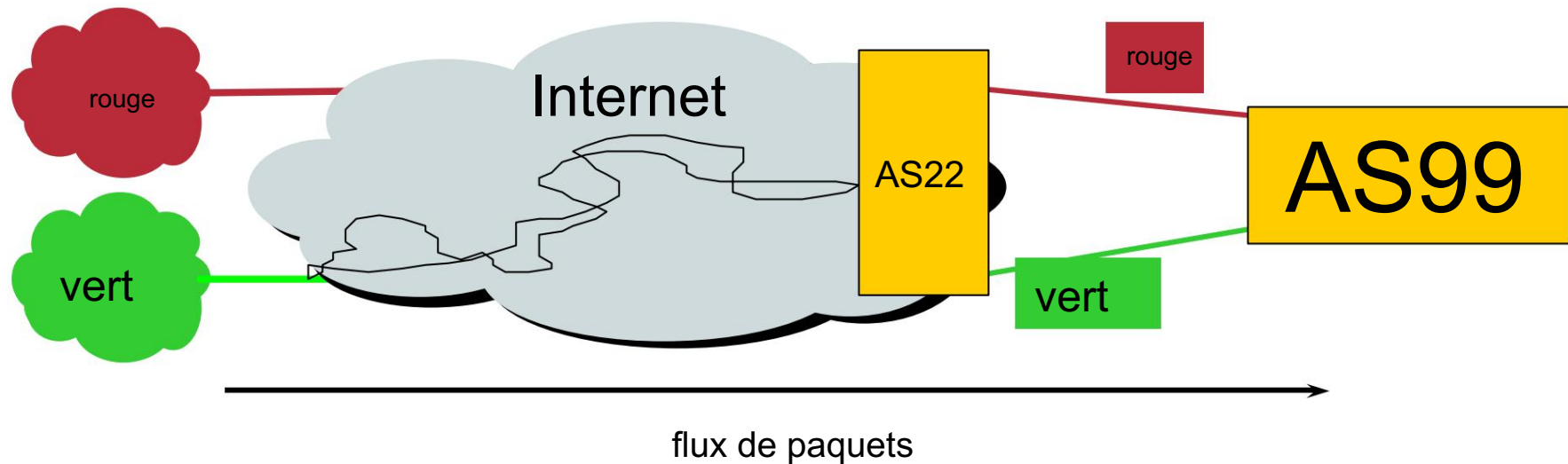
en œuvre cette politique, AS99 doit :

Accepter les routes provenant de l'AS rouge sur le lien rouge

Accepter tous les autres itinéraires sur le lien vert

Limitations de la politique de routage

reseauenclair.com



- AS99 souhaite que les paquets provenant de l'AS vert utilisent le lien vert.
- Mais à moins que l'AS22 ne coopère pour pousser le trafic de l'AS vert vers la liaison verte, l'AS99 ne peut pas faire grand-chose pour atteindre cet objectif

Problèmes de politique de routage

reseauenclair.com

- 131 000 préfixes (il n'est pas réaliste de définir une politique sur tous individuellement)
- 16 500 AS d'origine (trop nombreux)
- les routes liées à un AS ou à un chemin spécifique peuvent être instables quelle que soit la connectivité
- les groupes d'AS sont une abstraction naturelle à des fins de filtrage

Protocoles de routage

Nous savons maintenant ce que signifie le routage...

...mais que font les routeurs ?

Protocoles de routage

- Les routeurs utilisent des « protocoles de routage » pour échanger des informations de routage avec chaque autre

IGP est utilisé pour désigner le processus exécuté sur les routeurs à l'intérieur du réseau d'un FAI

EGP est utilisé pour désigner le processus exécuté entre les routeurs limitrophes directement connectés réseaux FAI

Qu'est-ce qu'un IGP ?

reseauenclair.com

- Protocole de passerelle intérieure
- Au sein d'un système autonome
- Contient des informations sur
préfixes d'infrastructure interne
- Exemples – OSPF, ISIS, EIGRP

Pourquoi avons-nous besoin d'un IGP ?

- Mise à l'échelle de la dorsale du FAI

Hiérarchie

Limiter la portée de l'échec

Utilisé uniquement pour les adresses d'infrastructure du FAI,
pas pour les clients

L'objectif de conception est de **minimiser** le nombre de
préfixes dans IGP pour favoriser l'évolutivité et la convergence rapide

Qu'est-ce qu'un EGP ?

- Protocole de passerelle extérieure
- Utilisé pour transmettre des informations de routage entre les systèmes autonomes
- Découplé de l'IGP
- L'EGP actuel est le BGP

Pourquoi avons-nous besoin d'un EGP ?

reseauenclair.com

- Mise à l'échelle vers un grand réseau

Hiérarchie

Limiter la portée de l'échec

- Définir les limites administratives • Politique

Contrôler l'accessibilité des préfixes

Fusionner des organisations distinctes

Connecter plusieurs IGP

Intérieur contre extérieur

Protocoles de routage

reseauenclair.com

- Intérieur

découverte automatique des voisins

faites généralement confiance à vos routeurs IGP

les préfixes vont à tous les routeurs IGP

relie les routeurs d'un même AS

- Extérieur

pairs spécifiquement configurés

connexion avec des réseaux extérieurs

fixer des limites administratives

lie les AS ensemble

Intérieur contre extérieur

Protocoles de routage

reseauenclair.com

- Intérieur

Transporte
uniquement les
adresses d'infrastructure du FAI

Les FAI visent à maintenir le
IGP de petite taille pour l'efficacité
et l'évolutivité

- Extérieur

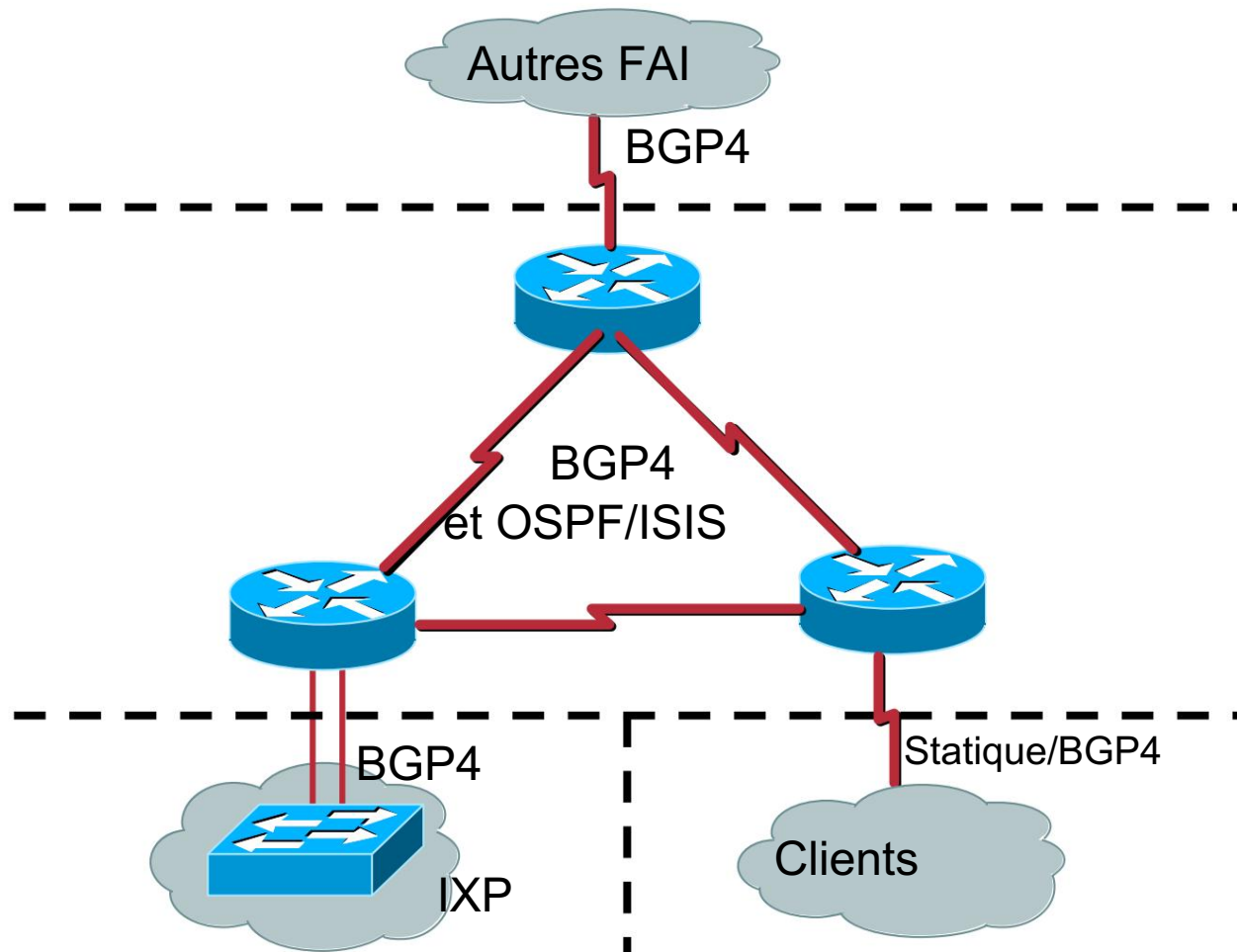
Transporte les préfixes
clients

Transporte les préfixes Internet

Les EGP sont indépendants de
la topologie du réseau du FAI

Hiérarchie des protocoles de routage

reseauenclair.com



Distances administratives par défaut

reseauenclair.com

Source de l'itinéraire	Distance par défaut
Interface connectée	0
Route statique	1
Route récapitulative IGRP améliorée	5
BGP externe	20
IGRP interne amélioré	90
IGRP	100
OSPF	110
EI-EI	115
DÉCHIRER	120
EGP	140
IGRP externe amélioré	170
BGP interne	200
Inconnu	255

BGP pour les fournisseurs de services Internet

reseauenclair.com

- Principes de base du routage
- Principes de base de BGP
- Attributs BGP
- Sélection du chemin BGP
- Politique BGP •
- Capacités BGP • Mise à l'échelle de BGP

Notions de base de BGP

Qu'est-ce que ce truc BGP ?

Protocole de passerelle frontalière

reseauenclair.com

- Protocole de routage utilisé pour échanger des informations de routage
informations entre réseaux

protocole de passerelle extérieure

- Décrit dans la RFC1771

travail en cours pour mettre à jour

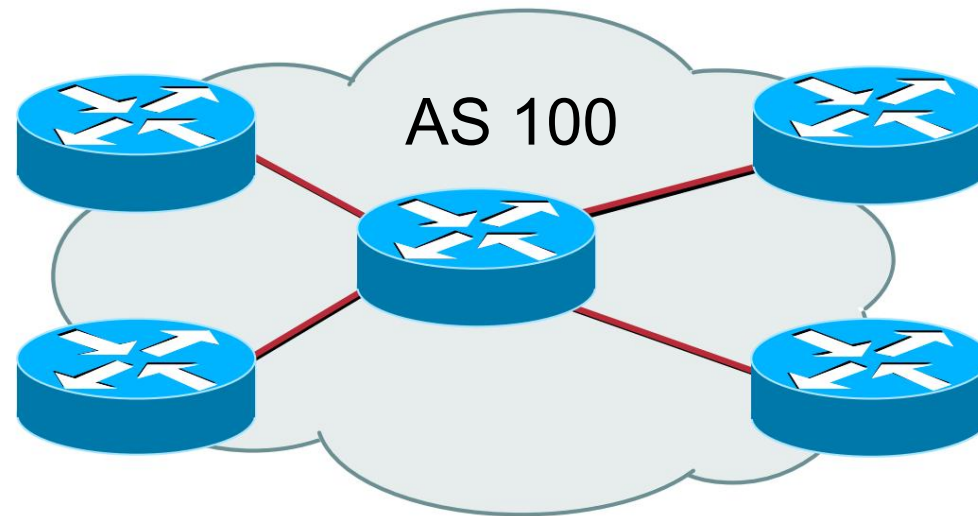
www.ietf.org/internet-drafts/draft-ietf-idr-bgp4-23.txt • Le système

autonome est l'unité opérationnelle fondamentale de BGP. Il est utilisé pour identifier de manière

unique les réseaux avec une politique de routage commune

Système autonome (AS)

reseauenclair.com



- Collection de réseaux avec la même politique de routage
- Protocole de routage unique
- Généralement sous une seule propriété, fiducie et contrôle administratif
- Identifié par un numéro unique

Numéro de système autonome (ASN)

reseauenclair.com

- Un ASN est un nombre de 16 bits

Les numéros 1-64511 sont attribués par les RIR

64512-65534 sont destinés à un usage privé et ne doivent jamais apparaître sur Internet

0 et 65535 sont réservés

- Les ASN 32 bits arrivent bientôt

www.ietf.org/internet-drafts/draft-ietf-idr-as4bytes-07.txt

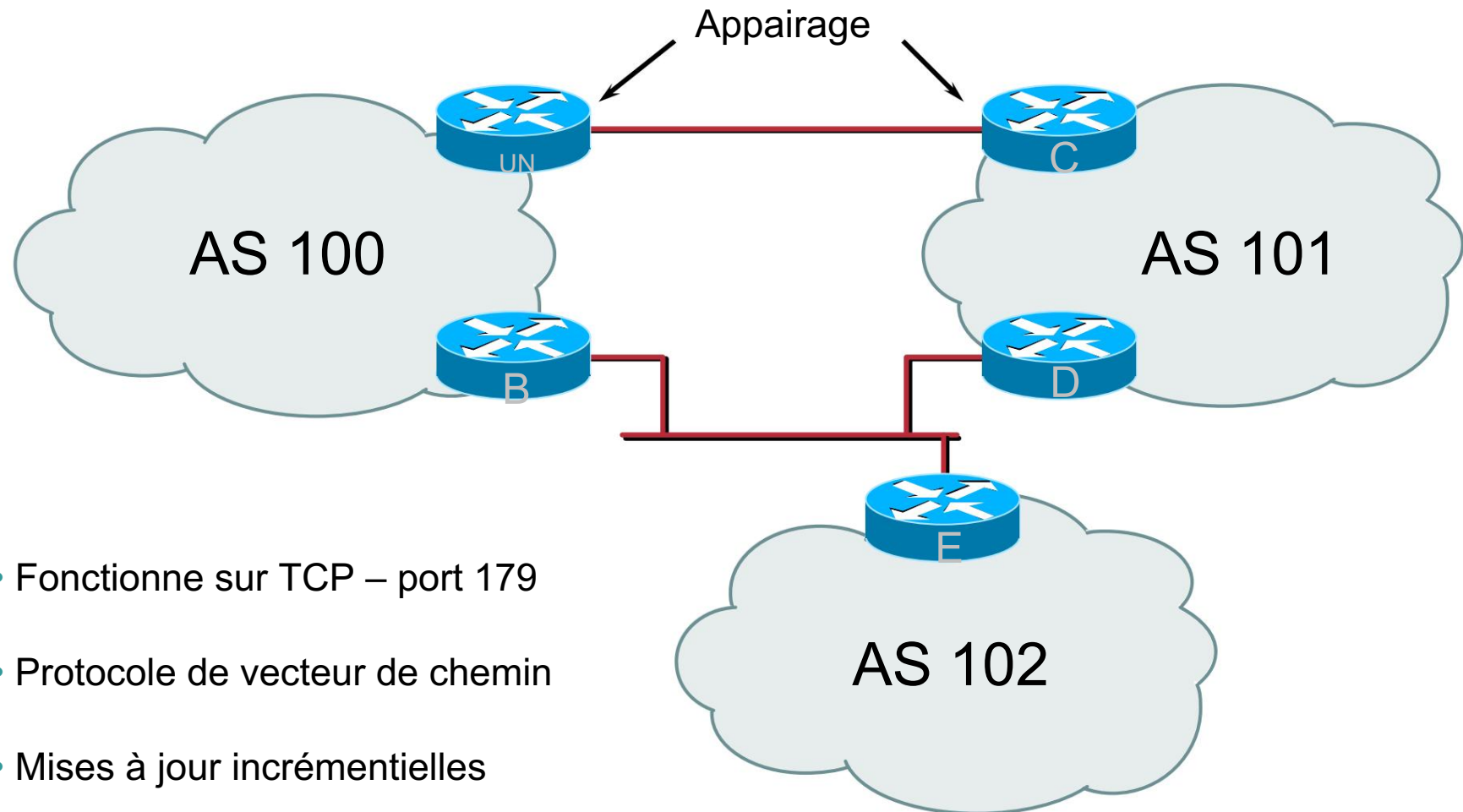
- Les ASN sont distribués par les registres Internet régionaux

Également disponible auprès des FAI en amont qui sont membres de l'un des RIR

Les allocations ASN actuelles jusqu'à 32 767 ont été accordées au RIR

Notions de base de BGP

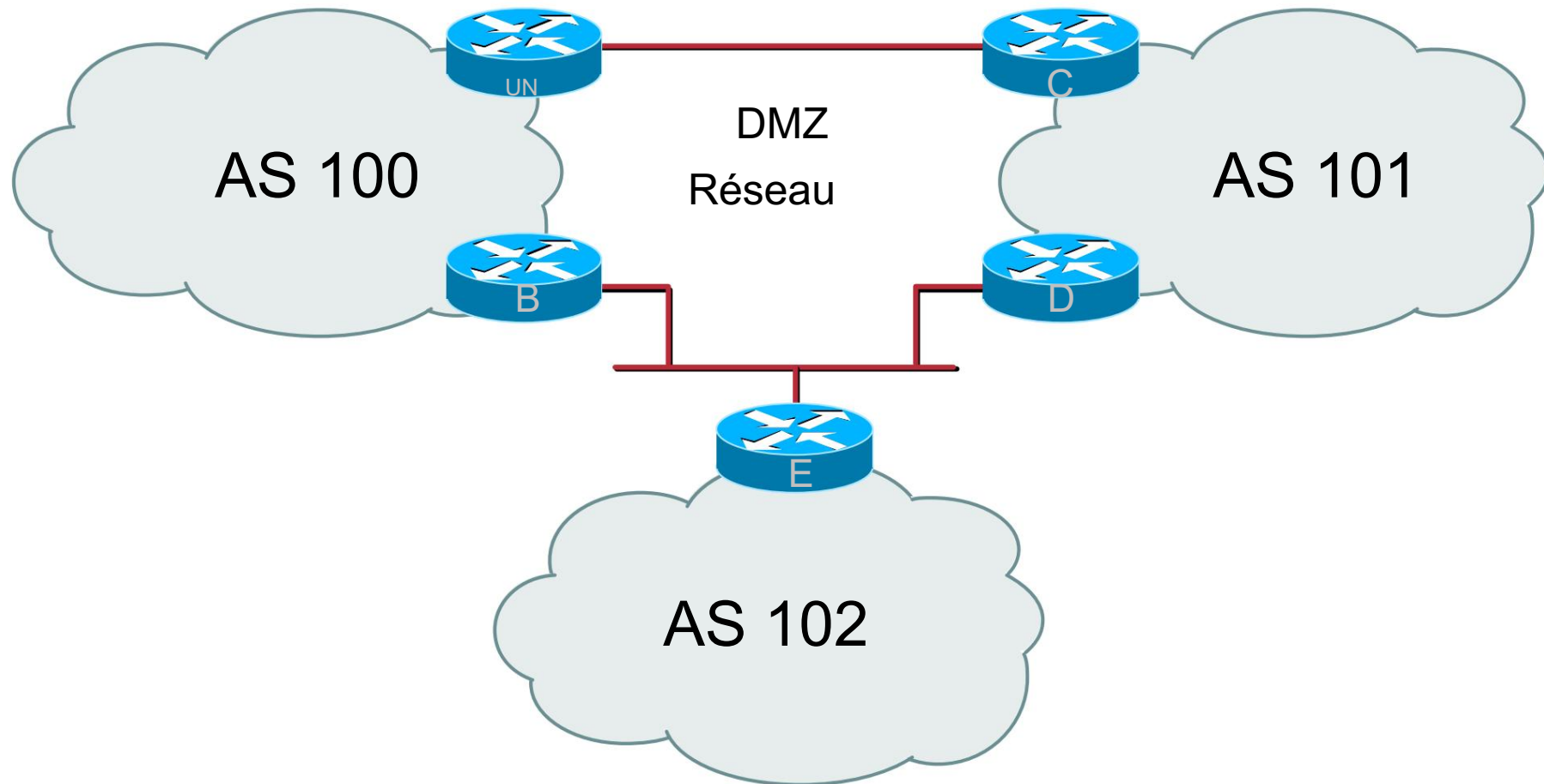
reseauenclair.com



- Fonctionne sur TCP – port 179
- Protocole de vecteur de chemin
- Mises à jour incrémentielles
- BGP « interne » et « externe »

Zone de démarcation (DMZ)

reseauenclair.com



- Réseau partagé entre AS

Fonctionnement général du BGP

reseauenclair.com

- Apprend plusieurs chemins via des haut-parleurs BGP internes et externes
- Choisit le meilleur chemin et l'installe dans la table de transfert
- Le meilleur chemin est envoyé aux voisins BGP externes
- Politiques appliquées en influençant la meilleure sélection de chemin

eBGP et iBGP

reseauenclair.com

- BGP utilisé en interne (iBGP) et en externe (eBGP) •

iBGP utilisé pour transporter

certains/tous les préfixes Internet sur la dorsale du FAI

Préfixes clients des FAI

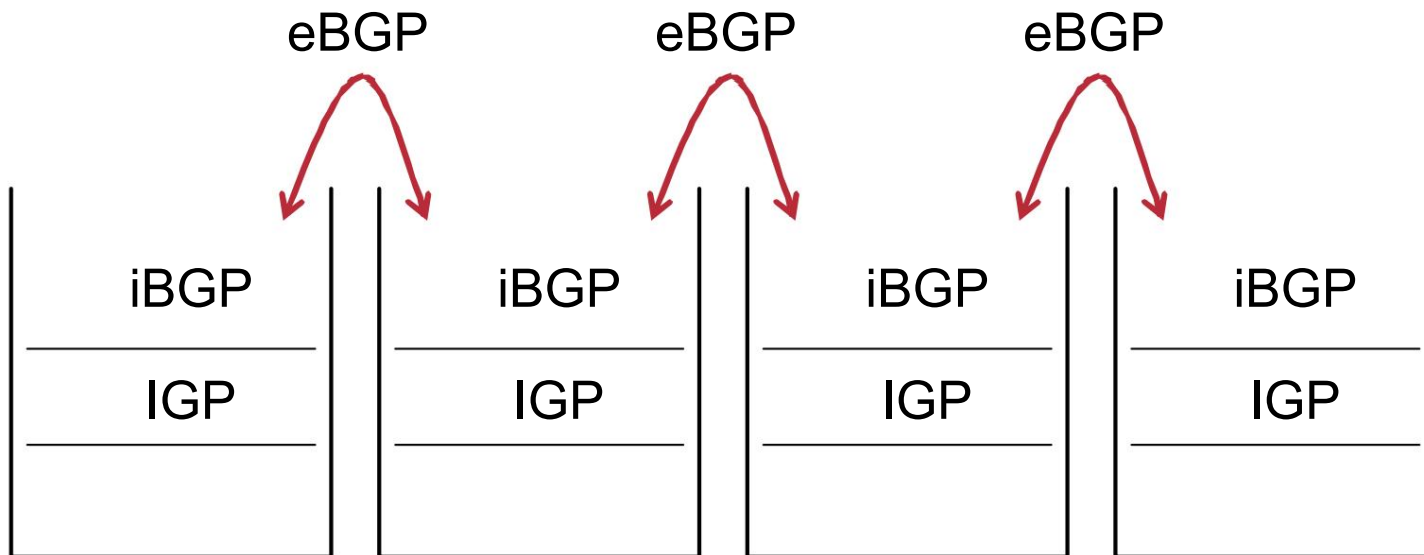
- eBGP utilisé pour

échanger des préfixes avec d'autres AS et mettre

en œuvre une politique de routage

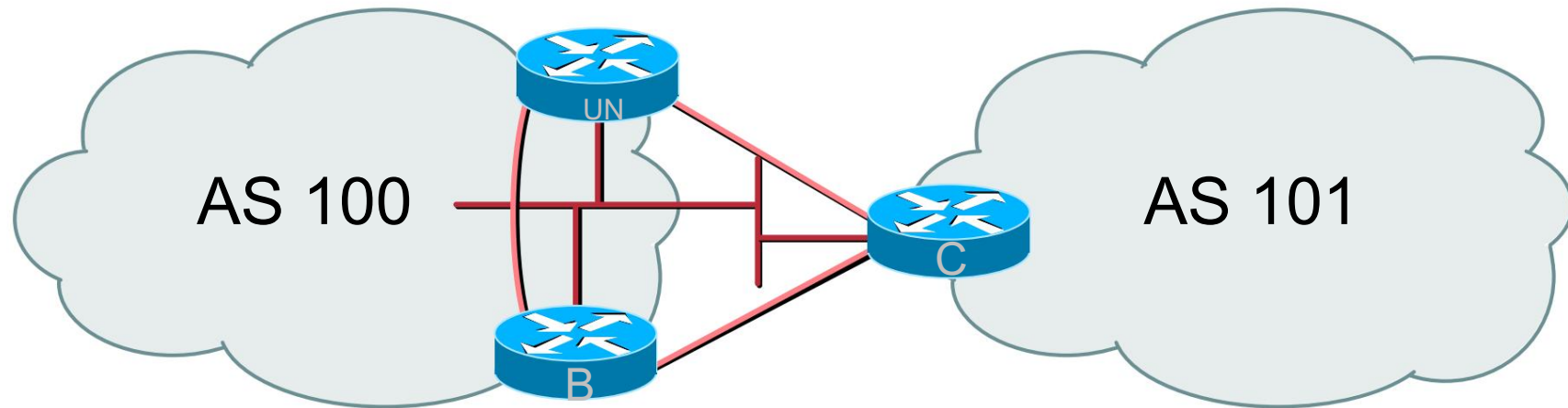
Modèle BGP/IGP utilisé dans les réseaux des FAI

- Représentation du modèle



Appairage BGP externe (eBGP)

reseauenclair.com



- Entre les locuteurs BGP dans différents AS
- Doit être directement connecté
- **Ne jamais** exécuter un IGP entre des homologues eBGP

Configuration du BGP externe

reseauenclair.com

Routeur A dans AS100

interface ethernet 5/0 adresse IP

222.222.10.2 255.255.255.240 !

routeur bgp 100 réseau

220.220.8.0 masque 255.255.252.0

voisin 222.222.10.1 remote-as 101 voisin 222.222.10.1 prefix-list

RouterC in voisin 222.222.10.1 prefix-list RouterC out !

adresse IP sur
l'interface Ethernet

ASN locale

ASN distant

adresse IP de l'interface
Ethernet du routeur C

Filtres entrants
et sortants

Configuration du BGP externe

reseauenclair.com

Routeur C dans AS101

interface Ethernet 1/0/0

adresse IP 222.222.10.1 255.255.255.240 !

routeur bgp 101 réseau

220.220.8.0 masque 255.255.252.0

voisin 222.222.10.2 distant-as 100 voisin 222.222.10.2 liste-de-

préfixes RouteurA dans voisin 222.222.10.2 liste-de-préfixes RouteurA en sortie !

adresse IP sur
l'interface Ethernet

ASN locale

ASN distant

adresse IP de l'interface
Ethernet du routeur A

Filtres entrants
et sortants

BGP interne (iBGP)

reseauenclair.com

- Pair BGP au sein du même AS
- Il n'est pas nécessaire qu'il soit directement connecté

IGP prend en charge la connectivité interne BGP

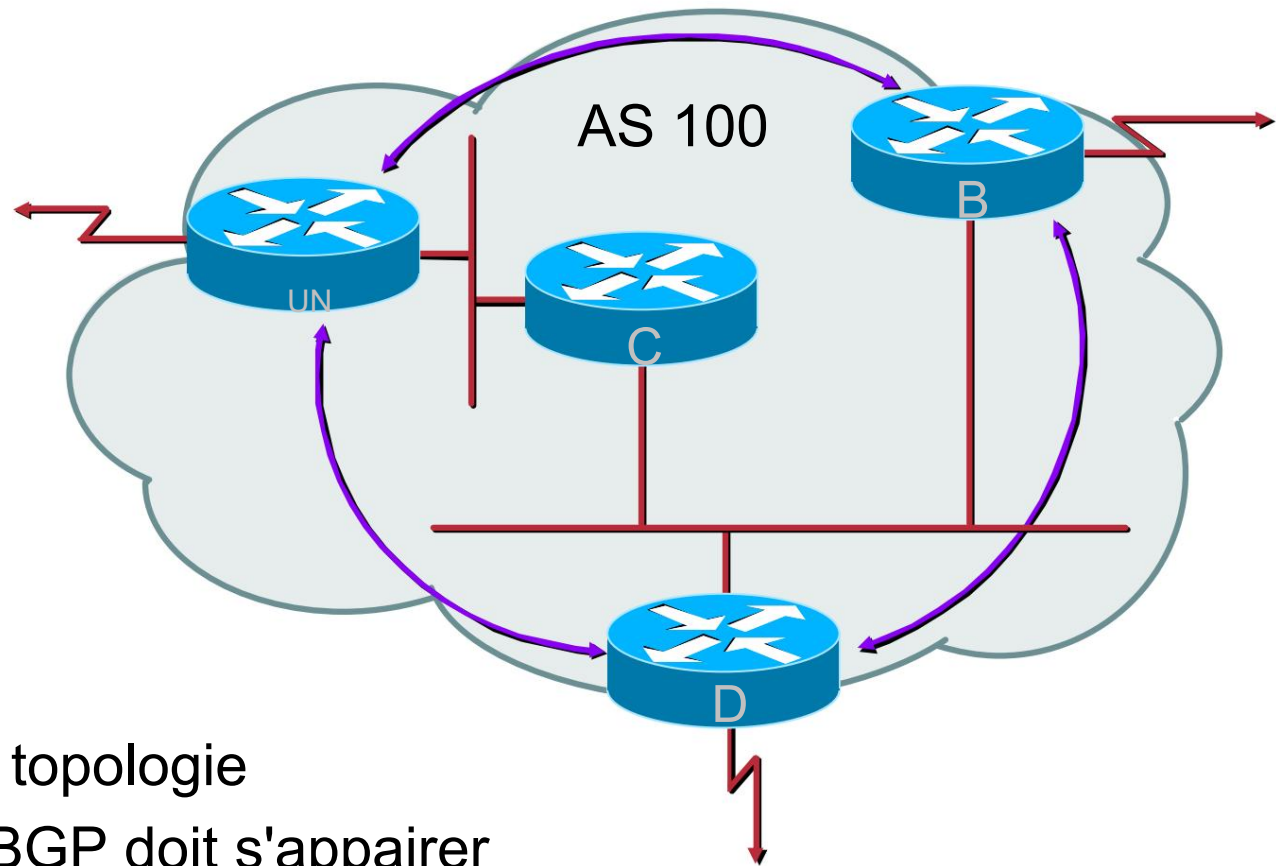
- Les haut-parleurs iBGP doivent être entièrement maillés

ils créent des réseaux connectés

ils ne transmettent pas les préfixes appris d'autres locuteurs iBGP

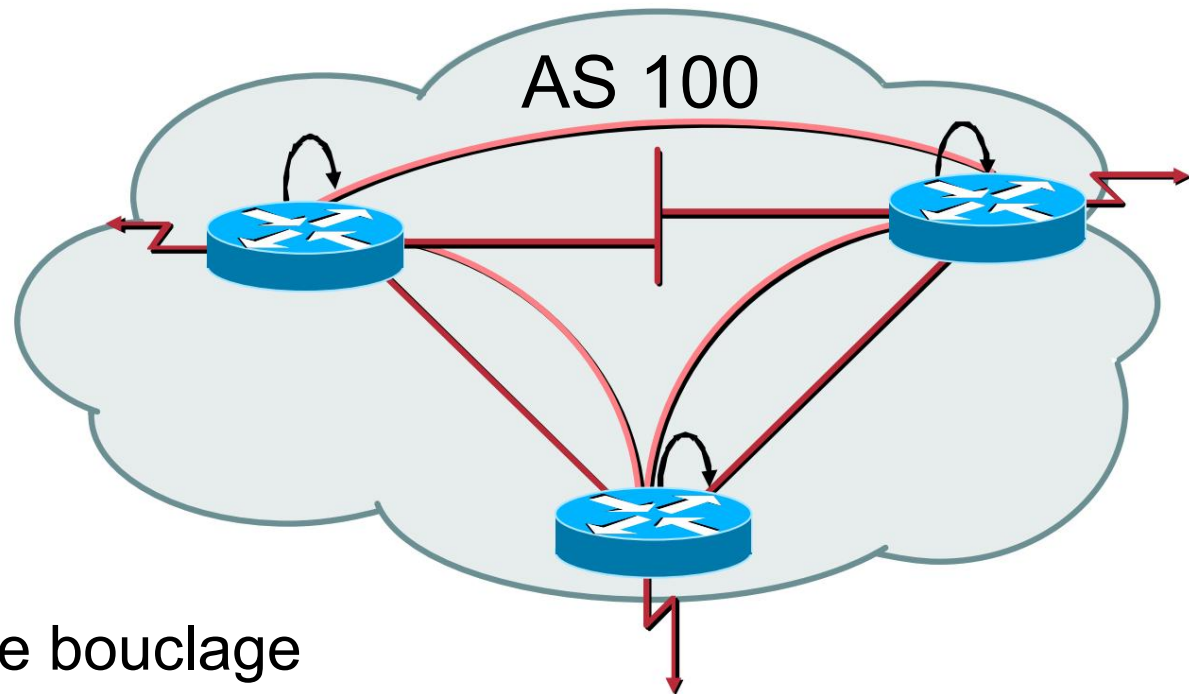
Peering BGP interne (iBGP)

reseauenclair.com



- Indépendant de la topologie
- Chaque locuteur iBGP doit s'appairer avec tous les autres locuteurs iBGP de l'AS

Appairage vers une adresse de bouclage



- Pair avec adresse de bouclage
L'interface de bouclage ne tombe jamais en panne !
- La session iBGP ne dépend pas de l'état d'un seul interface
- La session iBGP ne dépend pas de la topologie physique

Configuration du BGP interne

reseauenclair.com

Routeur A dans AS100

```
interface loopback 0 adresse IP
  215.10.7.1 255.255.255.255
!
routeur bgp 100 réseau
  220.220.1.0 voisin 215.10.7.2 distant-
  comme 100 voisin 215.10.7.2 source-de-mise-à-jour loopback0
  voisin 215.10.7.3 distant-comme 100 voisin 215.10.7.3 source-de-mise-à-jour
  loopback0
!
```

adresse IP sur
l'interface de bouclage

ASN locale

ASN locale

adresse IP de l'interface de
bouclage du routeur B

Configuration du BGP interne

reseauenclair.com

Routeur B dans AS100

```
interface loopback 0 adresse IP
  215.10.7.2 255.255.255.255
!
routeur bgp 100 réseau
  220.220.1.0 voisin 215.10.7.1 distant-
  comme 100 voisin 215.10.7.1 source de mise à jour loopback0
  voisin 215.10.7.3 distant-comme 100 voisin 215.10.7.3 source de mise à jour
  loopback0
!
```

adresse IP sur
l'interface de bouclage

ASN locale

ASN locale

adresse IP de l'interface de
bouclage du routeur A

BGP pour les fournisseurs de services Internet

reseauenclair.com

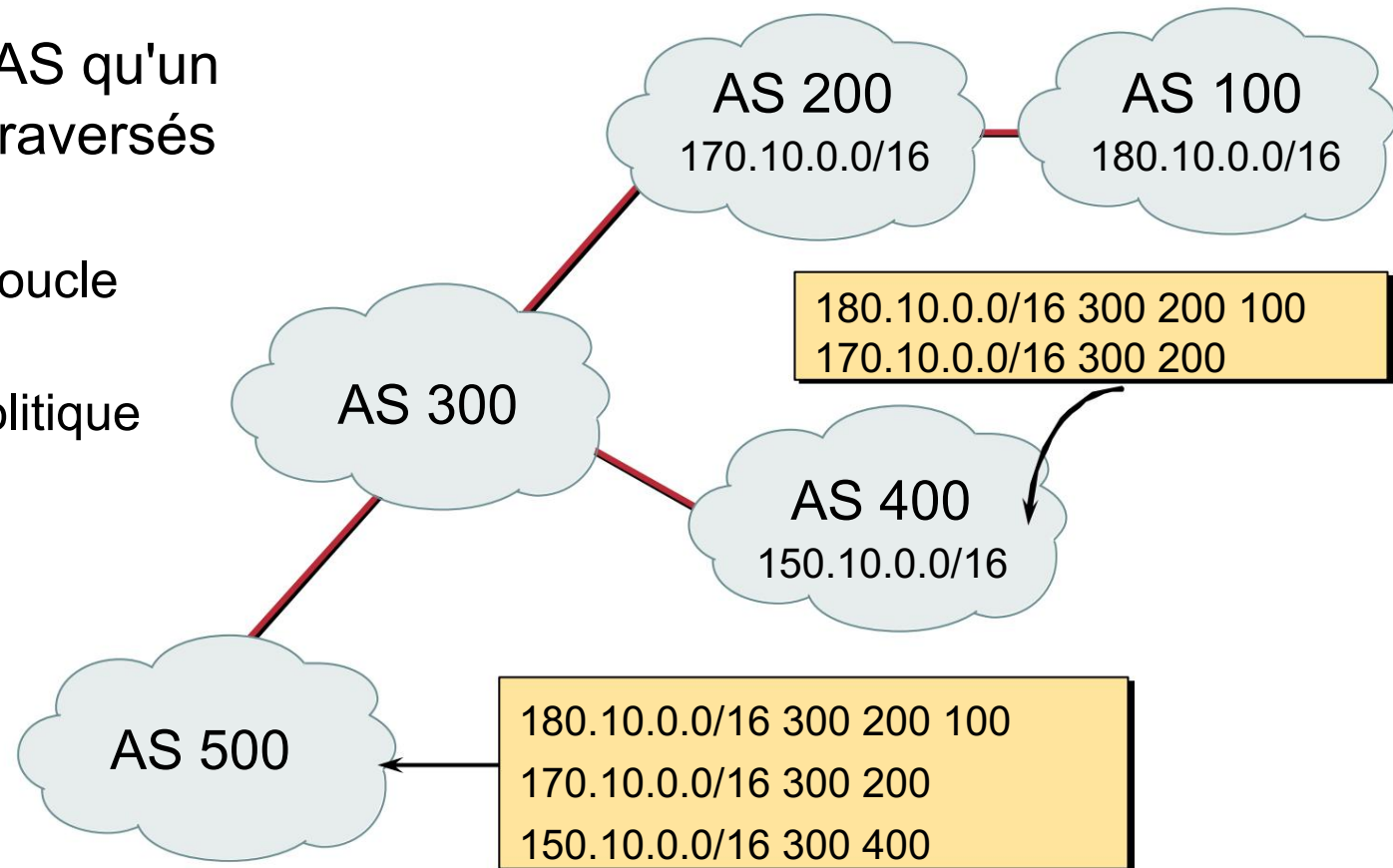
- Principes de base du routage
- Principes de base de BGP
- **Attributs BGP**
- Sélection du chemin BGP
- Politique BGP •
- Capacités BGP • Mise à
- l'échelle de BGP

Attributs BGP

Informations sur BGP

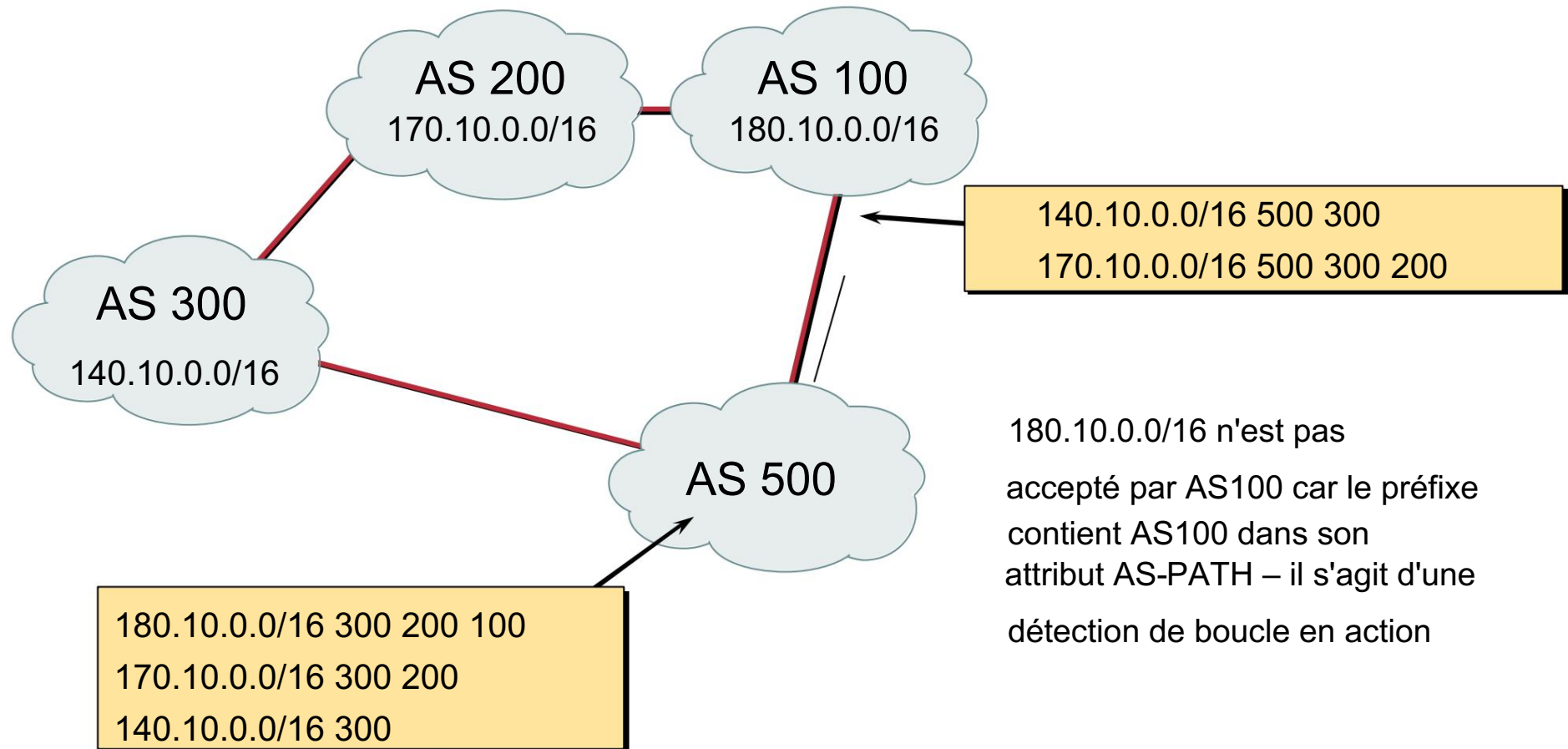
Chemin AS

- Séquence d'AS qu'un itinéraire a traversés
- Détection de boucle
- Appliquer la politique



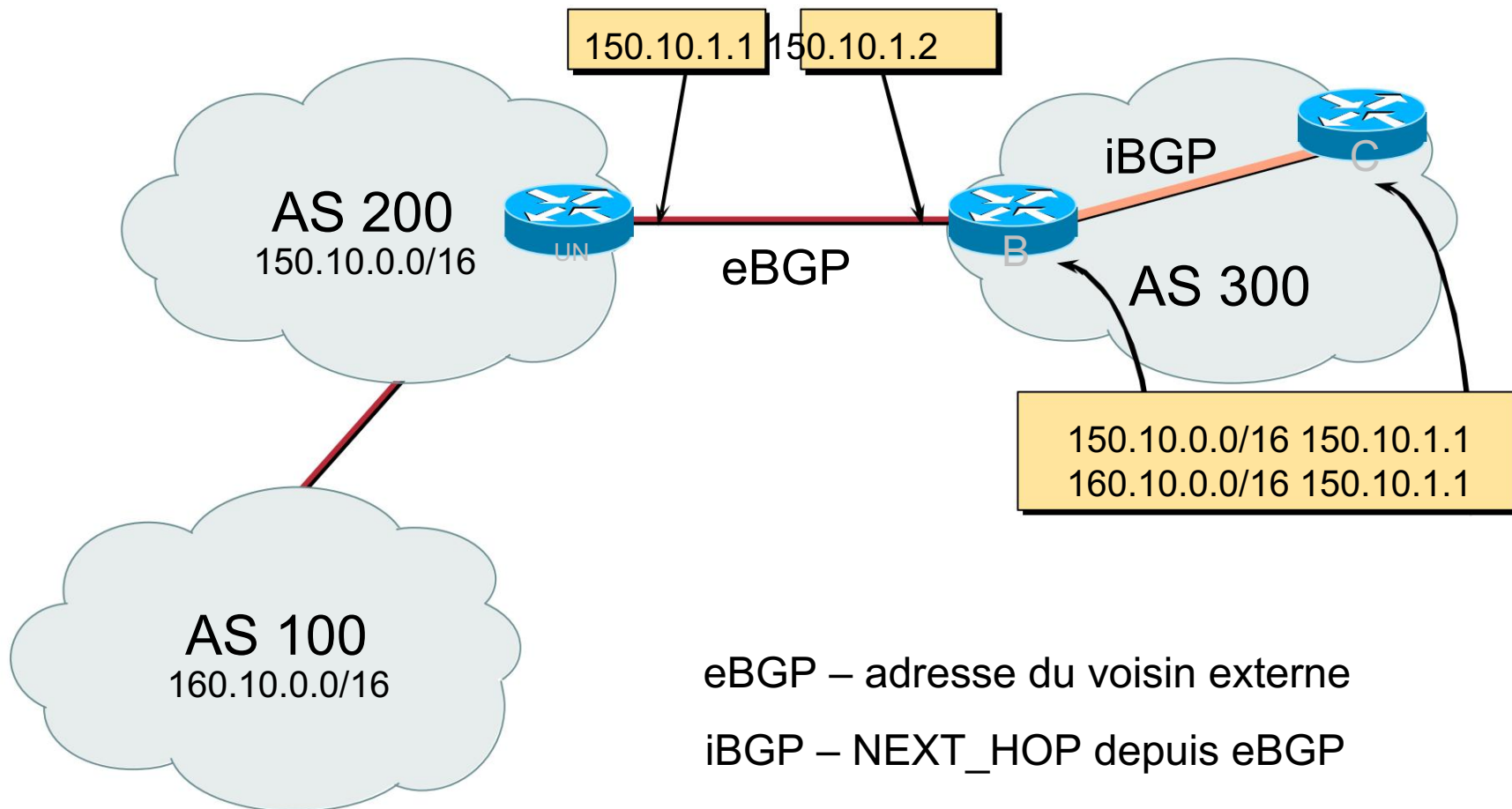
Détection de boucle AS-Path

reseauenclair.com



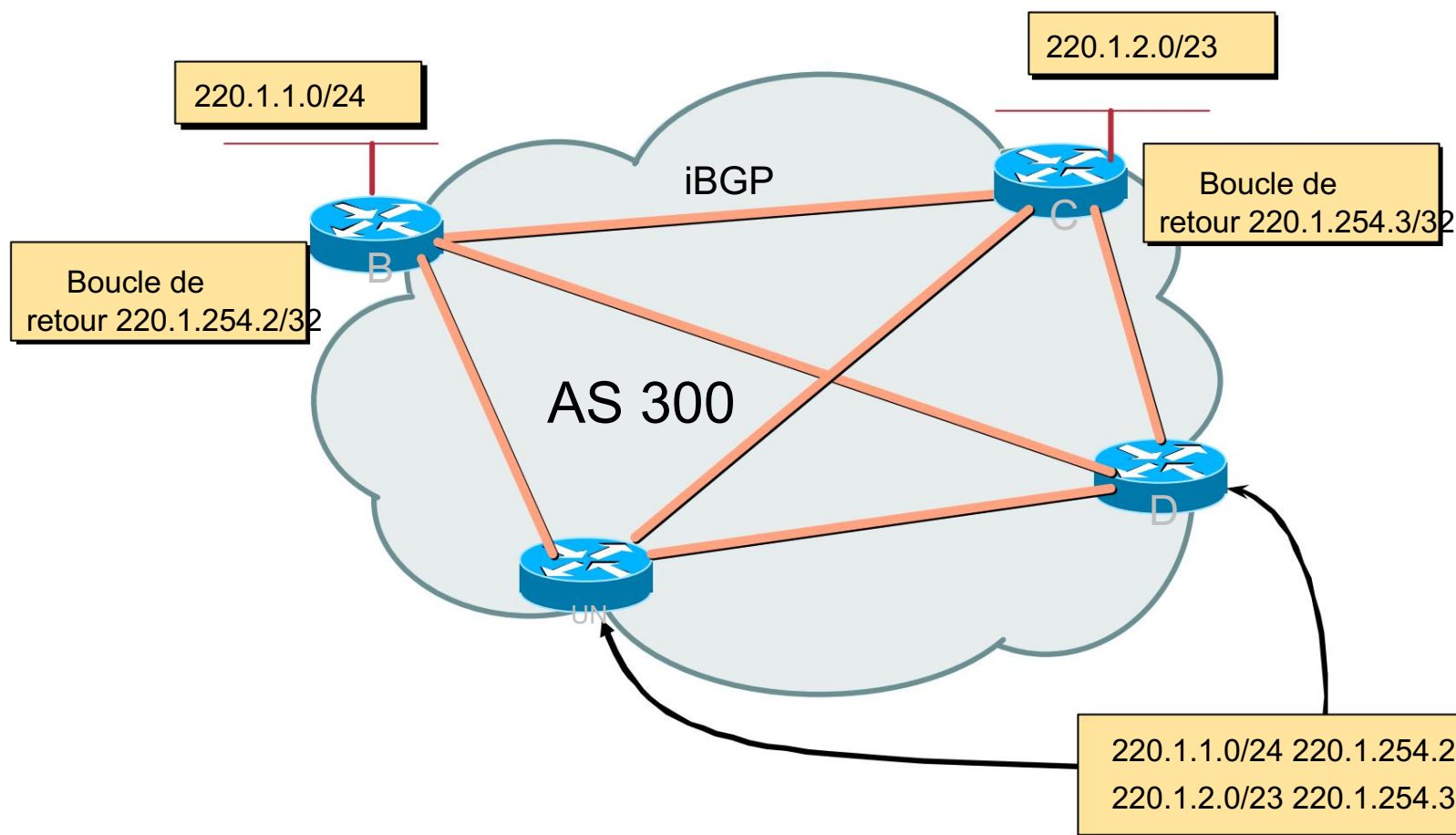
Prochain saut

reseauenclair.com



Prochain saut iBGP

reseauenclair.com



Le prochain saut est l'adresse de bouclage du routeur ibgp

Recherche d'itinéraire récursive

Prochain saut (résumé)

reseauenclair.com

- L'IGP doit transporter l'itinéraire vers les prochains sauts
- Recherche d'itinéraire récursive
- Dissocie BGP de la topologie physique réelle
- Permet à l'IGP de prendre des décisions de transfert intelligentes

Origine

reseauencclair.com

- Transmet l'origine du préfixe
- Attribut « Historique »
- Influence le choix du meilleur chemin
- Trois valeurs : IGP, EGP, incomplet

IGP – généré par la déclaration de réseau BGP

EGP – généré par EGP

incomplet – redistribué à partir d'un autre protocole de routage

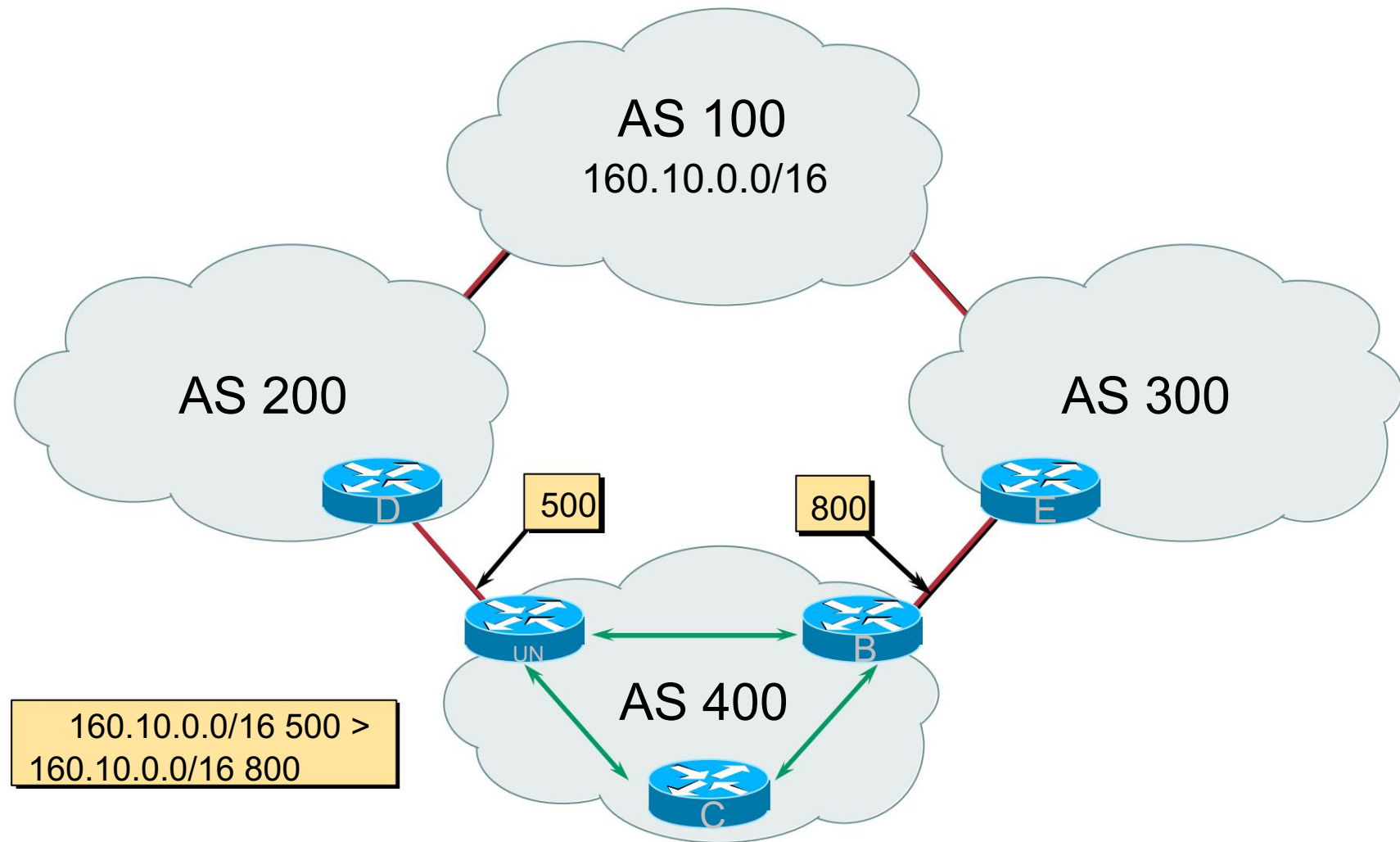
Agrégateur

reseauencclair.com

- Transmet l'adresse IP du routeur/haut-parleur BGP générant la route agrégée
- Utile à des fins de débogage
- N'influence pas le choix du meilleur chemin

Préférence locale

reseauenclair.com



Préférence locale

- Local à un AS – non transitif

La préférence locale par défaut est 100 (IOS)

- Utilisé pour influencer la sélection du chemin BGP

détermine le meilleur chemin pour le trafic **sortant**

- Le chemin avec la préférence locale la plus élevée gagne

Préférence locale

- Configuration du routeur B :

routeur bgp 400

voisin 220.5.1.1 distant-as 300 voisin 220.5.1.1 route-map

local-pref dans !

plan d'itinéraire permis local-pref 10

correspondance de la liste de préfixes d'adresses IP

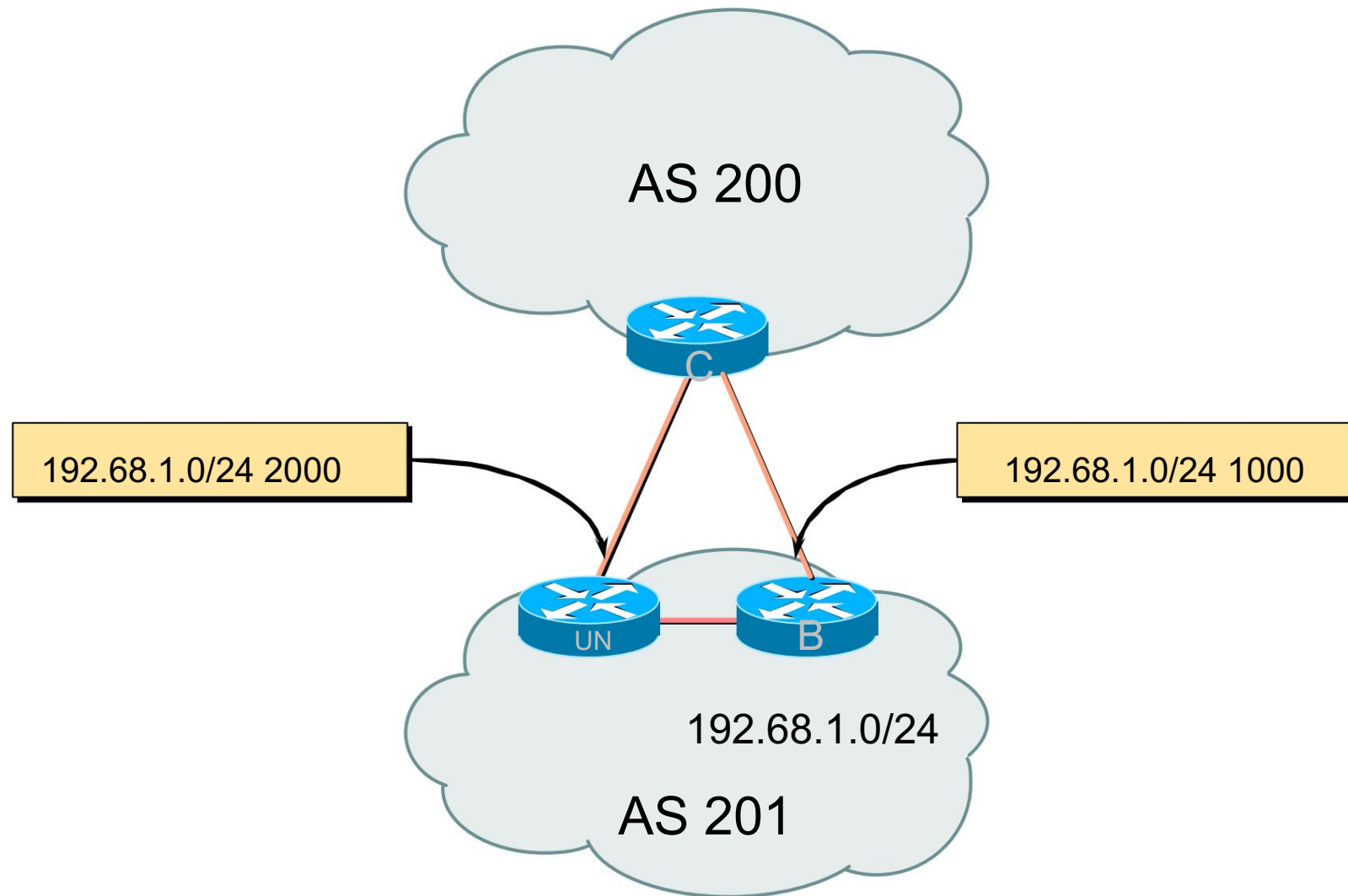
MATCH définir la préférence locale 800

!

liste de préfixes IP **MATCH** permis 160.10.0.0/16

Discriminateur à sorties multiples (MED)

reseauenclair.com



Discriminateur à sorties multiples

reseauenclair.com

- Inter-AS – non transitif
- Utilisé pour transmettre la préférence relative de l'entrée points

détermine le meilleur chemin pour le trafic **entrant**

- Comparable si les chemins proviennent du même AS
- La métrique IGP peut être transmise sous forme de MED

définir le type de métrique interne dans la carte d'itinéraire

Discriminateur à sorties multiples

reseauenclair.com

- Configuration du routeur B :

```
routeur bgp 400
```

```
voisin 220.5.1.1 distant-as 200 voisin 220.5.1.1 route-map
```

```
set-med out !
```

```
route-map set-med permit 10 match adresse IP
```

```
prefix-list MATCH
```

```
définir la métrique 1000
```

```
!
```

```
liste de préfixes IP MATCH permis 192.68.1.0/24
```

Poids

reseauencclair.com

- Pas vraiment un attribut – local au routeur

Permet le contrôle des politiques, similaire à la préférence locale

- Victoires avec le poids le plus élevé

- Appliqué à tous les itinéraires d'un voisin

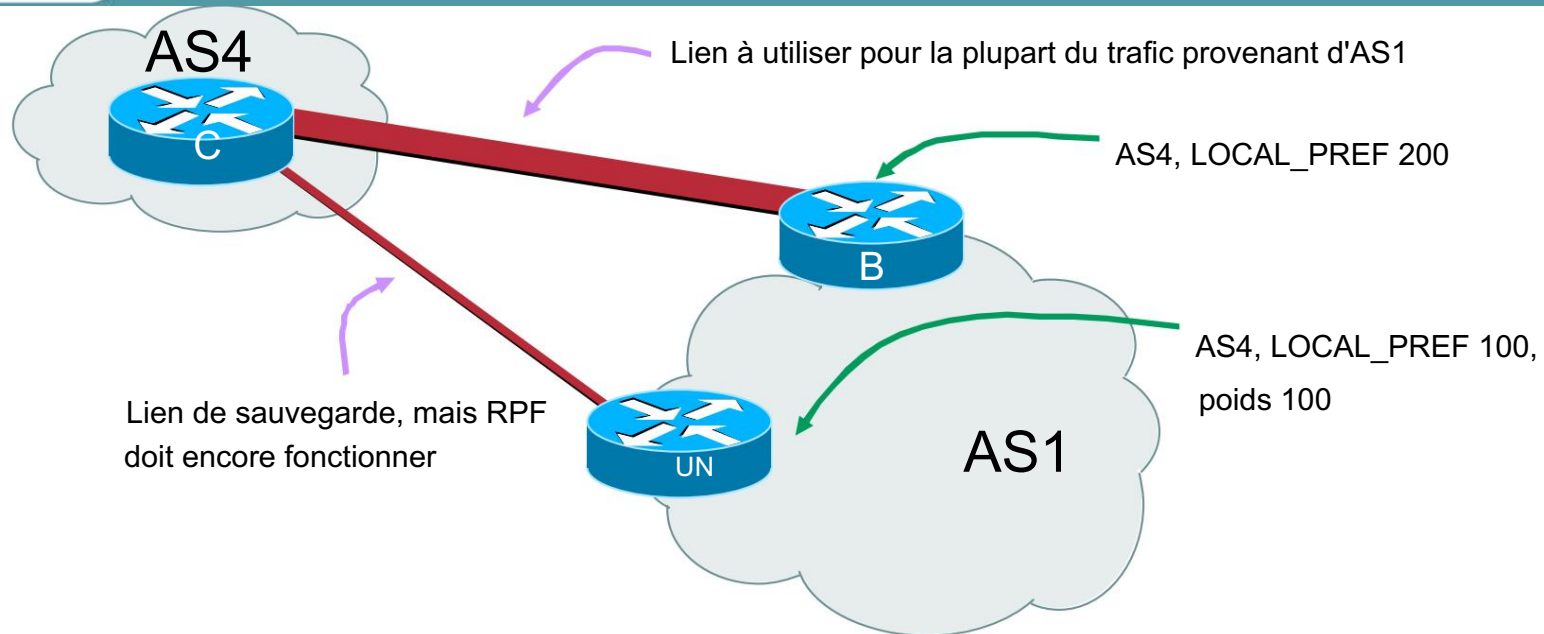
voisin 220.5.7.1 poids 100

- Poids attribué aux itinéraires en fonction du filtre

voisin 220.5.7.3 liste de filtres 3 poids 50

Poids – Utilisé pour aider au déploiement du RPF

reseauenclair.com



- Le meilleur chemin vers AS4 depuis AS1 passe toujours par B en raison de la préférence locale.
- Mais les paquets arrivant à A depuis AS4 via la liaison directe C vers A passeront le contrôle RPF car ce chemin a une priorité en raison du poids défini.

Si le poids n'était pas défini, le meilleur chemin pour revenir à AS4 serait via B, et le Le contrôle RPF échouerait

Communauté

reseauenclair.com

- Les communautés sont décrites dans la RFC1997
- entier 32 bits

Représenté sous forme de deux entiers de 16 bits (RFC1998)

Le format courant est <local-ASN>:xx

- Utilisé pour regrouper les destinations

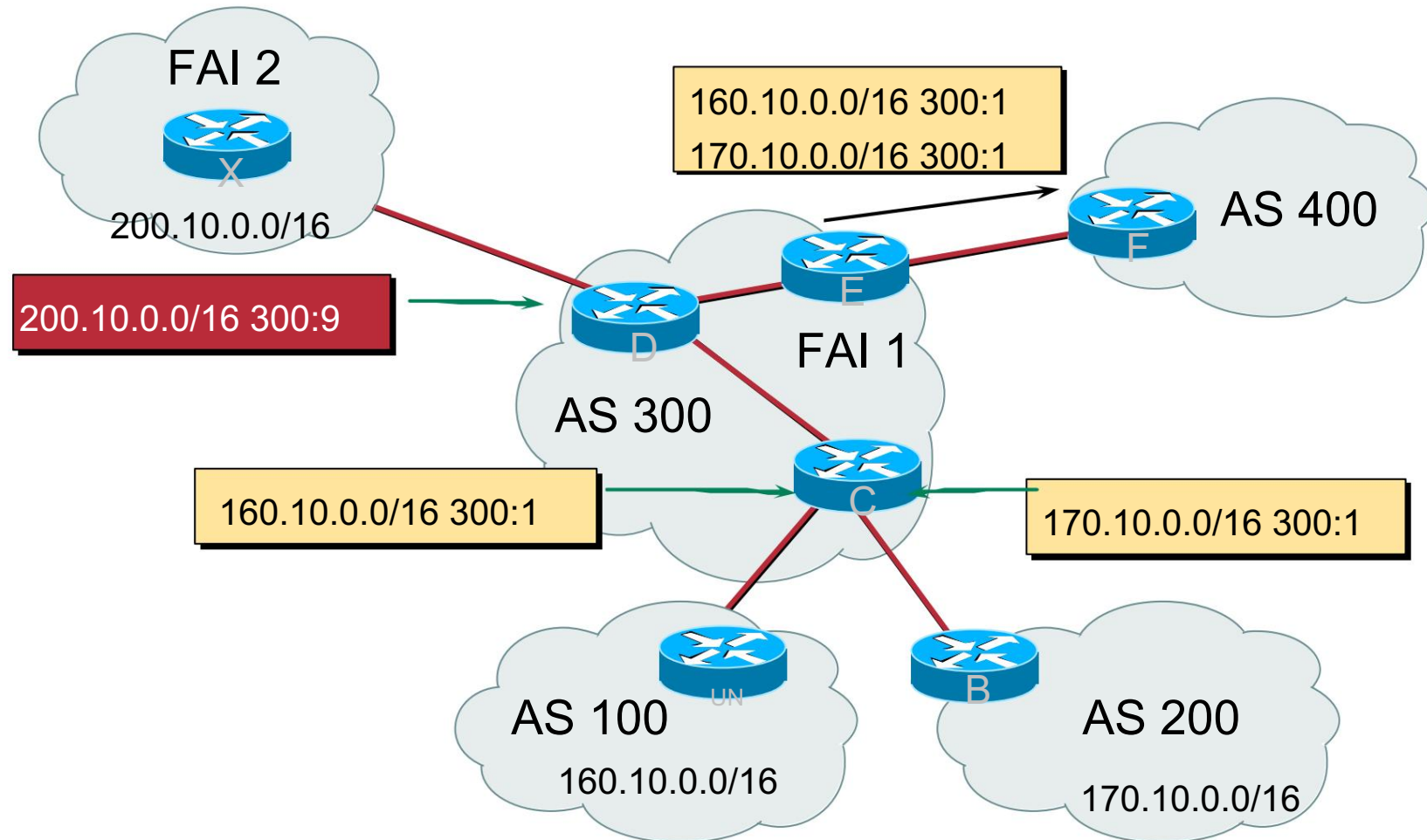
Chaque destination peut être membre de plusieurs communautés

- Attribut communautaire transporté à travers les AS •

Très utile dans l'application des politiques

Communauté

reseauenclair.com



Communautés bien connues

reseauenclair.com

- no-export ne pas

faire de publicité auprès des homologues eBGP

- pas de publicité

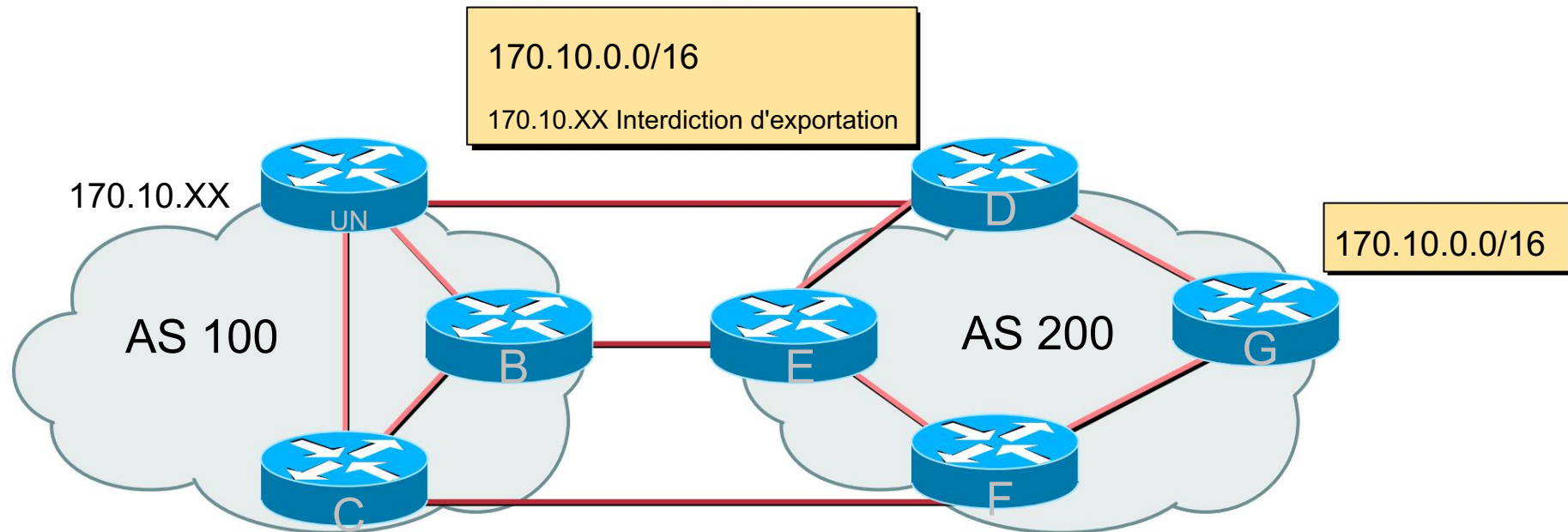
ne faites pas de publicité auprès d'un pair

- local-AS

ne pas faire de publicité en dehors de l'AS local (utilisé uniquement avec les confédérations)

Communauté sans exportation

reseauenclair.com



- AS100 annonce les agrégats et les sous-préfixes

l'objectif est d'améliorer le partage de charge en divulguant les sous-préfixes

- Sous-préfixes marqués avec une communauté **sans exportation** • Le routeur G dans AS200 n'annonce pas les préfixes avec une communauté **sans exportation** définie

BGP pour les fournisseurs de services Internet

reseauenclair.com

- Principes de base du routage
- Principes de base de BGP
- Attributs BGP
- Sélection du chemin BGP
- Politique BGP •
- Capacités BGP • Mise à
- l'échelle de BGP

Algorithme de sélection de chemin BGP

Pourquoi est-ce le meilleur chemin ?

- Ne pas prendre en compte le chemin s'il n'y a pas de route vers le prochain saut
- Ne pas prendre en compte le chemin iBGP s'il n'est pas synchronisé (Cisco IOS)
- Poids le plus élevé (local au routeur)
- Préférence locale la plus élevée (globale au sein de l'AS)
- Privilégiez les itinéraires d'origine locale
- Chemin AS le plus court

- Code d'origine le plus bas

IGP < EGP < incomplet

- Discriminateur multi-sorties le plus bas (MED)

Si **bgp déterministe-médical**, ordonnez les chemins avant de comparer

Si **bgp always-compare-med**, alors comparez pour tous les chemins

sinon MED n'est pris en compte que si les chemins proviennent du même AS (par défaut)

Algorithme de sélection de chemin BGP

Troisième partie

reseauenclair.com

- Préférer le chemin eBGP au chemin iBGP
- Chemin avec la métrique IGP la plus basse jusqu'au prochain saut
- ID de routeur le plus bas (ID d'origine pour le réfléchi)
itinéraires)
- Liste de clusters la plus courte

Le client **doit** être conscient des attributs de Route Reflector !

- Adresse IP du voisin le plus bas

BGP pour les fournisseurs de services Internet

reseauenclair.com

- Principes de base du routage
- Principes de base de BGP
- Attributs BGP
- Sélection du chemin BGP
- Politique BGP •

Capacités BGP • Mise à
l'échelle de BGP

Application de la politique avec BGP

Contrôle!

Application de la politique avec BGP

reseauenclair.com

- Application de la politique

Décisions basées sur le chemin AS, la communauté ou le préfixe

Rejeter/accepter les itinéraires sélectionnés

Définir des attributs pour influencer la sélection du chemin

- Outils:

Liste de préfixes (préfixes de filtrage)

Liste de filtres (filtrer les AS)

Cartes routières et communautés

- Filtrer les itinéraires en fonction du préfixe
- Entrant et sortant

routeur bgp 200

voisin 220.200.1.1 distant-as 210

voisin 220.200.1.1 liste de préfixes **PEER-IN** dans

voisin 220.200.1.1 liste de préfixes **PEER-OUT** sortie

!

liste de préfixes IP **PEER-IN** refuser 218.10.0.0/16 liste de

préfixes IP **PEER-IN** autoriser 0.0.0.0/0 le 32 liste de préfixes IP

PEER-OUT autoriser 215.7.0.0/16

- Filtrer les itinéraires en fonction du chemin AS
- Entrant et sortant

routeur bgp 100

voisin 220.200.1.1 distant-as 210 voisin

220.200.1.1 liste-de-filtres 5 sorties voisin 220.200.1.1

liste-de-filtres 6 entrées

!

ip as-path access-list 5 permit ^200\$ ip as-path access-list 6 permit ^150\$

Comme les expressions régulières Unix

.	Associez un caractère
*	Faire correspondre n'importe quel nombre d'expressions précédentes
+	Faites correspondre au moins une des expressions précédentes
^	Début de ligne
\$	Fin de ligne
_	Début, fin, espace blanc, accolade
	Ou
()	crochets pour contenir l'expression

Exemples simples

.*	Associez n'importe quoi
.+	Faites correspondre au moins un caractère
^\$	Faire correspondre les itinéraires locaux à cet AS
_1800\$	Originaire de 1800
^1800_	Reçu à partir de 1800
1800	Via 1800
_790_1800_	Passant par 1800 puis 790
(1800)+	Associez au moins un élément parmi 1 800 dans la séquence
\\(65350\\)	Via 65350 (confédération AS)

Exemples pas si simples

`^[0-9]+$`

Correspond à la longueur AS_PATH d'un

`^[0-9]+_[0-9]+$`

Correspond à la longueur AS_PATH de deux

`^[0-9]*_[0-9]+$`

Faites correspondre la longueur AS_PATH d'un ou deux

`^[0-9]*_[0-9]*$`

Faites correspondre la longueur AS_PATH d'un ou deux
(correspondra également à zéro)

`^[0-9]+_[0-9]+_[0-9]+$ (701|`

Correspond à la longueur AS_PATH de trois

`1800)_`

Faites correspondre tout ce qui est passé par
AS701 ou AS1800

`_1849(_+_)12163$`

Correspond à tout ce qui est d'origine AS12163
et passé par AS1849

- Que fait cet exemple ?

```
refuser ^\((6(451[2-9]4[6-9]..|5...)(_6(451[2-9]4[6-9]..|5...))*\)_.*\(\ permettre ^\((6(451[2-9]4[6-9]..|5...)(_6(451[2-9]4[6-9]..|5...))*\) refuser \(\ permettre .*
```

- Merci à Dorian Kim et John Heasley de Verio/NTT

- Un plan d'itinéraire est comme un « programme » pour IOS
- A des numéros de « ligne », comme des programmes
- Chaque ligne est une condition/action distincte • Le

concept est fondamentalement :

si correspondance alors exécuter l'expression et quitter
autre

si correspondance alors exécuter l'expression et quitter
sinon etc.

- Exemple utilisant des listes de préfixes

routeur bgp 100 voisin

1.1.1.1 **filtre** de carte de route dans ! **filtre de** carte de route autoriser 10

correspondance liste de préfixes d'adresses IP **HIGH-**

PREF définir la préférence locale 120 ! **filtre de** carte de route autoriser

20 correspondance liste de préfixes d'adresses

IP **LOW-PREF** définir la préférence locale 80 ! **filtre**

de carte de route autoriser 30 ! liste de préfixes IP **HIGH-PREF** autoriser

10.0.0.0/8 liste de préfixes IP **LOW-PREF**

autoriser 20.0.0.0/8

- Exemple d'utilisation de listes de filtres

routeur bgp 100 voisin

220.200.1.2 route-map **filter-on-as-path** dans ! route-map **filter-on-as-path** autoriser 10 correspondre

à as-path **1** définir la préférence locale 80 ! route-map **filter-on-as-path**

autoriser 20 correspondre à

as-path **2** définir la préférence locale 200 !

route-map **filter-on-as-path** autoriser 30 !

ip as-path access-list 1 permis **_150\$** ip as-path access-list 2 permis
210

- Exemple de configuration du préfixe AS-PATH

routeur bgp 300

réseau 215.7.0.0

voisin 2.2.2.2 distant-as 100 voisin 2.2.2.2

route-map SETPATH out

!

route-map SETPATH permis 10

définir comme chemin d'accès préfixe 300 300

- Utilisez votre propre numéro AS lorsque vous ajoutez un préfixe

Dans le cas contraire, la détection de boucle BGP peut provoquer des déconnexions

Contrôle des politiques

Établissement de communautés

reseauenclair.com

- Exemple de configuration du routeur

```
bgp 100
```

```
  voisin 220.200.1.1 distant-as 200
```

```
  voisin 220.200.1.1 envoyer-communauté voisin
```

```
  220.200.1.1 route-map définir-communauté sortie
```

```
!
```

```
ensemble de cartes d'itinéraires et de communautés, permis 10
```

```
  correspondance adresse IP liste de préfixes NO-ANNOUNCE
```

```
  définir communauté no-export
```

```
!
```

```
ensemble de cartes routières et de communautés, permis 20
```

```
!
```

```
liste de préfixes IP NO-ANNOUNCE permis 172.168.0.0/16 ge 17
```

BGP pour les fournisseurs de services Internet

reseauenclair.com

- Principes de base du routage
- Principes de base de BGP
- Attributs BGP
- Sélection du chemin BGP
- Politique BGP •
- Capacités BGP • Mise à l'échelle de BGP

Capacités BGP

Extension de BGP

Capacités BGP

- Documenté dans la RFC2842
- Paramètres de capacités transmis dans le message ouvert BGP
- Les fonctionnalités inconnues ou non prises en charge entraîneront un message de NOTIFICATION
- Codes :
 - 0 à 63 sont attribués par l'IANA par consensus IETF
 - 64 à 127 sont attribués par l'IANA « premier arrivé, premier servi »
 - 128 à 255 sont spécifiques au fournisseur

Capacités BGP

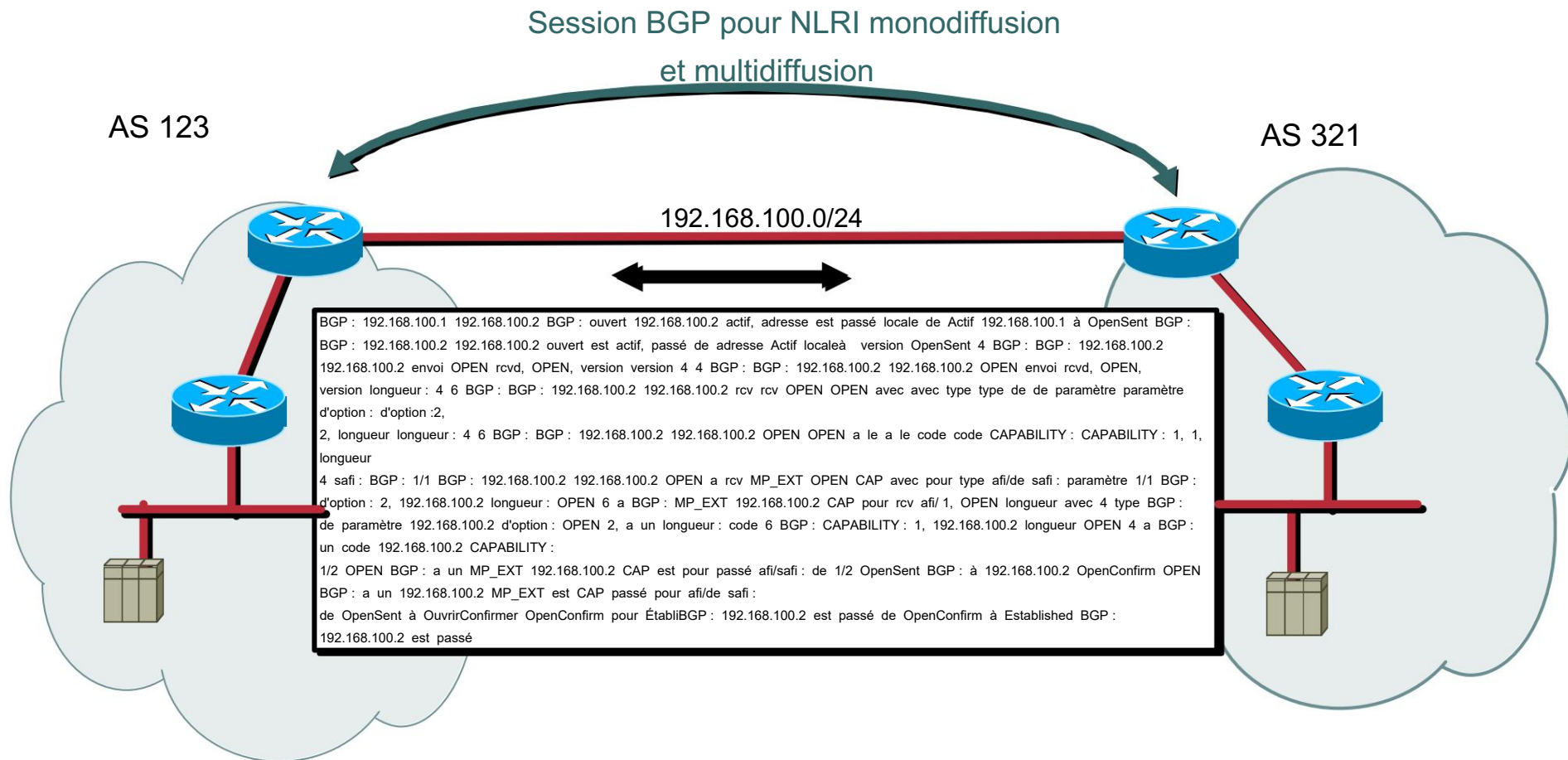
Les capacités actuelles sont :

0 Réserve	[RFC3392]
1 Extensions multiprotocoles pour BGP-4	[RFC2858]
2 Capacité de rafraîchissement de route pour BGP-4	[RFC2918]
3 Capacité de filtrage d'itinéraire coopératif	[]
4 Capacité de routes multiples vers une destination [RFC3107]	
64 Capacité de redémarrage progressif	[]
65 Prise en charge des ASN de 4 octets	[]
66 Prise en charge de la capacité dynamique	[]

Voir <http://www.iana.org/assignments/capability-codes>

Négociation des capacités BGP

reseauenclair.com



BGP pour les fournisseurs de services Internet

reseauenclair.com

- Principes de base du routage
- Principes de base de BGP
- Attributs BGP
- Sélection du chemin BGP
- Politique BGP •

Capacités BGP • Mise à
l'échelle de BGP

Techniques de mise à l'échelle BGP

Techniques de mise à l'échelle BGP

reseauenclair.com

- Comment un prestataire de services :

Faire évoluer le maillage iBGP au-delà de quelques pairs ?

Mettre en œuvre une nouvelle politique sans provoquer de remous ni de changements d'itinéraires ?

Réduire la surcharge des routeurs ?

Maintenir le réseau stable, évolutif et simple ?

Techniques de mise à l'échelle BGP

reseauenclair.com

- Actualisation de l'itinéraire
- Groupes de pairs •

Amortissement des volets de route

- Réflecteurs de route et confédérations

Actualisation de l'itinéraire

Problème:

- Réinitialisation matérielle des homologues BGP requise après chaque changement de politique, car le routeur ne stocke pas les préfixes rejetés par la politique

- Réinitialisation matérielle des homologues BGP :

Détruit le peering BGP

Consomme du CPU

Perturbe gravement la connectivité de tous les réseaux

Solution:

- Actualisation de l'itinéraire

Capacité de rafraîchissement de l'itinéraire

reseauencclair.com

- Facilite les changements de politique non perturbateurs • Aucune configuration n'est nécessaire

Négocié automatiquement lors de l'établissement des pairs

- Aucune mémoire supplémentaire n'est utilisée
- Nécessite que les routeurs homologues prennent en charge « route « capacité de rafraîchissement » – RFC2918
- effacer l'adresse IP bgp xxxx indique au pair de renvoyer l'annonce BGP complète
- effacer l'adresse IP bgp xxxx renvoie le BGP complet annonce aux pairs

Reconfiguration dynamique

reseauencclair.com

- Utiliser la fonction d'actualisation de l'itinéraire si elle est prise en charge

découvrez à partir de « show ip bgp neighbor »

Non perturbateur, « Bon pour Internet »

- Sinon, utilisez la reconfiguration logicielle IOS
fonctionnalité

- Réinitialisez uniquement un peering BGP en dernier

station balnéaire

Considérez l'impact comme équivalent à
un redémarrage du routeur

Reconfiguration souple

- Le routeur stocke normalement les préfixes qui ont été reçus du pair après l'application de la politique

L'activation de la reconfiguration logicielle signifie que le routeur stocke également les préfixes/attributs avant toute application de politique

- De nouvelles politiques peuvent être activées sans démontage et redémarrage de la session de peering

- Configuré sur une base par voisin • Utilise plus

de mémoire pour conserver les préfixes dont les attributs ont été modifiés ou n'ont pas été acceptés • Également **avantageux**

lorsque l'opérateur a besoin de savoir quels préfixes ont été envoyés à un routeur avant l'application de toute politique entrante

Configuration de la reconfiguration logicielle

reseauencclair.com

routeur bgp 100

voisin 1.1.1.1 distant-as 101

voisin 1.1.1.1 route-map infiltrer dans

voisin 1.1.1.1 reconfiguration logicielle entrante

! Le trafic sortant n'a pas besoin d'être configuré !

Ensuite, lorsque nous modifions la politique, nous émettons une commande exec

effacer l'ip bgp 1.1.1.1 soft [entrée | sortie]

Groupes de pairs

Groupes de pairs

Sans groupes de pairs

- Les voisins iBGP reçoivent la même mise à jour
- Le grand maillage iBGP est lent à construire
- Le processeur du routeur est gaspillé en calculs répétitifs

Solution – les groupes de pairs !

- Regrouper les pairs avec la même politique sortante
- Les mises à jour sont générées une fois par groupe

Groupes de pairs – Avantages

reseauenclair.com

- Facilite la configuration • Rend la configuration moins sujette aux erreurs
- Rend la configuration plus lisible
- Charge CPU du routeur réduite
- Le maillage iBGP se construit plus rapidement
- Les membres peuvent avoir une politique entrante différente
- Peut également être utilisé pour les voisins eBGP !

Configuration du groupe de pairs

reseauenclair.com

routeur bgp 100

voisin ibgp-peer groupe de pairs

voisin ibgp-peer remote-as 100

voisin ibgp-peer update-source loopback 0

voisin ibgp-peer send-community

voisin ibgp-peer route-map filtre de sortie

voisin 1.1.1.1 groupe de pairs ibgp-peer

voisin 2.2.2.2 groupe de pairs ibgp-peer

voisin 2.2.2.2 route-map infiltrer dans

voisin 3.3.3.3 groupe de pairs ibgp-peer

! notez comment 2.2.2.2 a un filtre entrant différent de celui du groupe homologue !

Configuration du groupe de pairs

reseauenclair.com

routeur bgp 100

voisin pair externe groupe de pairs

voisin pair externe communauté d'envoi

voisin homologue externe route-map set-metric out

voisin 160.89.1.2 distant-as 200

voisin 160.89.1.2 groupe de pairs pair externe

voisin 160.89.1.4 distant-as 300

voisin 160.89.1.4 groupe de pairs pair externe

voisin 160.89.1.6 distant-as 400

voisin 160.89.1.6 groupe de pairs pair externe

voisin 160.89.1.6 filtre-liste infiltré dans

Groupes de pairs

reseauencclair.com

- Configurez toujours les groupes de pairs pour iBGP

Même s'il n'y a que quelques homologues iBGP

Un réseau plus facile à faire évoluer à l'avenir

Facilite grandement la configuration des modèles

- Envisagez d'utiliser des groupes de pairs pour eBGP

Particulièrement utile pour plusieurs clients BGP utilisant le même AS (RFC2270)

Également utile aux points d'échange où la politique du FAI est généralement la même pour chaque homologue

Amortissement des volets de route

Stabiliser le réseau

Amortissement des volets de route

reseauenclair.com

- Volet de route

Montée et descente du chemin ou changement d'attribut

RETRAIT BGP suivi de MISE À JOUR = 1 volet

La réinitialisation du peering de voisinage eBGP n'est PAS un problème

Des répercussions sur l'ensemble d'Internet

Gaspille du CPU

- L'amortissement vise à réduire la portée de la propagation du battement de route

Amortissement des volets de route (suite)

reseauencclair.com

- Exigences

- Convergence rapide pour les changements d'itinéraire normaux

- L'histoire prédit le comportement futur

- Supprimer les routes oscillantes

- Annoncer des itinéraires stables

- Documenté dans la RFC2439

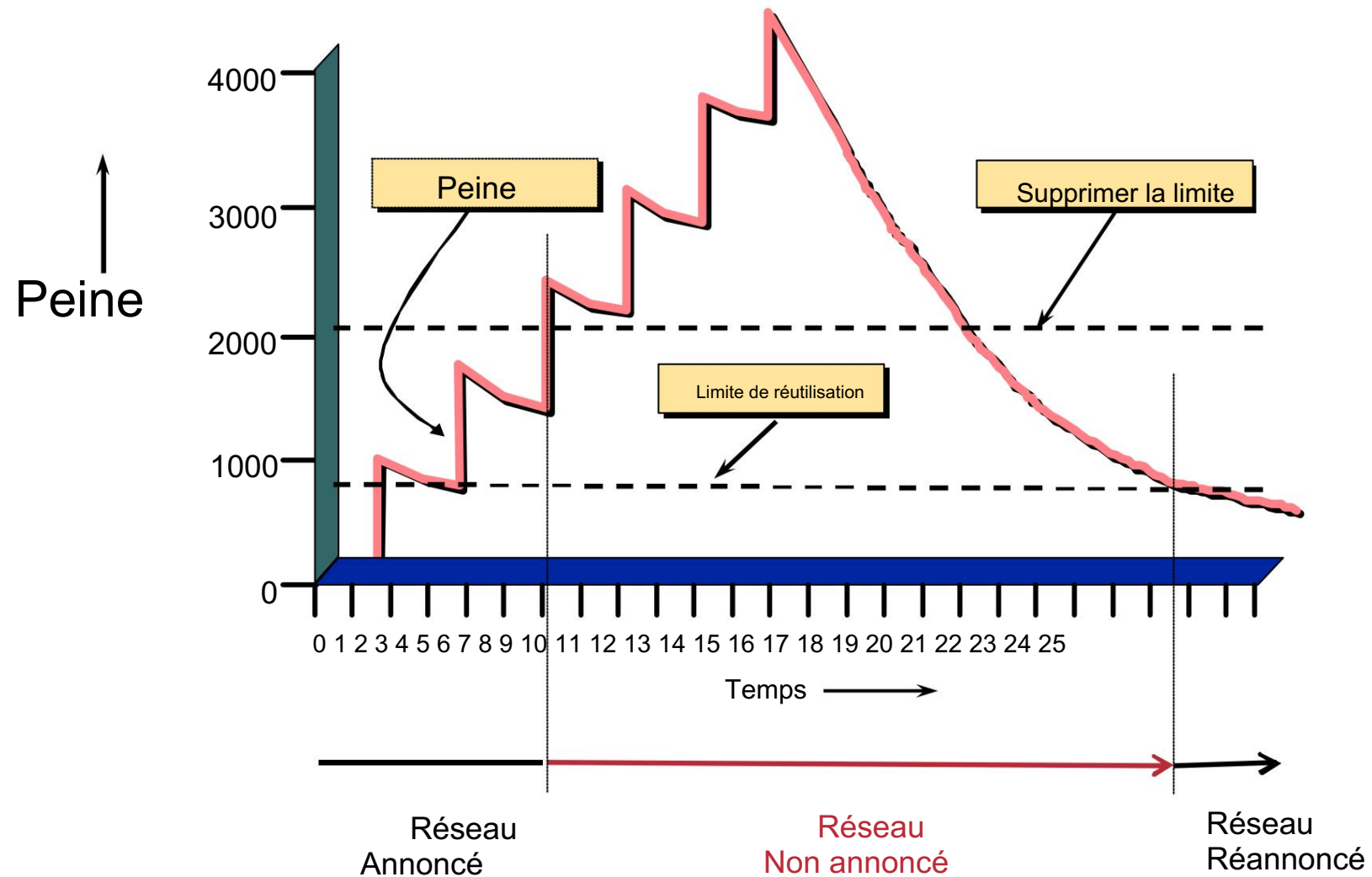
Opération

reseauencclair.com

- Ajouter une pénalité (1000) pour chaque volet
Le changement d'attribut entraîne une pénalité de 500
- La demi-vie de la pénalité de décroissance
exponentielle détermine le taux de décroissance
- Pénalité supérieure à la limite de suppression
ne pas annoncer la route aux homologues BGP
- Pénalité décrétée en dessous de la limite de réutilisation
réannoncer l'itinéraire aux homologues BGP, la
pénalité est réinitialisée à zéro lorsqu'elle atteint la moitié de la limite de réutilisation

Opération

reseauenclair.com



Opération

reseauencclair.com

- S'applique uniquement aux annonces entrantes provenant d'homologues

eBGP • Chemins alternatifs toujours

utilisables • Contrôlé par :

Demi-vie (par défaut 15 minutes)

limite de réutilisation (par

défaut 750) limite de suppression (par

défaut 2000) temps de suppression maximal (par défaut 60 minutes)

Configuration

reseauenclair.com

Amortissement fixe

routeur bgp 100

Amortissement BGP [<demi-vie> <valeur de réutilisation> <pénalité de suppression> <temps de suppression maximal>]

Amortissement sélectif et variable

amortissement bgp [route-map <nom>]

Recommandations

d'amortissement variable pour les FAI

<http://www.ripe.net/docs/ripe-229.html>

Opération

reseauenclair.com

- Attention requise lors du réglage des paramètres
- La pénalité doit être inférieure à la limite de réutilisation au temps de suppression maximal
- Le temps de suppression maximal et la demi-vie doivent permettre que la pénalité soit supérieure à la limite de suppression

Configuration

reseauenclair.com

- Exemples - ^o

amortissement bgp 30 750 3000 60

une limite de réutilisation de 750 signifie que la pénalité maximale possible est de 3 000 – aucun préfixe n'est supprimé car la pénalité ne peut pas dépasser la limite de suppression

- Exemples - ^s

amortissement bgp 30 2000 3000 60

la limite de réutilisation de 2 000 signifie que la pénalité maximale possible est de 8 000 – la limite de suppression est facilement atteinte

- La valeur maximale de la pénalité est

$$\text{max-penalty} = \text{reuse-limit} \times 2^{\left(\frac{\text{max-suppress-time}}{\text{half-life}} \right)}$$

- Assurez-vous toujours que la limite de suppression est **INFÉRIEUR** à la pénalité maximale sinon il n'y aura pas d'amortissement des volets

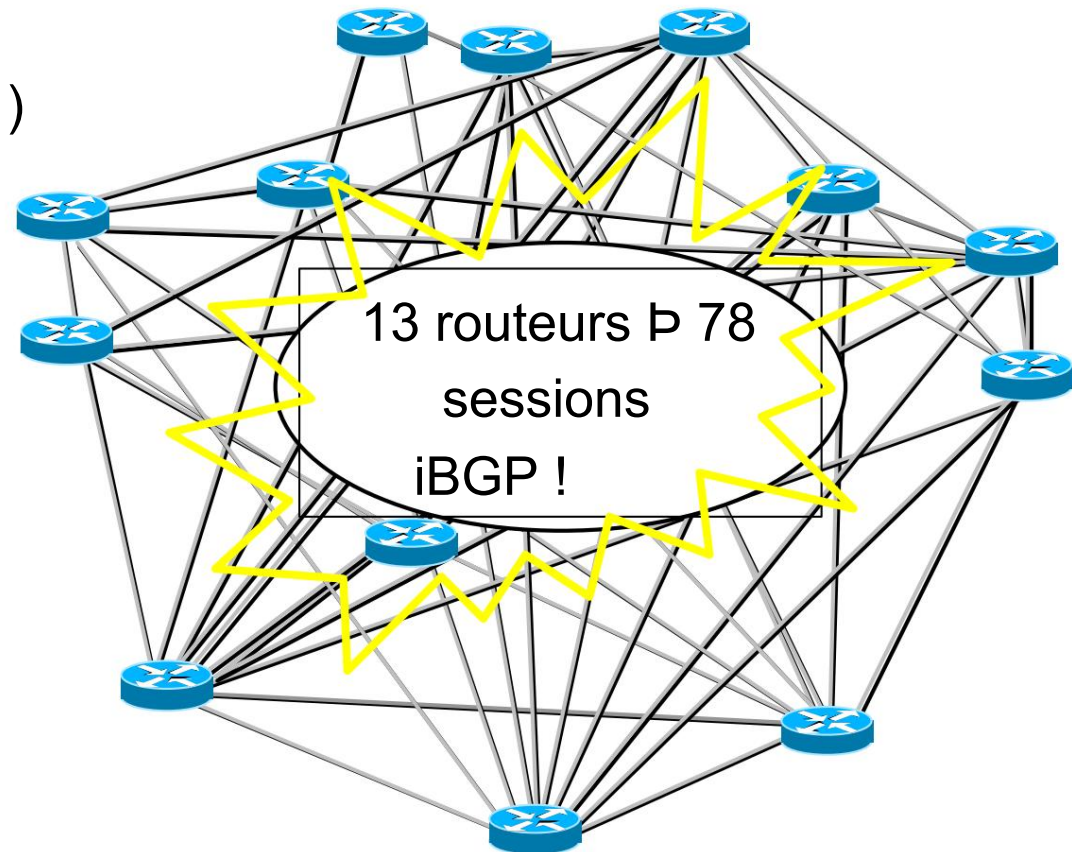
Réflecteurs de route et confédérations

Mise à l'échelle du maillage iBGP

reseauenclair.com

Évitez le maillage iBGP $\frac{1}{2}n(n-1)$

**$n=1000 \Rightarrow$ près d'un
demi-million de
sessions ibgp !**



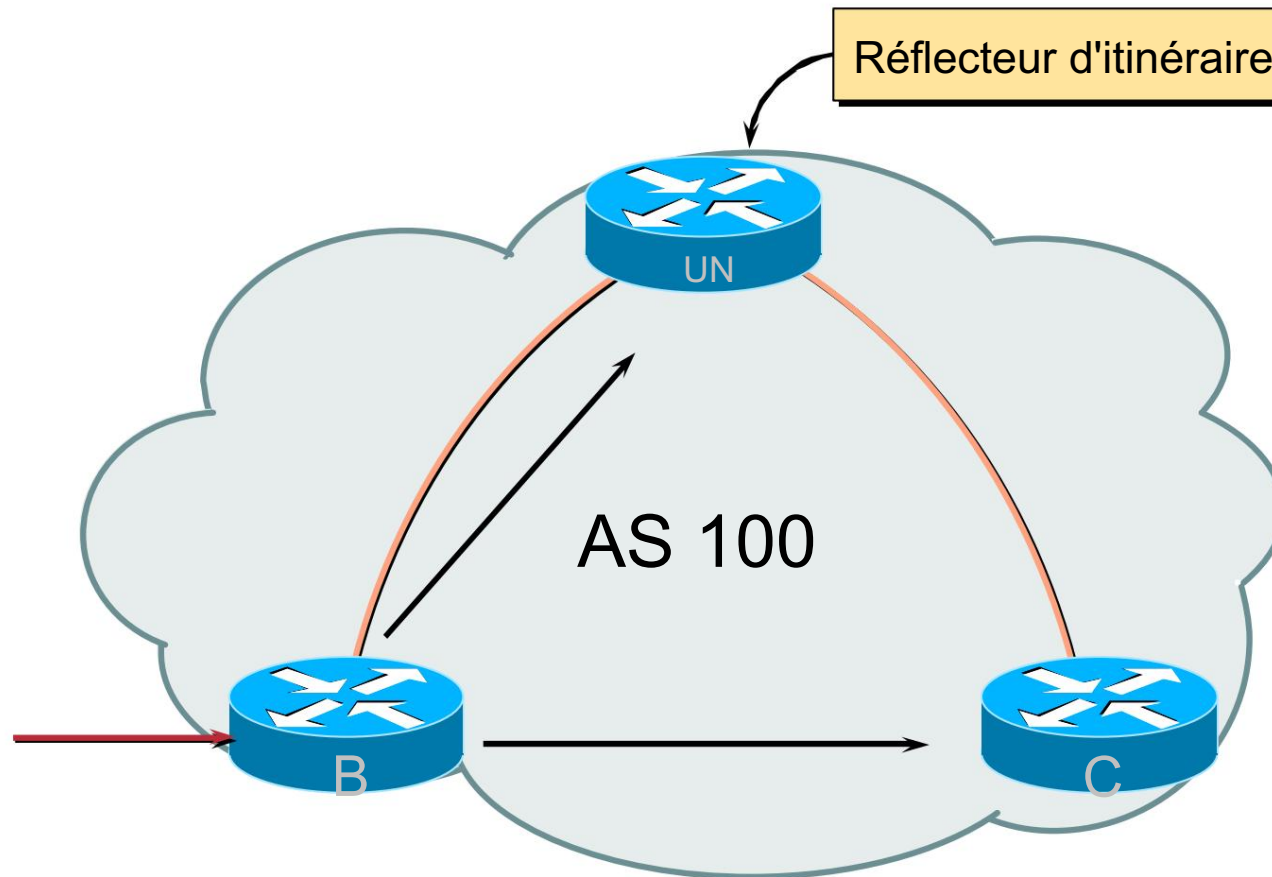
Deux solutions

Réflecteur d'itinéraire – plus simple à déployer et à exécuter

Confédération – avantages plus complexes et spécifiques aux cas particuliers

Réflecteur de route : principe

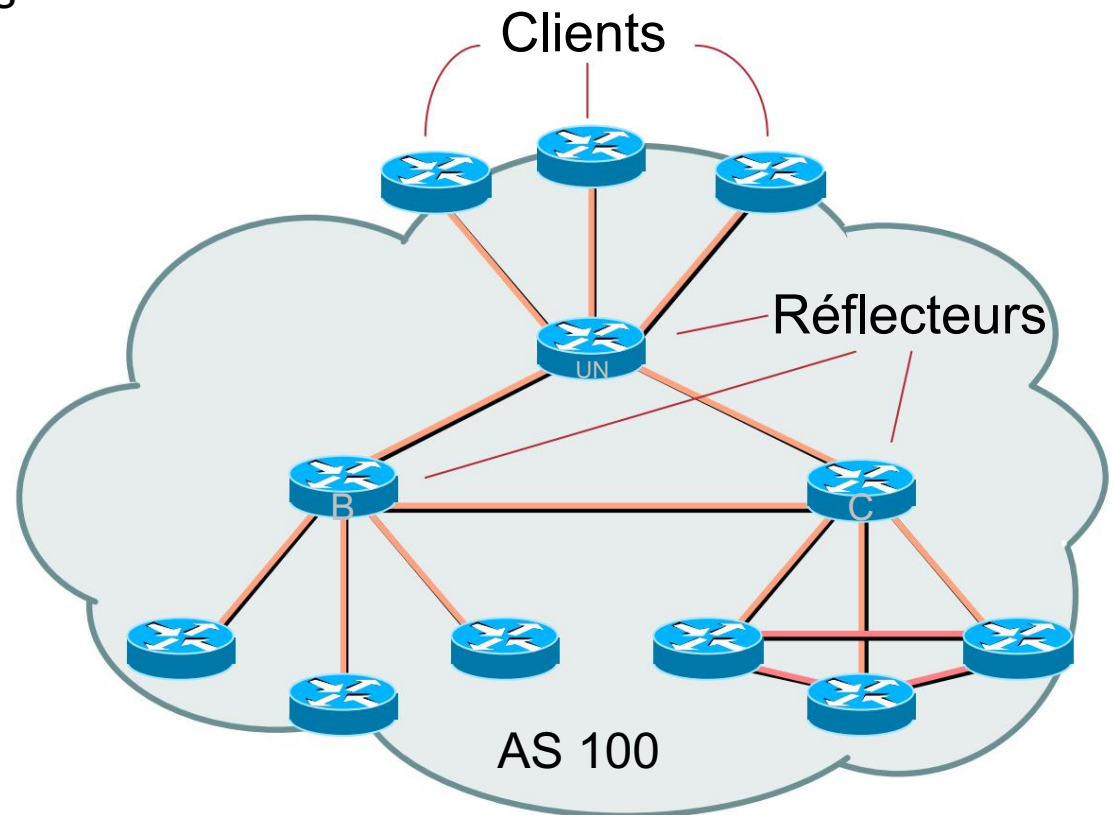
reseauenclair.com



Réflecteur d'itinéraire

reseauenclair.com

- Le réflecteur reçoit le chemin des clients et des non-clients
- Sélectionne le meilleur chemin
- chemin • Si le meilleur chemin vient de client, refléter auprès des autres clients et non-clients
- Si le meilleur chemin est celui des non-clients, réfléchissez-y uniquement pour les clients
- Clients non maillés
- Décrit dans la RFC2796



Topologie du réflecteur de route

reseauenclair.com

- Diviser la dorsale en plusieurs clusters
- Au moins un réflecteur de route et quelques clients par grappe
- Les réflecteurs de route sont entièrement maillés
- Les clients d'un cluster peuvent être entièrement maillés •

Un seul IGP pour transporter le prochain saut et les routes locales

Réflecteurs d'itinéraire :

Évitement de boucle

reseauencclair.com

- **Attribut Originator_ID**

Porte le RID de l'expéditeur de l'itinéraire dans le local AS (créé par le RR)

- **Attribut Cluster_list**

L'ID de cluster local est ajouté lorsque la mise à jour est envoyée par le RR

L'ID du cluster est automatiquement défini à partir de l'ID du routeur (adresse de bouclage)

N'utilisez PAS l'ID de cluster bgp xxxx

Réflecteurs d'itinéraire :

Redondance

reseauenclair.com

- Plusieurs RR peuvent être configurés dans le même cluster
– déconseillé !

Tous les RR du cluster **doivent** avoir le même identifiant de cluster (sinon, il s'agit d'un cluster différent)

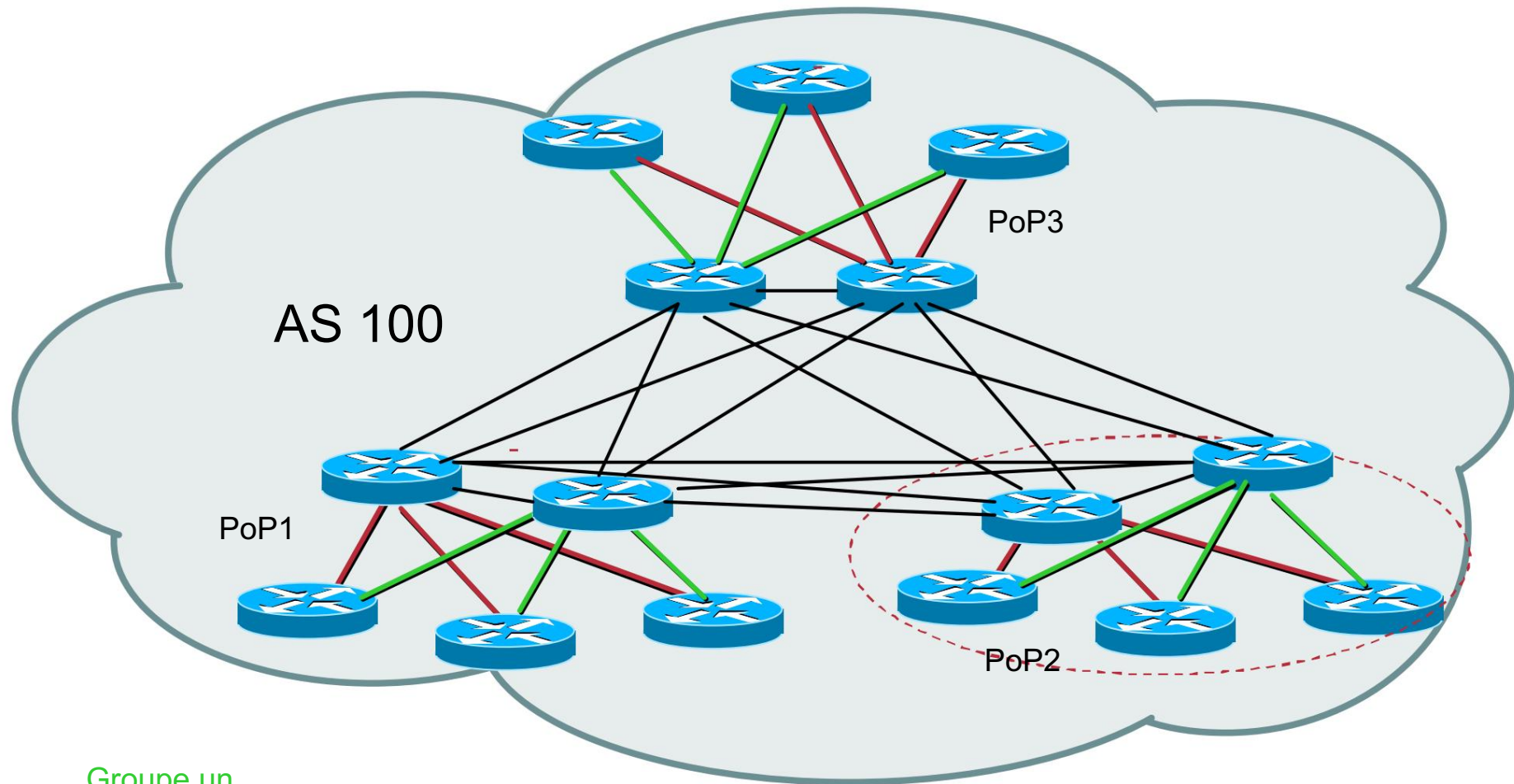
- Un routeur peut être client de RR dans différents groupes

Il est courant aujourd'hui dans les réseaux ISP de superposer deux clusters
– la redondance est ainsi obtenue ® Chaque

client dispose de deux RR = redondance

Réflecteurs d'itinéraire : Redondance

reseauenclair.com



Groupe un

Groupe deux

Réflecteurs d'itinéraire : Migration

reseauenclair.com

- Où placer les réflecteurs d'itinéraire ?

Suivez toujours la topologie physique !

Cela garantira que la transmission des paquets ne sera pas affectée

- Réseau FAI typique :

PoP dispose de deux routeurs principaux

Les routeurs principaux sont des RR pour le PoP

Deux clusters superposés

Réflecteurs d'itinéraire : Migration

reseauenclair.com

- Réseau FAI typique :

Les routeurs principaux ont un iBGP entièrement maillé

Créer une hiérarchie supplémentaire si le maillage principal est trop grand

Diviser la dorsale en régions

- Configurer une paire de clusters à la fois

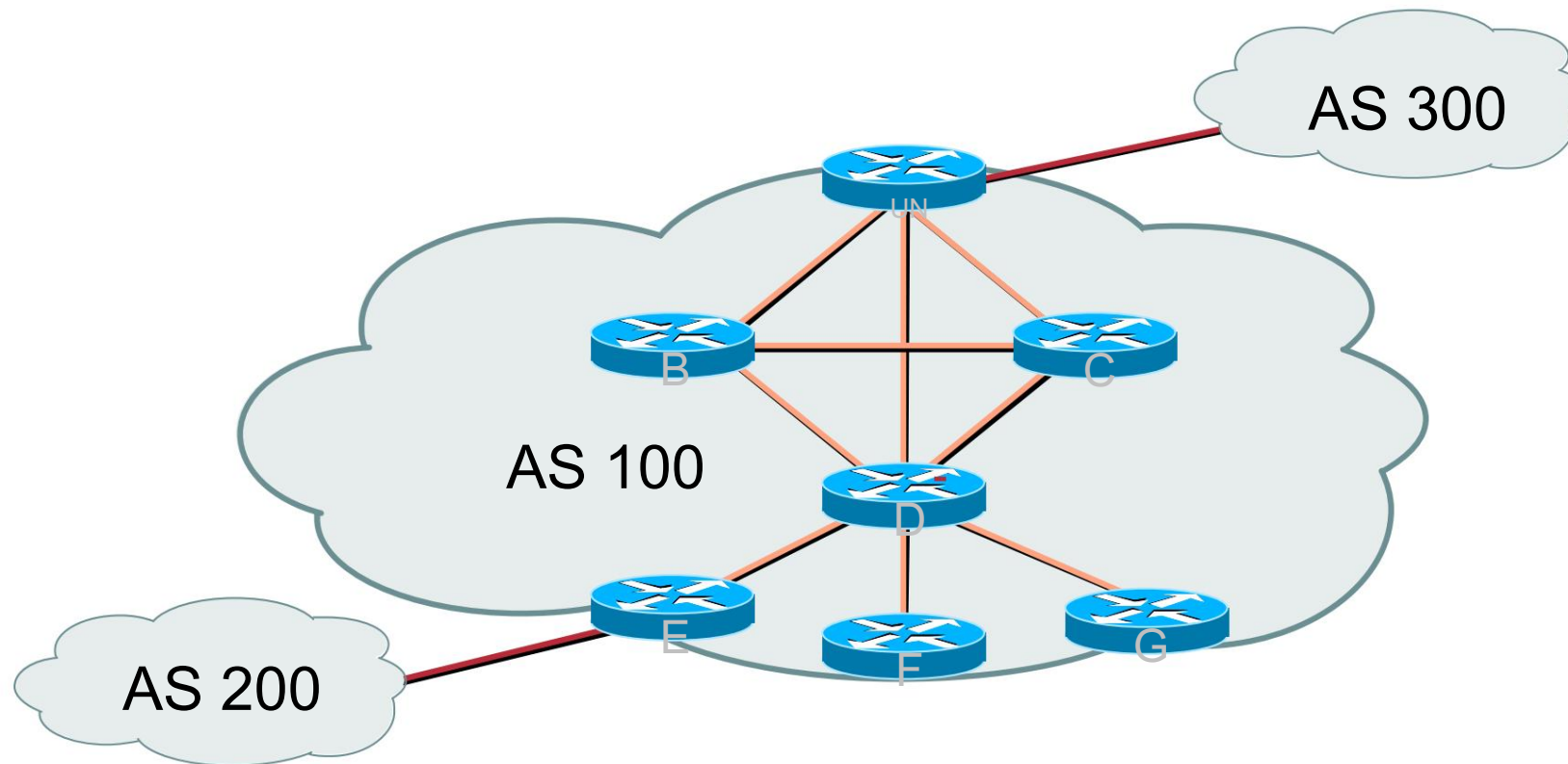
Éliminer les sessions iBGP redondantes

Placez au maximum un RR par cluster

Migration facile, plusieurs niveaux

Réflecteur d'itinéraire : Migration

reseauenclair.com



- Migrer de petites parties du réseau, une partie à la fois.

Configuration d'un réflecteur d'itinéraire

reseauenclair.com

```
routeur bgp 100
```

```
  voisin 1.1.1.1 distant-as 100
```

```
  voisin 1.1.1.1 route-reflector-client
```

```
  voisin 2.2.2.2 distant-as 100
```

```
  voisin 2.2.2.2 route-reflector-client
```

```
  voisin 3.3.3.3 distant-as 100
```

```
  voisin 3.3.3.3 route-reflector-client
```

```
  voisin 4.4.4.4 distant-as 100
```

```
  voisin 4.4.4.4 route-reflector-client
```


Confédérations

- Diviser l'AS en sous-AS

eBGP entre les sous-AS, mais certaines informations iBGP sont conservées

Préserver NEXT_HOP sur le sous-AS
(IGP transporte ces informations)

Conserver LOCAL_PREF et MED

- Généralement un seul IGP
- Décrit dans la RFC3065

Confédérations (suite)

reseauenclair.com

- Visible au monde extérieur comme un seul AS –
« Identifiant de la Confédération »

Chaque sous-AS utilise un numéro de la plage AS privée (64512-65534)

- Les haut-parleurs iBGP de chaque sous-AS sont entièrement maillés

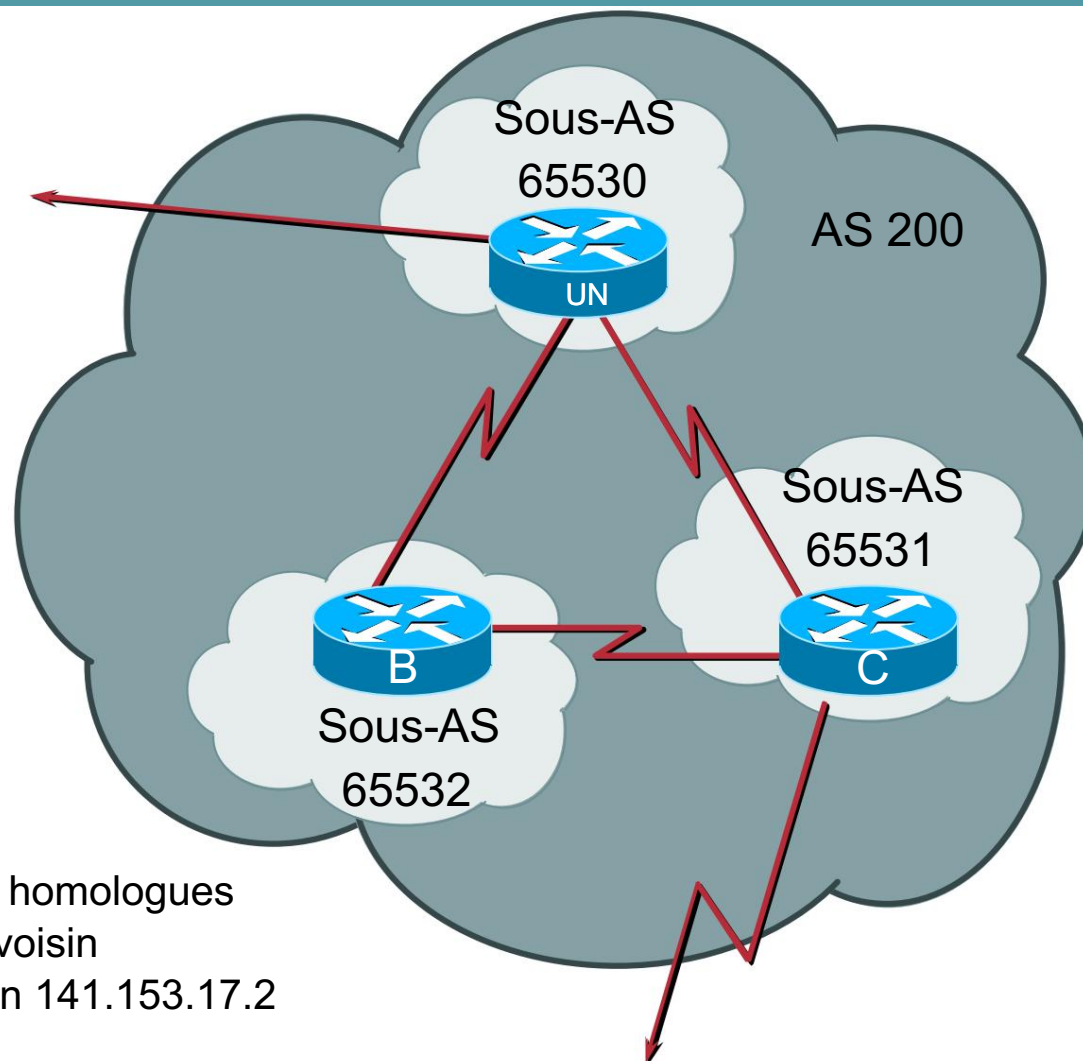
Le nombre total de voisins est réduit en limitant l'exigence de maillage complet aux seuls pairs du sous-réseau.

COMME

Peut également utiliser Route-Reflector dans le sous-AS

Confédérations (suite)

reseauenclair.com

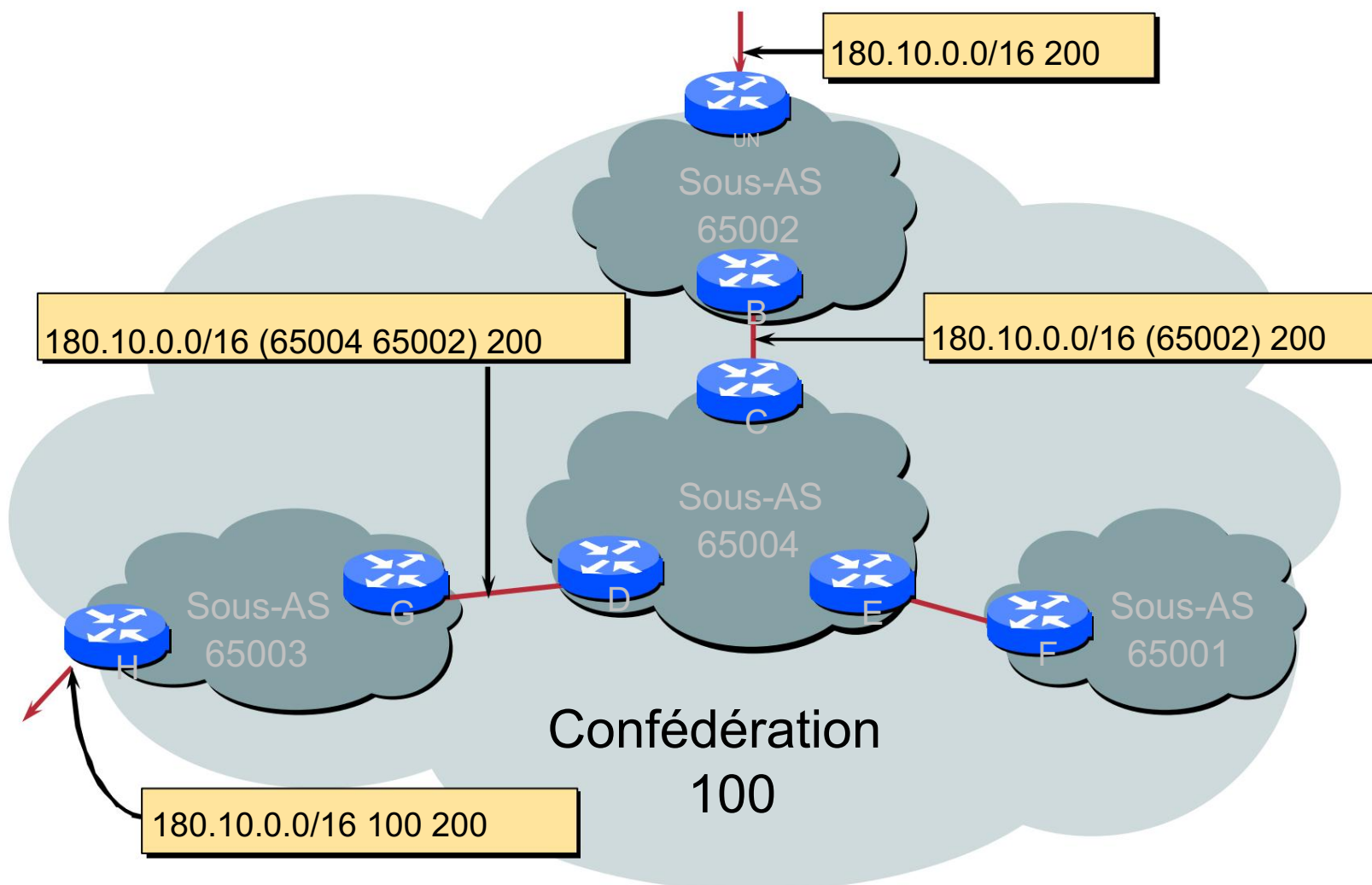


•Configuration (rtr B) :

```
routeur bgp 65532
  identifiant de confédération bgp 200 homologues
  de confédération bgp 65530 65531 voisin
  141.153.12.1 remote-as 65530 voisin 141.153.17.2
  remote-as 65531
```

Confédérations : Séquence AS

reseauenclair.com



Décisions de propagation d'itinéraire

reseauencclair.com

- Identique au BGP « normal » :

D'un pair dans le même sous-AS uniquement vers des pairs externes

Des pairs externes à tous les voisins • « Pairs externes » fait référence à :

Pairs hors de la confédération

Pairs dans un sous-AS différent

Conserver LOCAL_PREF, MED et NEXT_HOP

Confédérations (suite)

- Exemple (suite) :

La version de la table BGP est 78, l'ID du routeur local est 141.153.17.1

Codes d'état : s supprimé, d amorti, h historique, * valide, > meilleur, i - interne

Codes d'origine : i - IGP, e - EGP, ? - incomplet

Réseau	Prochain saut	Chemin de poids LocPrf métrique		
*> 10.0.0.0	141.153.14.3 0	100	0	(65531) 1 i
*> 141.153.0.0 141.153.30.2 0		100	0	(65530) je
*> 144.10.0.0 141.153.12.1 0		100	0	(65530) je
*> 199.10.10.0 141.153.29.2 0		100	0	(65530) 1 i

Réflecteurs de route ou Confédérations ?

reseauenclair.com

	Internet Connectivité	Multi-niveaux Hiérarchie	Politique Contrôle	Évolutivité	Migration Complexité
Confédérations	N'importe où dans le Réseau	Oui	Oui	Moyen	Moyen à haut
Itinéraire Réflecteurs	N'importe où dans le Réseau	Oui	Oui	Haut	Très faible

La plupart des nouveaux réseaux de fournisseurs de services déploient désormais des réflecteurs de route dès le premier jour

Plus de points sur les confédérations

reseauenclair.com

- Peut faciliter « l'absorption » d'autres FAI par votre FAI – par exemple, si un FAI en achète un autre

Ou peut utiliser la fonctionnalité [locale](#) pour faire une chose similaire

- Peut utiliser des réflecteurs de route avec un sous-AS de confédération pour réduire le maillage iBGP du sous-AS

Techniques de mise à l'échelle BGP

reseauenclair.com

- Ces 4 techniques devraient être des exigences fondamentales dans tous les réseaux FAI

Actualisation de l'itinéraire

Groupes de pairs

Amortissement des volets de route

Réflecteurs d'itinéraire

BGP pour les fournisseurs de services Internet

reseauenclair.com

- Principes de base du routage
- Principes de base de BGP
- Attributs BGP
- Sélection du chemin BGP
- Politique BGP •

Capacités BGP • Mise à
l'échelle de BGP

Tutoriel BGP

Fin de la partie 1 – Introduction

Partie 2 – Techniques de multihébergement cet après-midi