

Sécuriser le moteur de l'Internet



Arnaud FENIOUX - FranceIX
#NetSecure Day 2014

Internet

les usages





en 60
secondes

Dessine moi internet







Et sinon, IRL?

Des cables et des hommes

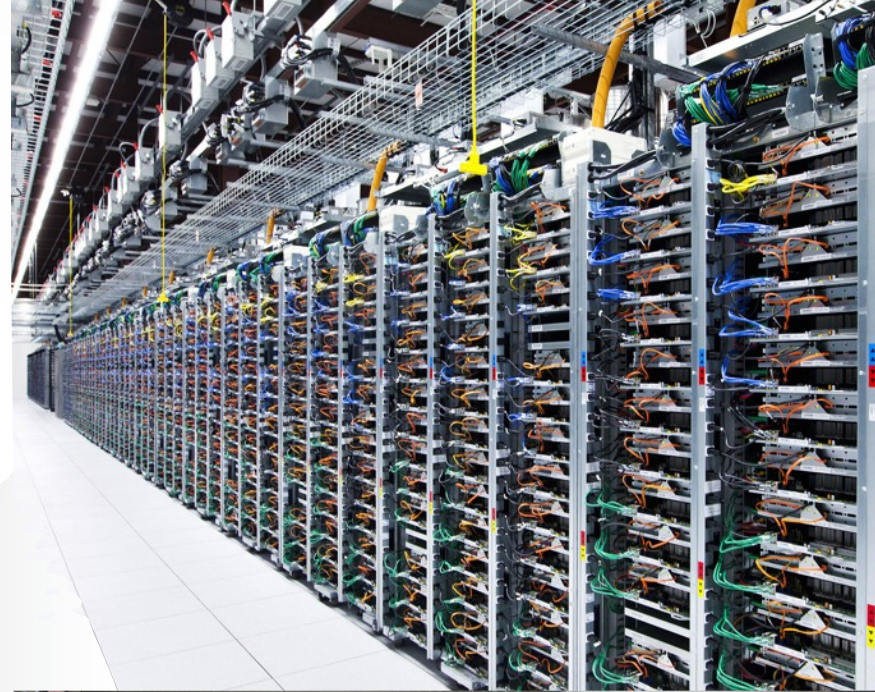


Opérateur de collecte

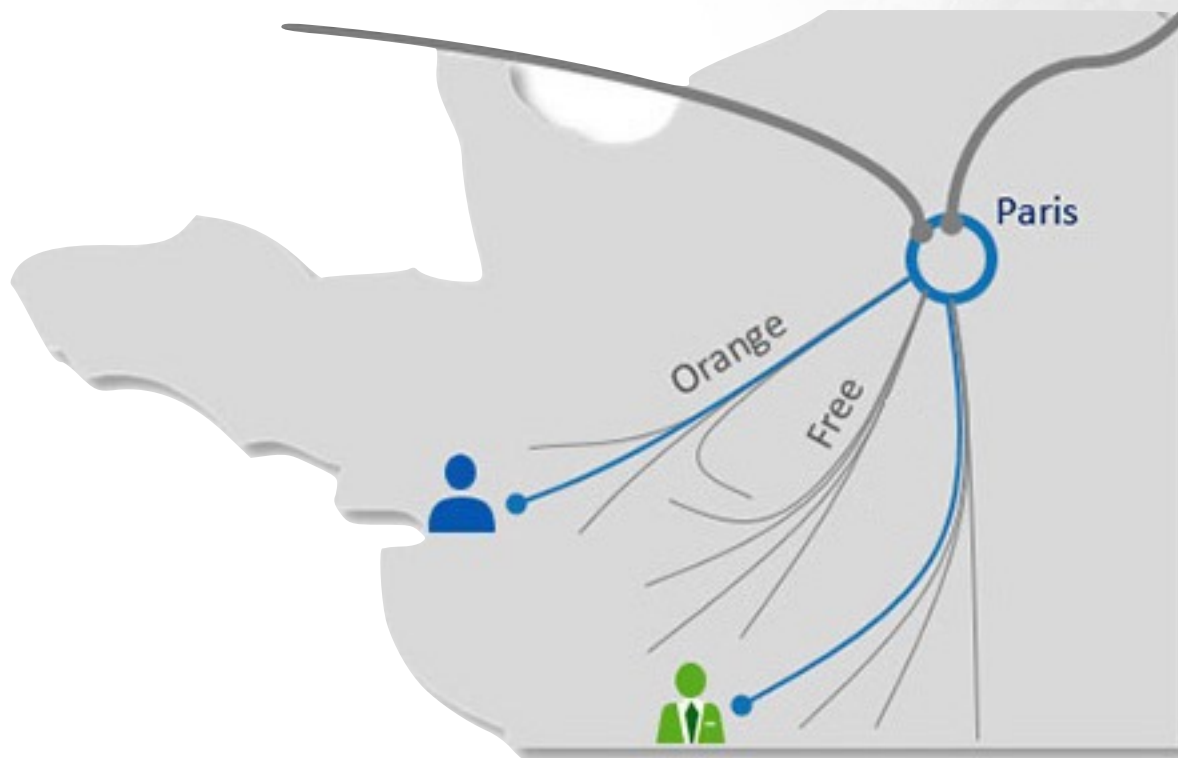
collecte cuivre / ADSL - NRA



Réseaux et POP



Un opérateur = Un réseau

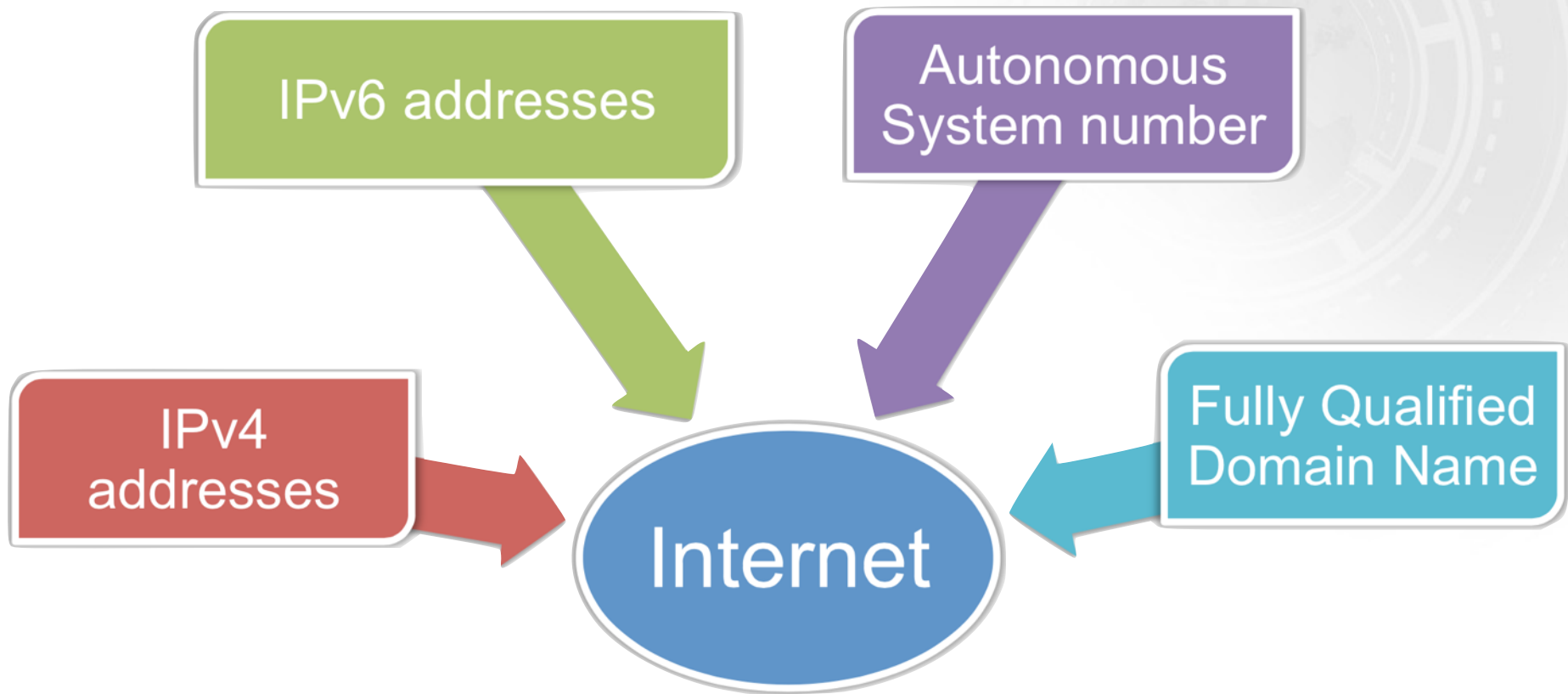


<http://www.ouestix.fr/>

Internet

les ressources que nous partageons

Les ressources Internet



FQDN

DNS

- root DNS / TLD
- Gestion par ICANN et délégation
- nom de domaine
- www.franceix.net

IPv4

Notation CIDR

- Codée sur 32 bits
- 37.49.236.1
- réseau 37.49.236.0/23
- Masque de sous réseau 255.255.254.0
- environ 512 000+ réseaux visibles sur Internet
- Broadcast (ARP)

IPv6

Notation CIDR

- Codée sur 128 bits
- 8 blocs de 2 octets séparés par des « : »
- Notation hexadécimale (RFC 5952)
- 2001:07f8:0054:0000:0000:0000:0000:0001
- 2001:7f8:54::1
- réseau 2001:7f8:54::/64
- environ 20 000 réseaux visibles sur Internet
- pas de Broadcast -> Multicast (NDP)

ASN

1 réseau/entreprise = 1 ASN

- codé sur 16 puis 32 bits

1-64495

23456

65535-131071

131072-4199999999

4200000000 – 4294967294

4294967295

Internet public

Réservé AS16/32bits

Réservé

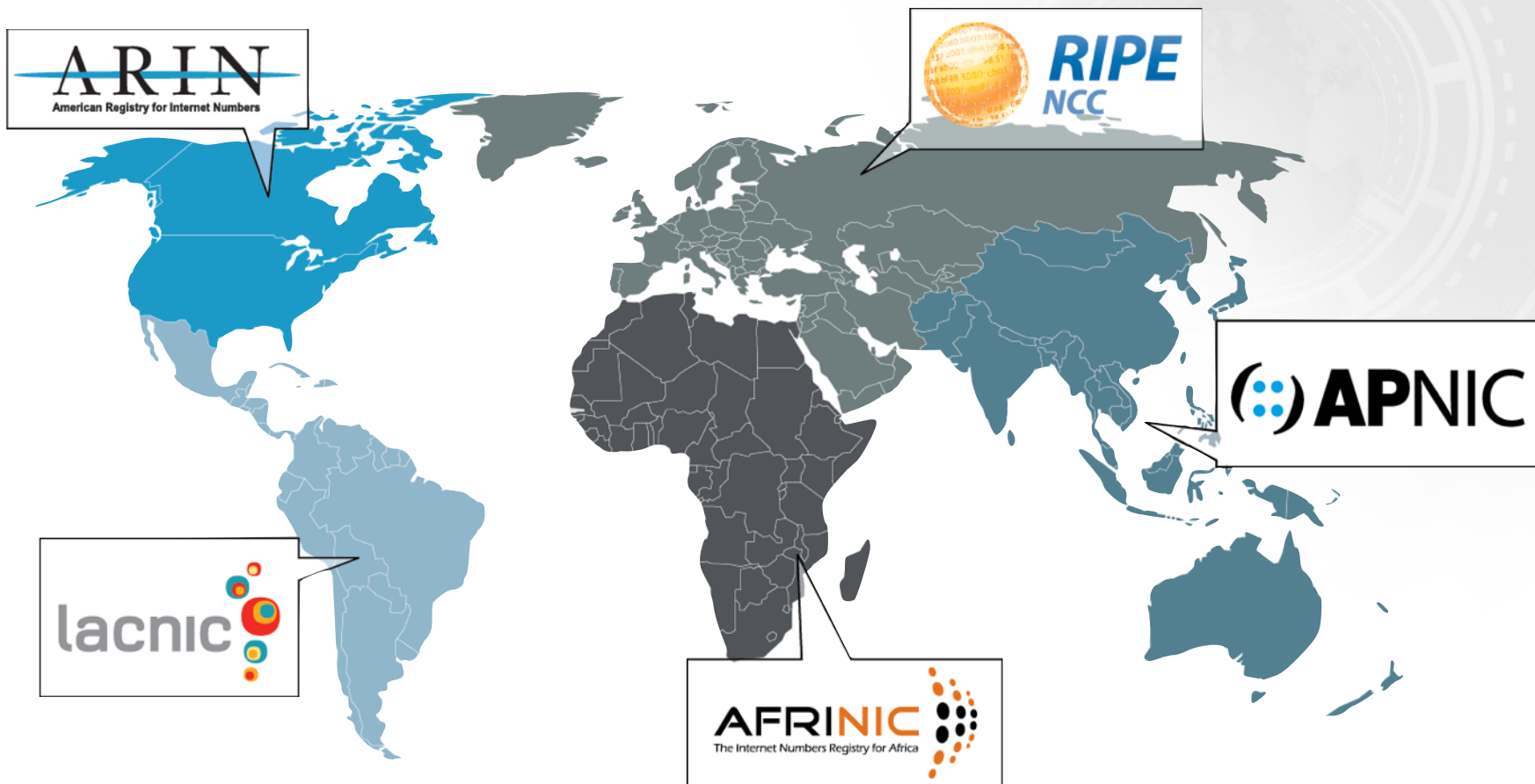
Internet public

Privé

Réservé

- environ 50 000 visibles sur Internet

Carte des RIR



<https://www.arin.net/knowledge/rirs/countries.html>

Internet

le routage



Routage

En mode circuit (connecté)

- Téléphonie
- Allocation des ressources

En mode datagrammes (non connecté)

- Chaque paquet est traité indépendamment
- Les paquets peuvent arriver dans le désordre
- Pas d'allocation de bande passante

Algorithme de routage

Critères de détermination du meilleur chemin

- Nombre de Hop (routeurs)
- Distance (km) / Temps (ms)
- Charge/utilisation (%tage / Mbps)
- Qualité (perte de paquets)
- Régularité (Gigue)
- Nombre d'AS traversés
- Prix





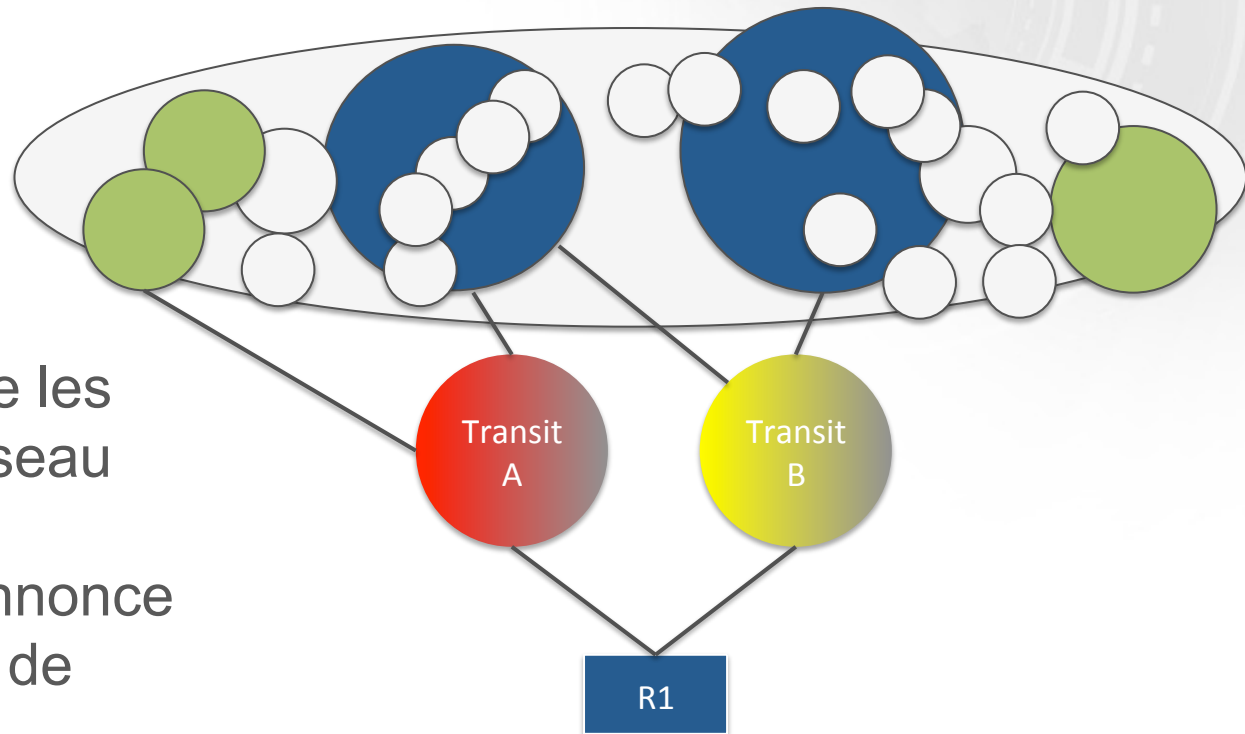
Peering, Transit

et Points d'échange

Définitions

Transit

- Acheminement de trafic sur tout internet
- Moyennant un paiement
- Le client annonce les routes de son réseau
- Le fournisseur annonce toutes les routes de l'internet

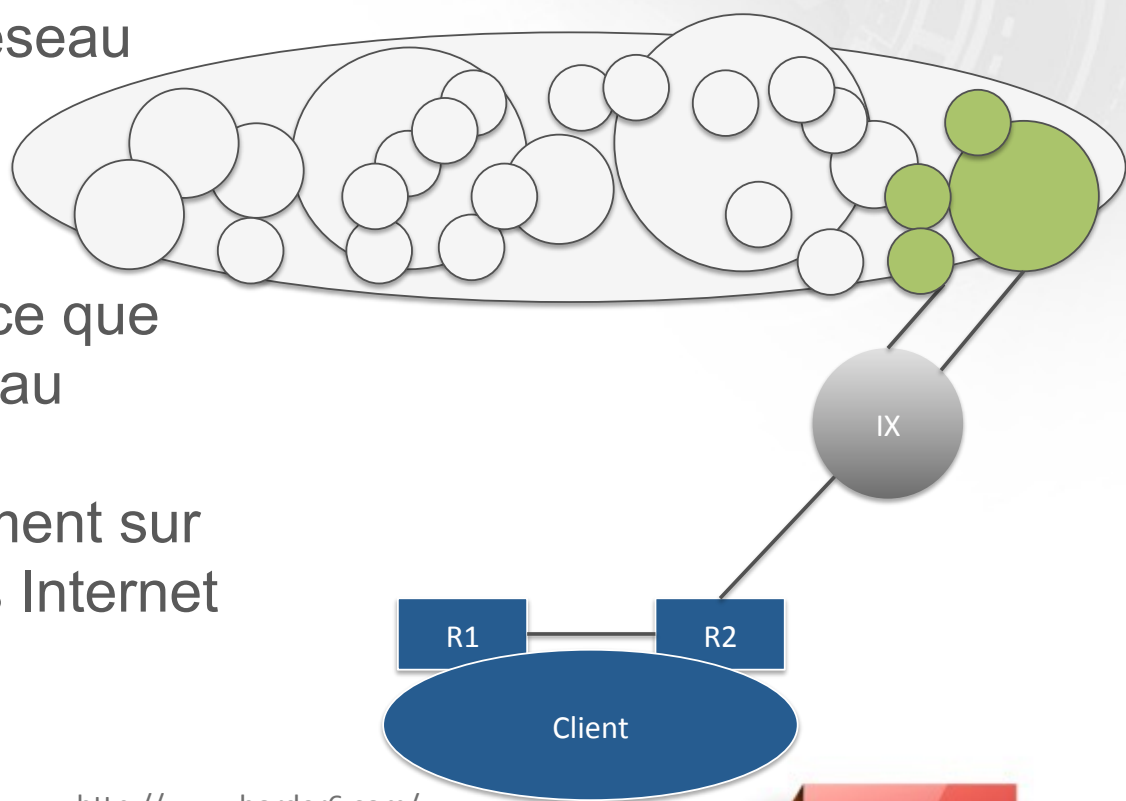


<http://www.border6.com/>

Définitions

Peering

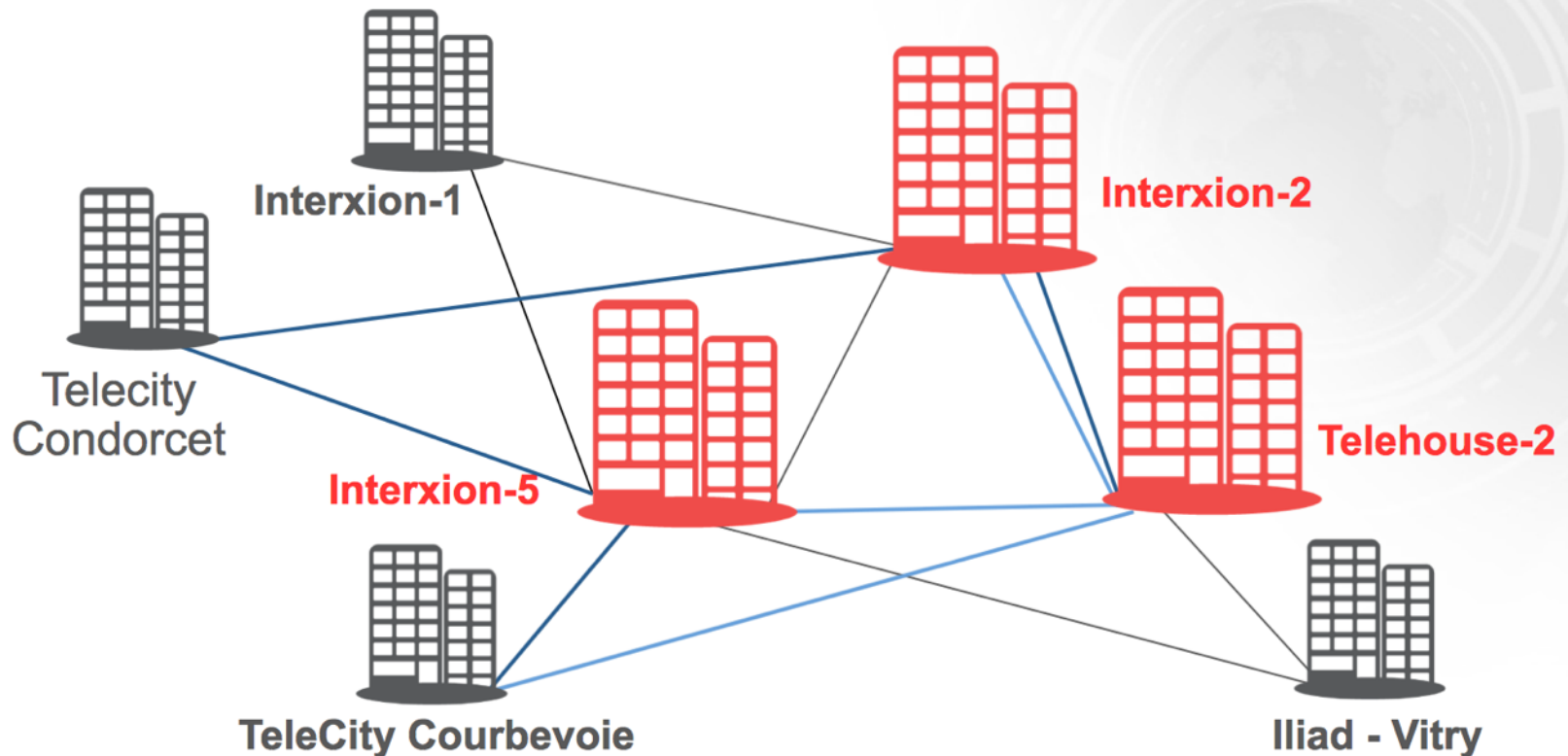
- Acheminement de trafic uniquement sur son réseau
- Généralement gratuit
- Chaque peer n'annonce que les routes de son réseau
- Se réalise majoritairement sur des points d'échanges Internet (IXP)



<http://www.border6.com/>

Infrastructure

FranceIX



FranceIX PoP - Edge



FranceIX PoP - Coeur



Protocole de Routage

BGP

Border Gateway Protocol **BGP**

Exterior gateway protocol **EGP**

- Protocole de routage utilisé pour échanger des informations de routage entre différents réseaux
- Initialement décrit dans la RFC1105 de Juin 89
- TCP port 179
- Le système autonome est la pierre angulaire de BGP
- Un AS est utilisé pour identifier de façon unique les réseaux ayant une politique de routage commune

Border Gateway Protocol **BGP**

Exterior gateway protocol **EGP**

- Largement utilisé pour le backbone Internet
- Sélection du meilleur chemin (next hop)
généralement sur l'AS-PATH le plus court
- Mises à jour incrémentales
- Path Vector Protocol (AS-PATH)
- Beaucoup d'options pour l'application des stratégies (filtrage)

BGP Path Vector Protocol

Liste les AS traversés jusqu'à la destination.

```
cisco#show ip bgp 185.9.20.0/24
```

```
BGP routing table entry for 185.9.20.0/24, version 2069615  
Paths: (2 available, best #2, table Default-IP-Routing-  
Table)
```

```
Not advertised to any peer
```

```
8487 25091 199627
```

AS Path

```
46.20.247.42 from 46.20.247.42 (46.20.247.249)
```

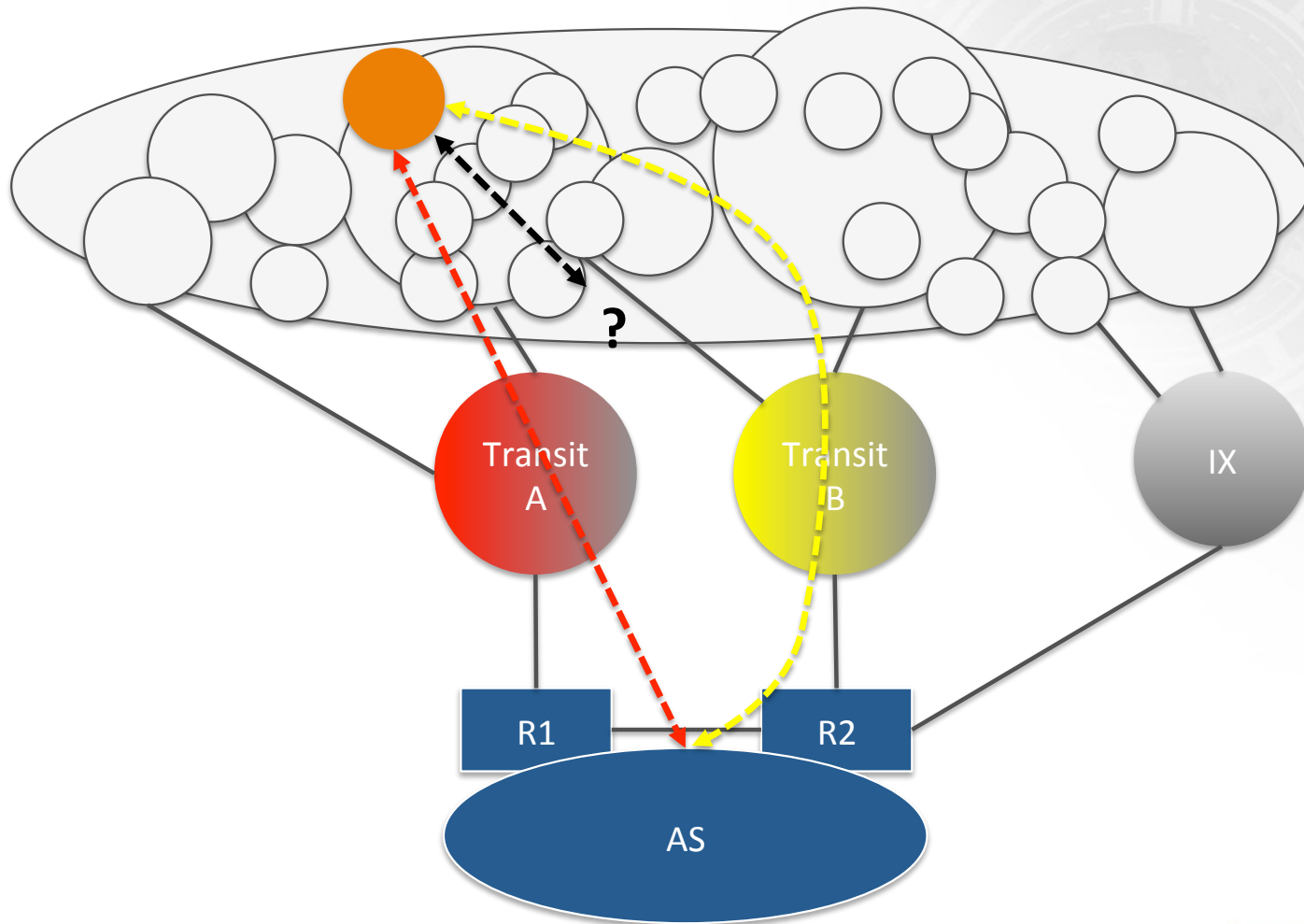
```
Origin IGP, metric 0, localpref 100, valid, external
```

```
43100 199627
```

```
81.18.177.37 from 81.18.177.37 (188.93.40.1)
```

```
Origin IGP, localpref 100, valid, external, best
```

Chemins BGP



<http://www.border6.com/>

BGP Qualité?

	BGP	Transit A	Transit B	
Location	Average RTT	Average RTT	Average RTT	Difference
Paris, France:	6.1	101.7	6.5	1464.6%
Singapore, Singapore:	334.7	335.1	273.3	22.6%
Zurich, Switzerland:	27.5	194.5	28.3	587.3%
Groningen, Netherlands:	82.7	15.8	86.7	448.7%
Beijing, China:	441.2	355	441.3	24.3%

<http://www.border6.com/>

Délai

Transit

- Vert = meilleur chemin

BGP

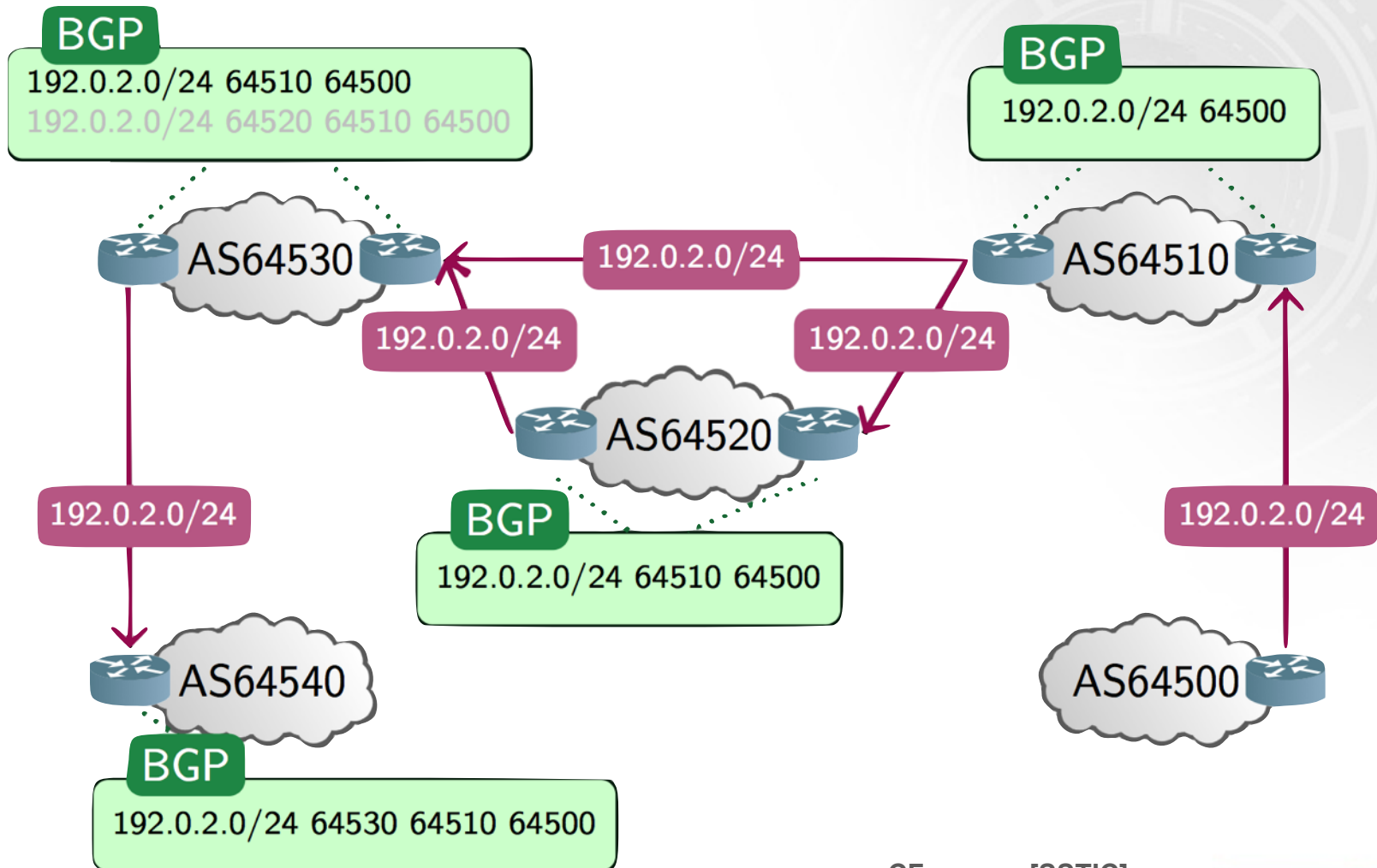
- Blanc = BGP a choisi le meilleur chemin
- Rouge = le chemin choisi est au moins 10% plus long que le chemin le plus court

Routage

les dangers

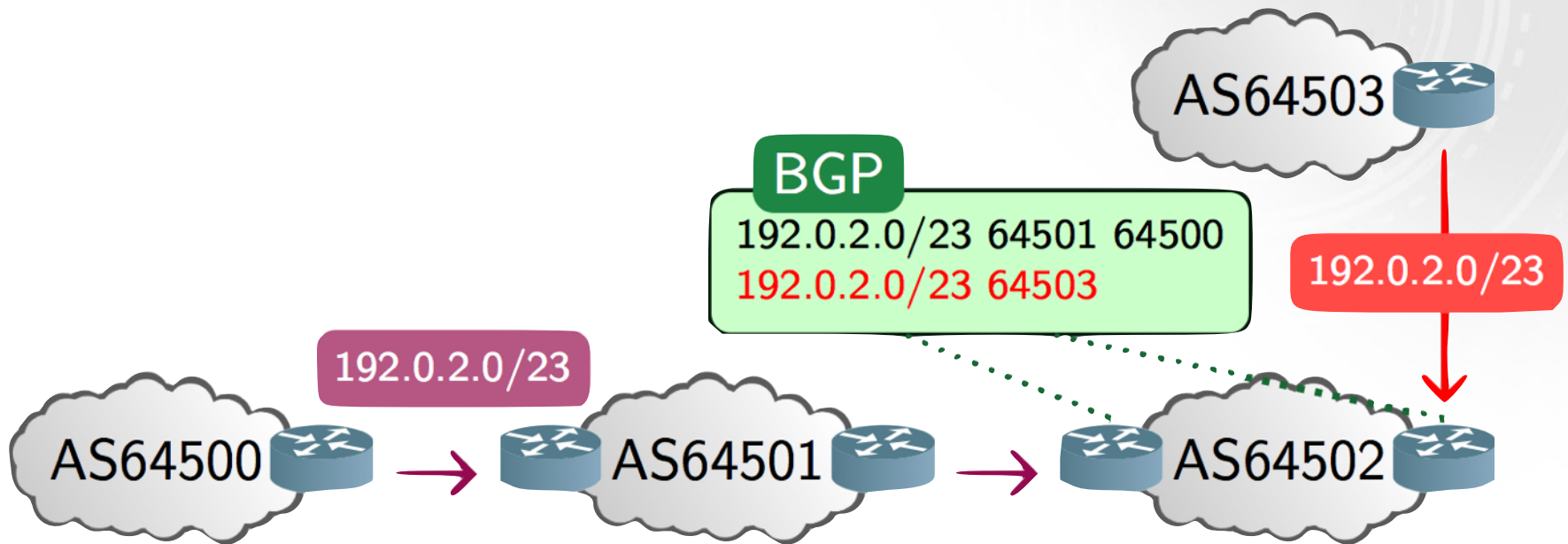


Annonce de préfixes



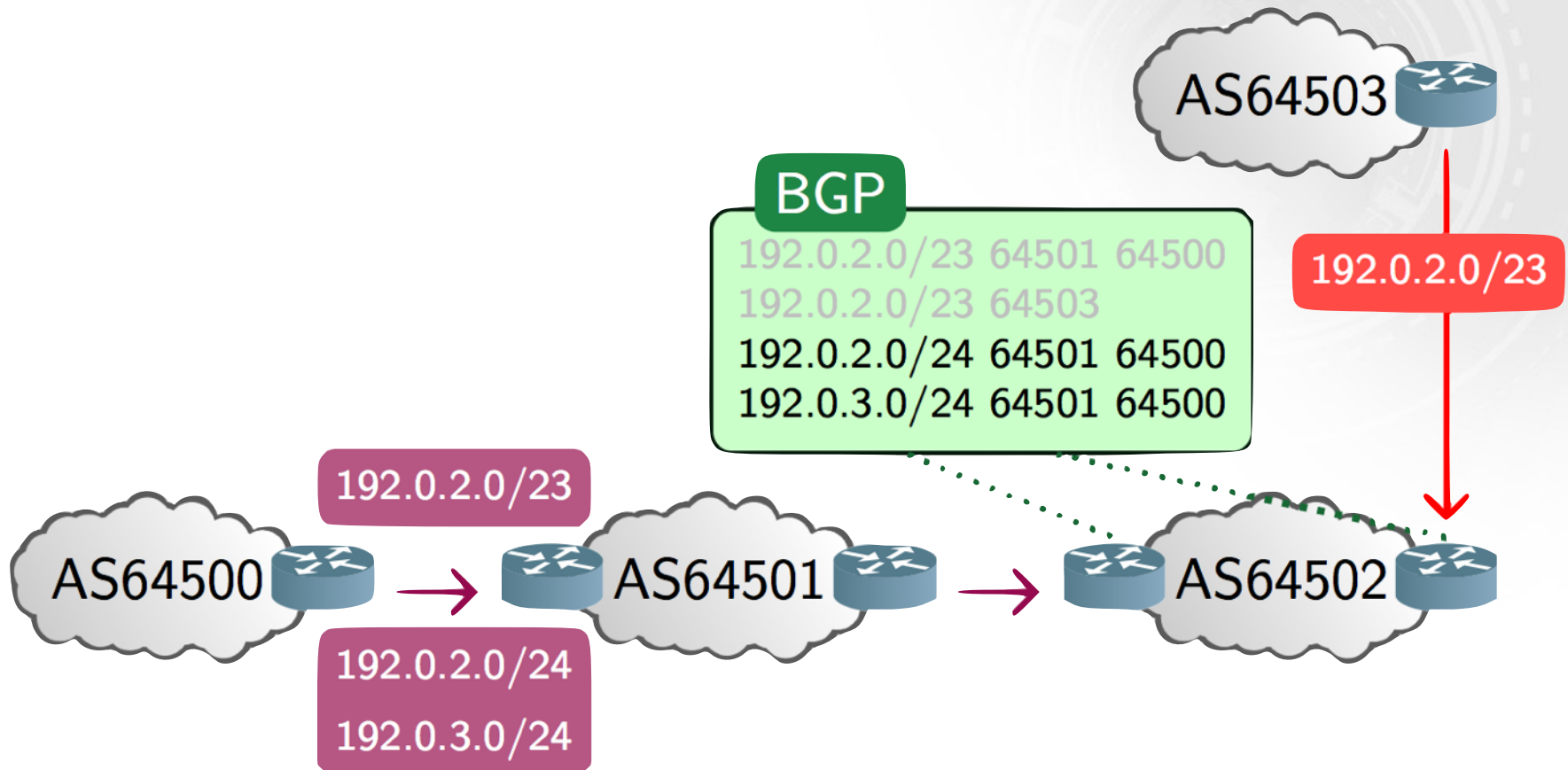
CF source [SSTIC]

Usurpation de préfixes



CF source [SSTIC]

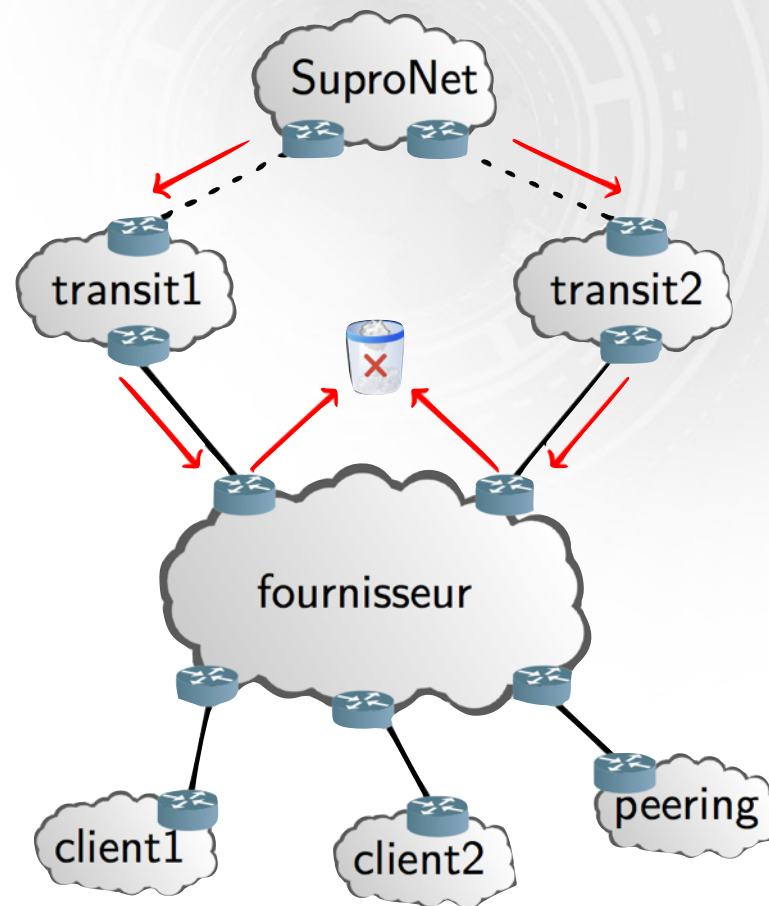
Annnonce plus spécifique



CF source [SSTIC]

Méthodes de Sécurisation

- Annoncer des préfixes les plus spécifiques autorisés
- Etre au plus proche de ses clients
- Mettre a jours ses informations (IRR / RPKI)
- Filtrer les annonces



CF source [SSTIC]

Sources

- **[SSTIC] Influence des bonnes pratiques sur les incidents BGP**

https://www.sstic.org/media/SSTIC2012/SSTIC-actes/influence_des_bonnes_pratiques_sur_les_incidents_b/SSTIC2012-Slides-influence_des_bonnes_pratiques_sur_les_incidents_bgp-contat_valadon_nataf.pdf

- **Workshop BGP : Routage, IPv4, IPv6 et BGP**

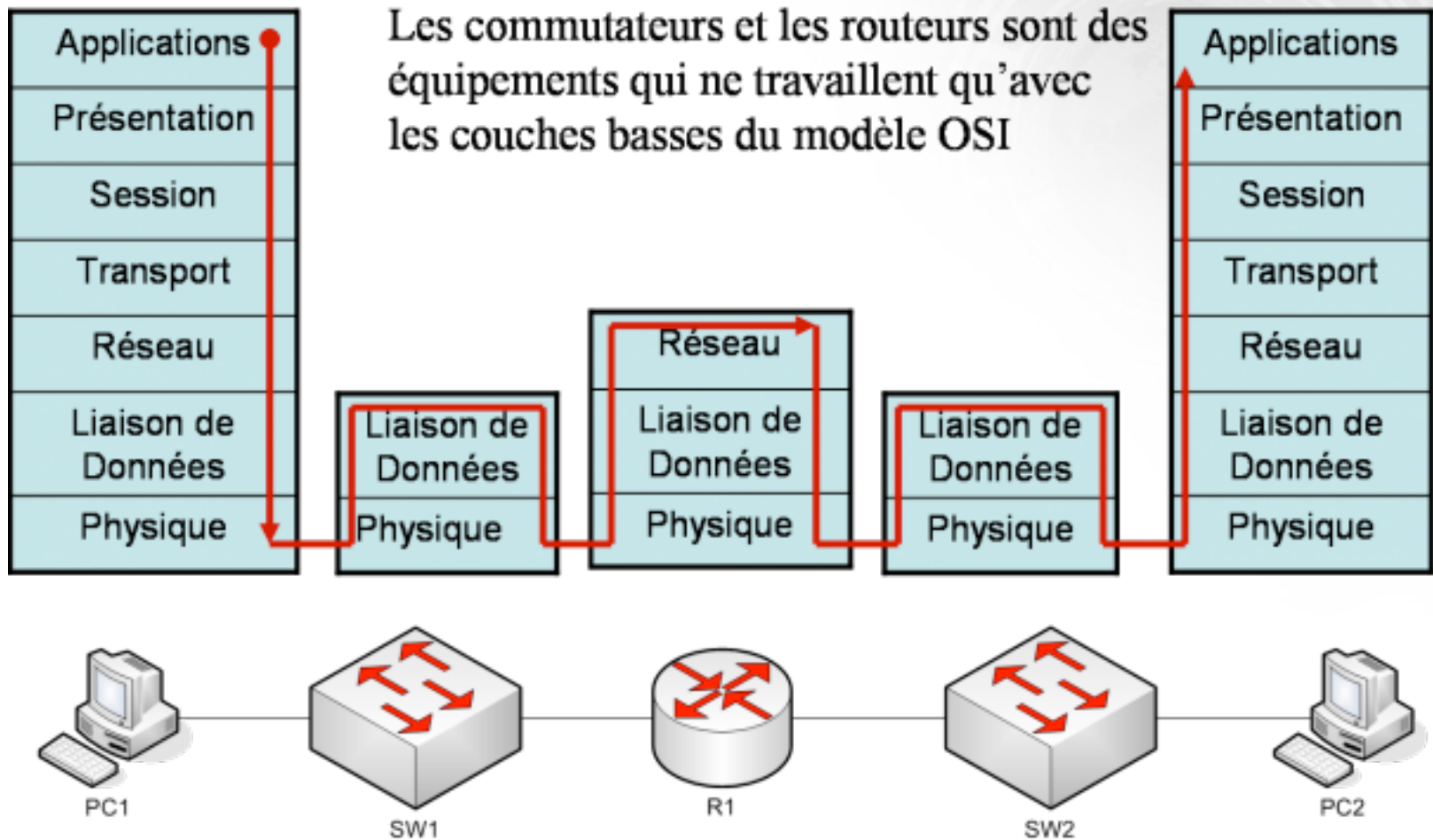
<http://www.afenioux.fr/doc/Workshop-BGP.pdf>

- **Photos des NRA**

<https://lafibre.info/reseau-orange/>



Couches ISO



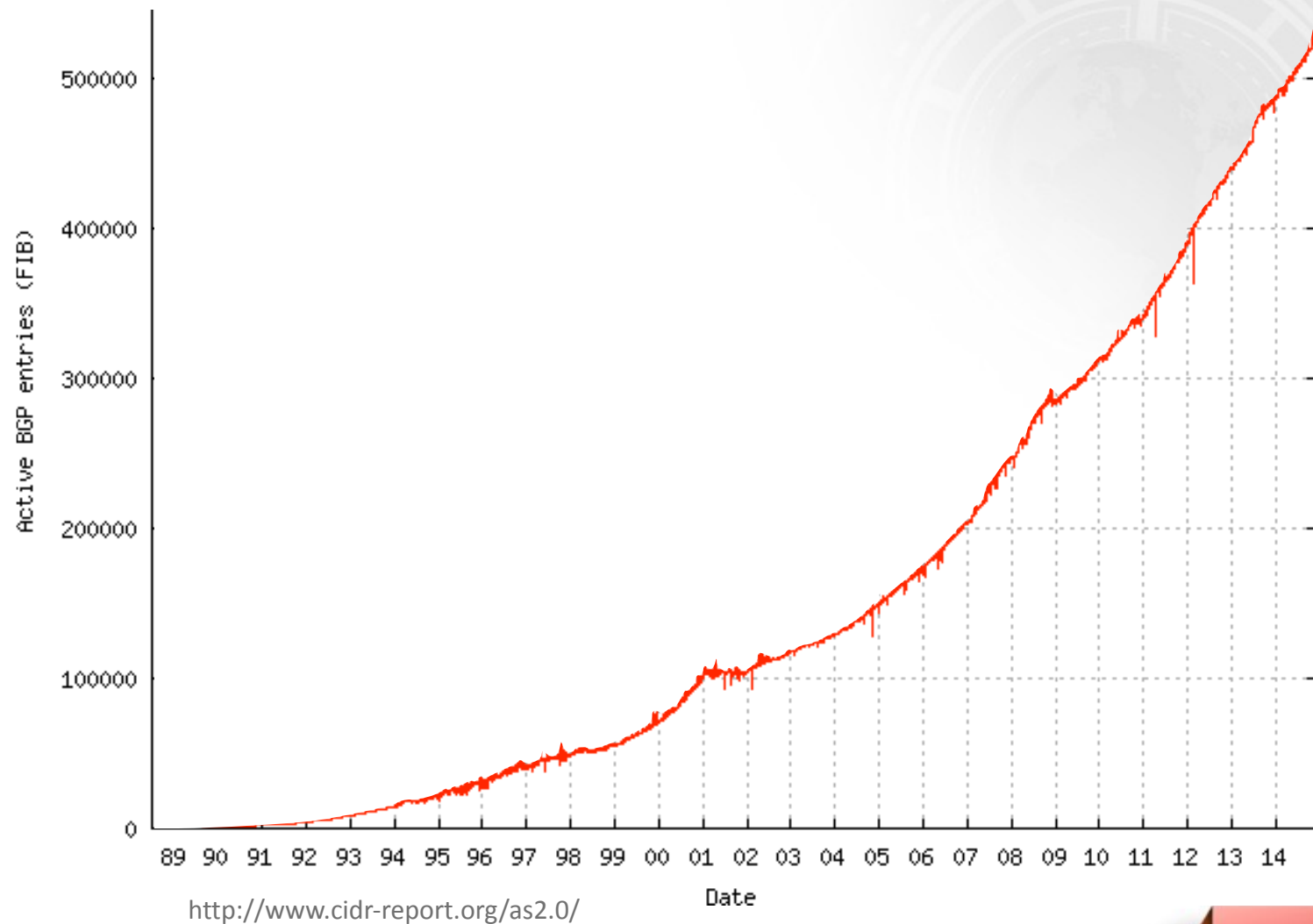
<http://reussirsonccna.fr/modele-osi/>

TCP vs UDP

TCP	UDP
Reliable	Unreliable
Connection-oriented	Connectionless
Segment retransmission and flow control through windowing	No windowing or retransmission
Segment sequencing	No sequencing
Acknowledge segments	No acknowledgement

<http://it20.info/2011/04/tcp-clouds-udp-clouds-design-for-fail-and-aws/>

Nbr routes Ipv4



BGP Best Path Selection Algorithm

- Weight le plus grand
- Local Pref la plus grande
- AS Path le plus court
- Origine (IGP, EGP, INCOMPLETE)
- MED (metric) la plus petite
- Route apprise en eBGP puis iBGP
- Chemin le plus ancien

```
inetnum:          37.49.232.0 - 37.49.239.255
netname:          FR-IX-20120126
descr:           France IX Services SASU
remarks:         FranceIX backbone
country:         FR
org:             ORG-FISS1-RIPE
admin-c:         FS1578-RIPE
tech-c:          FXAD
status:          ALLOCATED PA
mnt-by:          RIPE-NCC-HM-MNT
mnt-lower:       MNT-FRANCEIX
mnt-routes:      MNT-FRANCEIX
source:          RIPE # Filtered
```

```
route:          37.49.232.0/21
descr:          FranceIX Services
origin:         AS57734
mnt-by:         MNT-FRANCEIX
source:         RIPE # Filtered

aut-num:        AS57734
as-name:        FRANCEIX
descr:          France IX Services SASU
org:            ORG-FISS1-RIPE
mnt-by:         MNT-FRANCEIX
mnt-routes:     MNT-FRANCEIX
source:         RIPE # Filtered
```

```
router bgp 42
  network 10.42.0.0 mask 255.255.0.0
  neighbor 192.0.2.1 remote-as 1
  neighbor 192.0.2.1 prefix-list PFL-AS42-OUT out
  neighbor 192.0.2.1 prefix-list PFL-TRANSIT-IN in
  neighbor 192.0.2.1 soft-reconfiguration inbound

ip route 10.42.0.0 255.255.0.0 Null0

ip prefix-list PFL-AS42-OUT seq 5 permit 10.42.0.0/16
ip prefix-list PFL-TRANSIT-IN deny 10.42.0.0/16 le 32
ip prefix-list PFL-TRANSIT-IN deny 10.0.0.0/8 le 32
ip prefix-list PFL-TRANSIT-IN deny 172.16.0.0/12 le 32
ip prefix-list PFL-TRANSIT-IN deny 192.168.0.0/16 le 32
ip prefix-list PFL-TRANSIT-IN permit 0.0.0.0/0 le 24
```

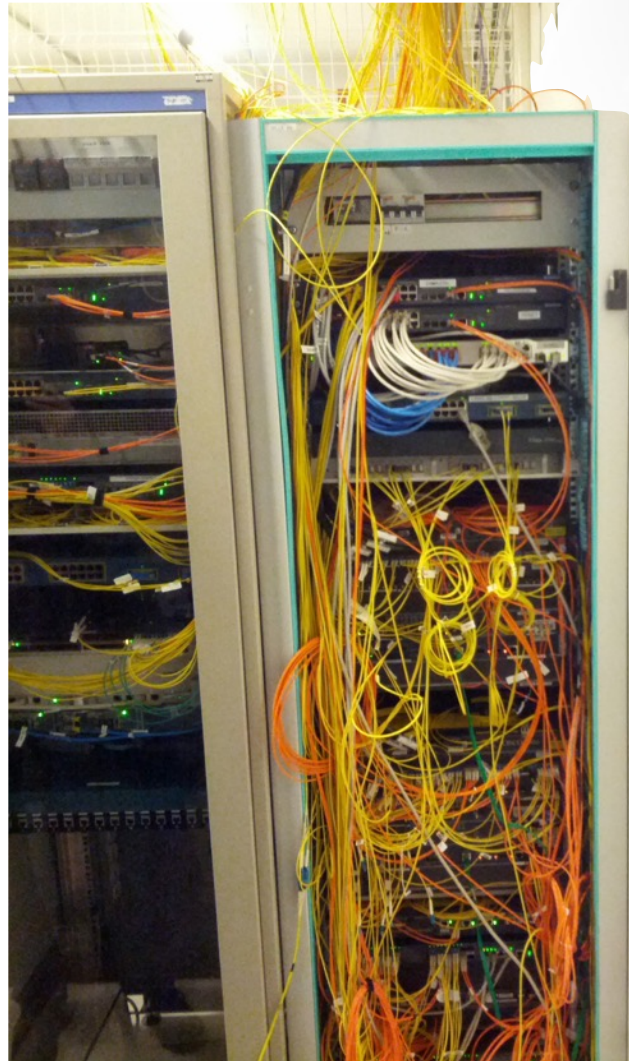
Internet

En France?



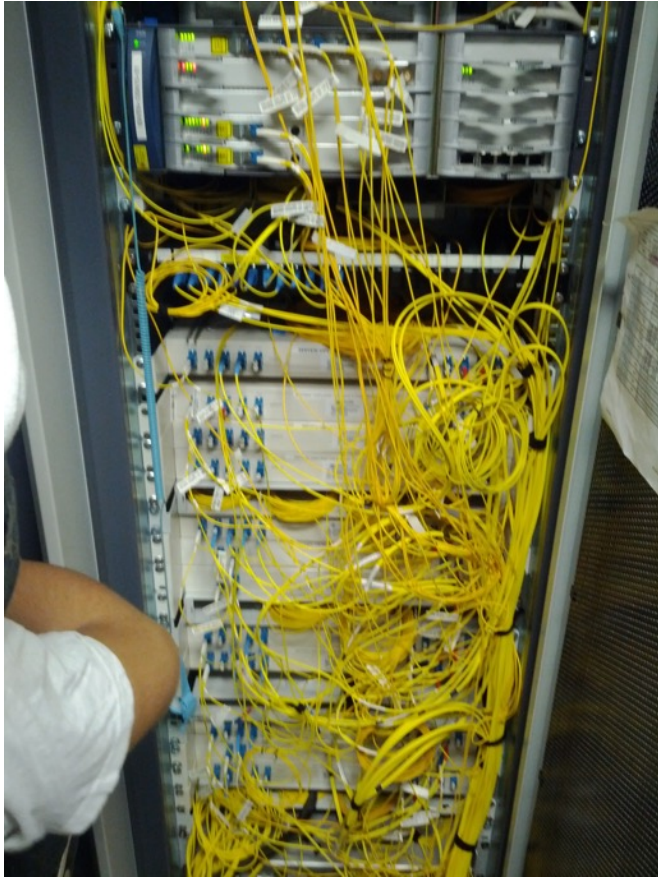
Internet?

A Strasbourg



Internet?

A Lyon



Internet?

A Paris



Merci !

Arnaud FENIOUX
@afenioux

