Attaques et sécurisation des couches OSI
BGP

Carlos Aguilar
carlos.aguilar-melchor@isae-supaero.fr
Benoît Morgan
benoit.morgan@enseeiht.fr

IRIT-IRT

Plan

Remerciements

Merci à :

- Carlos Aguilar-Melchor
- Cédric Blancher (EADS)
- Dan Boneh de Stanford University
- Pierre-François Bonnefoi du Master CRYPTIS à Limoges
- Céline Boyer (Canal+)
- Julien Cartigny du Master CRYPTIS à Limoges
- Ron Rivest du M.I.T.

Sources

Lecture intensive de :

[1] RFC 4271 - A Border Gateway Protocol 4 (BGP-4)

[2] http://www.guiguishow.info/wp-content/uploads/2013/09/RPKI-ROA/Soutenance/Soutenance-securiser-routage-internet.pdf

[3] Rover VS RPKI : https://eprint.iacr.org/2014/444.pdf

[4] ROVER : https://pdfs.semanticscholar.org/presentation/c9e8/36afcde334806ce9d61ca3d330ae659f4391.pdf

[5] S-BGP : https://ieeexplore.ieee.org/document/839934

[6] S-BGP : https://www.cc.gatech.edu/classes/AY2007/cs7260_spring/papers/sbgp.pdf

Routage : couche réseau

- Couche réseau du modèle OSI (3)

Routage : couche réseau

- Couche réseau du modèle OSI (3)
- Services essentiels ?

Routage : couche réseau

- Couche réseau du modèle OSI (3)
- Services essentiels ?
  - Le relayage (*forwarding*)

Routage : couche réseau

- Couche réseau du modèle OSI (3)
- Services essentiels ?
  - Le relayage (*forwarding*)
  - et le routage

Routage : couche réseau

- Couche réseau du modèle OSI (3)
- Services essentiels ?
  - Le relayage (*forwarding*)
  - et le routage
  - de paquets réseaux échangés par des machines interconnectées.

Routage : couche réseau

- Couche réseau du modèle OSI (3)
- Services essentiels ?
  - Le relayage (*forwarding*)
  - et le routage
  - de paquets réseaux échangés par des machines interconnectées.
- Routage : détermination d'un chemin permettant de relier deux machines distantes (non présentes sur le même domaine de diffusion).

Routage : couche réseau

- Couche réseau du modèle OSI (3)
- Services essentiels ?
  - Le relayage (*forwarding*)
  - et le routage
  - de paquets réseaux échangés par des machines interconnectées.
- Routage : détermination d'un chemin permettant de relier deux machines distantes (non présentes sur le même domaine de diffusion).
- Relayage : transmission par un routeur, d'un paquet réseau reçu, dont la destination n'est pas locale, de manière à le "rapprocher" de sa destination finale.

Routage : couche réseau

- Couche réseau du modèle OSI (3)
- Services essentiels ?
  - Le relayage (*forwarding*)
  - et le routage
  - de paquets réseaux échangés par des machines interconnectées.
- Routage : détermination d'un chemin permettant de relier deux machines distantes (non présentes sur le même domaine de diffusion).
- Relayage : transmission par un routeur, d'un paquet réseau reçu, dont la destination n'est pas locale, de manière à le "rapprocher" de sa destination finale.
- Protocoles de couche réseau actuellement majoritairement mises en œuvre :
  - IPv4 / ICMP
  - IPv6 / ICMPv6

Routage : détermination des routes

- Construction à l'aide de :
  - connaissance complète d'un / des réseaux traités ;
  - connaissance partielles (confidentialité, agrégation) ;
  - des informations administratives ;
  - et autres...

Routage : détermination des routes

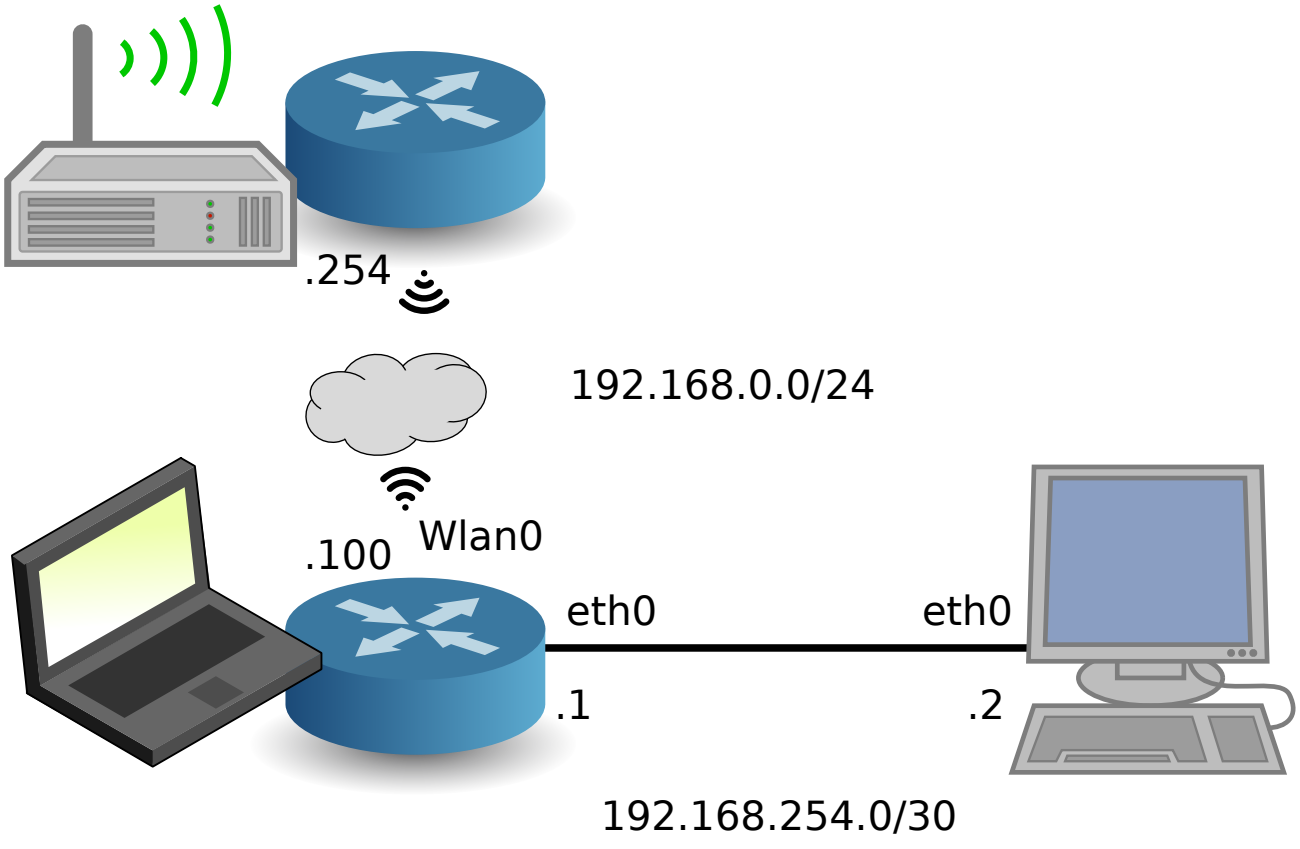
- Construction à l'aide de :
  - connaissance complète d'un / des réseaux traités ;
  - connaissance partielles (confidentialité, agrégation) ;
  - des informations administratives ;
  - et autres...
- De manière à :
  - atteindre la destination, avec pour politique de routage :
  - de passer par le plus cours en nombre de sauts ;
  - d'obtenir le débit le plus important ;
  - de coûter le moins possible ;
  - de respecter des contraintes politiques ;
  - ou une certain combinaison de ces contraintes.

Routage : relayage

- Prochain saut déterminé grâce aux routes calculées
- Concrètement mis en œuvre de manière performante grâce aux tables de routages des routeurs
- Liste ordonnée ayant des entrées du type n-uplet suivant :
  - une destination : un réseau ou une machine ;
  - le prochain saut associé pour se rapprocher de la destination ;
  - un coût (pour les routes ex æquo) ;
  - éventuellement une interface de sortie.

Routage statique avec *netfilter*

Problème : profiter du lien réseau d'un ordinateur portable connecté à un point d'accès.



Routage statique avec *netfilter*

Laptop

```
$ modprobe iptable_nat
$ sysctl net.ipv4.ip_forward=1 # Pour les jeunes
# echo 1 > /proc/sys/net/ipv4/ip_forward # pour les anciens
$ iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
$ iptables -A FORWARD -i eth0 -j ACCEPT
$ ip link set up dev eth0
$ ip addr add 192.168.254.1/30 dev eth0
```

Routage statique avec *netfilter*

Station de travail

```
$ ip link set up dev eth0
$ ip addr add 192.168.254.2/30 dev eth0
$ ip route add default via 192.168.254.1 dev eth0
$ ip route add 192.168.1.0 via 192.168.254.2
$ ip route
default via 192.168.254.2 dev eth0 src 192.168.254.1 metric 204
192.168.254.0/30 dev eth0 scope link src 192.168.254.1 metric 204
192.168.1.0/24 via 192.168.254.2 dev eth0
```

Routage statique avec *netfilter*

Station de travail

```
$ ip link set up dev eth0
$ ip addr add 192.168.254.2/30 dev eth0
$ ip route add default via 192.168.254.1 dev eth0
$ ip route add 192.168.1.0 via 192.168.254.2
$ ip route
default via 192.168.254.2 dev eth0 src 192.168.254.1 metric 204
192.168.254.0/30 dev eth0 scope link src 192.168.254.1 metric 204
192.168.1.0/24 via 192.168.254.2 dev eth0
```

Super, j'ai du réseau, mais est-ce viable à l'échelle d'une entreprise ou d'un fournisseur d'accès à internet ?

Protocoles de routage

- Services :
  - Constituer la base de connaissance de la topologie réseau
  - Calculer les routes nécessaires au relayage des paquets
  - Support du dynamise de la topologie du réseau

Protocoles de routage

- Services :
  - Constituer la base de connaissance de la topologie réseau
  - Calculer les routes nécessaires au relayage des paquets
  - Support du dynamise de la topologie du réseau
- Types de protocoles de routages :
  - Dépend du type de réseau à supporter

Protocoles de routage

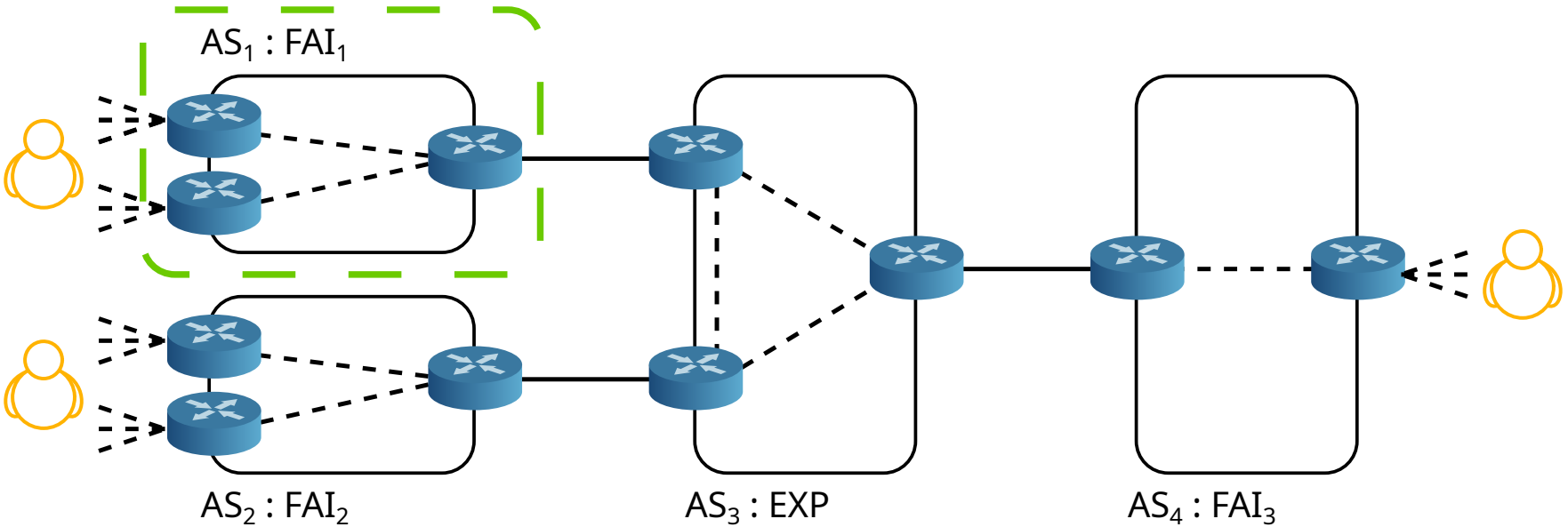
- Services :
  - Constituer la base de connaissance de la topologie réseau
  - Calculer les routes nécessaires au relayage des paquets
  - Support du dynamise de la topologie du réseau
- Types de protocoles de routages :
  - Dépend du type de réseau à supporter
  - Routage au sein d'un seul système autonome
    - $\Rightarrow$ Protocole de routage intradomaine, *Interior Gateway Protocol* (IGP)
      - Exemples : *Routing Information Protocol* (RIP), *Open Shortest Path First* (OSPF), *Intermediate System to Intermediate System* (IS-IS)

Protocoles de routage

- Services :
  - Constituer la base de connaissance de la topologie réseau
  - Calculer les routes nécessaires au relayage des paquets
  - Support du dynamise de la topologie du réseau
- Types de protocoles de routages :
  - Dépend du type de réseau à supporter
  - Routage au sein d'un seul système autonome
    - ⇒ Protocole de routage intradomaine, *Interior Gateway Protocol* (IGP)
      - Exemples : *Routing Information Protocol* (RIP), *Open Shortest Path First* (OSPF), *Intermediate System to Intermediate System* (IS-IS)
  - Routage entre plusieurs systèmes autonomes
    - ⇒ Protocole de routage interdomaines, *Exterior Gateway Protocol* (EGP)

Systèmes autonomes

- Un ensemble de réseaux dont la politique de routage est cohérente
- Généralement une entité ou organisation unique
- Exemple : fournisseurs d'accès à Internet



Exemple d'IGP : RIP

distance-vector protocol

$$(\text{distance} = \text{hop count}, \text{vector} = \text{next hop})$$

- Échange des accessibilités réseau de routeur en routeur voisin
- Construction d'un graphe orienté pondéré de la topologie du réseau
- Calcul de plus court chemin avec Bellman Ford en $O(S^3)$ sur en graphe dense simple
- Simple, facile à configurer
- Convergence lente, complexité forte, problème de passage à l'échelle, pas de sécurité

$\Rightarrow$ RIP RIP

Exemple d'IGP : OSPF

distance-vector protocol

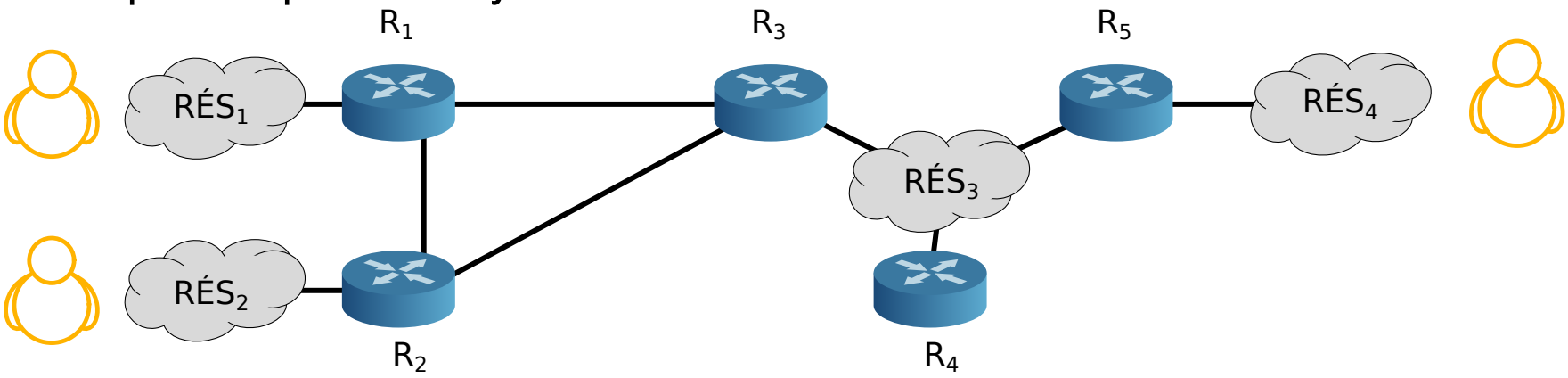
$$(\text{distance} = \text{hop count}, \text{vector} = \text{next hop})$$

- Échange des accessibilités réseau vers un routeur désigné
- Construction d'un graphe orienté pondéré de la topologie du réseau
- Calcul de plus court chemin avec l'algorithme de Dikjstra en $O(Sxlog(S))$
- Convergence plus rapide grâce au routeur désigné
- Complexité meilleure
- Passe à l'échelle grâce à l'utilisation de routeur désigné
- Sécurité : authentification des routeurs par mot de passe
  - Authentification mutuelle
  - Intégrité des accessibilités échangées ?
  - Confidentialité des routes et informations échangées ?
  - Disponibilité du service ?

$\Rightarrow$ Une des références actuelle d'*IGP* avec EIGRP (CISC0), IS-IS...

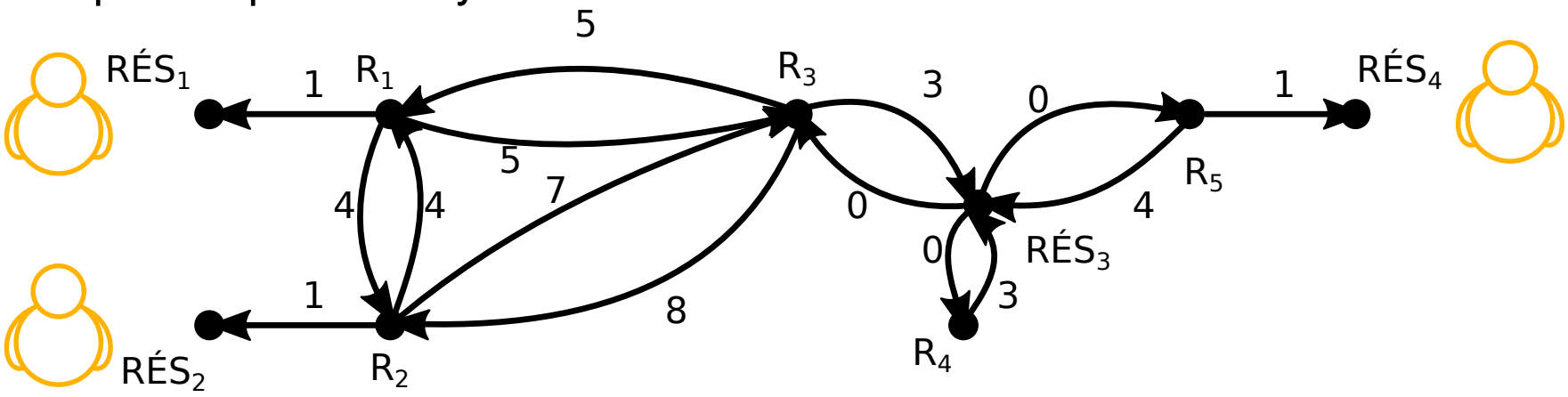
Exemple d'IGP : OSPF

Exemple simplifié de système autonome



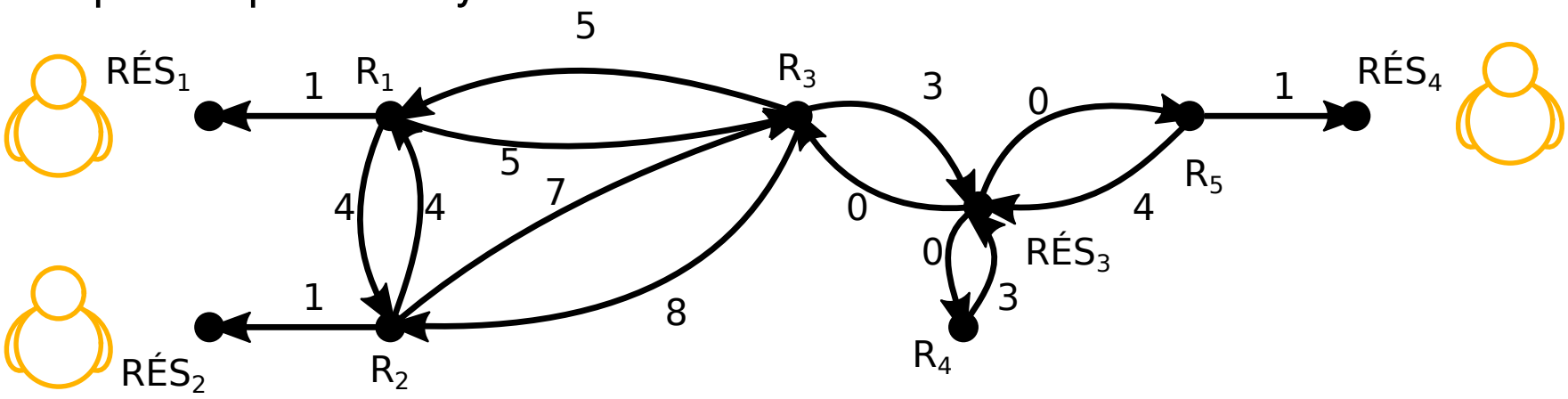
Exemple d'IGP : OSPF

Exemple simplifié de système autonome



Exemple d'IGP : OSPF

Exemple simplifié de système autonome



Routes calculées par routeur 2 :

1 R2 → R1 = 5

3 R2 → R3 = 10

4 R2 → R3 → R5 = 11

Table de routage du routeur 2 :

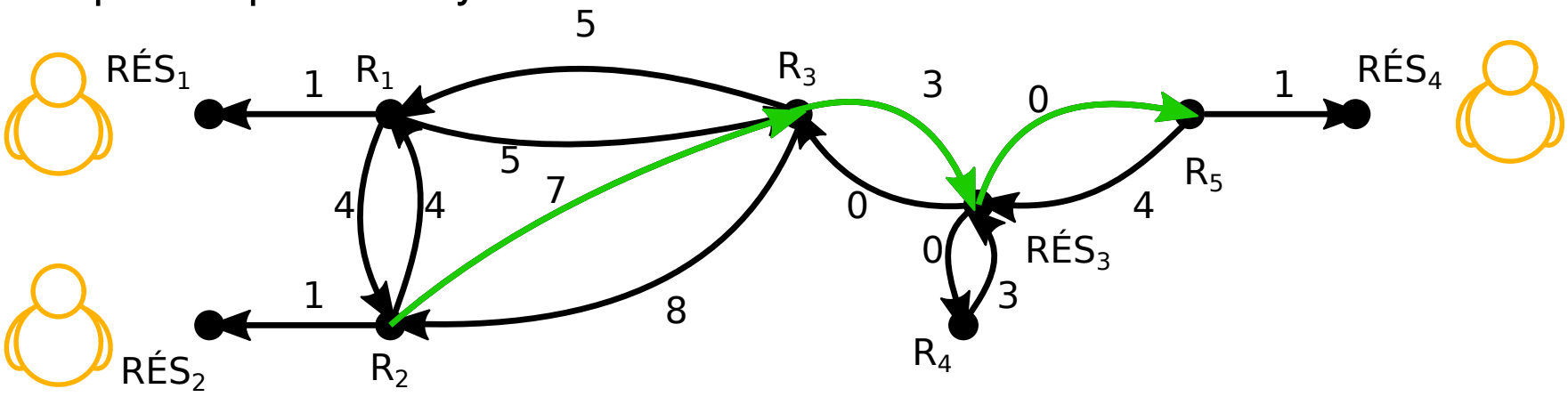
1 → R1

3 → R3

4 → R3

Exemple d'IGP : OSPF

Exemple simplifié de système autonome



Routes calculées par routeur 2 :

1. R2 → R1 = 5
3. R2 → R3 = 10
4. R2 → R3 → R5 = 11

Table de routage du routeur 2 :

1. → R1
3. → R3
4. → R3

Sécurité des protocoles de routages internes

Quels sont les éléments critiques à protéger / à assurer ?

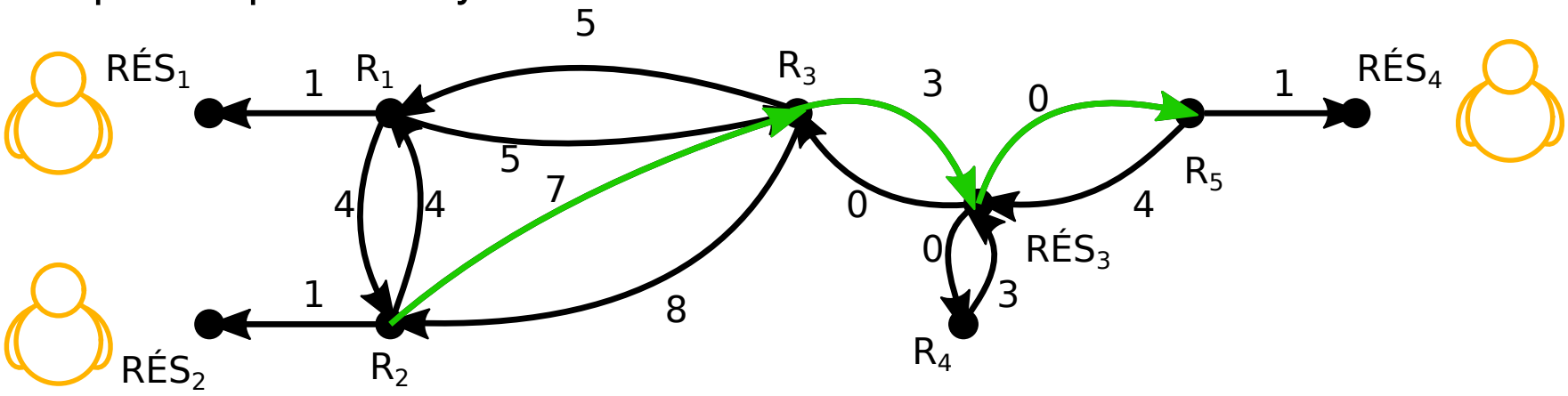
Sécurité des protocoles de routages internes

Quels sont les éléments critiques à protéger / à assurer ?

- Authenticité de l'identité des routeurs
- L'intégrité des accessibilités échangées
- L'intégrité des routeurs
- Leur confidentialité ?

Sécurité d'OSPF, un exemple d'attaque

Exemple simplifié de système autonome



Routes calculées par routeur 2 :

1 R2 → R1 = 5

3 R2 → R3 = 10

4 R2 → R3 → R5 = 11

Table de routage du routeur 2 :

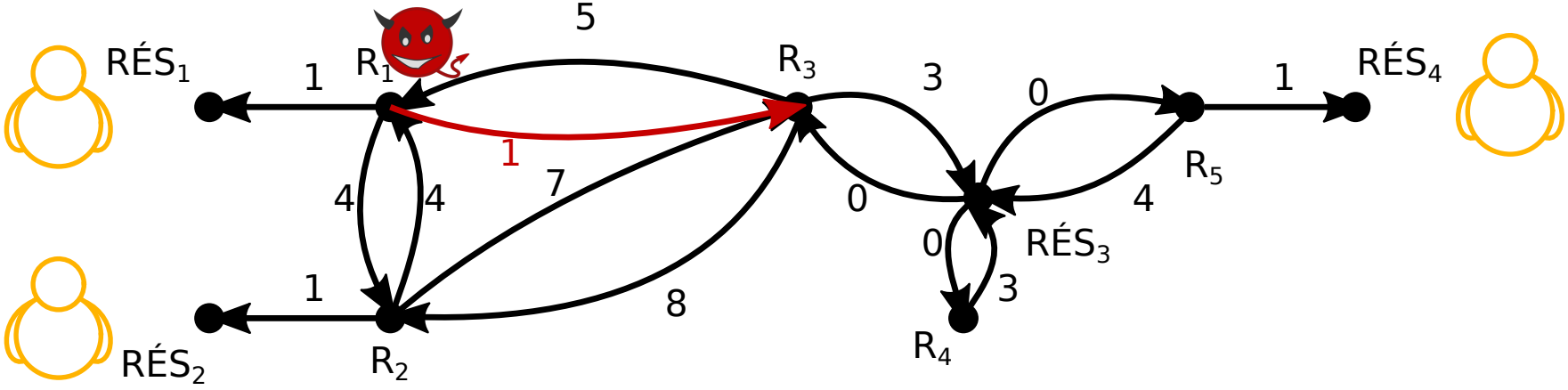
1 → R1

3 → R3

4 → R3

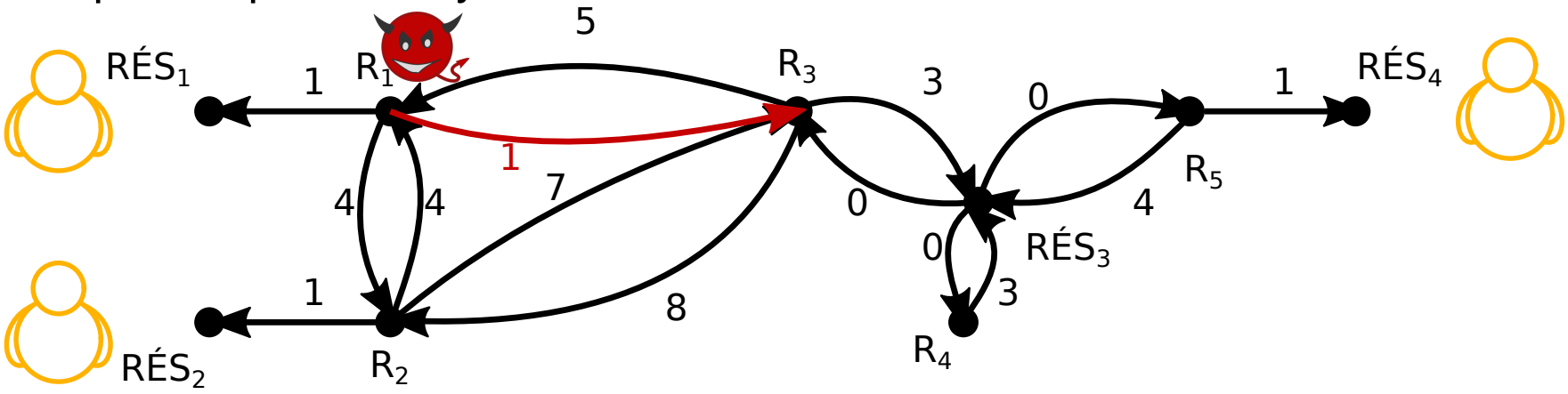
Sécurité d'OSPF, un exemple d'attaque

Exemple simplifié de système autonome



Sécurité d'OSPF, un exemple d'attaque

Exemple simplifié de système autonome



Routes calculées par routeur 2 :

1 R2 → R1 = 5

3 R2 → R1 → R3 = 8

4 R2 → R1 → R3 → R5 = 9

Table de routage du routeur 2 :

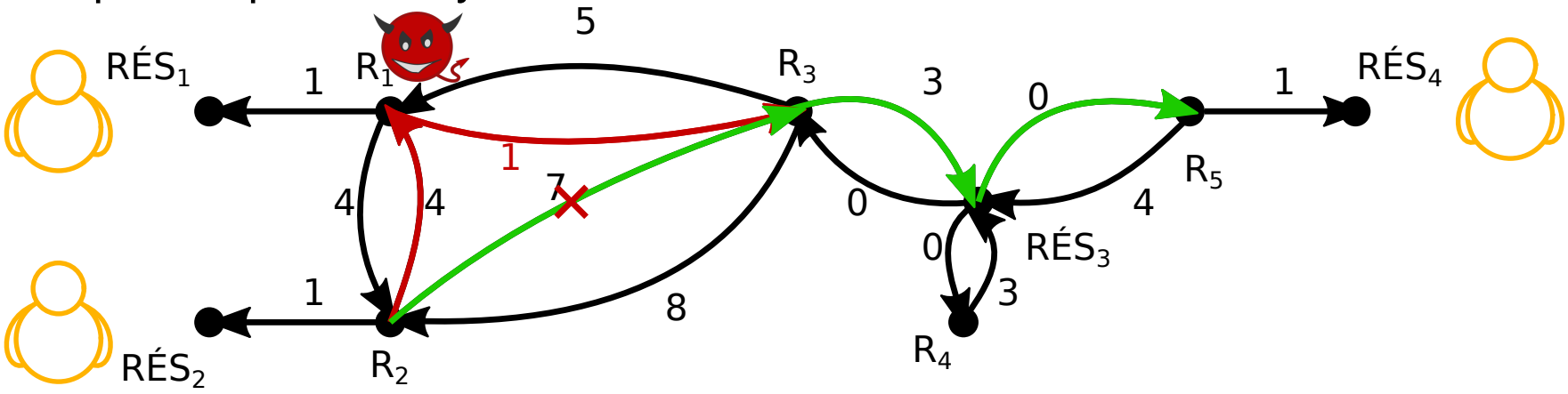
1 → R1

3 → R1

4 → R1

Sécurité d'OSPF, un exemple d'attaque

Exemple simplifié de système autonome



Routes calculées par routeur 2 :

1 R2 → R1 = 5

3 R2 → R1 → R3 = 8

4 R2 → R1 → R3 → R5 = 9

Table de routage du routeur 2 :

1 → R1

3 → R1

4 → R1

Les protocoles de routage externe

Service

- Constituer une certaine vision de la topologie du réseau inter systèmes autonomes contraintes par des politiques d'autres systèmes autonomes
- Choisir une route préférée selon un jeu de politiques locales à un système autonome

Les protocoles de routage externe

Service

- Constituer une certaine vision de la topologie du réseau inter systèmes autonomes contraintes par des politiques d'autres systèmes autonomes
- Choisir une route préférée selon un jeu de politiques locales à un système autonome

Politiques inter systèmes autonomes

- Annoncer une accessibilité à d'autres systèmes impose de gérer le trafic arrivant
- Choisir une route vers un système autonome impose de se contraindre au système autonome traversé
- Choix dictés par :
  - Performances (agrégation de routes annoncées, choix du meilleur débit)
  - Coût (choix du coût le plus faible)
  - Politique

Border Gateway Protocol

path-vector protocol

(path = `{ASN :: ... {AS2 :: { AS1 :: }}} []`, vector = next hop

- Protocole de routage interdomaine
- Utilisé pour interconnecter les systèmes autonomes IP formant internet

Constitution de la topologie réseau

- Défini un protocole connecté (TCP 179) d'échange entre routeurs BGP voisins connus
- Défini les messages d'échange de mise à jour d'accessibilités

Politique de sélection et de diffusion

- Politiques de sélection des la meilleures routes reçues en fonction de politiques configurables
- Politiques de sélection de routes valides pour annonces aux voisins

Annonce de routes et topologie réseau

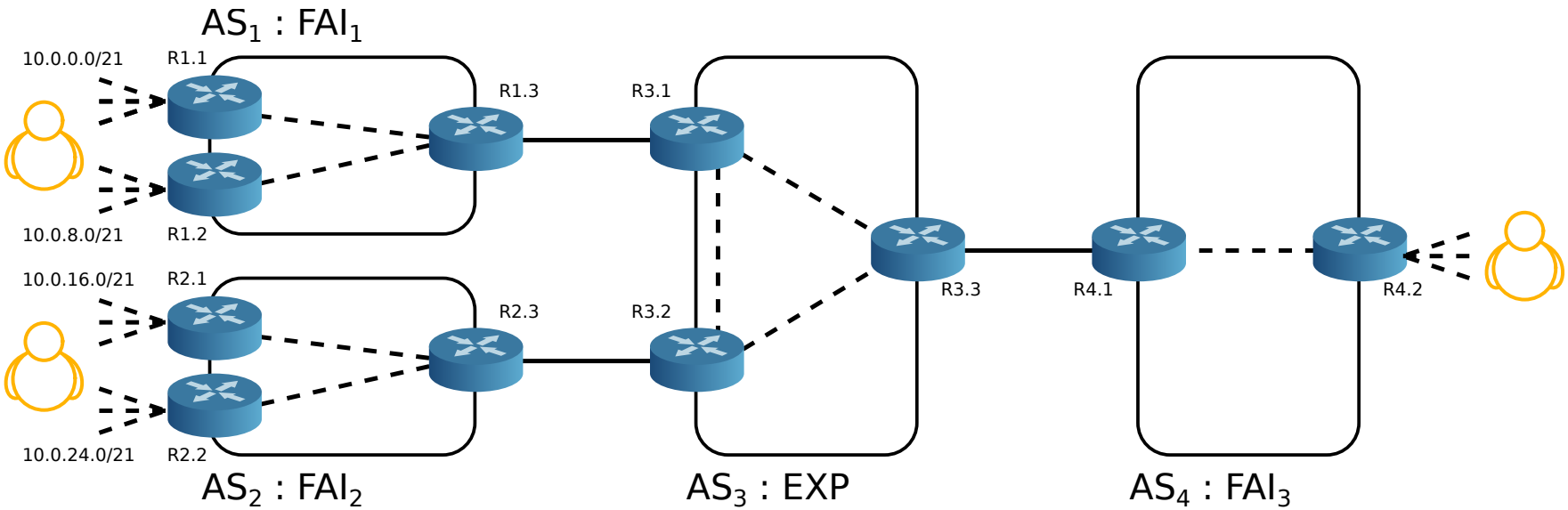
Basé sur l'échange de messages décrivant les accessibilités réseau de systèmes autonomes, de routeur BGP en routeur BGP.

Message UPDATE

- Liste des préfixes annoncés comme plus accessibles
- Description du chemin pris par l'annonce
  - Liste(s) des systèmes autonomes traversés par ce message
  - Prochain saut pour se rapprocher des préfixes annoncés
  - Liste des préfixes annoncés comme accessibles

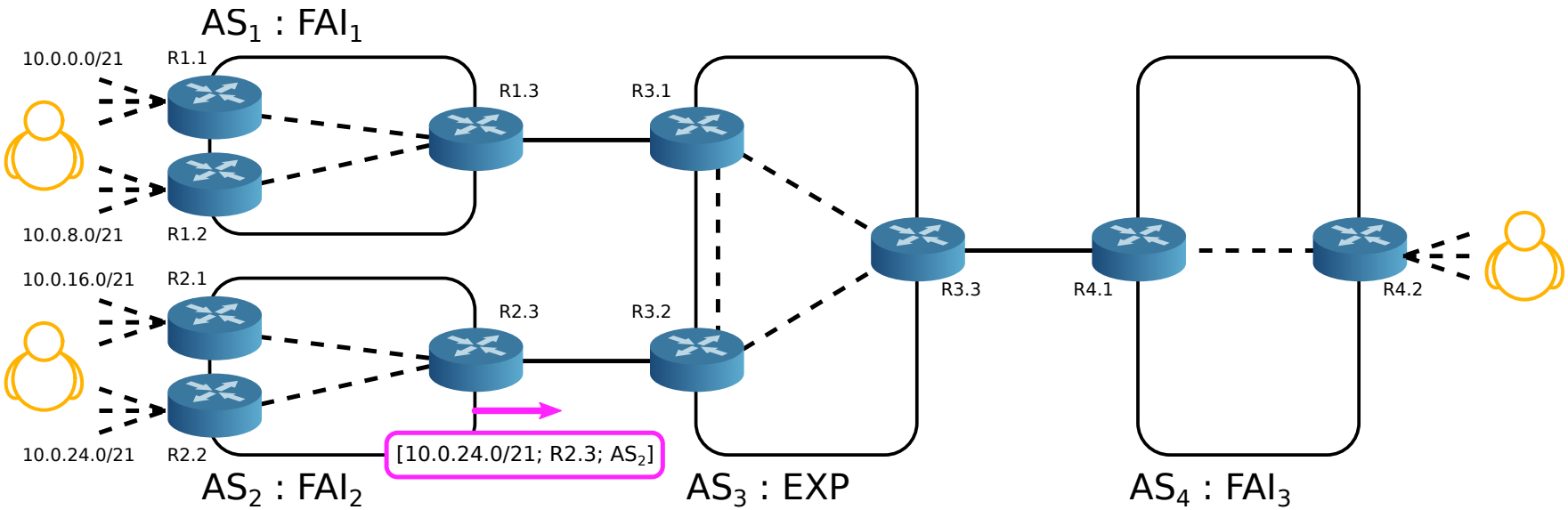
Gestion du chemin traversé : *AS_PATH*

Annonce du préfixe `10.0.0.0/21` par le routeur `R2.3`



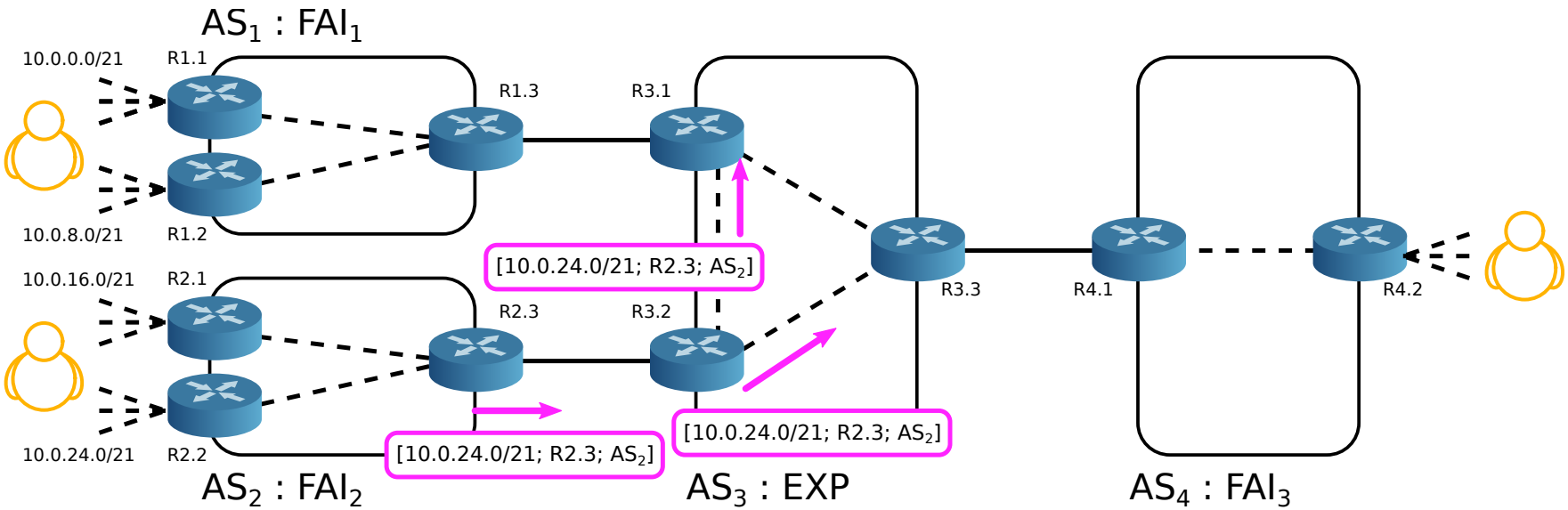
Gestion du chemin traversé : *AS_PATH*

Annonce du préfixe `10.0.0.0/21` par le routeur `R2.3`



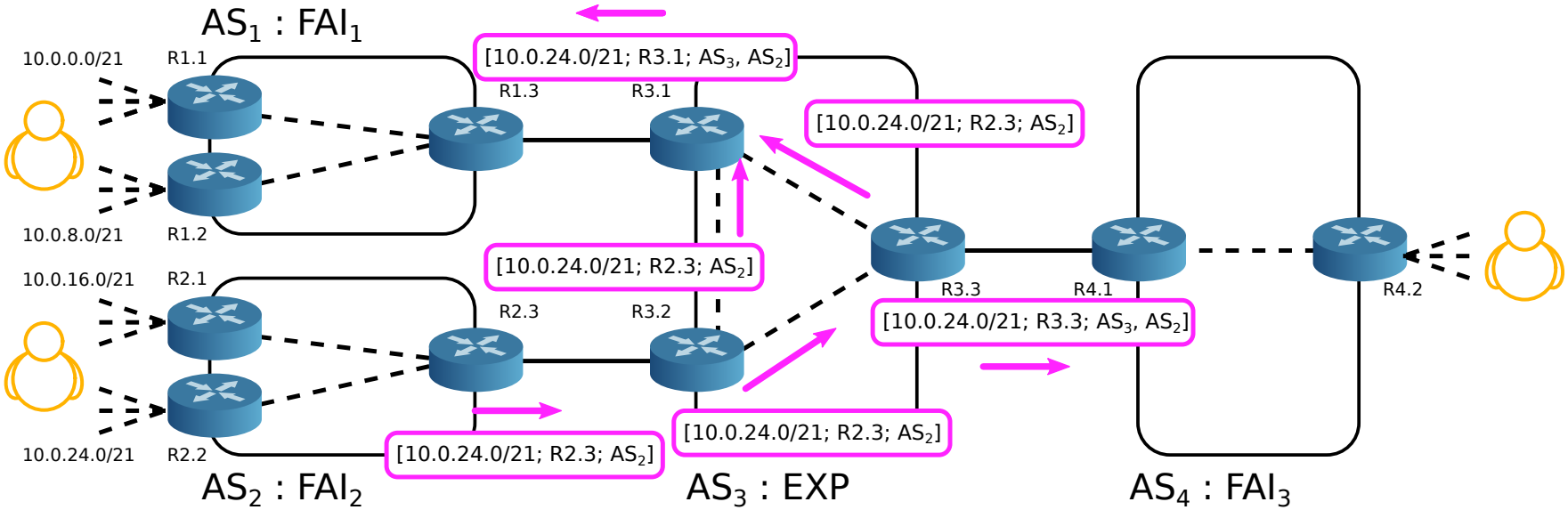
Gestion du chemin traversé : *AS_PATH*

Annonce du préfixe `10.0.0.0/21` par le routeur `R2.3`



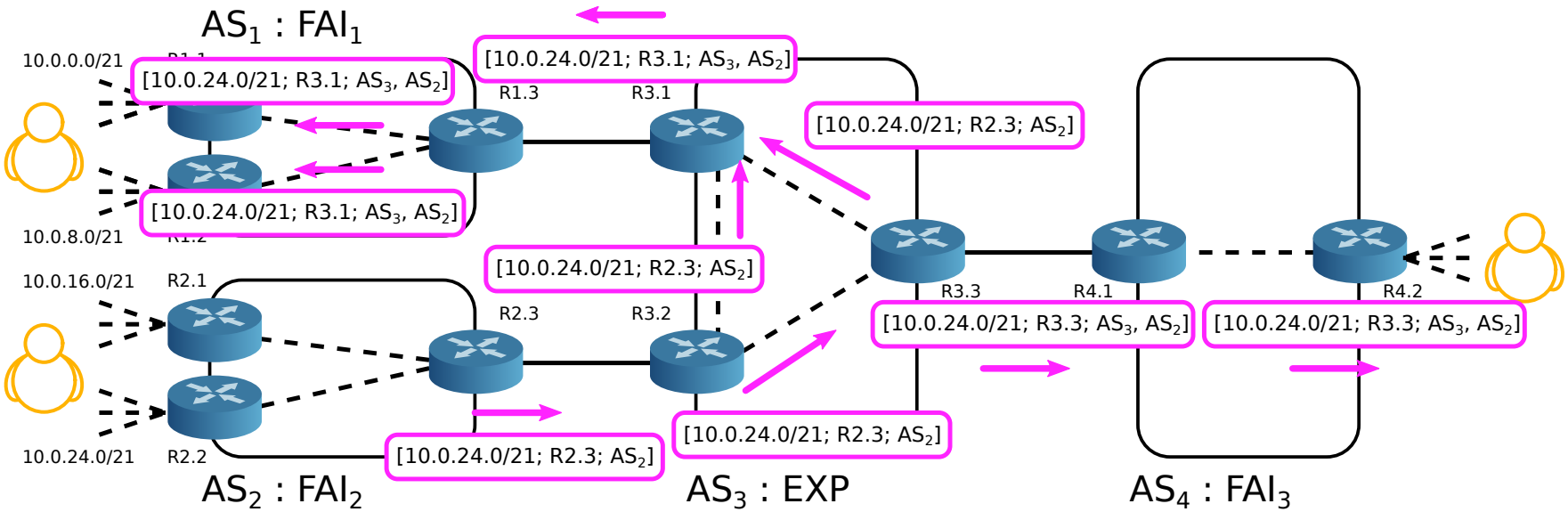
Gestion du chemin traversé : *AS_PATH*

Annonce du préfixe `10.0.0.0/21` par le routeur `R2.3`



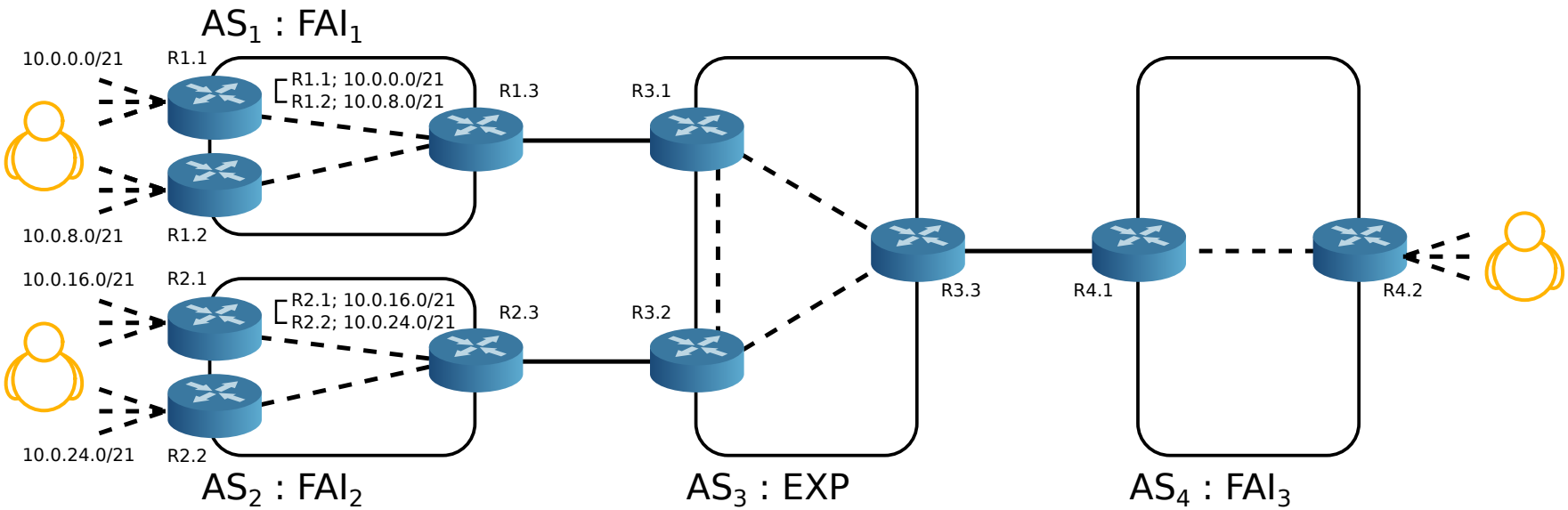
Gestion du chemin traversé : *AS_PATH*

Annonce du préfixe `10.0.0.0/21` par le routeur `R2.3`



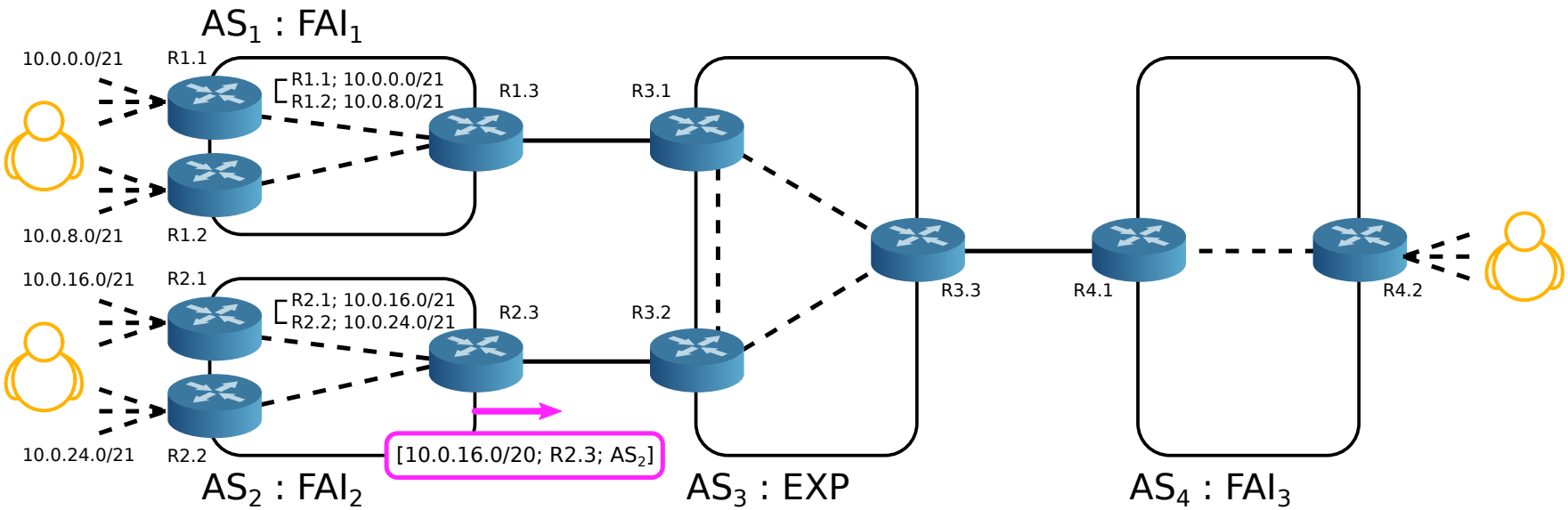
Agrégation de préfixes

Les routeurs `R1.3`, `R2.3` et `R3.3` agrègent successivement les routes hiérarchiquement cohérentes.



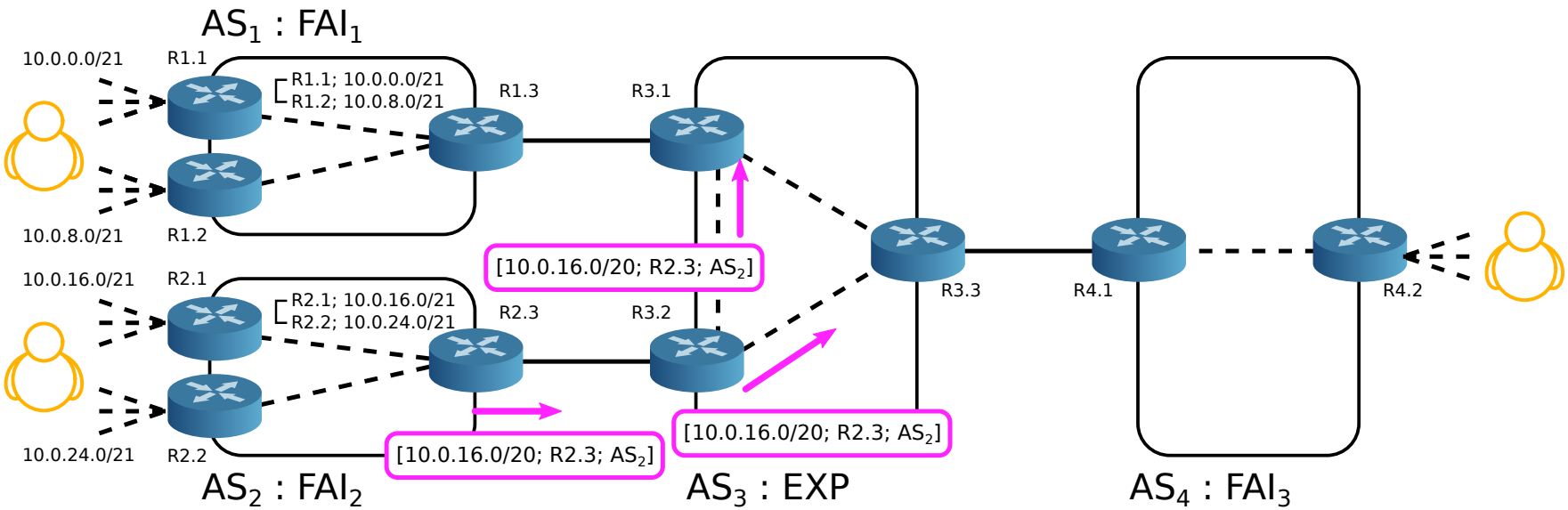
Agrégation de préfixes

Les routeurs `R1.3`, `R2.3` et `R3.3` agrègent successivement les routes hiérarchiquement cohérentes.



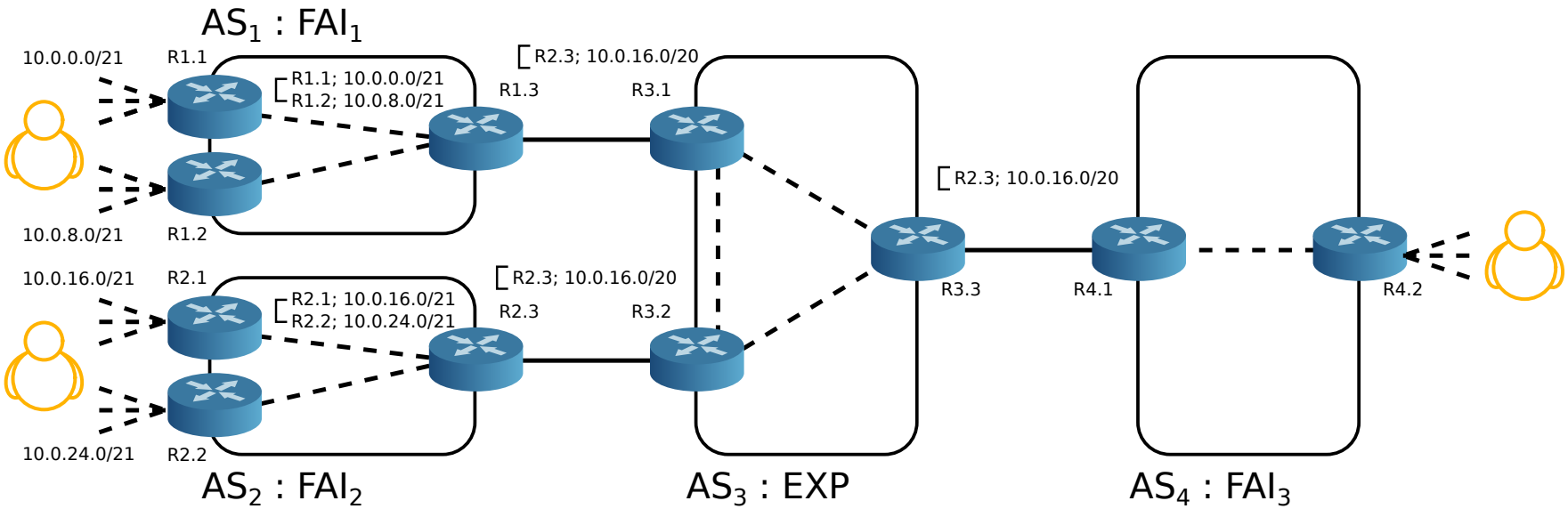
Agrégation de préfixes

Les routeurs `R1.3`, `R2.3` et `R3.3` agrègent successivement les routes hiérarchiquement cohérentes.



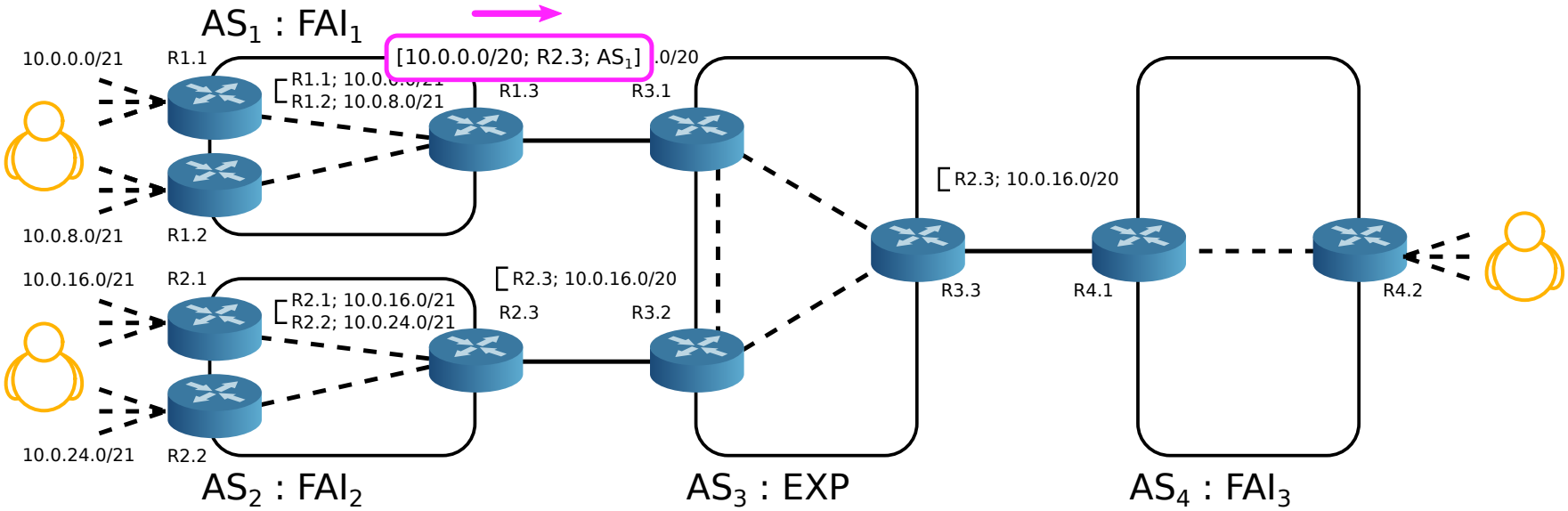
Agrégation de préfixes

Les routeurs `R1.3`, `R2.3` et `R3.3` agrègent successivement les routes hiérarchiquement cohérentes.



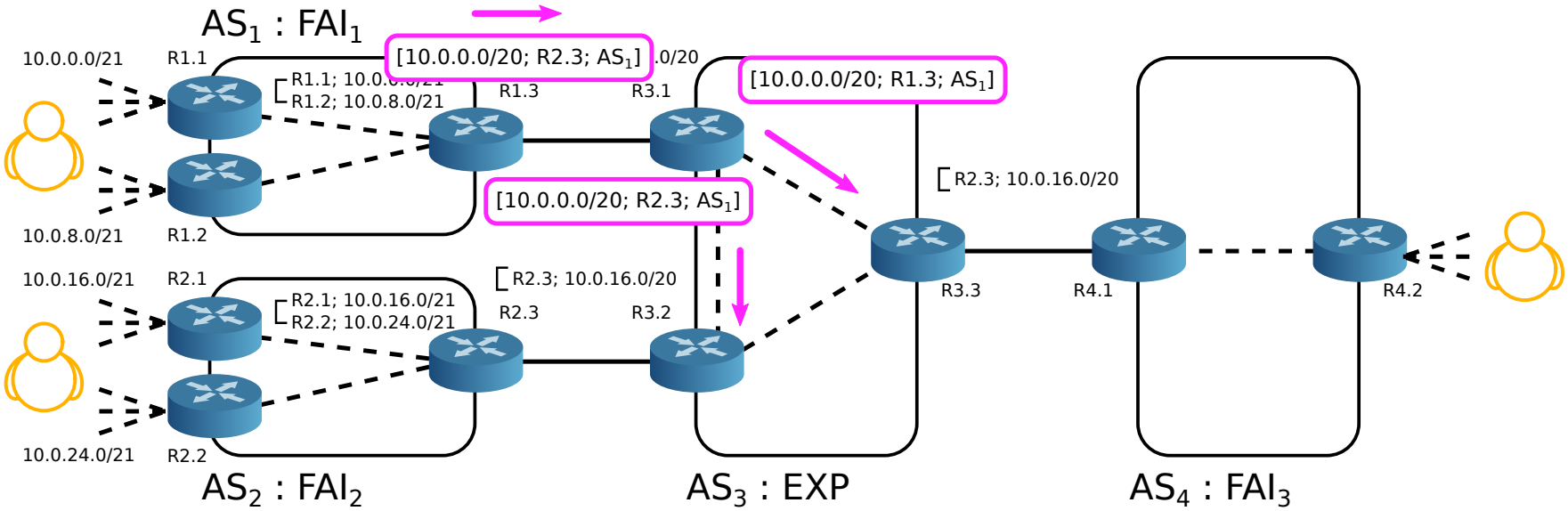
Agrégation de préfixes

Les routeurs `R1.3`, `R2.3` et `R3.3` agrègent successivement les routes hiérarchiquement cohérentes.



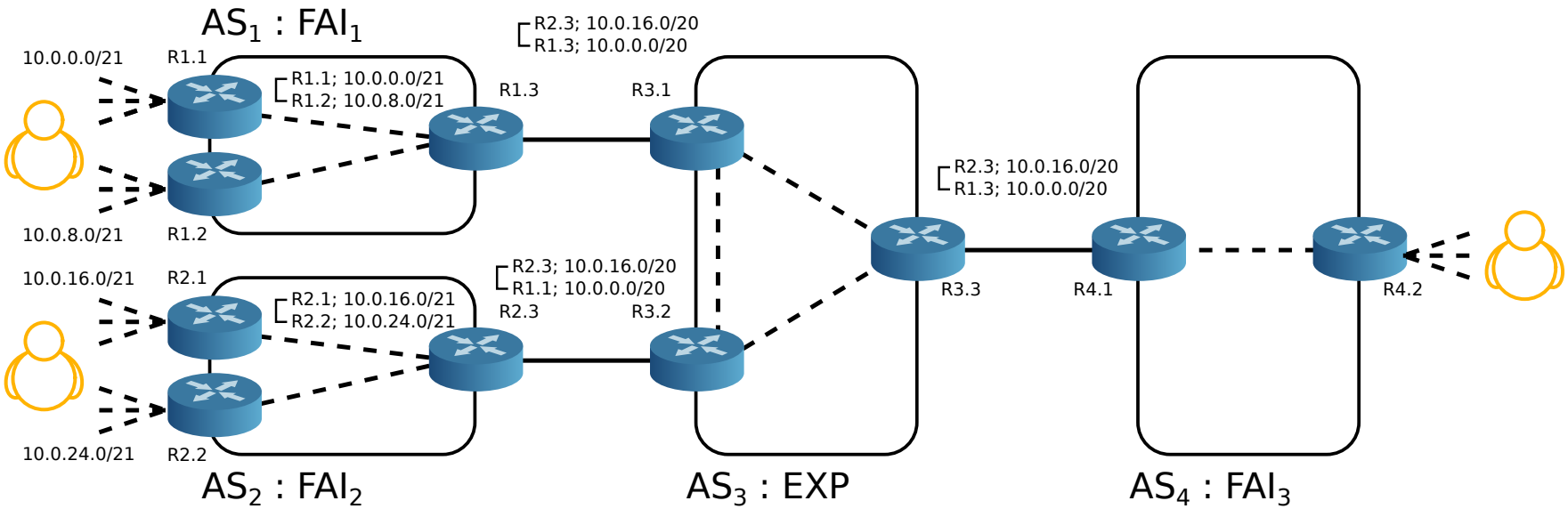
Agrégation de préfixes

Les routeurs `R1.3`, `R2.3` et `R3.3` agrègent successivement les routes hiérarchiquement cohérentes.



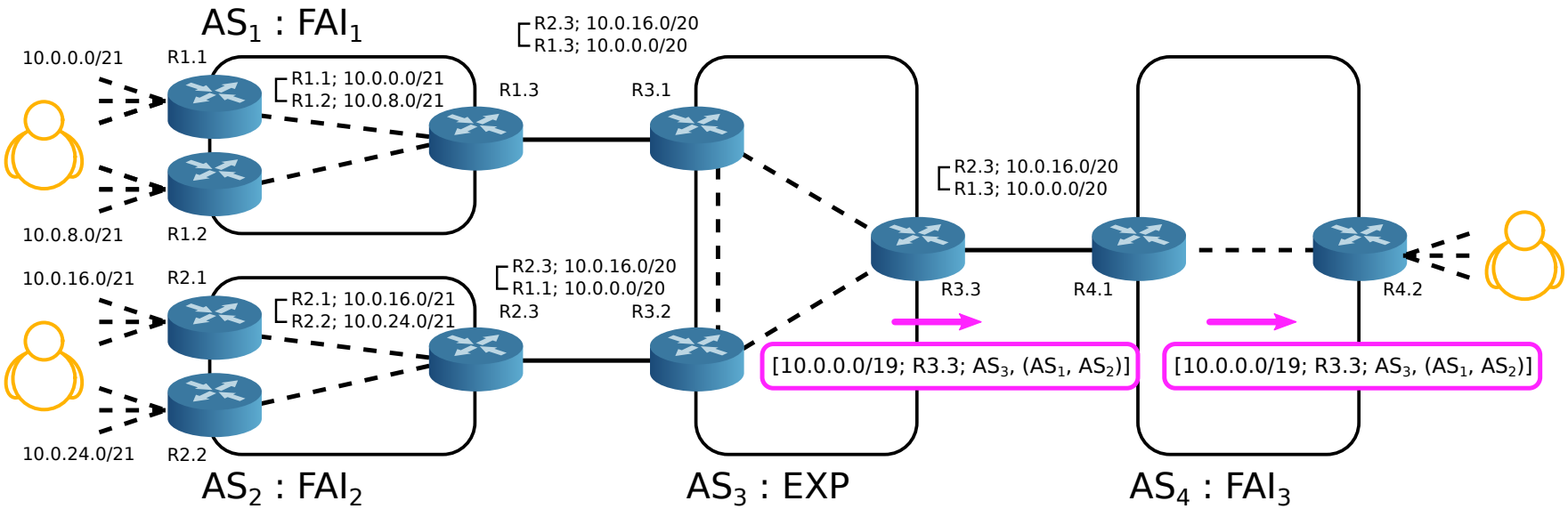
Agrégation de préfixes

Les routeurs `R1.3`, `R2.3` et `R3.3` agrègent successivement les routes hiérarchiquement cohérentes.



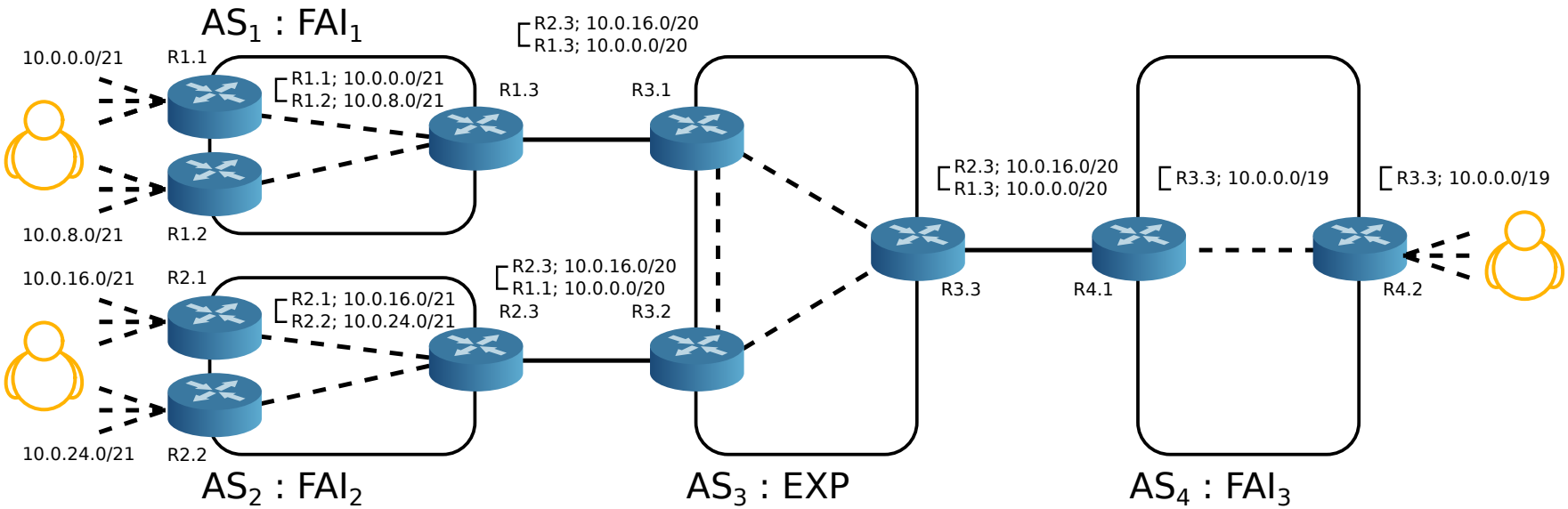
Agrégation de préfixes

Les routeurs `R1.3`, `R2.3` et `R3.3` agrègent successivement les routes hiérarchiquement cohérentes.

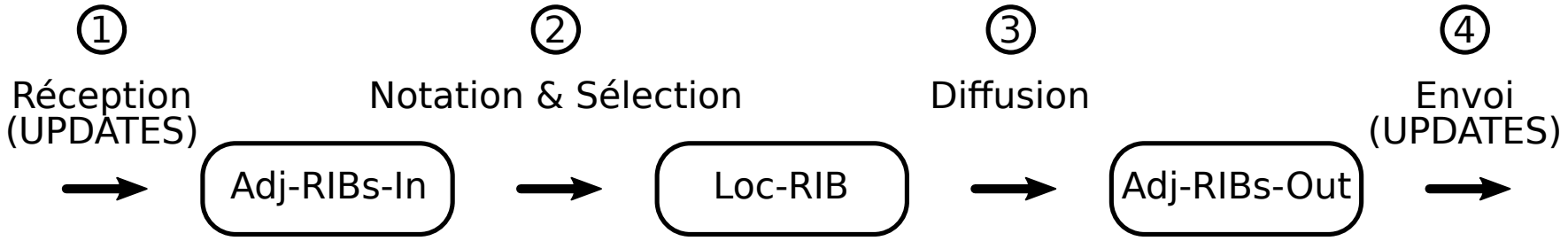


Agrégation de préfixes

Les routeurs `R1.3`, `R2.3` et `R3.3` agrègent successivement les routes hiérarchiquement cohérentes.



Sélection et diffusion des routes



1. Réception : les routes reçues et non dépréciées sont stockées pour sélection
2. Notation & sélection : notation et filtrage des routes à l'aide des politiques locales puis stockage avec les routes actives
3. Diffusion : filtrage des routes actives à annoncer aux voisin, puis stockage pour diffusion
4. Envoi : envoi des routes aux routeurs voisins

Notation & sélection

Notation

1. Note déjà attribuée (si annonce locale)
2. Nombre de sauts en terme de systèmes autonome
3. Si chevauchement de préfixes, le plus précis est le meilleur
4. Politique locale

Sélection

1. Suppression des routes non relayables
2. Suppression des boucles présentes dans le chemin (*AS_PATH*)
3. On prend la route qui a la meilleure note
4. Si égalité, algorithme de gestion des égalités

Processus de décision : diffusion & envoi

Diffusion

- Politique locale :
  - Commercial
  - Performances
  - Confiance

Envoi

- Aux routeurs voisins
- Routes locales mises à jours (IGP, ou BGP interne)
- On ne renvoie pas une route déjà annoncée si elle n'est pas mise à jour

L'incident AS7007 (1997)

Internet coupé partout aux USA pendant plusieurs heures

Pourquoi (fond)

- Critères classiques pour le choix d'une route
  1. Si A (3 hops) est plus court que B (4 hops) prendre A
  2. Si A (network/16) est plus précis que B (network/8) prendre A
- Quelle règle est appliquée en priorité ?
- On traite tout le trafic indépendamment de l'envoyeur et du contenu

Pourquoi (pratique)

1. AS7007 reçoit d'un de ses clients 23000 routes (pas normal)
2. AS7007 désagrège toutes les routes sous la forme network/24 (pas normal)
3. AS7007 remplace l'AS-path par seulement lui (catastrophique)
4. AS7007 envoie 70000 routes fausses ...

L'incident AS7007 (1997)

Internet coupé partout aux USA pendant plusieurs heures

Pourquoi (fond)

- Critères classiques pour le choix d'une route
  1. Si A (3 hops) est plus court que B (4 hops) prendre A
  2. Si A (network/16) est plus précis que B (network/8) prendre A
- Quelle règle est appliquée en priorité ?
- On traite tout le trafic indépendamment de l'envoyeur et du contenu

Pourquoi (pratique)

1. AS7007 reçoit d'un de ses clients 23000 routes (pas normal)
2. AS7007 désagrège toutes les routes sous la forme network/24 (pas normal)
3. AS7007 remplace l'AS-path par seulement lui (catastrophique)
4. AS7007 envoie 70000 routes fausses ... $\rightarrow$ trou noir :)

A-t-on appris la leçon ? (1/2)

Oui, en partie

Les gros AS limitent sur quoi peuvent parler les petits AS
Les gros AS limitent combien de choses peuvent dire les petits AS

Youtube et Pakistan Telecom (2008)

Youtube annonce une route avec pour préfixe 208.65.153.0/22
Gouv. Pakistanais demande le blocage de Youtube (en national)
Pakistan Telecom (gros AS): Annonce BGP pour router vers trou noir 208.65.153.0/24 ... !

Que se passe-t-il ?

A-t-on appris la leçon ? (1/2)

Oui, en partie

Les gros AS limitent sur quoi peuvent parler les petits AS
Les gros AS limitent combien de choses peuvent dire les petits AS

Youtube et Pakistan Telecom (2008)

Youtube annonce une route avec pour préfixe 208.65.153.0/22
Gouv. Pakistanais demande le blocage de Youtube (en national)
Pakistan Telecom (gros AS): Annonce BGP pour router vers trou noir 208.65.153.0/24 ... !

Que se passe-t-il ? Toute la planète route vers le trou noir ...

Conséquences

Youtube inaccessible pendant environ deux heures

A-t-on appris la leçon ? (2/2)

F | I-Root DNS en Chine (2010-11)

Serveurs basés sur de l'anycast (même préfixe diffusé à différents endroits)

- Préfixe IPv6 `2001:500:2f::/48`
- Dans AS3557 ISC-F-ROOT Internet Systems Consortium, Inc
- Route diffusée 6939 23911 18344 37944 24151 55439 3557
  - AS55439 ISC-PEK2 Internet Systems Consortium, (Beijing, China)
  - ...
  - AS23911 China Next Generation Internet Beijing IX
  - AS6939 Hurricane Electric (fournisseur IPv6)

Pourquoi prendre cette route depuis la France ?

Conséquences

Les requêtes étaient répondues derrière le Great Firewall of China (25h) ...
Pour le serveur I-Root ça duré 22 jours !

Environ une dizaine de grosses "erreurs" par an !

A-t-on appris la leçon ? (2/2)

F | I-Root DNS en Chine (2010-11)

Serveurs basés sur de l'anycast (même préfixe diffusé à différents endroits)

- Préfixe IPv6 `2001:500:2f::/48`
- Dans AS3557 ISC-F-ROOT Internet Systems Consortium, Inc
- Route diffusée 6939 23911 18344 37944 24151 55439 3557
  - AS55439 ISC-PEK2 Internet Systems Consortium, (Beijing, China)
  - ...
  - AS23911 China Next Generation Internet Beijing IX
  - AS6939 Hurricane Electric (fournisseur IPv6)

Pourquoi prendre cette route depuis la France ?
Hurricane Electric principal fournisseur IPv6 au monde !

Conséquences

Les requêtes étaient répondues derrière le Great Firewall of China (25h) ...
Pour le serveur I-Root ça duré 22 jours !

Environ une dizaine de grosses "erreurs" par an !

Plan

Principaux problèmes de sécurité de BGP

Problèmes

- Pas d'authentification des routeurs BGP voisins.
- Pas d'intégrité des annonces échangées (authenticité)

Principaux problèmes de sécurité de BGP

Problèmes

- Pas d'authentification des routeurs BGP voisins.
- Pas d'intégrité des annonces échangées (authenticité)

Vecteurs d'attaques potentiels

- Annonce illégitime d'origine de préfixe
- Relayer une annonce manipulée

Principaux problèmes de sécurité de BGP

Problèmes

- Pas d'authentification des routeurs BGP voisins.
- Pas d'intégrité des annonces échangées (authenticité)

Vecteurs d'attaques potentiels

- Annonce illégitime d'origine de préfixe
- Relayer une annonce manipulée

Comment ?

- En homme dans le milieu, sur le chemin de la route
- En injectant de fausses annonce à des routeurs BGP voisins

Principaux problèmes de sécurité de BGP

Problèmes

- Pas d'authentification des routeurs BGP voisins.
- Pas d'intégrité des annonces échangées (authenticité)

Vecteurs d'attaques potentiels

- Annonce illégitime d'origine de préfixe
- Relayer une annonce manipulée

Comment ?

- En homme dans le milieu, sur le chemin de la route
- En injectant de fausses annonce à des routeurs BGP voisins

Coséquences ?

- Détournement de préfixes
- Performances (désagrégation)

Objectifs de sécurité pour BGP

Que peut-on / doit-on assurer ?

Objectifs de sécurité pour BGP

Que peut-on / doit-on assurer ?

Validité de l'origine

- Est-ce qu'un système autonome est autorisé à annoncer tel préfixe ?
- Problème relativement simple : peu de préfixes, enregistrés et peu de changements

Objectifs de sécurité pour BGP

Que peut-on / doit-on assurer ?

Validité de l'origine

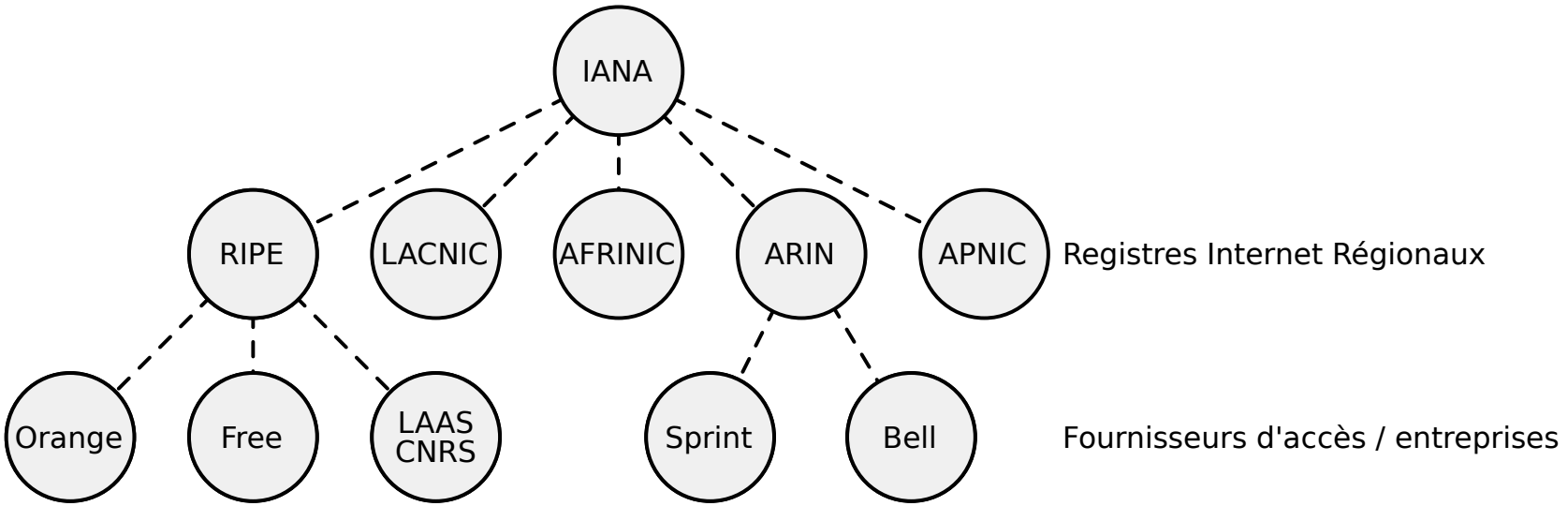
- Est-ce qu'un système autonome est autorisé à annoncer tel préfixe ?
- Problème relativement simple : peu de préfixes, enregistrés et peu de changements

Validité du chemin (*AS-PATH*)

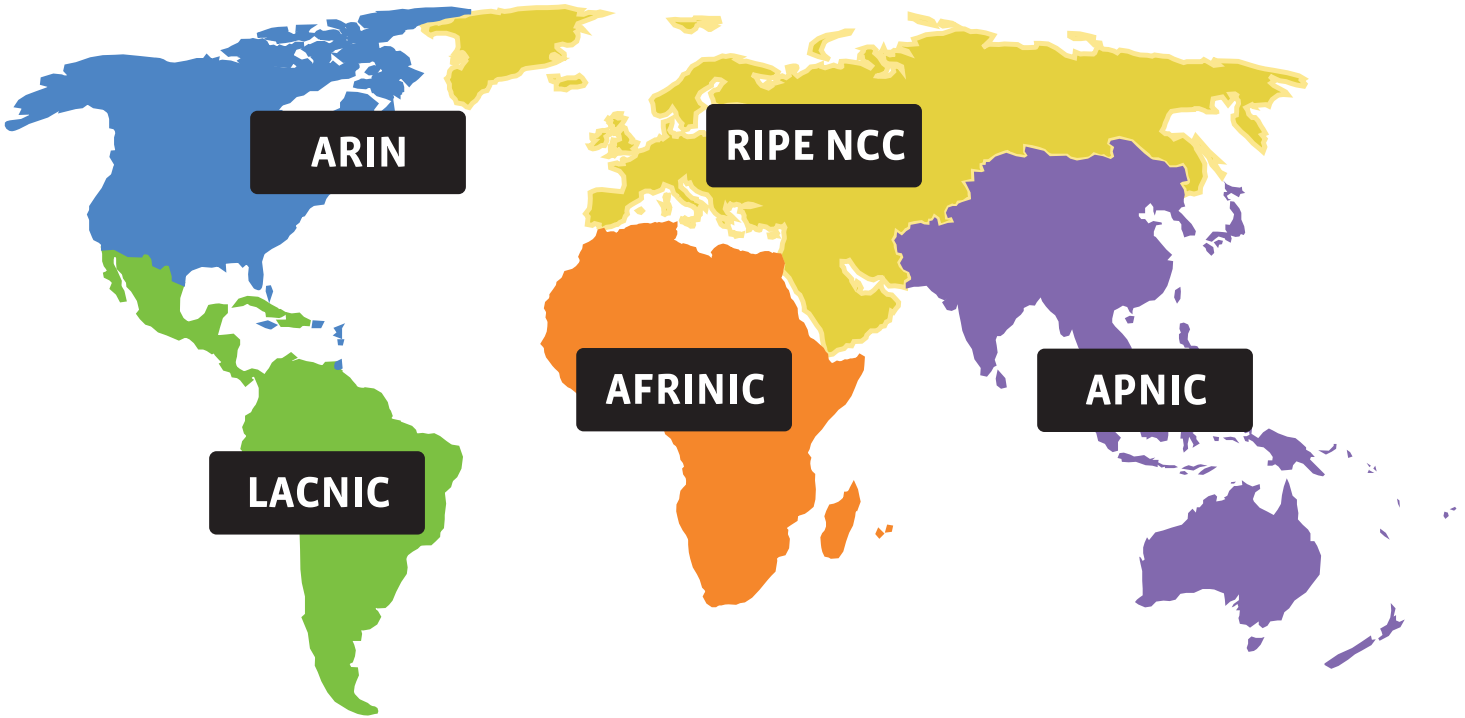
- Est-ce que le système autonome X a le droit de relayer l'annonce y ?
- Problème complexe : explosion combinatoire, performances, changements fréquents à ce niveau là

Autorité d'affectation d'IP et d'*AS number*

- *Internet Assigned Numbers Authority* (IANA), département de l'ICANN
- Délègue des préfixes `/8` aux registres Internet régionaux
- Les registres Internet régionaux allouent des préfixes IP aux fournisseurs de services Internet et / ou aux entreprises
- Délègue des intervalles d'identifiants de systèmes autonomes aux registres internet régionaux



Regional Internet Registry



https://www.iana.org
https://www.ripe.net
exemple : 140.93.0.0/16

Bonne pratiques et solutions de contournement

Bonne pratiques

- Filtrage des annonces invalides
- Limitation du nombre de préfixes annoncés

Exemple *looking glass* :

`http://www.cloudtacker.com/Route-servers`

```
$ telnet route-views.oregon-ix.net
```

`https://lg.gitoyen.net`

Bonne pratiques et solutions de contournement

Bonne pratiques

- Filtrage des annonces invalides
- Limitation du nombre de préfixes annoncés
- Peu suivies...

Exemple *looking glass* :

`http://www.cloudtacker.com/Route-servers`

```
$ telnet route-views.oregon-ix.net
```

`https://lg.gitoyen.net`

Bonne pratiques et solutions de contournement

Bonne pratiques

- Filtrage des annonces invalides
- Limitation du nombre de préfixes annoncés
- Peu suivies...

Monitoring des zones annoncées

- Monitoring des annonces à l'aide de serveurs *looking glass*
- Systèmes passifs

Exemple *looking glass* :

`http://www.cloudtacker.com/Route-servers`

```
$ telnet route-views.oregon-ix.net
```

`https://lg.gitoyen.net`

Bonne pratiques et solutions de contournement

Bonne pratiques

- Filtrage des annonces invalides
- Limitation du nombre de préfixes annoncés
- Peu suivies...

Monitoring des zones annoncées

- Monitoring des annonces à l'aide de serveurs *looking glass*
- Systèmes passifs
- Réaction humaine...
- Zones non couvertes...

Exemple *looking glass* :

`http://www.cloudtacker.com/Route-servers`

```
$ telnet route-views.oregon-ix.net
```

`https://lg.gitoyen.net`

Secure BGP

Objectifs de sécurité

- *Le marteau piqueur*

Secure BGP

Objectifs de sécurité

- *Le marteau piqueur*

(a) Vérification de l'origine : couple préfixe et *AS number*

Secure BGP

Objectifs de sécurité

- *Le marteau piqueur*

(a) Vérification de l'origine : couple préfixe et *AS number*

(b) Vérification du chemin *AS_PATH*

Secure BGP

Objectifs de sécurité

- *Le marteau piqueur*

(a) Vérification de l'origine : couple préfixe et *AS number*

(b) Vérification du chemin *AS_PATH*

(c) Authentification des routeurs BGP voisins

Secure BGP

Objectifs de sécurité

- *Le marteau piqueur*

(a) Vérification de l'origine : couple préfixe et *AS number*

(b) Vérification du chemin *AS_PATH*

(c) Authentification des routeurs BGP voisins

Principe

- Mise en place de PKIs dédiées au routage (IANA,RIR,LIR,ISPs)

(a) Signature d'autorisations à router un préfixe

Secure BGP

Objectifs de sécurité

- *Le marteau piqueur*

(a) Vérification de l'origine : couple préfixe et *AS number*

(b) Vérification du chemin *AS_PATH*

(c) Authentification des routeurs BGP voisins

Principe

- Mise en place de PKIs dédiées au routage (IANA,RIR,LIR,ISPs)

(a) Signature d'autorisations à router un préfixe

(b) Signature d'autorisations à diffuser des routes (pour AS voisins)

Secure BGP

Objectifs de sécurité

- *Le marteau piqueur*

(a) Vérification de l'origine : couple préfixe et *AS number*

(b) Vérification du chemin *AS_PATH*

(c) Authentification des routeurs BGP voisins

Principe

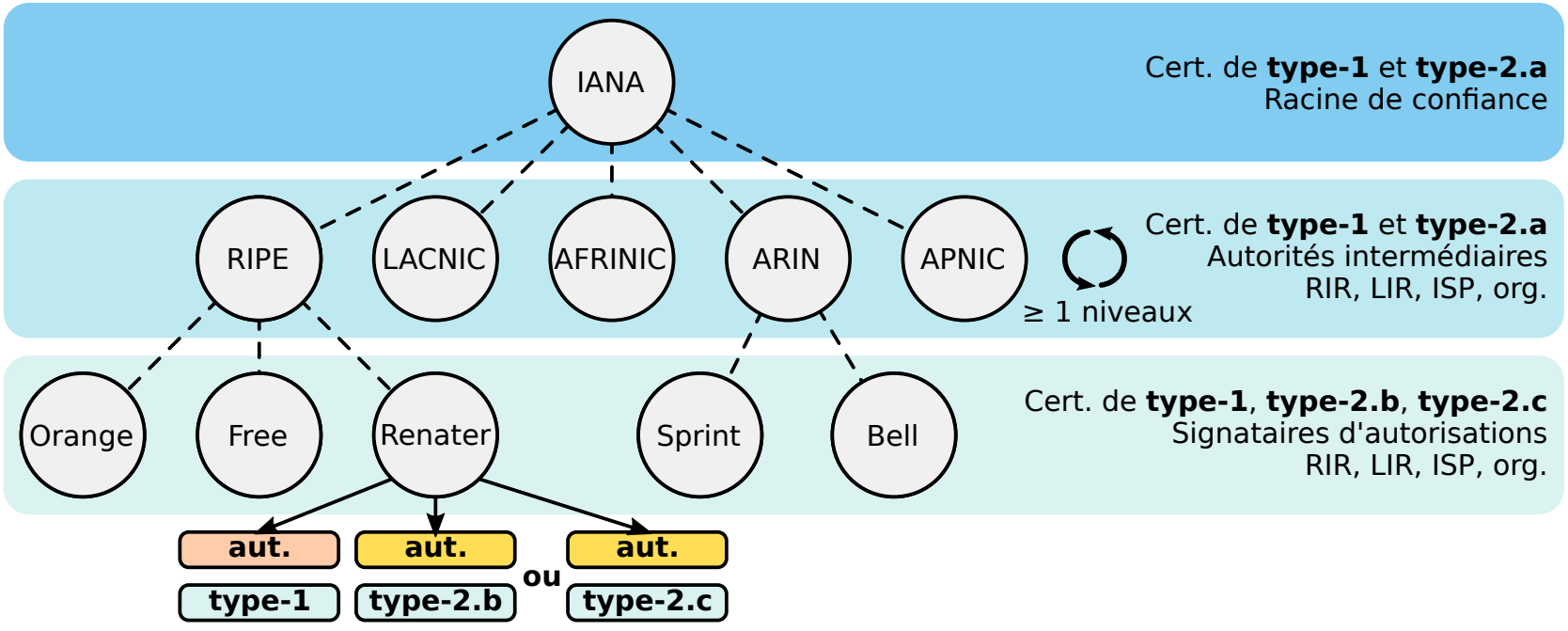
- Mise en place de PKIs dédiées au routage (IANA,RIR,LIR,ISPs)

(a) Signature d'autorisations à router un préfixe

(b) Signature d'autorisations à diffuser des routes (pour AS voisins)

(c) Utiliser IPSec pour sécuriser les comms point à point entre routeurs

Secure BGP : PKIs



- **type-1** : délégation d'adresses IP à une organisation et signature d'autorisations de routage (être origine d'une route)
- **type-2.a** : délégation d'identifiants d'AS à une organisation
- **type-2.b** : signature d'autorisation de diffusion de route
- **type-2.c** : signature d'autorisation de diffusion de route + IPSEC

Autorisations et distribution des informations

Autorisations

(1) Autorisation de router le préfixe. Diffusion *out of band*

(2) Autorisation de diffusion de route, distribuées avec les messages de mise à jour BGP. Distribution à l'aide d'un nouvel attribut aux messages BGP UPDATE

Diffusion des informations *out of band*

- Dépôts publics d'autorisation de router un préfixe
- Dépôts publics de certificats **type-1** et **type-2**

Route Origin VERification

Principe

- Vérification de l'origine d'une route
- Utilisation des zone DNS de recherche inversée
- Ajout d'enregistrements DNS supplémentaires :
  - *Route LOCK* : la zone supporte *ROVER* ?
  - *Secure Route Origin* : système autonome d'origine

Processus de décision

1. Recherche DNS inversée de l'enregistrement *RLOCK* sur le préfixe IP le plus proche en *class-full*
2. Recherche de l'enregistrement SRO sur l'adresse *class-less*

Route Origin VERification : exemple

Validation de l'origine des routes publiées par l'université du Colorado

- Annonce 1 route `/16` et 4 `/18`
- `129.82.0.0/16` et les 4 `/18`

```
$ ORIGIN 82.129.in-addr.arpa
$ TTL 3600

@      IN   RLOCK     ; secure entire zone
m      IN   SRO 12145 ; 129.82.0.0/16
0.0.m  IN   SRO 12145 ; 129.82.0.0/18
1.0.m  IN   SRO 12145 ; 129.82.64.0/18
0.1.m  IN   SRO 12145 ; 129.82.128.0/18
1.1.m  IN   SRO 12145 ; 129.82.192.0/18

; PTR records or delegation
```

Route Origin VERification

Projet mort depuis 2012-2013

Avantages

- Basé sur l'infrastructure DNS existante
- Pas de modification du protocole

Inconvénients

- Dépend de DNS SEC pour être vraiment sûr
- Ajout de nouveau enregistrements non standards

Plan

RPKI : Ressource Public Key Infrastructure

Qu'est-ce ?

Un premier pas vers la sécurisation du routage. Définit:

- Infrastructure pyramidale de clés (IANA, RIR, NIR, LIR/ISP) comme S-BGP
- Certificats pour l'AS origine d'une route (Route Origination Authorization)
- Infrastructure de dépôts contenant les clés publiques certifiées et les ROA

Permet à une entité de prouver qu'elle possède des IPs ou des ASs et de déléguer le droit de les router (par les ROA)

Pour le moment compatible IPv4 IPv6 (MPLS à venir?)

Utilisation d'autres standards

Certificats X.509 (et extension IP/AS RFC3779)
Cryptographic Message Syntax (CMS RFC5652)

Certificats d'allocation de ressources (certificats CA)

C'est quoi ?

Les éléments de base de RPKI
Certificats associant des ressources (plages IP, ou ASs) à une clé publique

Qu'est ce que ça prouve ?

L'émetteur du certificat cède des ressources au possesseur du certificat (i.e. de la clé secrète associée à la clé publique du certificat)

Pour qui / pour quoi faire ?

Pour les entités intermédiaires (IANA $\rightarrow$ ISP)

- Donne le rôle d'Autorité de Certification (CA) pour la gestion de ces ressources
- Permet de déléguer des ressources par des certificats EE (End-Entity)

Certificats pour entité finale (EE)

C'est quoi ?

Certificats associant des plages IP à une clé publique

Qu'est ce que ça prouve ?

L'émetteur du certificat atteste que le possesseur du certificat est l'ayant droit des plages IP

Pour qui / pour quoi faire ?

Entités finales utilisant les ressources (pas de sous-allocation)

Permet de signer UN SEUL ROA (ou un *manifeste*). Après la clé privée est supprimée (si on veut recommencer on redemande un autre certificat EE)

Route Origination Authorizations (ROAs)

Contenu

$\mathtt{ROA} = \mathtt{EE} \| \mathtt{AS\#} \| \mathtt{IP}_1/\mathtt{min}_1[-\mathtt{max}_1], \ldots, \mathtt{IP}_n/\mathtt{min}_n[-\mathtt{max}_n] \| \sigma$

1. Un certificat EE
2. Un numéro d'AS
3. Une série de préfixes IP + une longueur de masque maximale (optionnel par préfixe)
4. Une signature du tout avec le certificat EE

Que veut-il dire ?

Moi possesseur des ressources décrites dans EE autorise AS# à être *AS-origine* des préfixes entre IP_i/min_i et IP_i/max_i pour $i \in \{1, .., n\}$

Validité

- Il faut que les préfixes IP du ROA et du certificat EE soient les mêmes
- Durée de validité du ROA: implicitement celle du certificat EE
- Révocation du ROA: vérifier si le certificat EE est révoqué

Utilisation de la RPKI

Mise en place d'un cache

Pour utiliser un objet signé de la PKI on demande le téléchargement complet d'un cache de l'infrastructure (i.e. certificats, manifestes, CRLs)

Les dépôts sont obligés de mettre en place `rsync` donc à chaque mise à jour on ne télécharge que les différences.

Procédure de vérification

1. Pour chaque certificat CA vérifier la signature du manifeste et qu'on est avant la date d'actualisation prévue
2. Vérifier que tous les certificats et CRLs indiqués dans le manifeste sont présents et ont le bon hash (sinon notifier la corruption)
3. Vérifier chaque certificat EE par sa chaîne de certification

Utilisation des ROAs (1/2)

Validation des routes

Pour chaque route on prend tous les ROAs avec des préfixes qui matchent ou englobent le préfixe de la route

1. Si cet ensemble est vide le résultat est *unknown*
2. Si pour un ROA de la liste le préfixe de la route correspond à celui du ROA (sans être plus précis qu'autorisé) et l'AS est bon le résultat est *valid*
3. Sinon le résultat est *invalid*

Conséquences

- Les routes avec un préfixe correspondant à un ROA valide sont valides si l'AS est bon, et invalides sinon
- Une fois un préfixe P est décrit dans un ROA, toute route pour un préfixe englobé par P est invalide si elle n'a pas elle-même un ROA
- Les routes correspondant à un préfixe qui n'est pas dans un ROA ni englobé complètement par celui d'un ROA ont pour résultat *unknown*

Utilisation des ROAs (2/2)

Que faire de valid/invalid/unknown ?

Toute latitude est laissée aux opérateurs sur leurs stratégies de choix

"Valid is to be preferred over unknown which is to be preferred over invalid"

Utilisation du AS 0

- AS réservé par l'IANA pour désigner des réseaux non-routés
- On peut émettre un ROA avec un AS 0 pour dire qu'on ne souhaite pas qu'un préfixe soit routé
- Vu la procédure de validation (une validation suffit pour passer d'invalid à valid) ça peut permettre un comportement par défaut pour un ensemble des préfixes sauf s'ils sont indiqués comme routables par un autre ROA

Fin !

Prochain cours

Dénis de service