Le Rézoléo

Présentation générale

onxzy

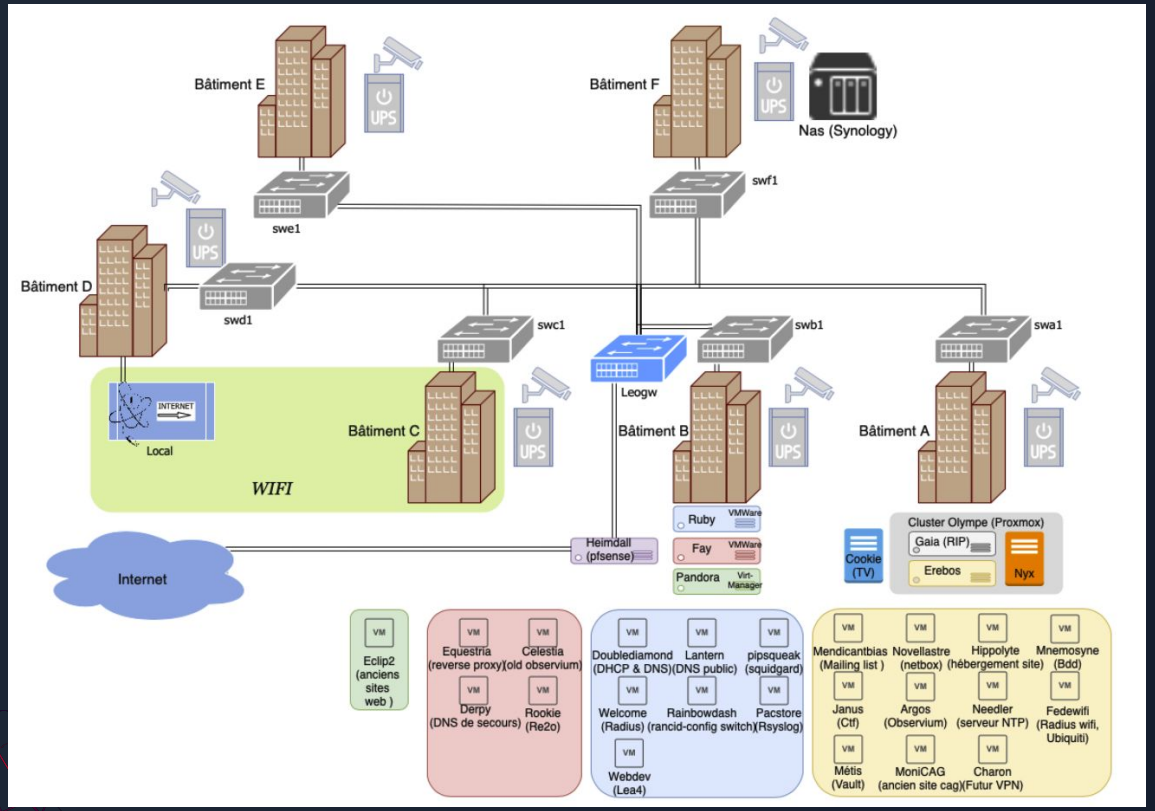
Le Rézoléo

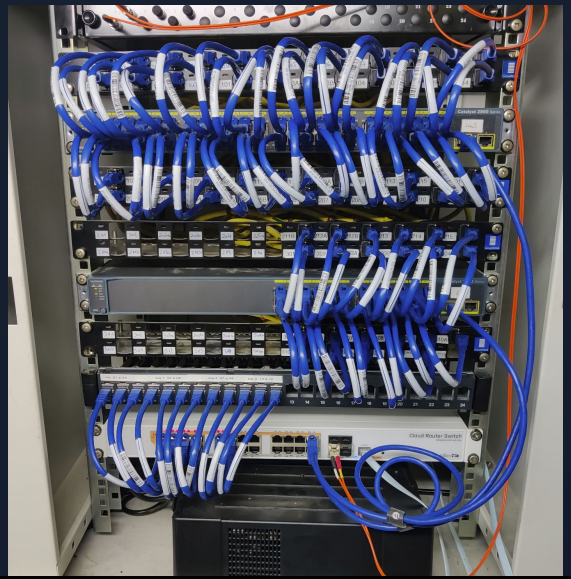
FAI	*Association Loi 1901 indépendante de Centrale mais lié par un contrat avec l'AGR*
Membres	
Services	*Internet, Hébergement, Réparations, Formations, LAN*
FedeRez	*Journées et nocturnes, échanges inter-assos*
Nos projets	*Léa5, Serveur de stockage, Ansible*

Les bases d’un Réseau

- Connecter les machines *(Câbles, Switch, Bornes Wifi)*
- Identifier les machines *(MAC, IP, DHCP)*
- Nommer les machines *(DNS)*
- Accéder à Internet *(Passerelle, Pare feu)*
- Autoriser les machines *(Radius)*
- Les serveurs *(Virtualisation)*

Connecter les machines





Identifier les machines

L’adresse MAC

- *Adresse de la carte réseau*
- *Une adresse par carte physique (donc par exemple une pour la carte wifi et une pour la carte ethernet)*
- *Représentée en hexadécimal*
- *Codée sur 6 octets*
- *xx:xx:xx:xx:xx:xx (x allant de 0 à f)*
- *~ 4.10^{14} adresses possibles (les 3 premiers octets étant les octets du constructeur)*

L’adresse IP (v4)

- *Adresse pour identifier les réseaux et pour identifier les machines*
- *Codée sur 32 bits = 4 octets*
- *10101100.00011110.10001000.11000100*
- *Représentée en décimal : 172.30.136.196*
- *X.X.X.X (X allant de 0 à 255)*
- *~ 4.10^{9} adresses possibles*

Identifier les machines

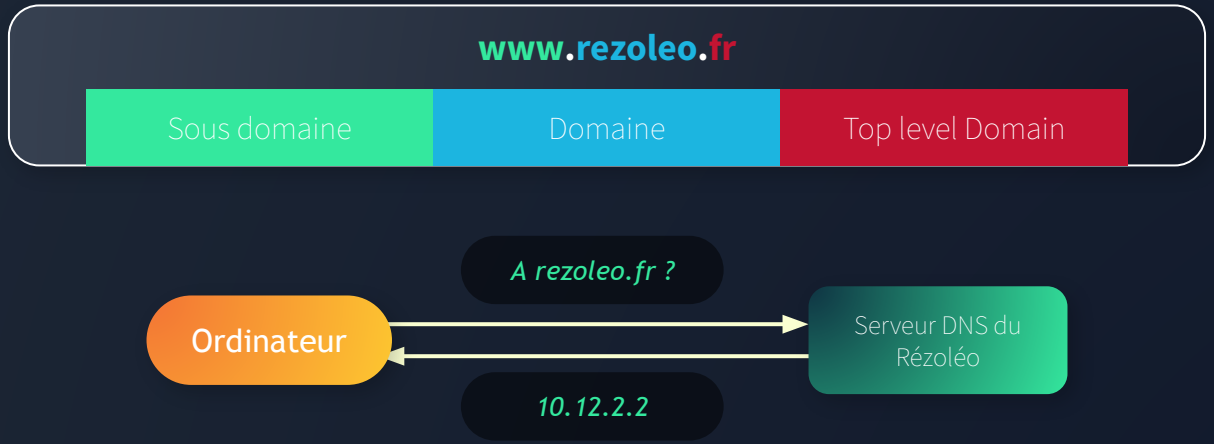
Le DHCP

- *Protocole pour distribuer des IPs*
- *Permet de s'assurer de l'unicité des IPs*
- *Permet de donner aux machines du réseau des informations indispensables : adresse IP, masque de sous réseau, passerelle, serveur DNS*

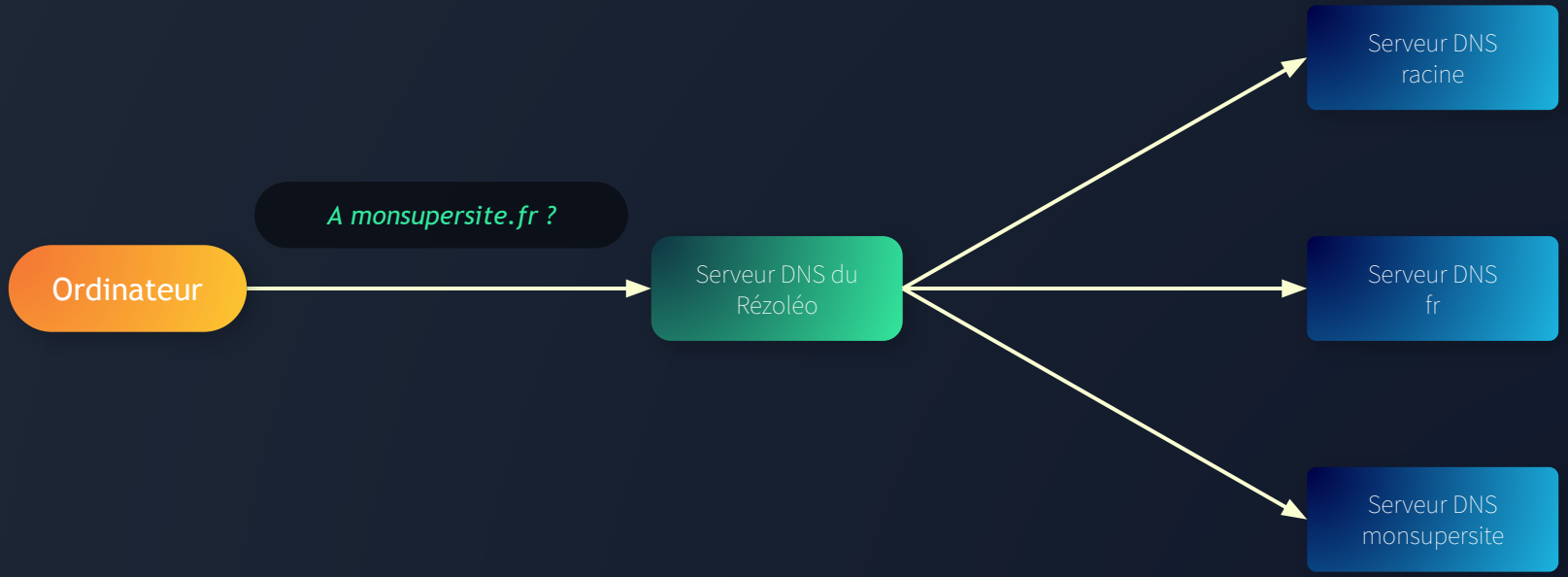
```
ipconfig /all
```

```
$ ip a
```

Nommer les machines : le DNS



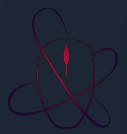
Nommer les machines : le DNS



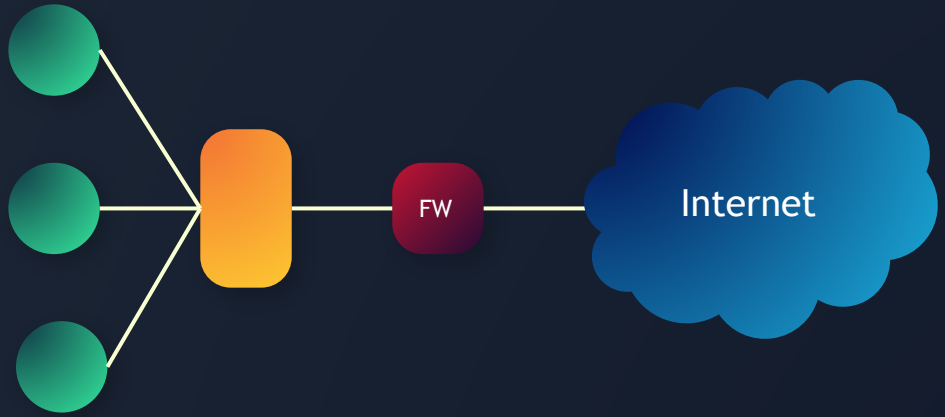
Nommer les machines : le DNS

```
nslookup rezoleo.fr
```

```
$ dig rezoleo.fr
$ dig @1.1.1.1 rezoleo.fr
$ dig . NS
```



Accéder à internet



route print

$ ip route show

Autoriser les machines

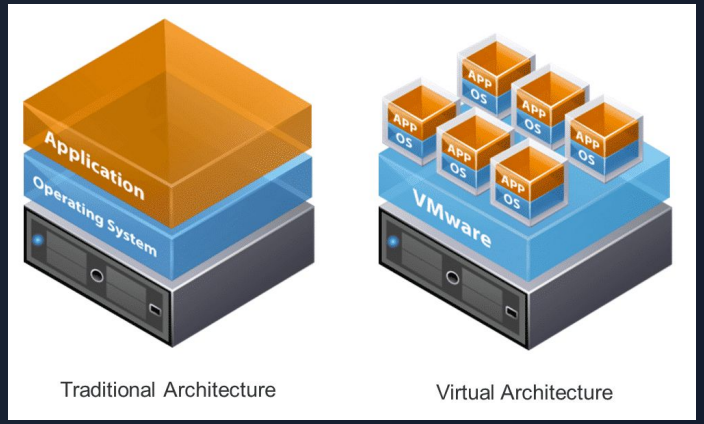
Le Radius

- *Authentication, Authorization, Accounting*
- *Filaire*
  - *Utilise la MAC*
- *Wifi*
  - *Identifiant + Mot de passe*

Les serveurs

Rôle de l'hyperviseur

- *Assure le contrôle du processeur et des ressources de la machine hôte.*
- *Alloue à chaque VM les ressources dont elle a besoin.*
- *S'assure que ces VMs n'interfèrent pas les unes avec les autres.*



Routage

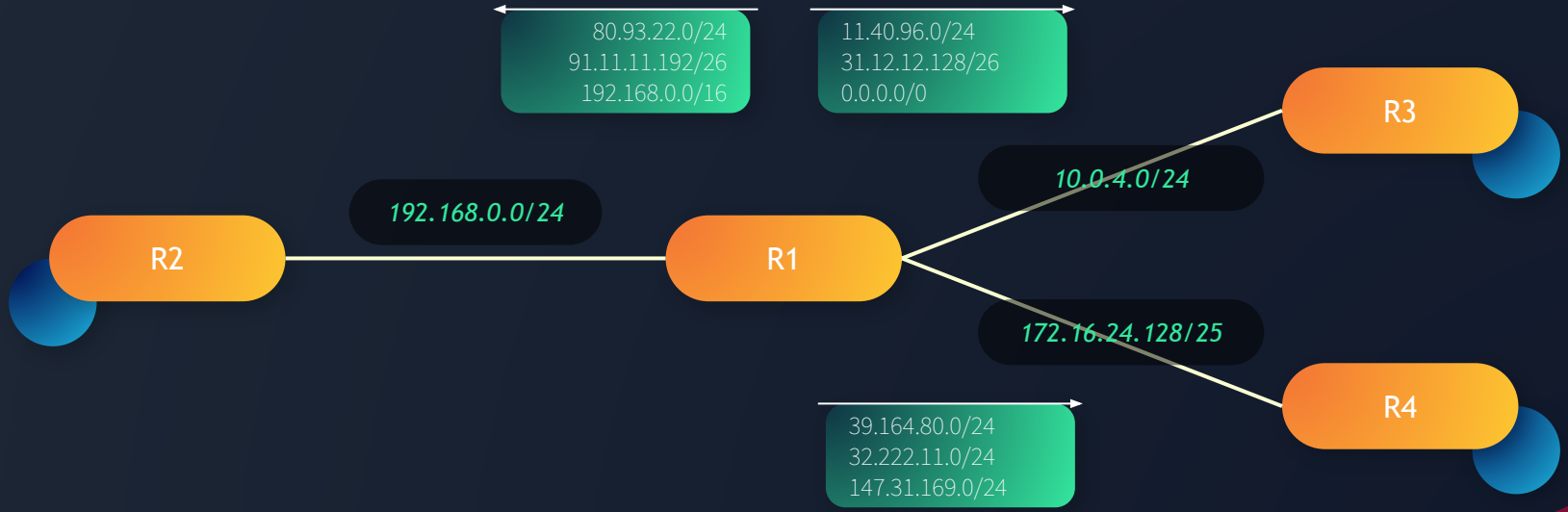

80.93.22.0/24
91.11.11.192/26
192.168.0.0/16
11.40.96.0/24
31.12.12.128/26
0.0.0.0/0
R3
10.0.4.0/24
192.168.0.0/24
R2
R1
172.16.24.128/25
R4
39.164.80.0/24
32.222.11.0/24
147.31.169.0/24

Table de routage

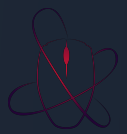
Packet Header
→ 192.168.1.1

IP Routing Table

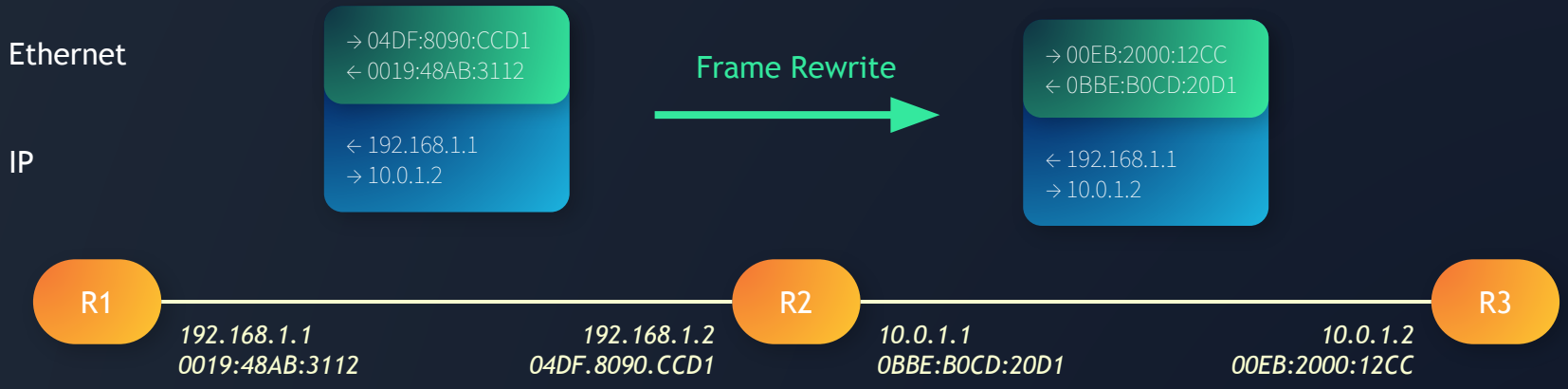
Target Network	Mask	Next Hop

(*192.168.1.1*	&&	*255.255.255.0*	)	≠	10.0.1.0	→	deny	10.0.0.1
(*192.168.1.1*	&&	*255.255.255.0*	)	≠	192.168.2.0	→	deny	10.0.8.1
(*192.168.1.1*	&&	*255.255.0.0*	)	≠	172.16.0.0	→	deny	172.16.1.1
(*192.168.1.1*	&&	*255.255.252.0*	)	≠	10.4.0.0	→	deny	10.0.0.1
(***192.168.1.1***	**&&**	***255.255.255.128***	**)**	**=**	**192.168.1.0**	**→**	**permit**	**10.0.8.1**

En cas de conflit / overlap → règle la plus spécifique



Routage : Frame rewrite



Utilisation d’une table pour améliorer les performances : *Express Forwarding*

Routage dynamique

IGP : Interior Gateway Protocol

- *ne connaissent que les réseaux IP internes à l'AS*
- *via broadcast ou multicast → pas de connexions établies entre routeurs*
- *sur toutes les interfaces du routeur émetteur vers tous les voisins*

EGP : Exterior Gateway Protocol

- *Permet de contrôler parfaitement les informations transmises*
- *mises à jour vers voisins identifiés → connexion établie entre eux*
- *diffusées de routeur à routeur*
- *possibilité de filtrer*

IGP : RIP (Routing Information Protocol)

Plus vieux protocole de routage dynamique : 1988
Protocole à vecteur de distance

Très simple, rarement utilisé en production mais utile pour apprendre

Converging : Routeurs cherchent les meilleurs routes
Converged : Tous les routeurs ont leurs routes à jour

IGP : RIP (Routing Information Protocol)

Annonce des routes :

- *Dès la connexion le routeur broadcast sa Route Table à tous ses voisins*
- *Processus à sens unique, sans mécanisme de retransmission*
- *Mise à jour de la table après réception de l'annonce des voisins*
- *Toutes les 30 secondes, indépendamment de la réception des mises à jour*

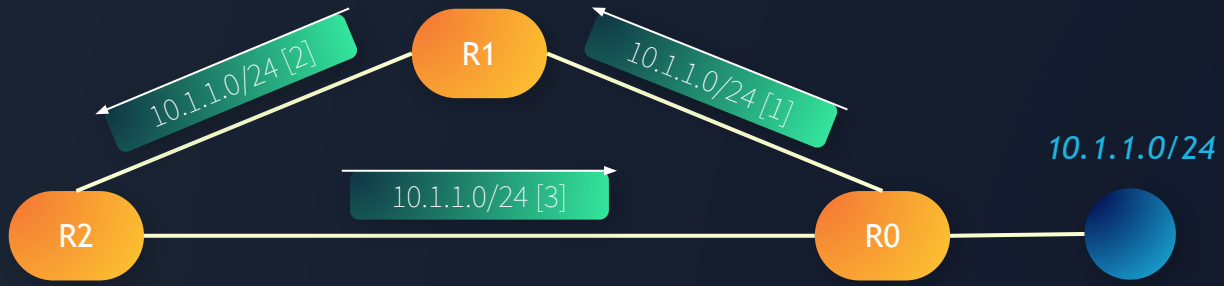
La mesure :

- *Représente la qualité d'une route*
- *RIP : Nombre de sauts, entre 1 et 16*
- *Limite de ce protocole : ne prend pas en compte la vitesse, la qualité, le coût …*

IGP : RIP (Routing Information Protocol)

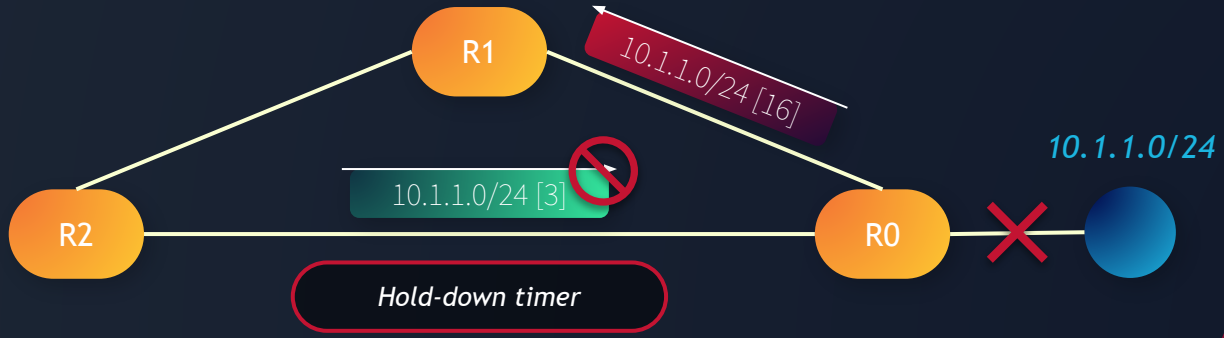
Prévention des boucles :

- *Boucle : envoi du trafic sur le même chemin encore et encore*
- *Utilisation de la mesure :*
  Si 2 fois la même route, RIP garde uniquement la route de mesure la plus faible
  Route Poisoning : Mesure de 16 ⇒ oublier la route
- *Split Horizon : Un routeur n'envoi pas à son voisin ce qu'il a appris par lui*

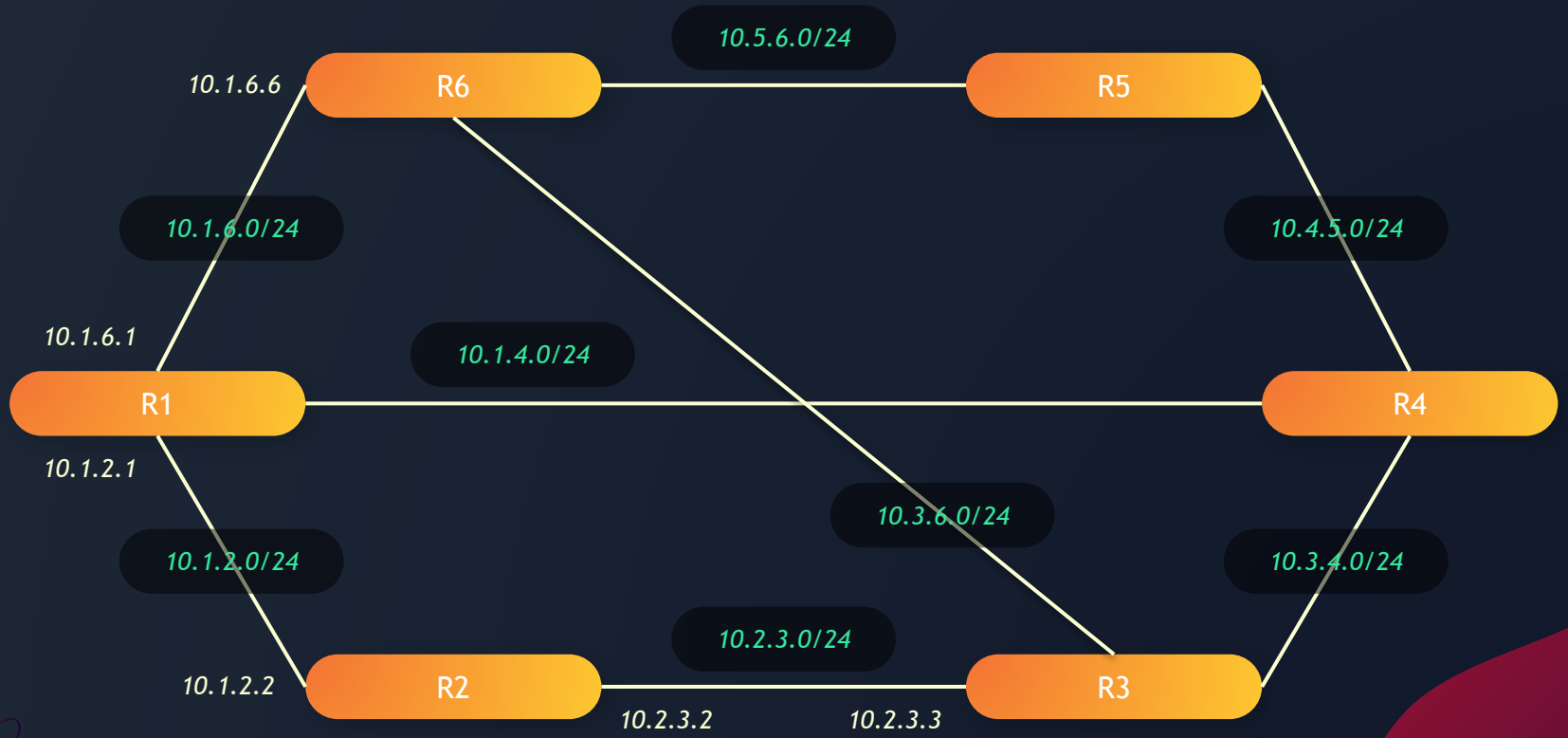


IGP : RIP (Routing Information Protocol)

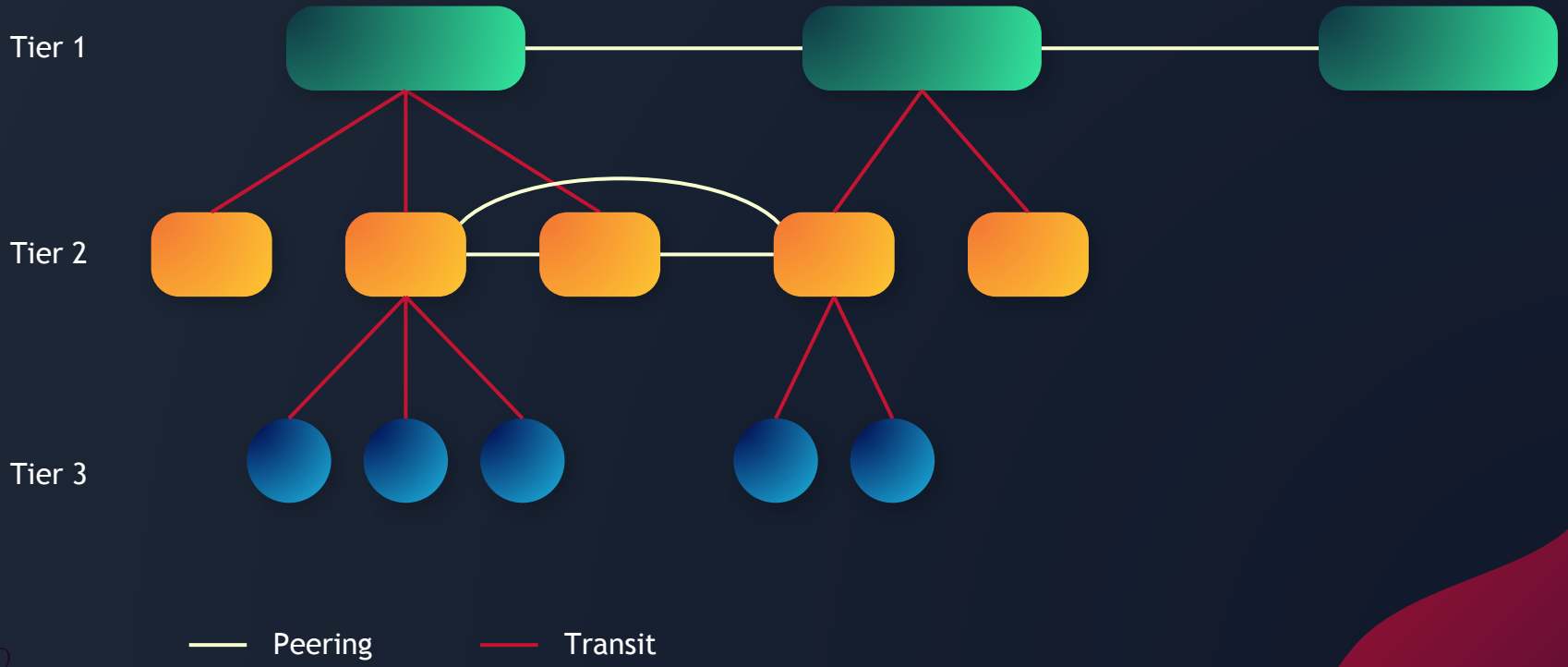
UPDATE	*30s*	
INVALID	*180s*	Durée durant laquelle la route reste valide en l'attente d'une mise à jour
HOLD-DOWN	*180s*	*(Spécifique Cisco)* Ne prendre en compte aucune mise à jour pour cette route → Permet d'attendre la propagation de la chute de la route
FLUSH	*240s*	Si HOLD-DOWN expiré, le routeur accepte les routes avec mesure différente Une fois expiré, les nouvelles updates pour cette route seront traitées comme une nouvelle route



Routage interne : RIP



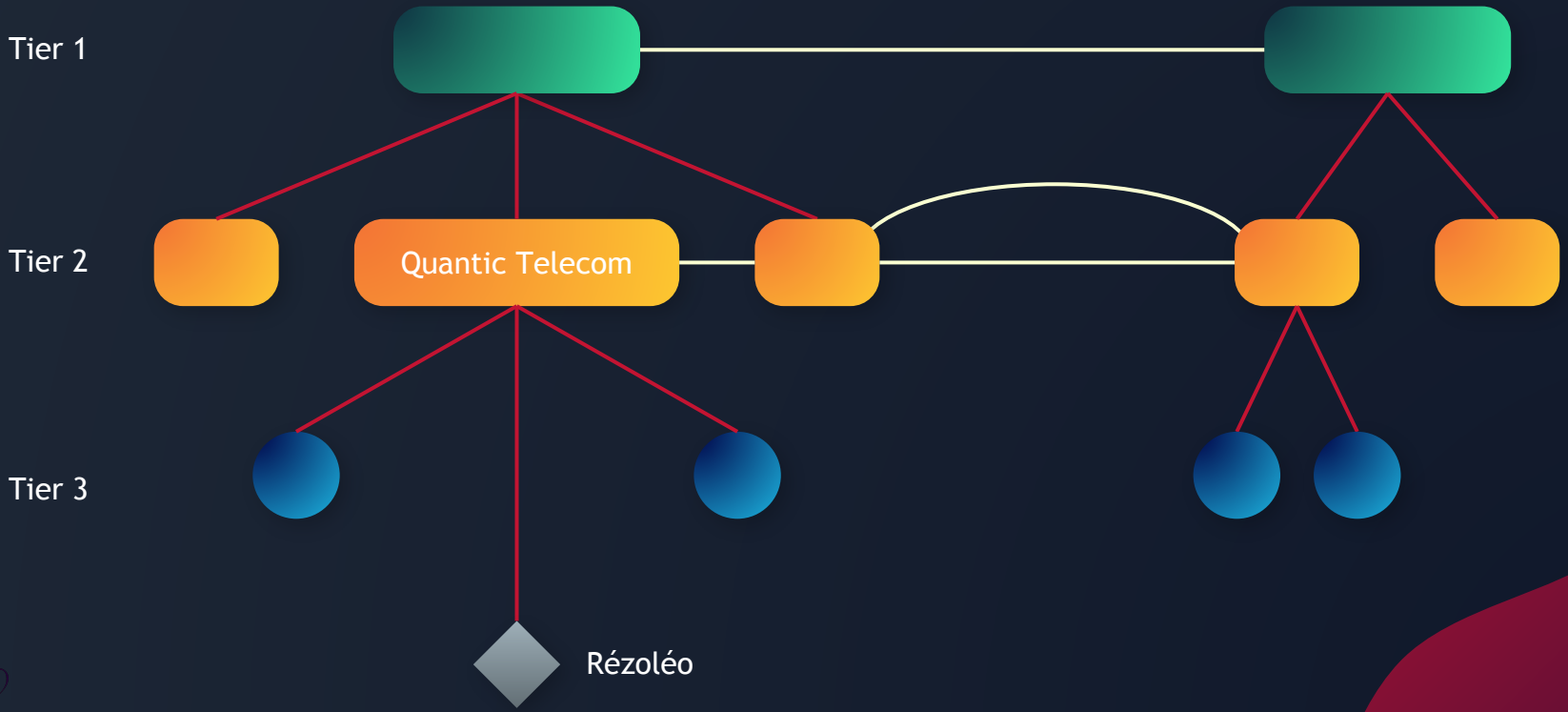
Fournisseurs d’accès internet



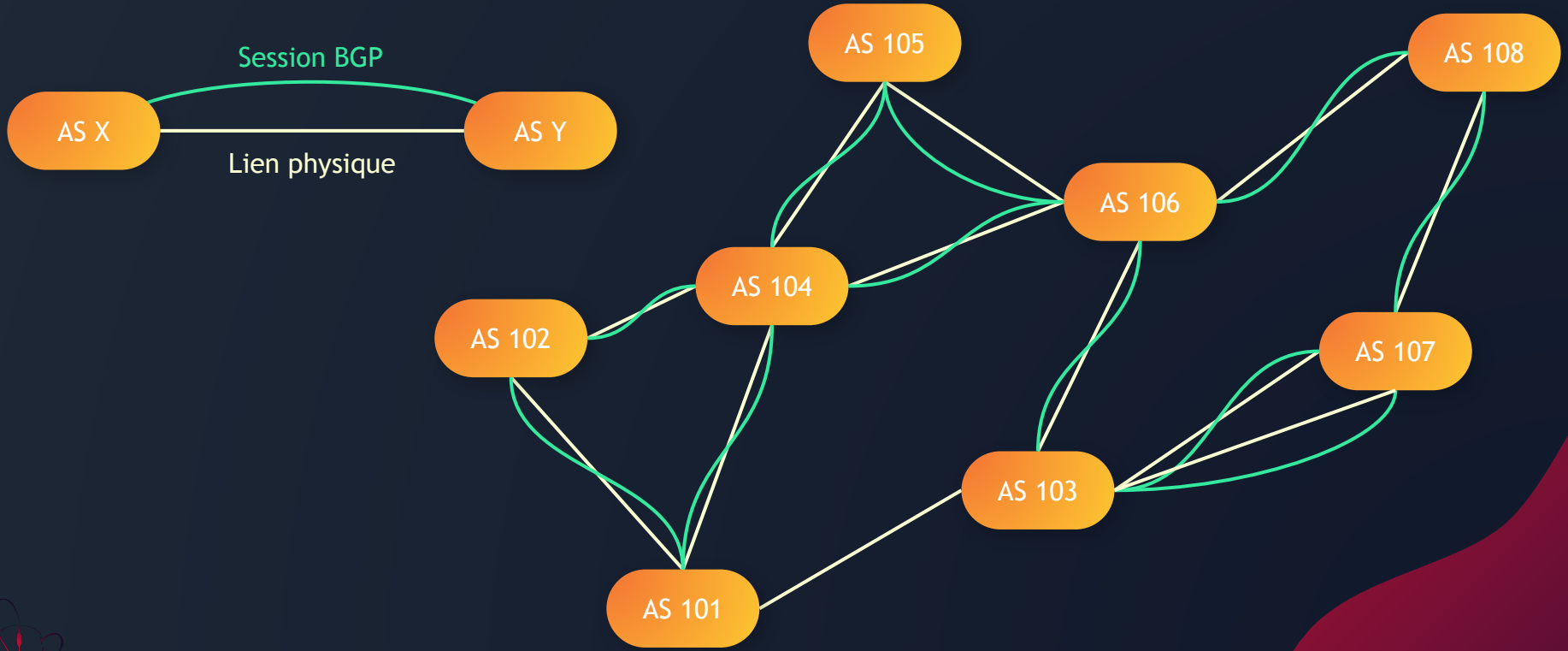
Carte réseau d’Orange

https://internationalcarriers.orange.com/en/network.html

Fournisseurs d’accès internet

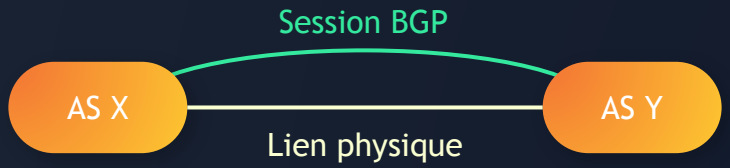


BGP


Session BGP
AS X
AS Y
Lien physique
AS 105
AS 108
AS 106
AS 104
AS 102
AS 107
AS 103
AS 101

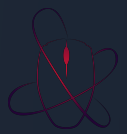
BGP : Les messages

OPEN	Utilisé dès que la connexion TCP est établie entre les voisins BGP Permet d'échanger des informations telles que les numéros d'AS respectifs et les router ID de chacun, et de négocier les capacités de chacun des pairs
KEEPALIVE	Maintient la session ouverte. Par défaut envoyé toutes les 30 secondes 90 secondes sans message UPDATE ni KEEPALIVE entraîne la fermeture de la session
UPDATE	Permet l'annonce de nouvelles routes ou le retrait de routes ;
NOTIFICATION	Message de fin de session BGP à la suite d'une erreur



BGP : Les attributs

AS Path	WM	Liste ordonnée des systèmes autonomes traversés
Next Hop	WM	Adresse IP du voisin BGP
Origin	WM	Origine de la route (IGP, EGP ou Incomplète)
Atomic Aggregate	WD	Si agrégation "atomique" (supprimant les AS agrégés) : Liste des AS supprimés après l'agrégation
Local Preference	WD	Métrique destinée aux routeurs internes en vue de préférer certaines routes
Community	OT	Marquage de route
Aggregator	OT	Si agrégation: Identificateur et AS du routeur qui a réalisé l'agrégation
Multiple Exit Discriminator (MED)	ON	Métrique destinée au départ aux routeurs externes en vue de leur faire préférer certains routes (utilisable finalement plus largement)



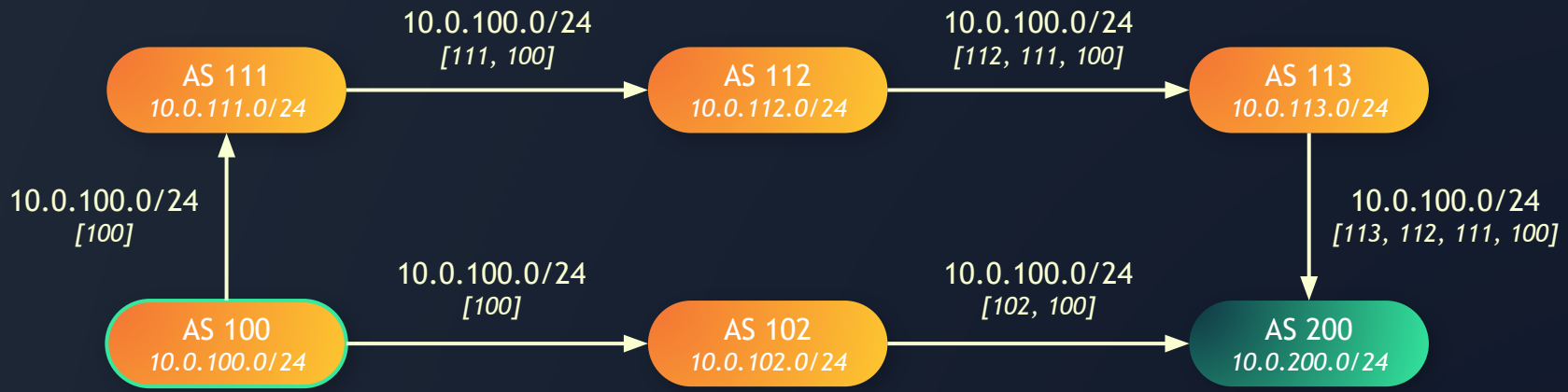
WM Doit être pris en charge et propagé

OT Pas nécessairement pris en charge mais propagé

WD Doit être pris en charge, propagation optionnelle

ON Pas nécessairement pris en charge ni propagé

BGP



2 Routes pour AS 100 *(10.0.0.100)*

- 113, 112, 111, 100
- 102, 100

Processus de décision du routage BGP

Pas forcément le chemin le plus court !

- Poids
- Préférence locale
- Origine
- Longueur du chemin AS
- Code d'origine
- MED (Multi Exit Discriminator)
- Chemin eBGP sur chemin iBGP
- Chemin IGP le plus court vers le prochain saut BGP
- Chemin le plus ancien
- ID du routeur
- Adresse IP du voisin

BGP : Problèmes

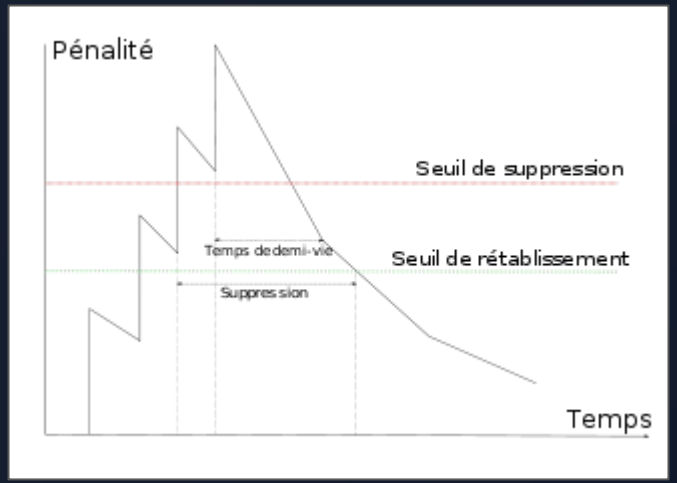
Vitesse de convergence

- *Hold-Time de 90s par défaut*
- *Nombre important de préfixes*

Instabilité et damping

- *Sensible à l'oscillation rapide des routes*
- *damping va accroître une pénalité numérique associée à cette route*

Préfixe avec origines multiples

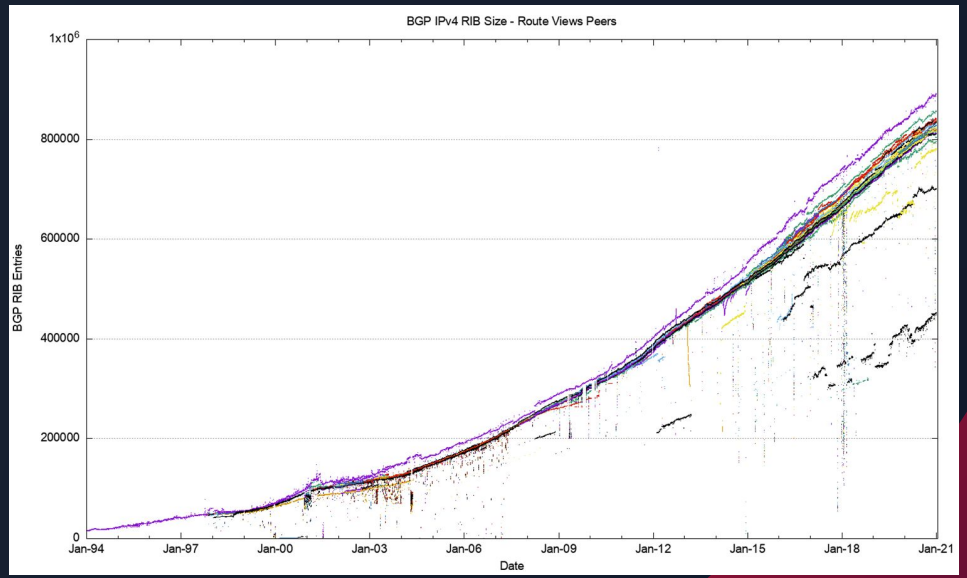


Taille des tables BGP

Chaque routeur stocke une base de donnée locale des préfixes annoncés

Capacité de calcul limitée
→ mise en file d'attente
→ retard en temps réel
→ propagation de routes fantômes

2018 : 700 000 routes et 60 000 AS



BGP : Incidents

Youtube, février 2008

- *IP Hijacking*
- *Pakistan ordonné un blocage de Youtube*
- *Pakistan Telecom a annoncé à tous les routeurs des fournisseurs d'accès qu'il était la meilleure route à qui envoyer tout le trafic YouTube, qui a alors été coupé sur l'ensemble de la planète.*
- *Pendant ~2h*

Plus d'exemples : https://fr.wikipedia.org/wiki/Border_Gateway_Protocol

Bibliographie

https://racine.gatoux.com/lmdr/index.php/igp-egp-et-as/

https://www.kadiska.com/fr/blog-qu-est-ce-que-le-protocole-de-routage-bgp/
https://www.kadiska.com/fr/blog-comment-fonctionne-le-routage-bgp/
https://fr.wikipedia.org/wiki/Border_Gateway_Protocol

https://ftp.registro.br/pub/gter/gter30/TutorialBGP/7%20-%20Transit.pdf
https://www.cisco.com/c/fr_ca/support/docs/ip/border-gateway-protocol-bgp/213952-configure-bgp-to-advertise-a-default-rou.pdf

https://www.ictshore.com/free-ccna-course-start/
https://www.ictshore.com/advanced-networking/route-map-cisco/
https://asrank.caida.org/
https://www.ictshore.com/free-ccna-course/bgp-single-homed/

https://bgpfilterguide.nlnog.net/guides/bogon_prefixes/
https://learningnetwork.cisco.com/s/question/0D53i00000Kt26MCAR/origin-codes-i-igp-e-egp-incomplete