GRAND DUCHY OF LUXEMBOURG
Ministry of Foreign Affairs

Directorate for Development Cooperation

European Union Africa
Infrastructure Trust Fund

Conception de réseaux d'ISP

Conception de réseau évolutive

Remerciements et attribution

Le contenu et informations de cette présentation sont initialement développés et maintenus par l'(les) organisation(s)/individu(s) ci-dessous et mis à la disposition du project AXIS de l' Union Africaine

Cisco ISP/IXP Workshops

Philip Smith: - pfsinoz@gmail.com

www.apnic.net

Conception de réseaux d'ISP

- Topologie et conception de PoP
- Conception du backbone
- Adressage
- Protocoles de routage
- La sécurité
- La gestion hors bande
- Considérations opérationnelles

Topologies Point de Présence

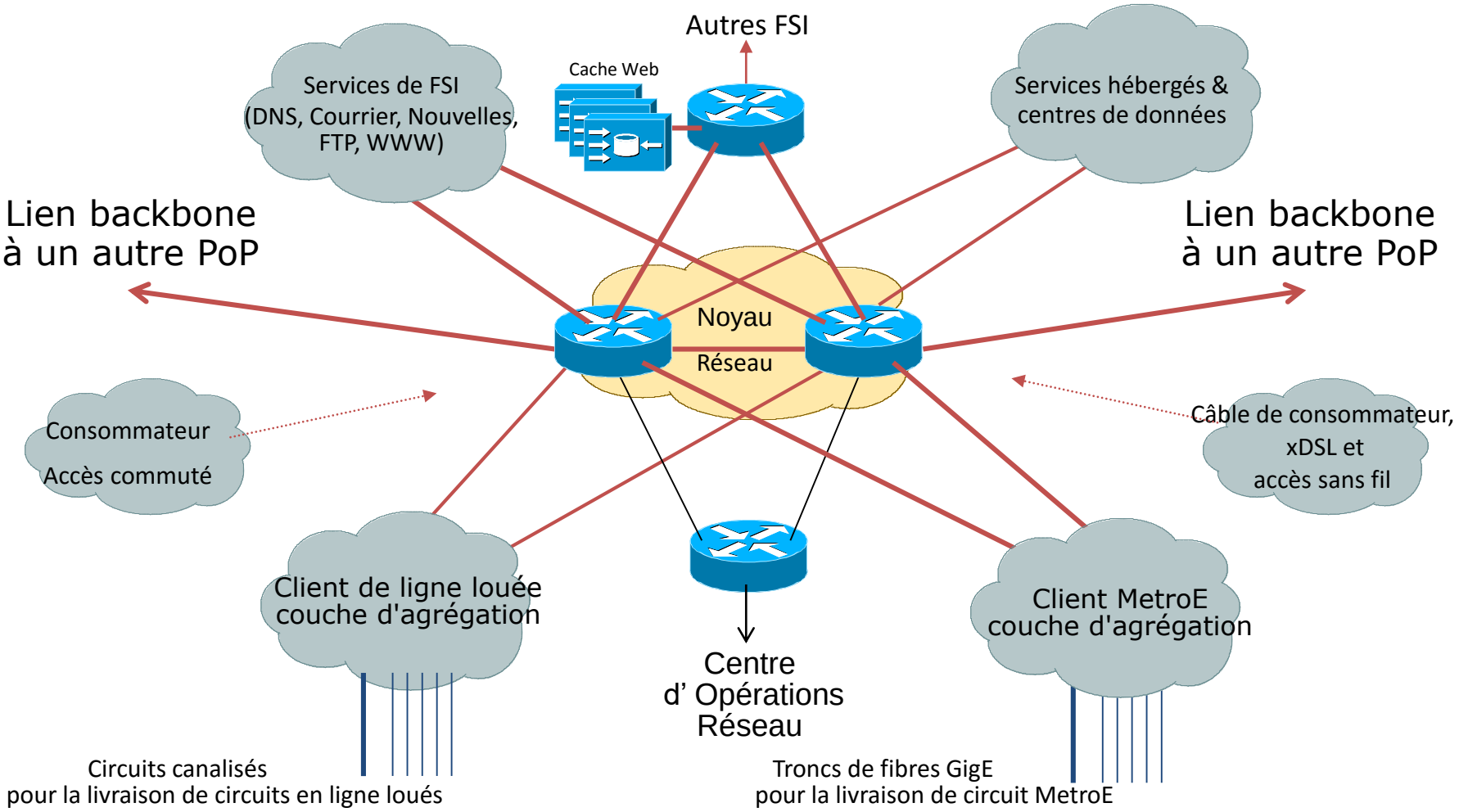
Topologies PoP

- Routeurs principaux – connexions tronc à haute vitesse
- Routeurs de distribution et routeurs d'accès – densité de ports élevée
- Routeurs frontières - connexions vers d'autres fournisseurs
- Routeurs de services - hébergement et serveurs
- Certaines fonctions pourraient être gérées par un seul routeur

Conception PoP

- Conception modulaire
- Services d'agrégation séparés en fonction de:
  - la vitesse de connexion
  - service aux clients
  - taux de contention
  - Considérations de sécurité

Conception modulaire de PoP



Conception de Protocole de Routage Modulaire ISPplus petits

- mise en œuvre d' IGP Modulaire
  - "Zone“ IGP par PoP
  - Routeurs Core dans zone backbone (zone 0/L2)
  - Agrégation, si possible dans le Core
- Mise en œuvre modulaire d'iBGP
  - Groupe de réflecteurs de route BGP par module
  - Les Routeurs Core sont les routes reflector
  - Les routeurs restants sont des clients et s'apparient seulement avec des réflecteurs de route

Conception de protocole de routage modulaire ISP plus grands

- mise en œuvre d' IGP Modulaire
  - "zone" IGP par module (mais éviter de surcharger les routeurs de Core)
  - Routeurs de Core dans zone backbone (zone 0/L2)
  - Agrégation, si possible dans le Core
- Mise en œuvre modulaire d'iBGP
  - Groupe de réflecteurs de route BGP par module
  - Réflecteurs de route dédiés adjacents à des routeurs Coez
  - Les clients s'apparient avec les réflecteurs de route seulement

Conception de Point de Présence

Modules PoP

- Connexions clients à faible vitesse
  - PSTN/ISDN dialup
  - Besoins en bande passante faible
  - Revenu faible, nombres importants
- Connexions clients par ligne louée
  - Plage de vitesse E1/T1
  - Livraison à travers des médias canalisés
  - Besoins en bande passante moyenne
  - Revenu moyen, nombres moyens

Modules PoP

- Connexions clients haut débit
  - xDSL, Câble et system sans fil
  - Besoins en bande passante élevée
  - Revenu faible, nombres importants
- Connexions clients MetroE et Highband
  - Tronc sur GigE ou 10 GigE de 10 Mbps et plus
  - Livraison OC3/12 canalisée de E3/T3 et plus
  - Besoins en bande passante élevée
  - Revenu élevé, nombres faibles

Modules PoP

- PoP Core
  - Deux routeurs dédiés
  - Interconnexion haute vitesse
  - Liens Backbones SEULEMENT
  - *Ne les touchez pas!*
- Réseau frontière (Border)
  - Routeur frontière dédié à d'autres ISP
  - Gateway du fournisseur d'accès Internet
  - Mise en cache Web transparent?
  - Deux au niveau du backbone est garantie minimale pour la redondance

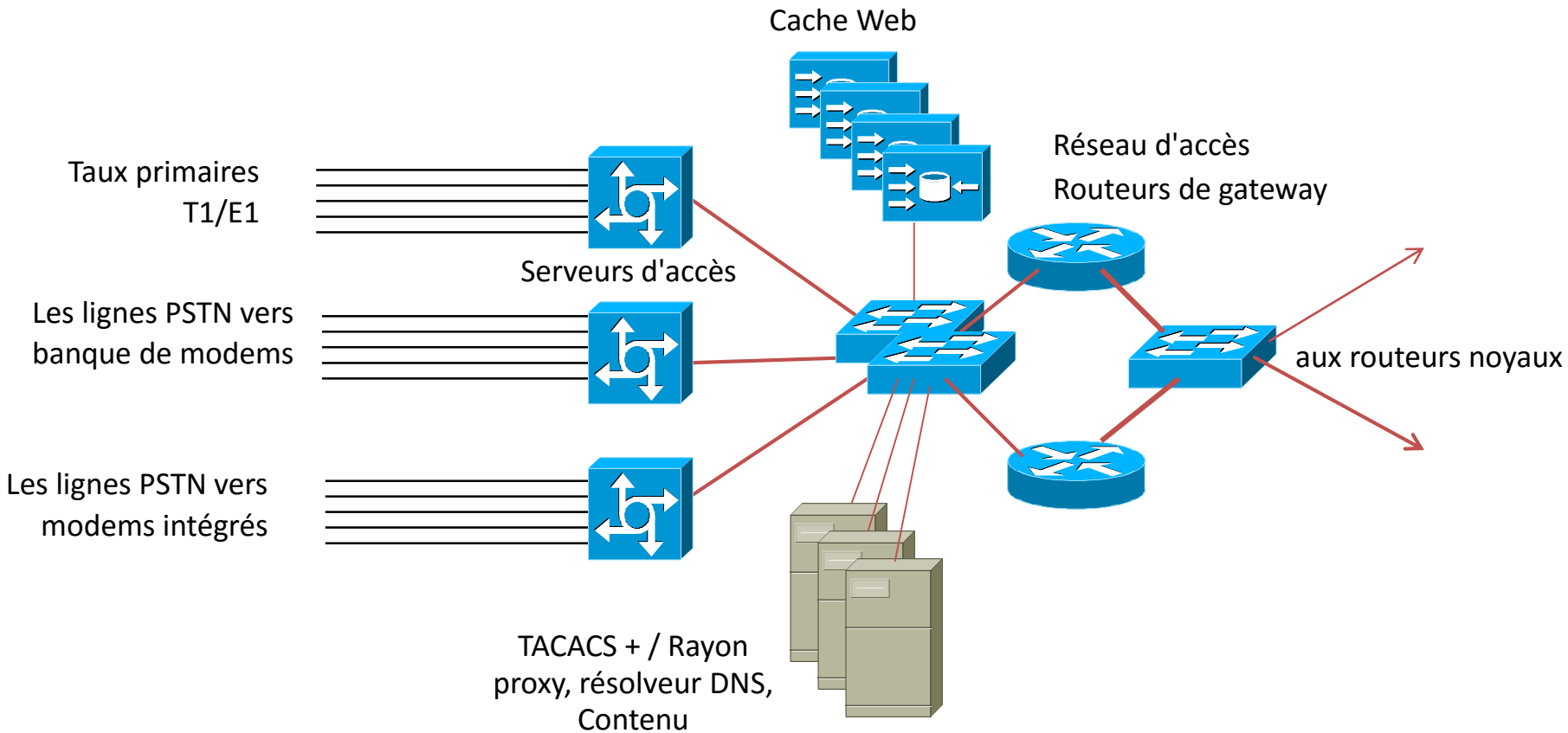
Modules PoP

- Services de Fournisseurs de Service Internet
  - DNS (cache, secondaire)
  - Nouvelles (toujours d'actualité?)
  - Courrier (POP3, relais, Anti-Virus/Anti-Spam)
  - www (serveur, proxy, cache)
- Services hébergés / centres de données
  - Web virtuel, www (serveur, proxy, cache)
  - Informations / Services de contenu
  - Commerce électronique

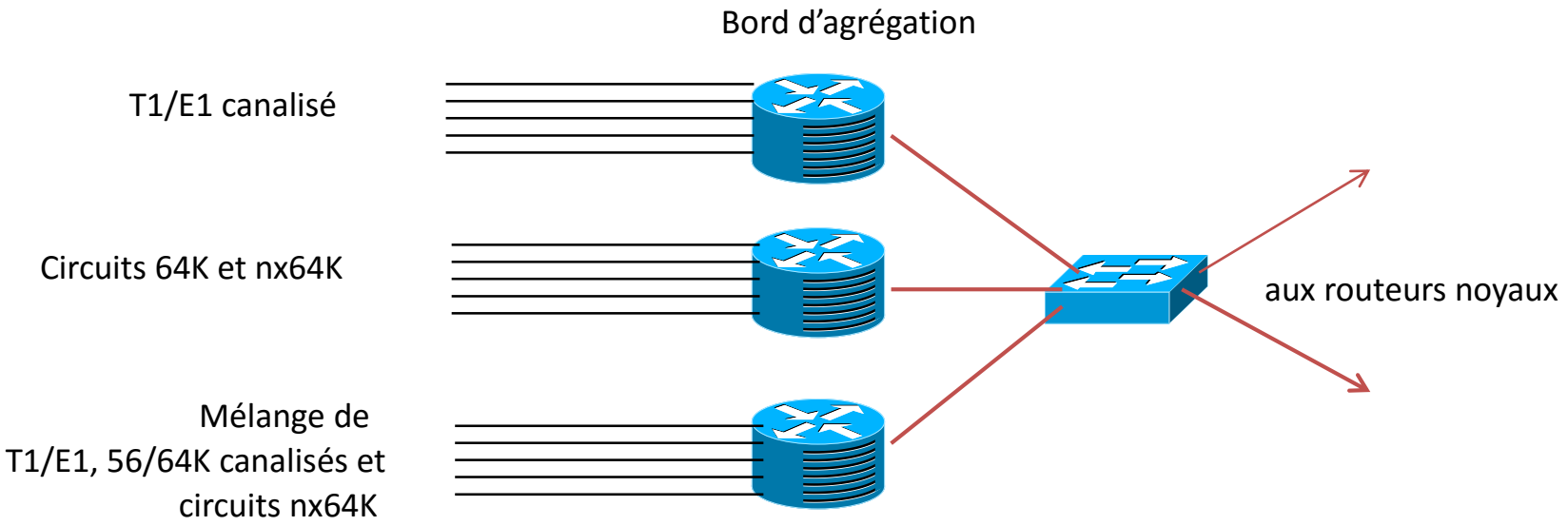
Modules PoP

- Centre d’opérations de réseau
  - Envisagez un emplacement principal et un de secours
  - Surveillance de réseau
  - Statistiques et collecte de journal
  - Accès direct mais sécurisé
- Réseau de gestion de Hors Bande
  - "Ceinture de sécurité" du réseau FSI

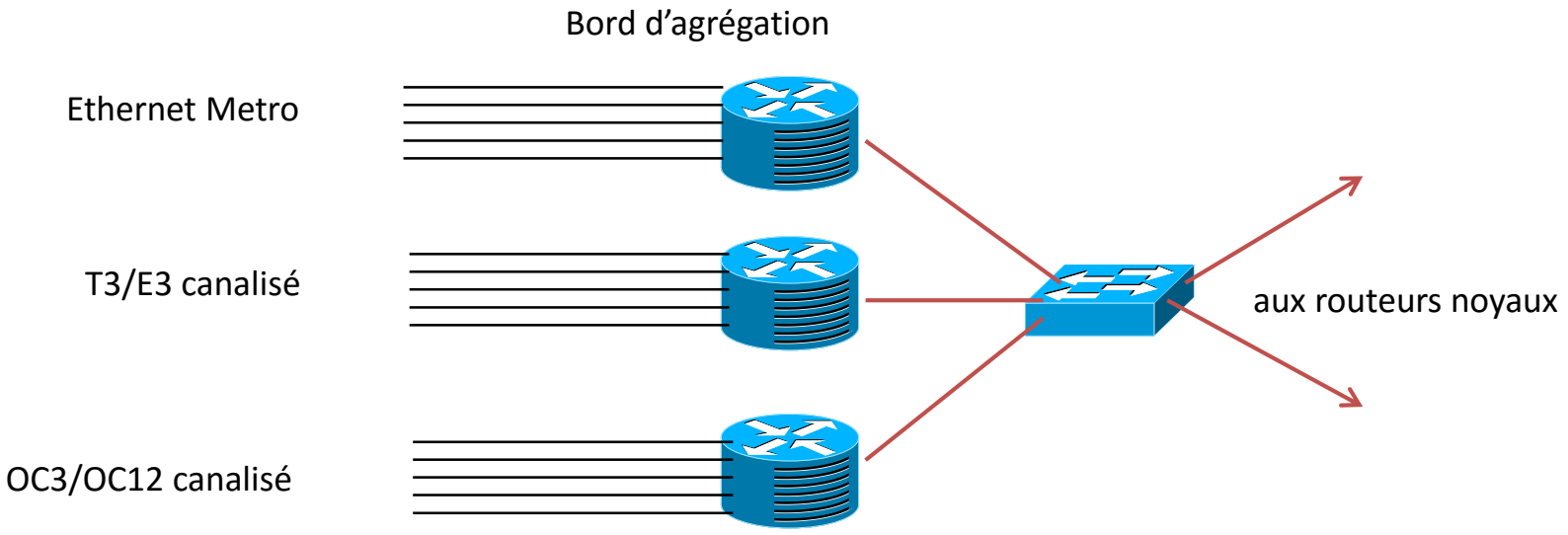
Module d'accès à faible vitesse



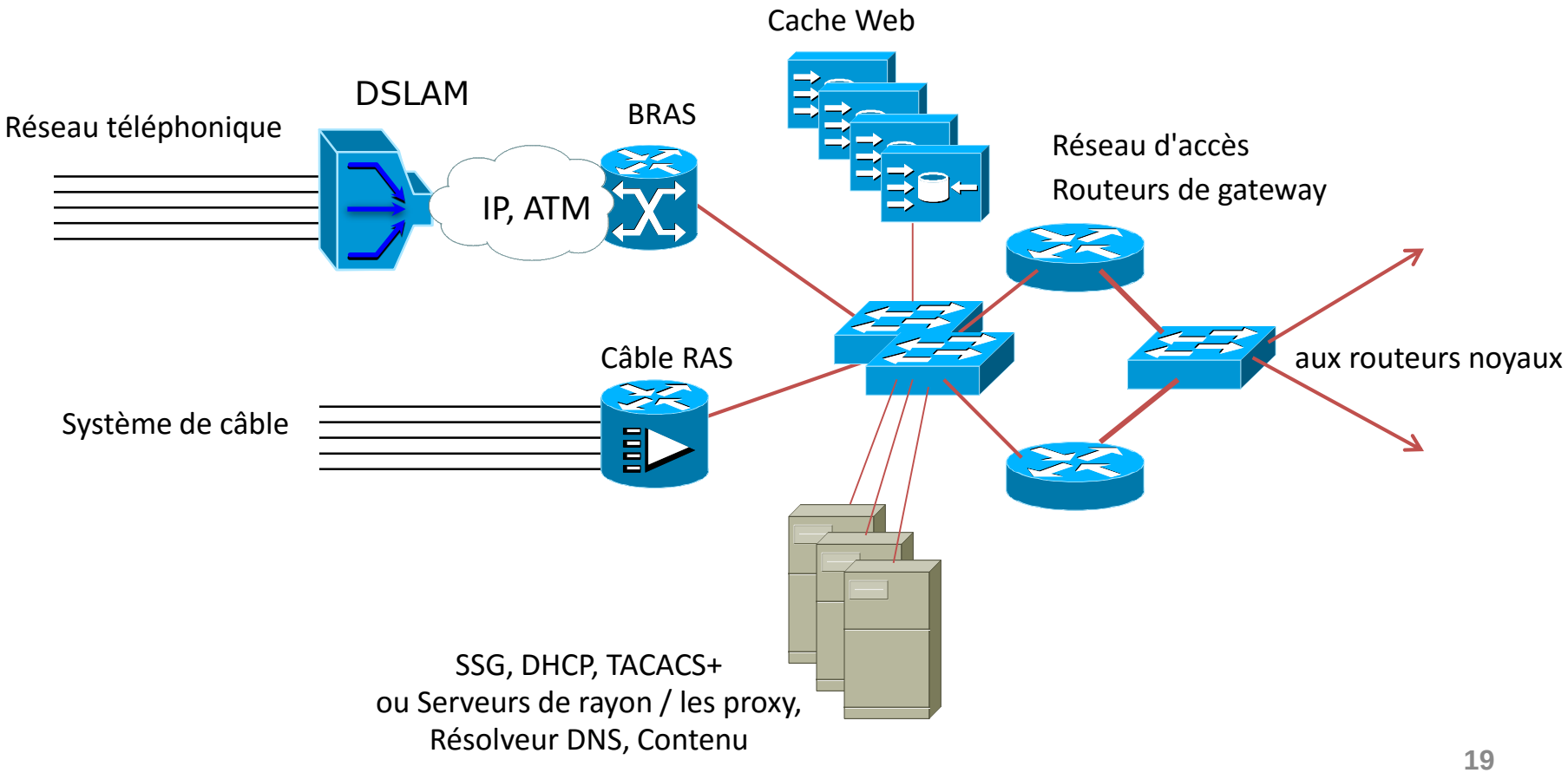
Module d’accès à vitesse moyenne



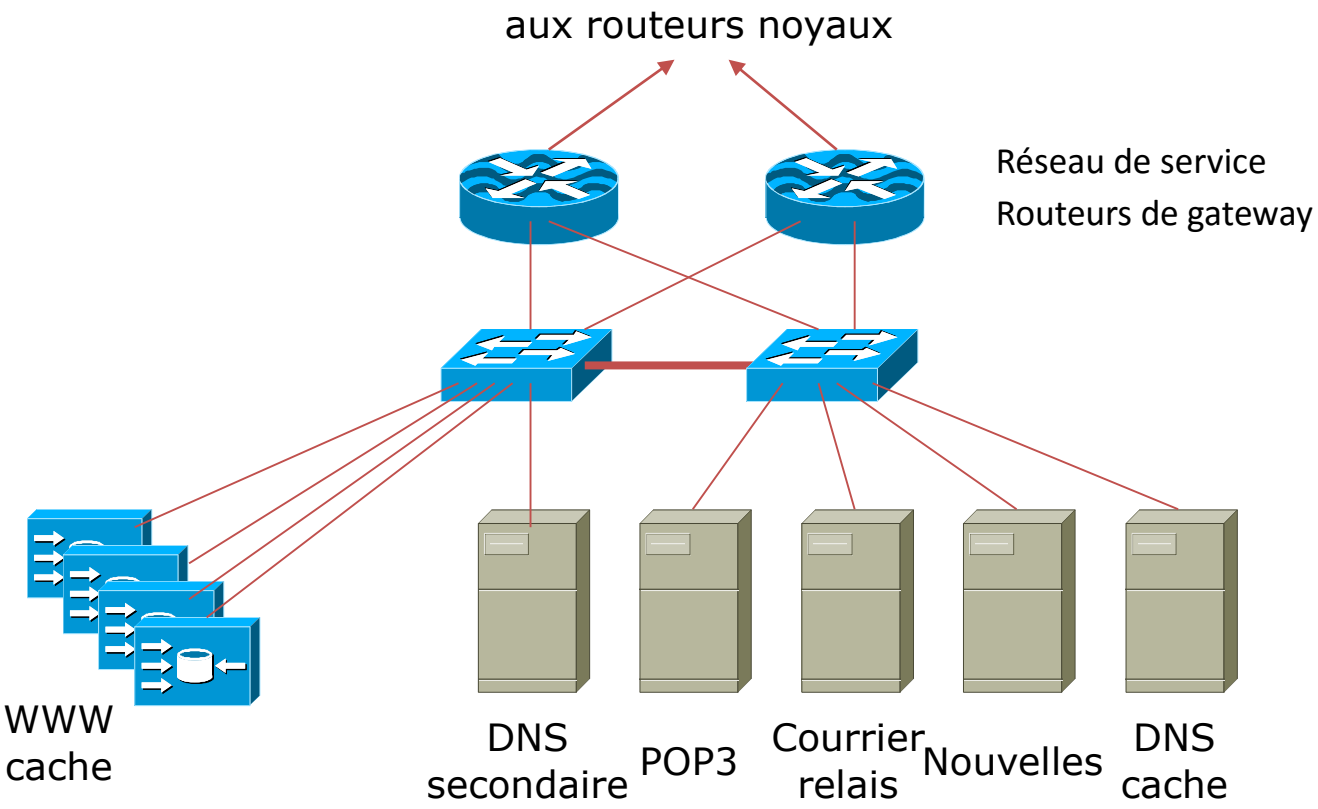
Module d'accès haute vitesse



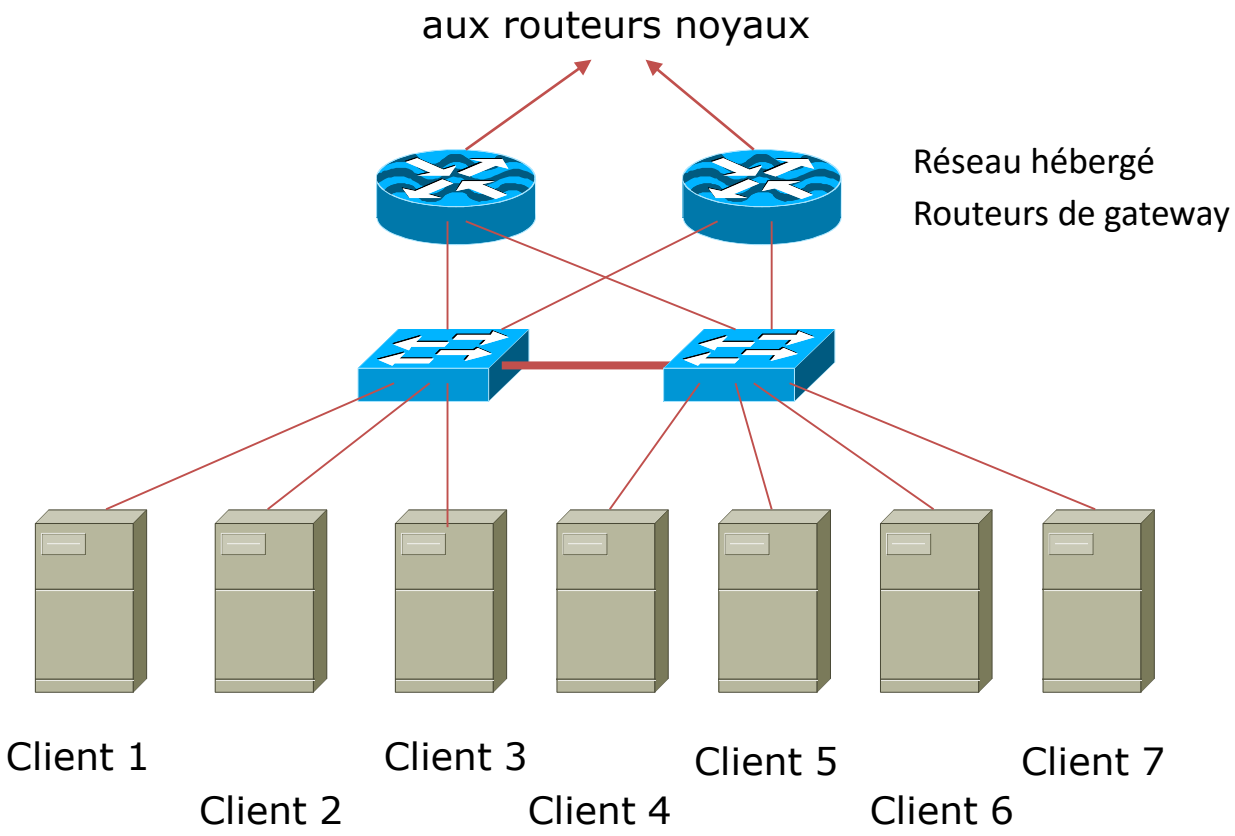
Module d'accès haut débit



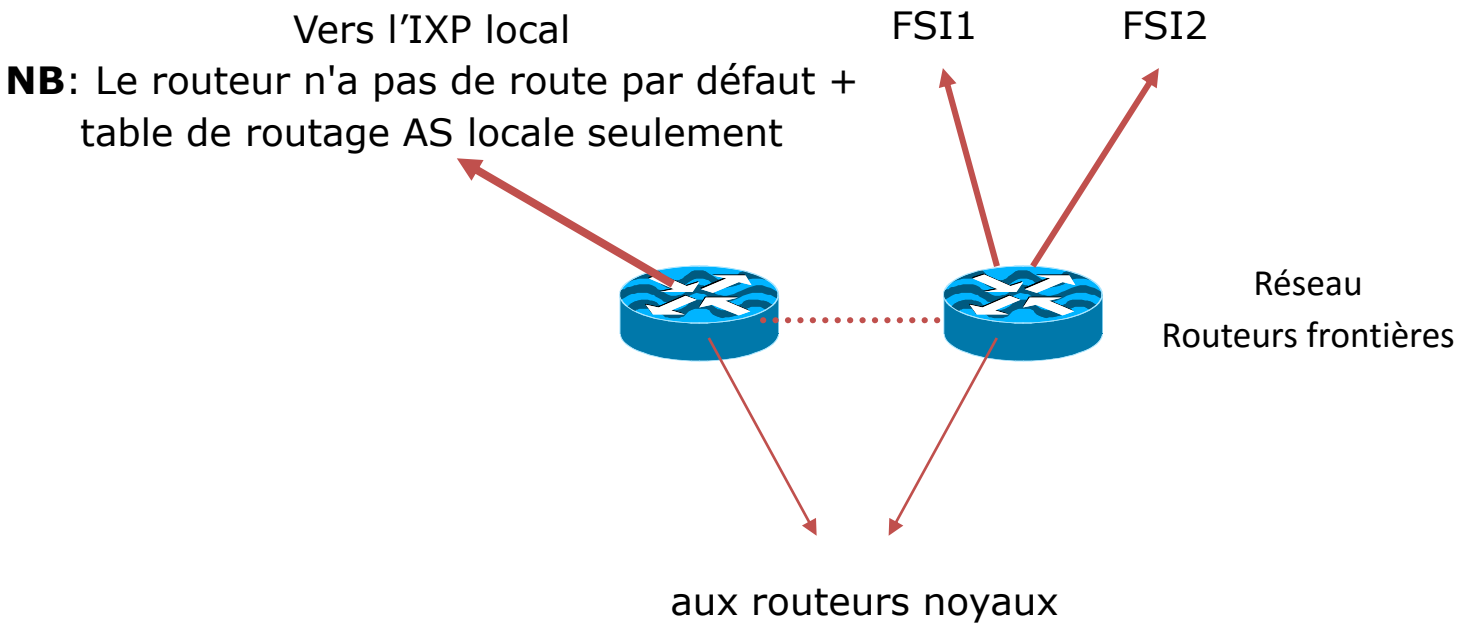
Module des services ISP



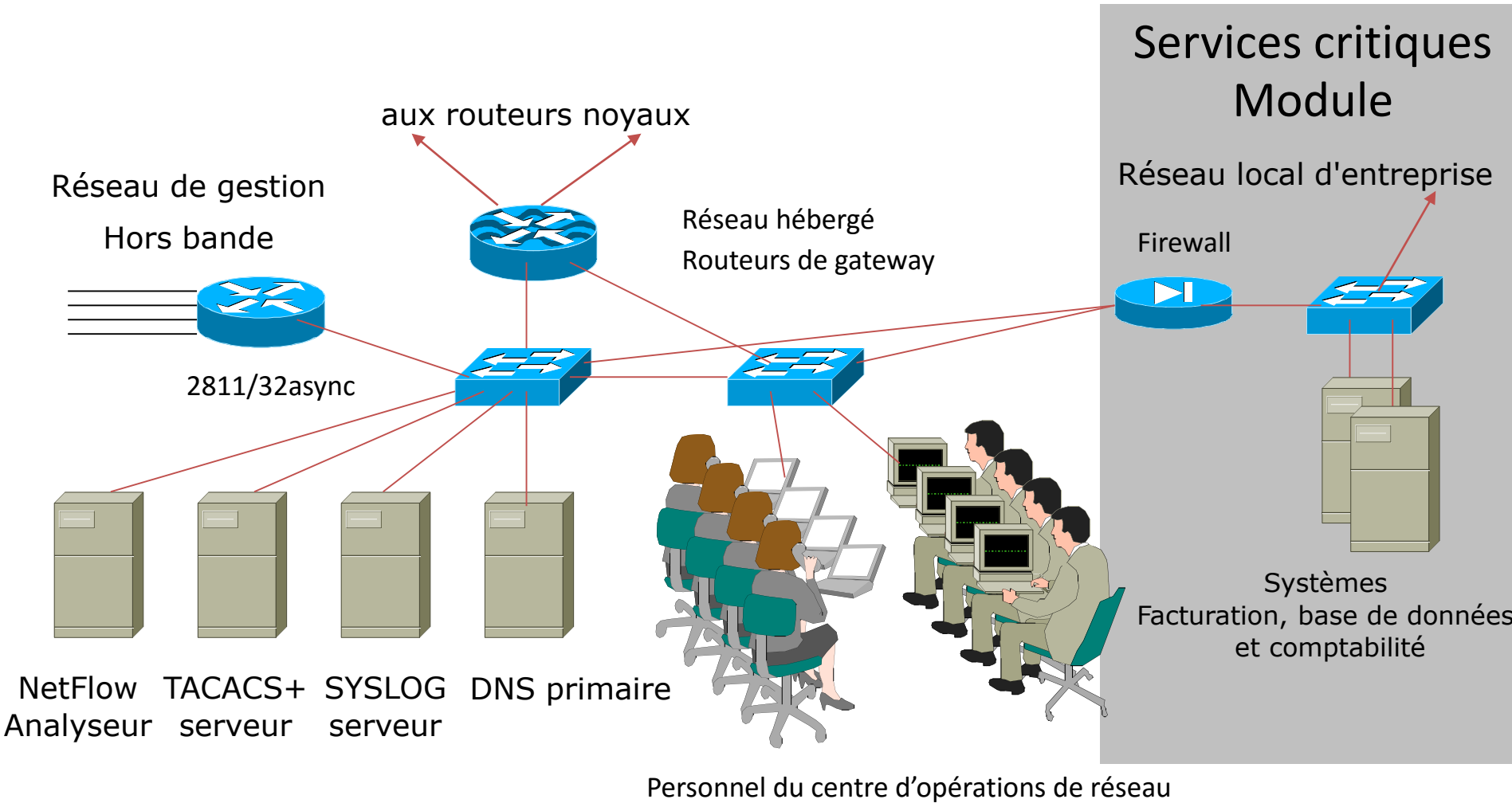
Module de services hébergés



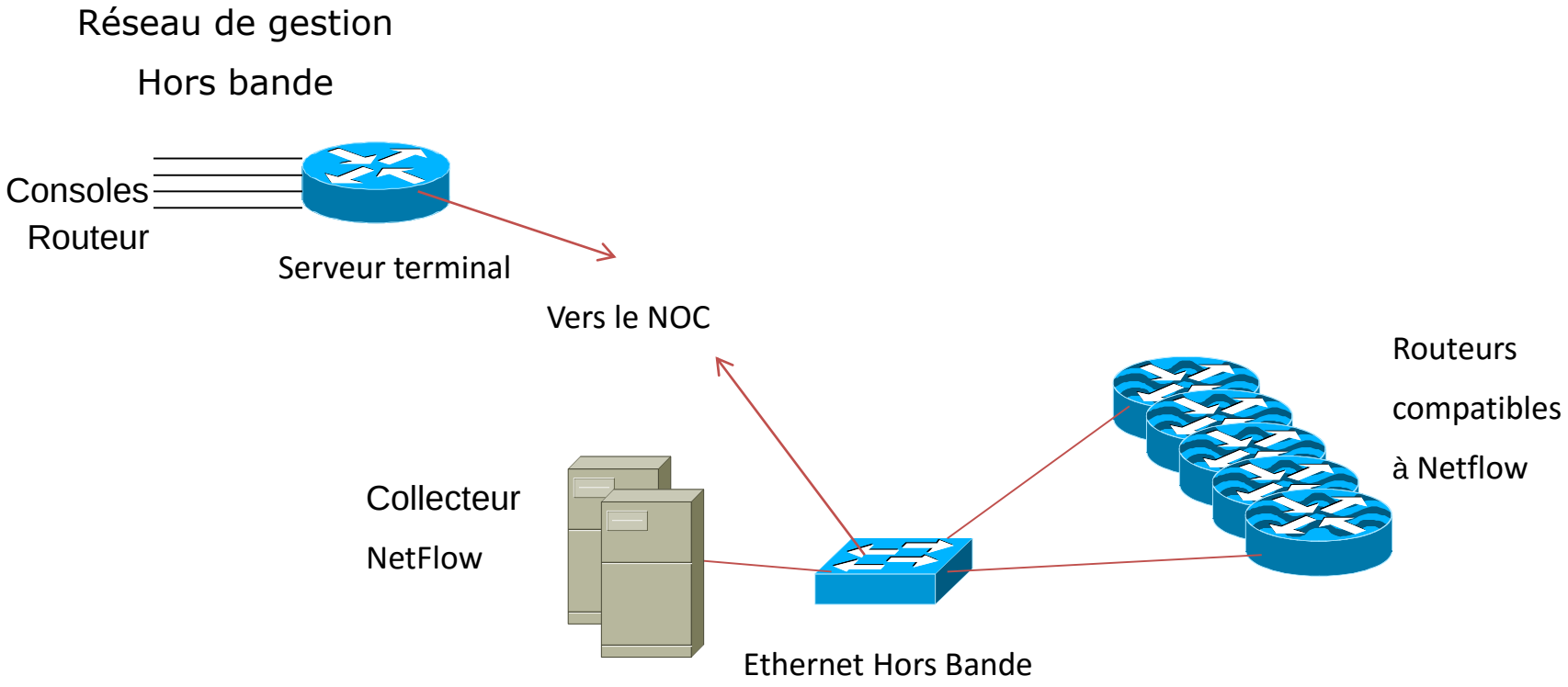
Module frontière



Module NOC


Services critiques
Module
Réseau local d'entreprise
aux routeurs noyaux
Réseau de gestion
Hors bande
Réseau hébergé
Routeurs de gateway
Firewall
2811/32async
Systèmes
Facturation, base de données
et comptabilité
NetFlow
Analyseur
TACACS+
serveur
SYSLOG
serveur
DNS primaire
Personnel du centre d'opérations de réseau

Réseau Hors Bande



Conception de réseau backbone

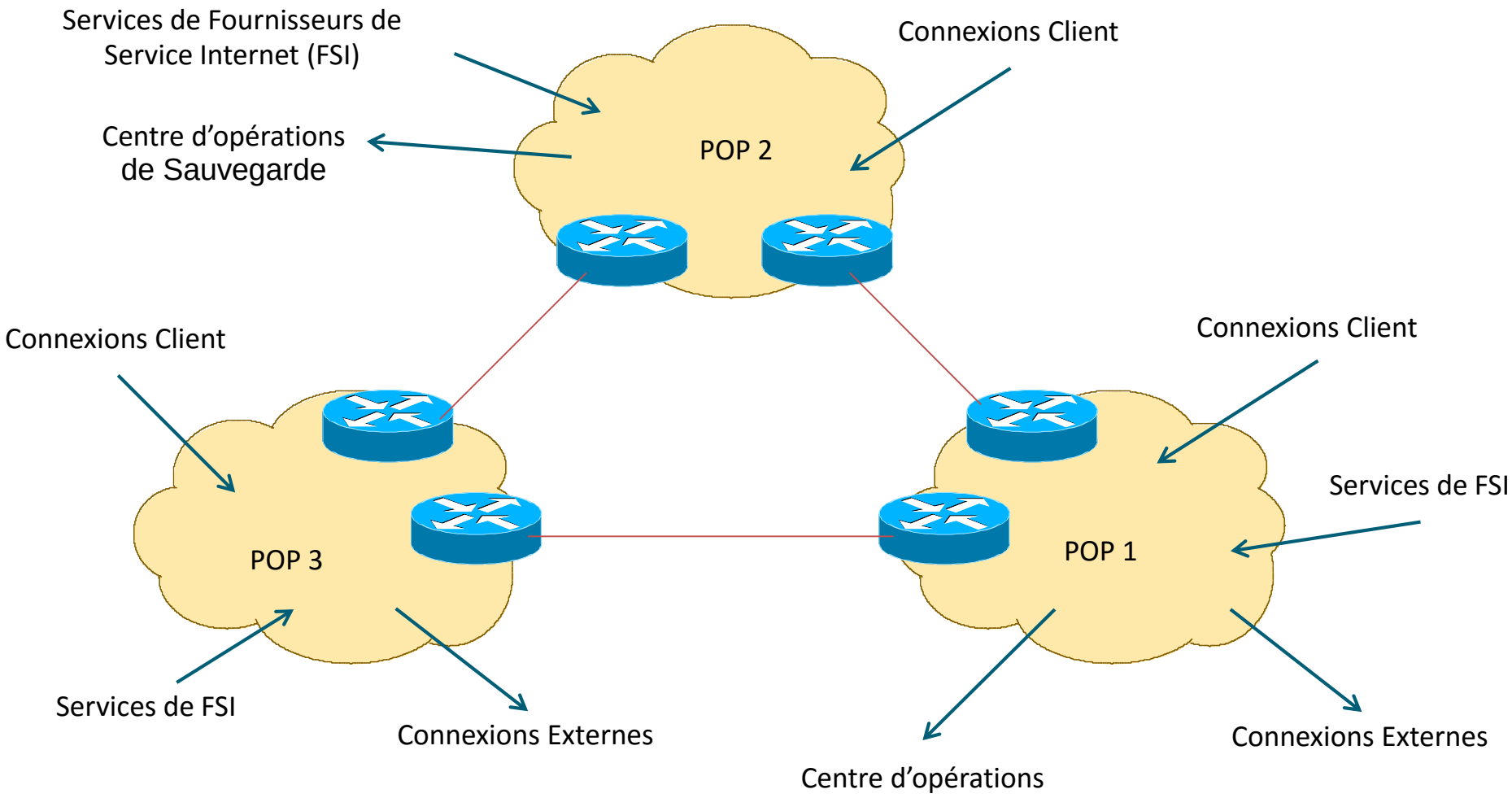
Conception du backbone

- Backbone dirigé
- Backbone commuté
  - Virtuellement obsolète
- Circuits point-à-point
  - nx64K, T1/E1, T3/E3, OC3, OC12, GigE, OC48, 10GigE, OC192, OC768
- Service de relais ATM/Frame de telco
  - Livraison T3, OC3, OC12, ...
  - Bande passante facilement évolutive (CIR)
  - Presque pas disponible maintenant

Conception de réseaux distribués

- Conception PoP “standardisée”
  - Evolutivité et simplicité opérationnelle
- Services essentiels des FSI répartis autour du backbone
- NOC et NOC de “sauvegarde”
- Liens backbone redondants

Conception de réseaux distribués



Liens backbone

- Relais ATM/Frame
  - Pratiquement disparu en raison de frais généraux, d'équipement supplémentaire, et du partage avec d'autres clients de telco
  - MPLS a remplacé ATM et FR comme le favori de telco
- Ligne louée / Circuit
  - Le plus populaire auprès des fournisseurs de backbone
  - IP sur optique et Metro Ethernet très courants dans de nombreuses régions du monde

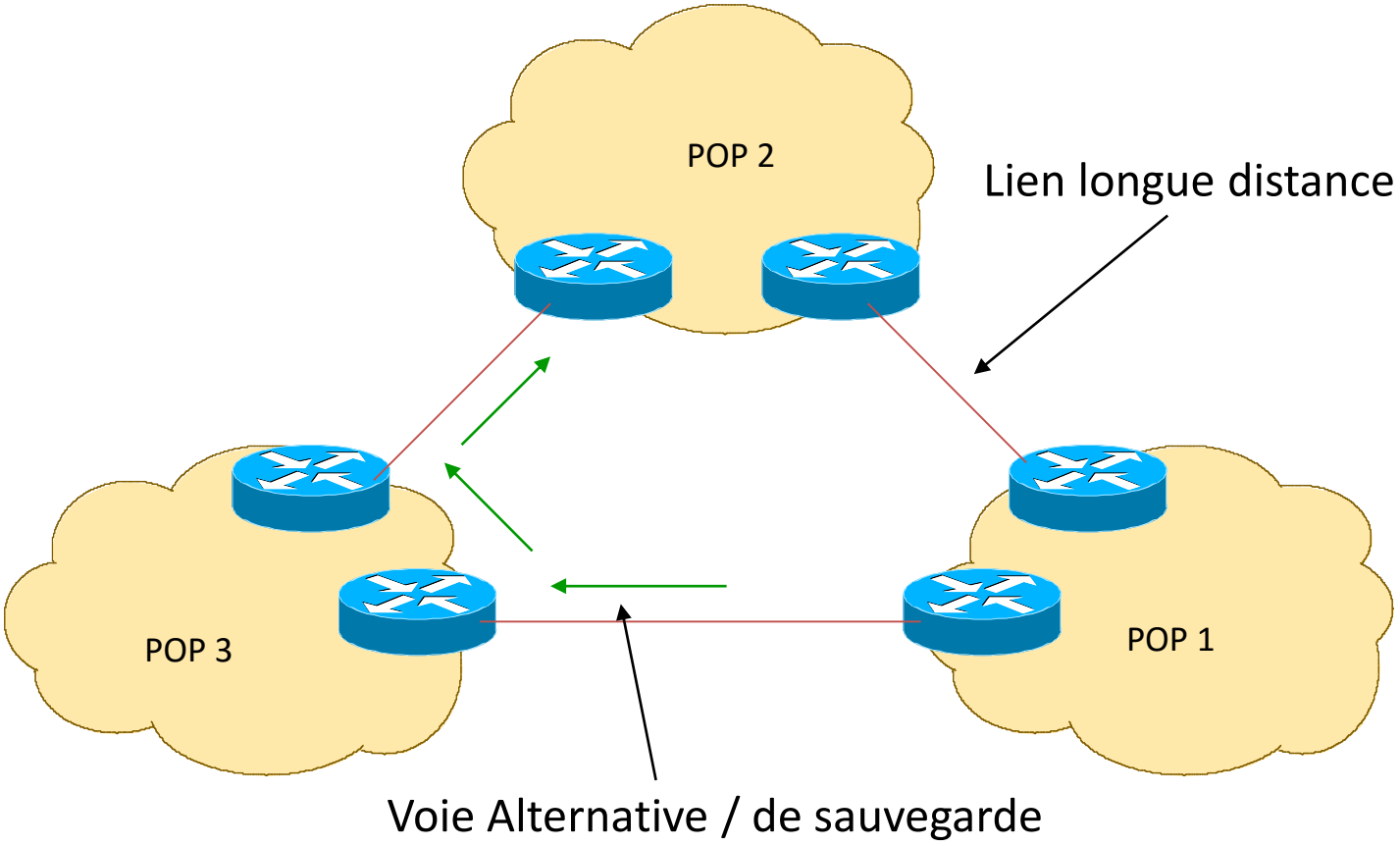
Liens de backbone longue distance

- Ceux-ci coûtent généralement plus
- Important de planifier pour l'avenir
  - Cela signifie au moins avec deux ans d'avance
  - Rester dans le budget, rester réaliste
  - Des mises à niveau "d'urgence" imprévues seront perturbatrices s’il n’y a pas redondance dans l'infrastructure du réseau

Liens de backbone longue distance

- Installer une capacité suffisante sur des solutions alternatives pour faire face aux situations d'échec
  - Suffisante peut dépendre de la stratégie d'entreprise
  - Suffisante peut descendre aussi bas que 20%
  - Suffisante est généralement au dessus de 50%, comme ceci offre une « continuité d'activités » pour les clients en cas de défaillance des liens
  - Certaines entreprises choisissent 0%
    - Très myope, ce qui signifie qu'ils n'ont pas la capacité de réserve du tout!!!

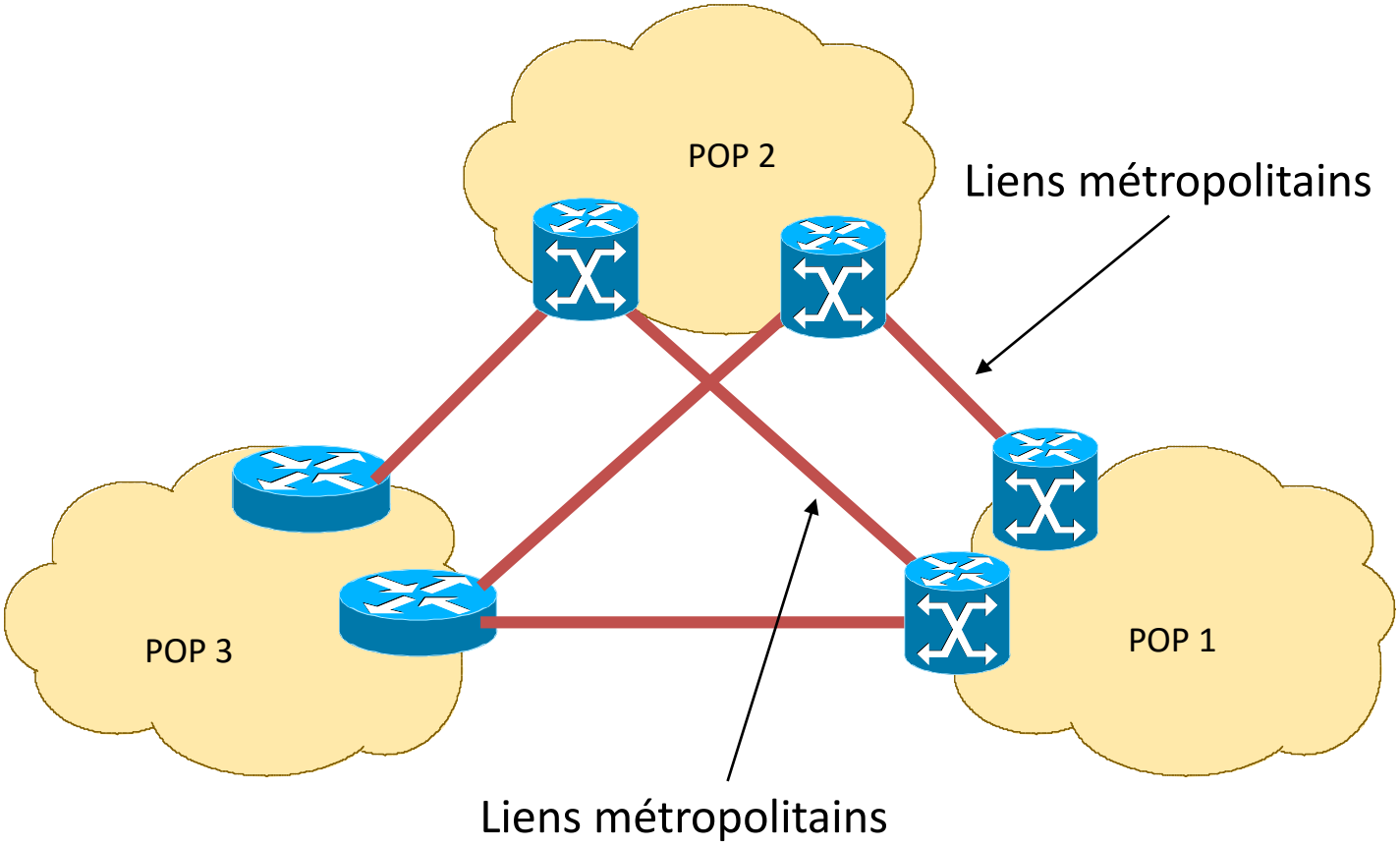
Liens longue distance



Liens backbone des régions Métropolitaines

- Ont tendance à être moins cher
  - Concentration de circuit
  - Choisissez parmi plusieurs fournisseurs
- Pensez grand
  - Plus de redondance
  - Moins d'incidence au cours des mises à niveau
  - Moins d'incidence lors des défaillances

Liens backbone des régions Métropolitaines



Liens traditionnels point à point

Connectivité en amont et échange de trafic

Transits

- Le fournisseur de transit est un autre système autonome qui est utilisé pour fournir au réseau local accès à d'autres réseaux
  - Peut être local ou régional
  - Mais plus généralement l'Internet dans son ensemble
- Les fournisseurs de transit doivent être choisis judicieusement:
  - Un seulement
    - Pas de redondance
  - Un trop grand nombre
    - plus difficile d'équilibrer la charge
    - pas d'économie d'échelle (coûte plus par Mbps)
    - difficile d'assurer la qualité des services
- **Recommandation: au moins deux, pas plus de trois**

Erreurs fréquentes

- Les FSI souscrivent avec trop de fournisseurs de transit
  - Beaucoup de petits circuits (coûtent plus par Mbps que les grands)
  - Les taux de transit par Mbps diminuent avec l'augmentation de la bande passante de transit achetée
  - Difficile à mettre en œuvre une ingénierie de trafic fiable qui n'a pas besoin d’être affinée au quotidien en fonction des activités des clients
- Pas de diversité
  - Des fournisseurs de transit choisis ont tous accédés au même satellite ou même câble sous-marin
  - Des fournisseurs de transit choisis ont un transit et un échange de trafic ultérieurs pauvres

Les Pairs (Peers)

- Un pair est un autre système autonome avec lequelle le réseau local a convenu d'échanger des routes et du trafic d'origine locale
- Pair privé
  - Liaison privée entre deux fournisseurs en vue d'interconnexion
- Pair public
  - Point d'échange Internet, où des fournisseurs se rencontrent et décident librement avec qui ils vont s'interconnecter
- **Recommandation: formez des pairs, autant que possible!**

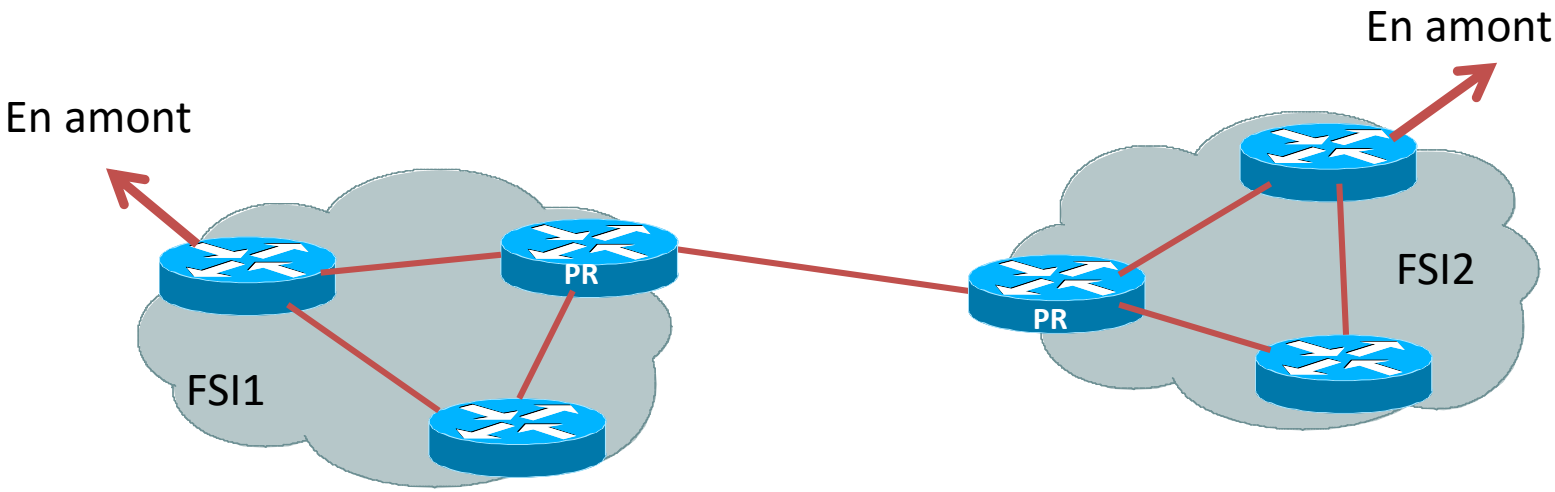
Erreurs fréquentes

- Confondre les activités d'"Echanges" d'un fournisseur de transit pour un point d'échange de trafic public sans frais
- Ne pas fournir assez d'effort pour former autant de pairs que possible
  - Physiquement proche d'un point d'échange Internet (IXP) mais ne pas y être
  - (Le transit est parfois moins cher que l'échange de trafic!)
- Ignorer / éviter des concurrents parce qu'ils sont de la concurrence
  - Même s'ils sont des partenaires d'échange de trafic potentiellement précieux pour donner aux clients une meilleure expérience

Interconnexion privée

- Deux fournisseurs de services acceptent d'interconnecter leurs réseaux
  - Ils échangent des préfixes qu'ils puisent dans le système de routage (généralement l'agrégat de leurs blocs adresses)
  - Ils partagent le coût de l'infrastructure qui a permis l'interconnexion
    - En général, chacun paie la moitié du coût de la liaison (que ce soit du circuit, satellite, micro-ondes, fibres, ...)
    - Connecté à leurs routeurs d'échange de trafic respectifs
  - Les Routeurs d'échanges de trafic ne portent que les préfixes domestiques

Interconnexion privée

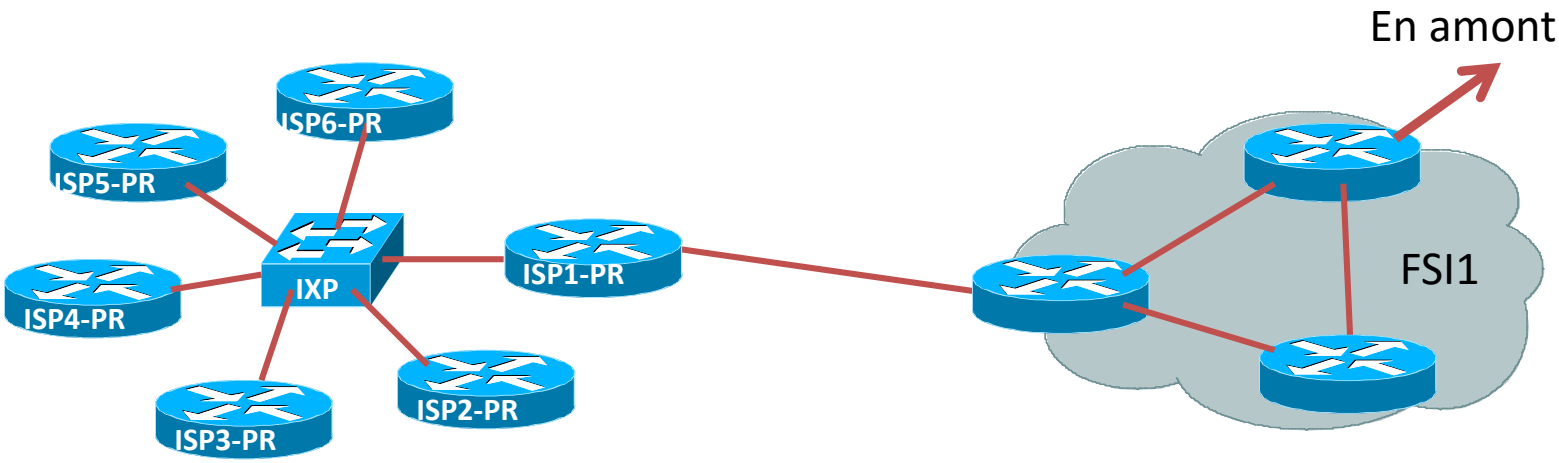


- PR = Routeur d'échange de trafic (peering router)
  - Exécute iBGP (interne) et eBGP (avec les pairs)
  - Pas de route par défaut
  - Pas de "table pleine de BGP"
  - Préfixes domestiques uniquement
- Routeur d'échange de trafic utilisé pour tous les interconnexions privées

Interconnexion publique

- Le fournisseur de services participe à un point d'échange Internet
  - Il échange des préfixes qu'il puise dans le système de routage avec les participants de l'IXP
  - Il choisit avec qui former des pairs à l'IXP
    - Echange de trafic bilatéral (comme interconnexion privée)
    - Echange de trafic multilatéral (via le serveur route de l'IXP)
  - Il fournit le routeur à l'IXP et fournit la connectivité de leur PoP à l'IXP
  - Le routeur de l'IXP ne transporte que les préfixes domestiques

Interconnexion publique

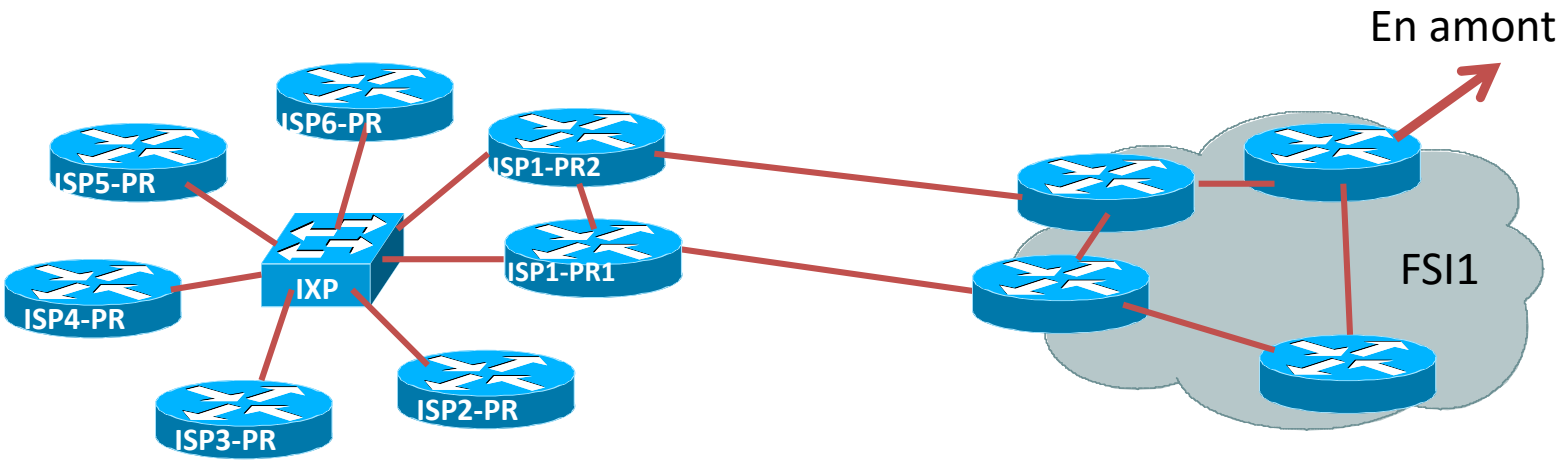


- ISP1-PR = Routeur d'échange de traffic de notre FSI (peering router of our ISP)
  - Exécute iBGP (interne) et eBGP (avec les pairs IXP)
  - Pas de route par défaut
  - Pas de "table pleine de BGP"
  - Préfixes domestiques uniquement
- Physiquement situé à l'IXP

Interconnexion publique

- Routeur du FSI routeur d’échange de trafic de l’IXP nécessite une configuration soignée
  - Il est éloigné du backbone domestique
  - Ne doit créer aucun préfixe domestique
  - (Aussi, pas de route par défaut, pas de table BGP complète)
  - Filtrage d’annonces BGP des pairs IXP (entrée et sortie)
- Fourniture d'une deuxième liaison à l'IXP:
  - (pour la redondance ou capacité supplémentaire)
  - Signifie généralement l'installation d'un deuxième routeur
    - Connecté à un deuxième commutateur (si l'IXP a deux interrupteurs de plus)
    - Interconnecté avec le routeur d'origine (et une partie de la maille iBGP)

Interconnexion publique

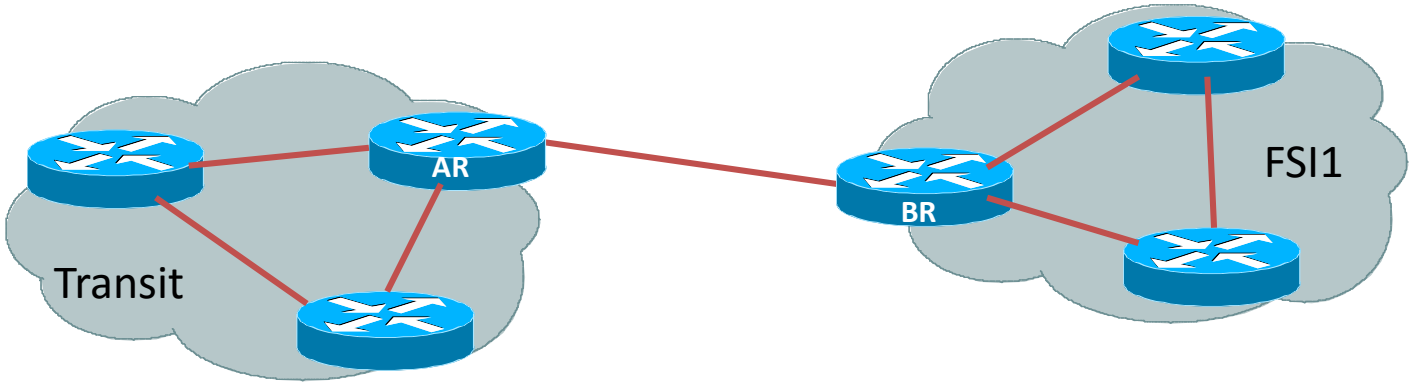


- La fourniture d'une seconde liaison à l'IXP signifie prendre en considération la redondance dans le backbone du SP
  - Deux routeurs
  - Deux liens indépendants
  - Interrupteurs séparés (si l'IXP a deux ou plusieurs commutateurs)

Connexion en amont / de transit

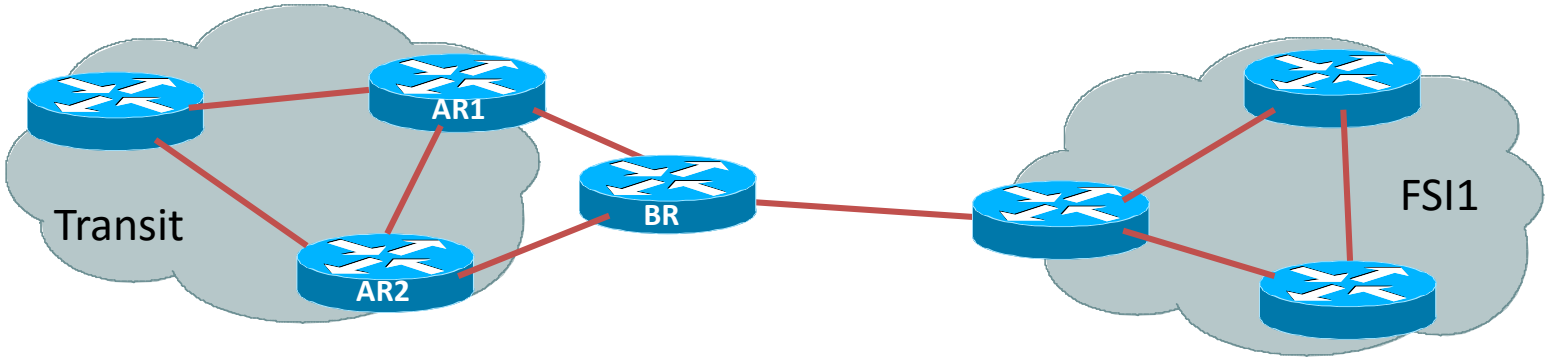
- Deux scénarios:
  - Le fournisseur de transit se trouve dans la localité
    - Ce qui signifie que la bande passante n'est pas chère, abondante, facile à fournir et à mettre à niveau
  - Le fournisseur de transit est à une longue distance
    - Par câble sous-marin, satellite, fibre longue distance, etc
- Chaque scénario a des considérations différentes qui doivent être prises en compte

Fournisseur de transit local



- BR = Routeur frontière des FSI (ISP's Border Router)
  - Exécute iBGP (interne) et eBGP (avec transit)
  - Soit il reçoit la route par défaut ou le tableau BGP complet de l'amont
  - Les politiques BGP sont mises en œuvre ici (en fonction de la connectivité)
  - Filtrage de paquets est mis en œuvre ici (au besoin)

Fournisseur de transit distant



- BR = Routeur frontière des FSI (ISP's Border Router)
  - Co-situé dans un centre de co-lo (typique) ou dans les locaux du fournisseur en amont
  - Exécute iBGP avec le reste du backbone FSI1
  - Exécute eBGP avec le(s) routeur(s) du fournisseur de transit
  - Met en œuvre des politiques BGP, filtrage de paquets, etc
  - Ne crée aucun préfixe domestique

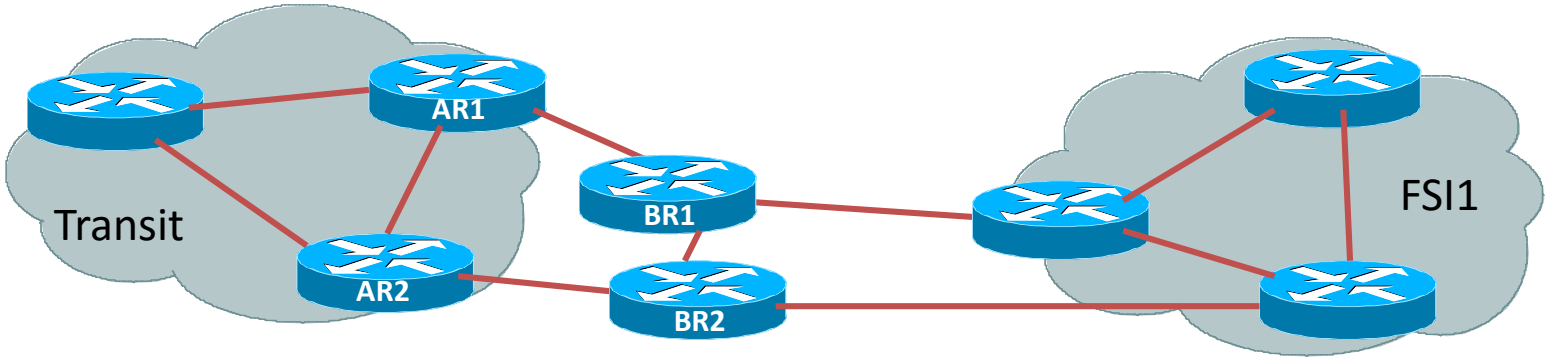
Fournisseur de transit distant

- Positionner un routeur à proximité des infrastructures du fournisseur de transit est fortement encouragé:
  - Les circuits longues distances sont chers, donc le routeur permet au FSI de mettre en place un filtrage approprié au départ
  - Déplace le problème de tamponnage loin du fournisseur de transit
  - Co-lo à distance permet au FSI de choisir un autre fournisseur de transit et de migrer des liens avec un minimum de temps

Fournisseur de transit distant

- Autres points à considérer:
  - Nécessite le soutien de mains à distance
  - (Les mains à distance serviraient à brancher ou à débrancher des câbles, des équipements de cycle d'alimentation, remplacer le matériel, etc. comme indiqué)
  - Contrat de support approprié auprès des vendeurs d'équipements
  - Raisonnable d'envisager deux routeurs et deux liens longues-distances pour la redondance

Fournisseur de transit distant



- Scénario de mise à niveau :
  - Fourniture de deux routeurs
  - Deux circuits indépendants
  - Considérez un deuxième fournisseur de transit et / ou pointer chez un IXP

Résumé

- Considérations de conception pour:
  - Interconnexions privées
    - Echange de trafic simple et privé
  - Interconnexions publiques
    - Routeur co-lo à un IXP
  - Fournisseur de transit local
    - Interconnexion simple en amont
  - Fournisseur de transit longue distance
    - Co-lo à routeur distant dans les locaux des centres de données ou de transit

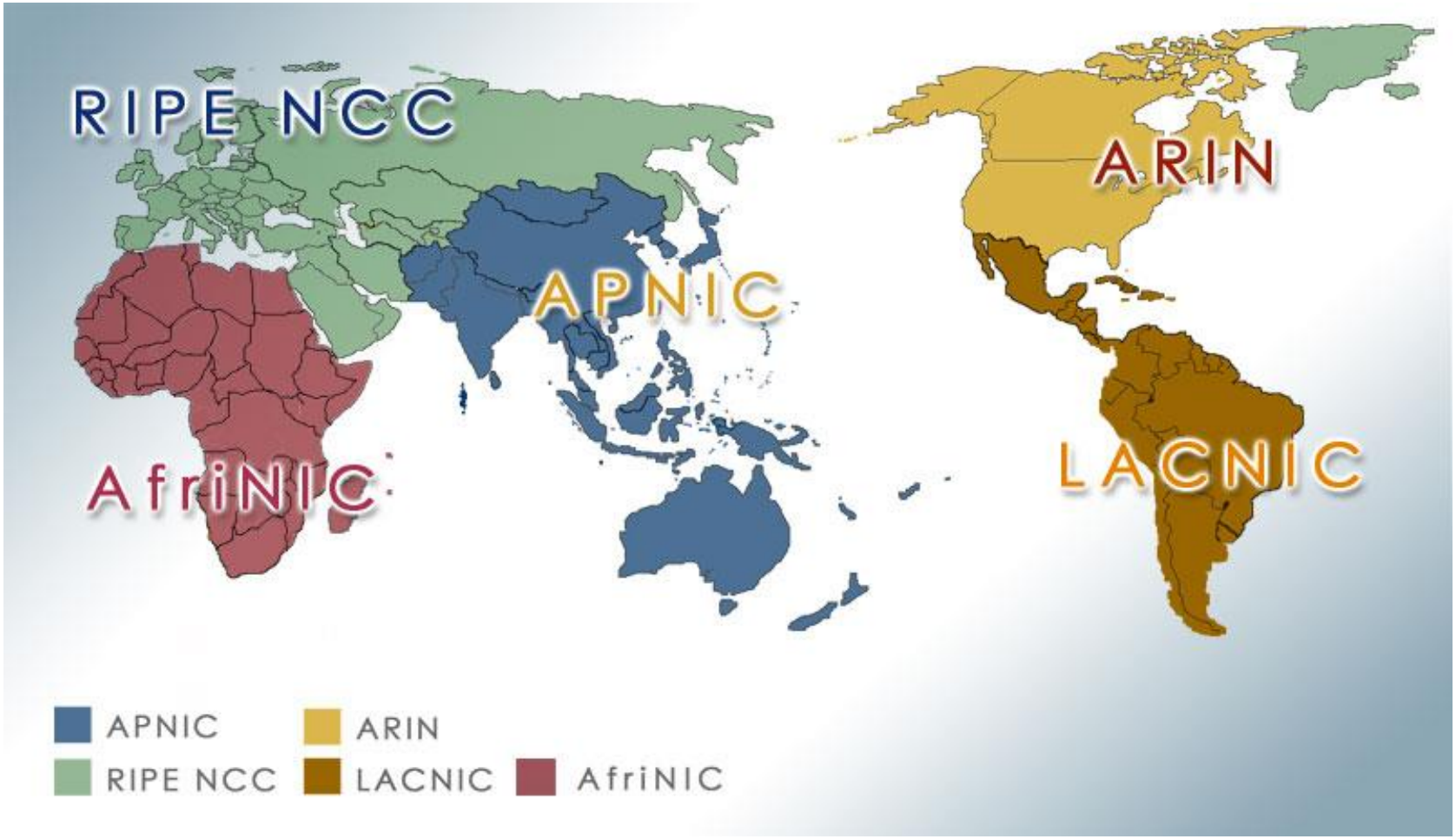
Adressage

Ressources et protocoles d'adressage

Où obtenir les adresses IP et les numéros AS

- Votre FSI en amont
- Afrique
  - AfriNIC – http://www.afrinic.net
- Asie et Pacifique
  - APNIC – http://www.apnic.net
- Amérique du Nord
  - ARIN – http://www.arin.net
- Amérique latine et les Caraïbes
  - LACNIC – http://www.lacnic.net
- Europe et Moyen-Orient
  - RIPE NCC – http://www.ripe.net/info/ncc

Régions de Registre Internet



Obtenir une espace d’adresse IP

- Participez à l’espace PA du FSI en amont

  ou bien

- Devenez membre de votre registre Internet régional et obtenez votre propre allocation
  - Exiger un plan d'un an d'avance
  - Les politiques générales sont décrites dans RFC2050, des détails plus précis se trouvent sur le site Web RIR individuel
- Il n'y a plus d'espace pour adresse IPv4 à l'IANA
  - La plupart des RIR sont maintenant dans la “finale /8” des politiques de délégation de IPv4
  - Un nombre limité d’IPv4 disponible
  - Les allocations d’IPv6 sont faciles à obtenir dans la plupart des régions RIR

Qu'en est-il de l’adressage RFC1918?

- RFC1918 définit les adresses IP réservées pour les réseaux privés
  - Ne sont pas à utiliser sur les backbones Internet
  - **http://www.ietf.org/rfc/rfc1918.txt**
- Couramment utilisé à l’intérieur des réseaux d’utilisateurs finaux
  - NAT utilisé pour traduire de l'adressage interne privé à l'adressage externe public
  - Permet au réseau d'utilisateurs finaux de migrer les FSI sans un exercice de renumérotation interne majeur
- La plupart des FSI filtre l’adressage RFC1918 à la périphérie de leur réseau
  - **http://www.cymru.com/Documents/bogon-list.html**

Qu'en est-il de l’adressage RFC1918?

- Liste des problèmes bien connus avec cette approche pour un backbone SP:
  - Empêche la détection du MTU
  - Conflits potentiels avec l'utilisation d’adressage privé à l'intérieur de réseaux clients
  - La sécurité par l'obscurité n’assure pas la sécurité
  - Le dépannage à l’extérieur du réseau local devient très difficile
    - Les adresses d'interface du routeur sont visibles seulement au niveau local
    - Internet devient invisible depuis le routeur
  - Le dépannage des problèmes de connectivité à l'échelle d'Internet devient impossible
    - Les traçages et les pings ne fournissent aucune information
    - Aucune distinction entre “réseau invisible” et “réseau cassé”
  - Augmente la complexité opérationnelle de l'infrastructure réseau et de la configuration du routage

Adressage IP privé par rapport à l'adressage IP routable à l'échelle mondiale

- Infrastructure de sécurité: non améliorée par l'utilisation d'adressage privé
  - Peut encore être attaqué de l'intérieur, ou par un client, ou par des techniques de réflexion à partir de l'extérieur
- Dépannage: rendu à un ordre de grandeur plus difficile
  - Pas de vue sur Internet depuis les routeurs
  - Les autres FSI ne peuvent pas distinguer entre l'interrompu et le cassé
- Performance: rupture PMTUD
- Résumé:
  - Utilisez TOUJOURS l'adressage IP routable mondialement pour l'Infrastructure FSI

Plans d'adressage – infrastructure FSI

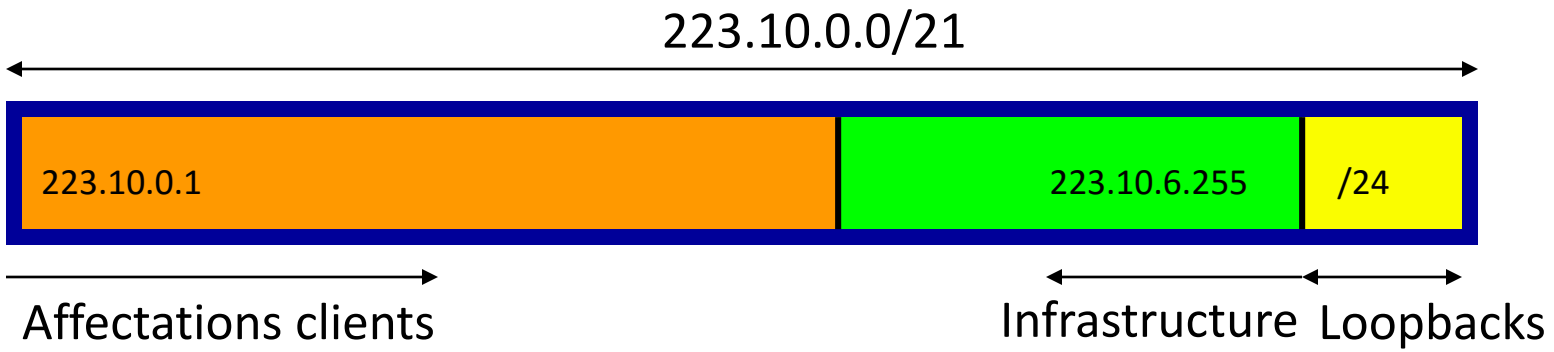
- Bloc d'adresse pour les interfaces loop-back des routeurs
- Bloc d'adresse pour les infrastructures
  - Par PoP ou backbone entier
  - Résumer entre les sites si cela donne sens
  - Allouer en fonction des besoins réels, et non des frontières historiques basées sur des classes
- Des politiques d’attribution similaires doivent être utilisées pour IPv6 aussi
  - Les FSI obtiennent simplement un bloc sensiblement plus grand (relativement) afin que les affectations au sein du backbone soient plus faciles à faire

Plans d'adressage – Client

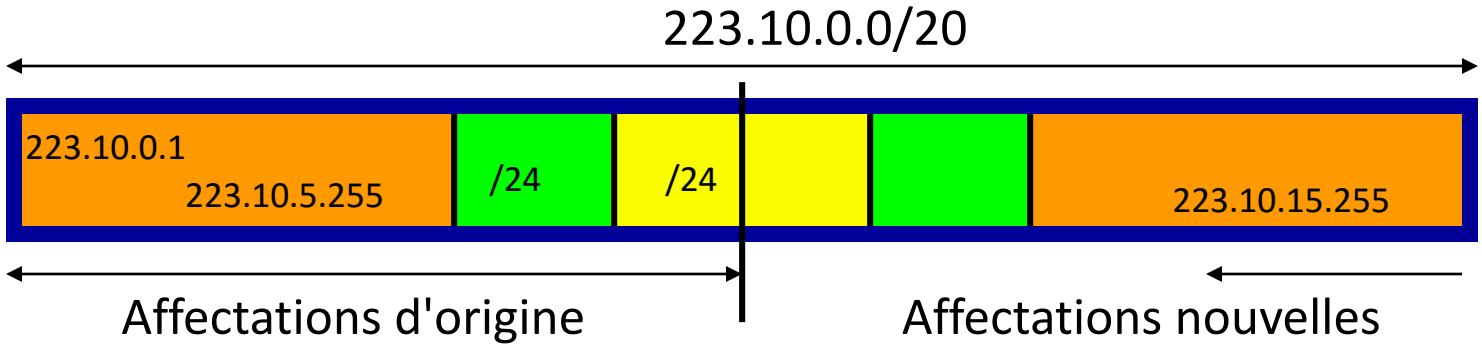
- Les clients reçoivent un espace d'adresse en fonction de leurs besoins
- Ne doit pas être réservé ou affecté sur une logique à base par PoP
  - FSI iBGP porte des filtres des clients
  - L'agrégation n'est pas requise et n'est généralement pas souhaitable

Plans d'adressage – infrastructure FSI

- Phase une



- Phase deux



Planification des plans d'adressage

- Les registres vont attribuer généralement le bloc suivant de façon à ce qu'il soit contigu à la première affectation
  - L'affectation minimale pourrait être / 21
  - Très probable qu'une attribution ultérieure rendra cela jusqu'à /20
  - Donc, planifier en conséquence

Plans d'adressage (Suite)

- Documenter les affectations d’infrastructure
  - Facilite l'opération, le débogage et la gestion
- Documenter les affectations de clients
  - Contenu dans l'iBGP
  - Facilite l'opération, le débogage et la gestion
  - Soumettre l’objet de réseau à la base de données RIR

Protocoles de routage

Protocoles de routage

- IGP – Interior Gateway Protocol
  - porte les adresses d'infrastructures, les liens point-à-point
  - des exemples : OSPF, ISIS, ...
- EGP – Exterior Gateway Protocol
  - porte des préfixes de clients et des voies d'Internet
  - L'EGP actuel est la version BGP 4
- Pas de connexion entre IGP et EGP

Pourquoi avons-nous besoin d'une IGP?

- Mise à l'échelle du backbone FSI
  - Hiérarchie
  - Construction d'infrastructures modulaires
  - Limiter la portée de l'échec
  - Réparation des défauts d'infrastructure par utilisation du routage dynamique avec convergence rapide

Pourquoi avons-nous besoin d'un EGP?

- Mise à l'échelle d'un grand réseau
  - Hiérarchie
  - Limiter la portée de l'échec
- Politique
  - Contrôler l’accessibilité aux préfixes
  - Fusionner des organismes distincts
  - Connecter plusieurs IGP

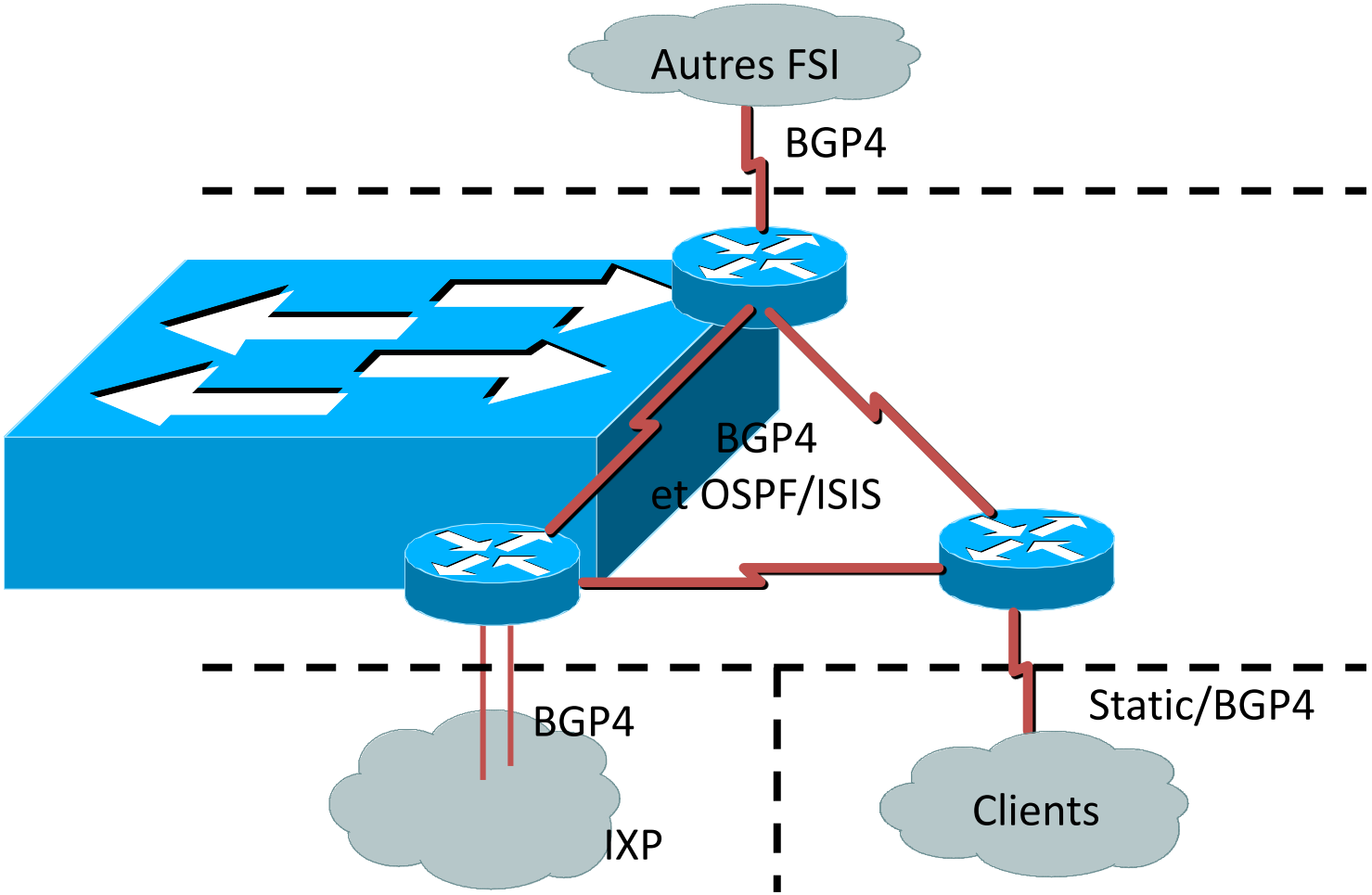
Protocoles de routage intérieurs contre extérieurs

- Intérieur
  - Découverte automatique de voisin
  - Généralement, faites confiance à vos routeurs IGP
  - Les préfixes vont à tous les routeurs IGP
  - Lie ensemble des routeurs dans un AS
- Extérieur
  - Pairs spécifiquement configurés
  - Connexion avec des réseaux extérieurs
  - Fixer des limites administratives
  - Lie les AS ensemble

Protocoles de routage intérieurs contre extérieurs

- Intérieur
  - Transporte les adresses d’infrastructure FSI uniquement
  - Les FSI s'efforcent de maintenir l'IGP petit pour l'efficacité et l'évolutivité
- Extérieur
  - Transporte des préfixes de client
  - Transporte les préfixes de l'Internet
  - Les EGP sont indépendantes de la topologie du réseau ISP

Hiérarchie des protocoles de routage



Protocoles de routage: Choix d'une IGP

- Consultez la présentation “OSPF vs ISIS” :
  - OSPF et ISIS ont des propriétés très similaires
- Le FSI choisit généralement entre OSPF et ISIS
  - Choisissez ce qui convient à l'expérience de vos opérateurs
  - Dans la plupart des versions des fournisseurs, à la fois OSPF et ISIS ont suffisamment de “nerd knobs” pour modifier le comportement du IGP
  - OSPF fonctionne sur IP
  - ISIS fonctionne sur l'infrastructure, aux côtés d’IP

Protocoles de routage: Recommandations IGP

- Gardez la table de routage IGP le plus petit possible
  - Si vous pouvez compter les routeurs et les liaisons point à point dans le backbone, ce total est le nombre d'entrées IGP que vous devriez voir.
- Détails IGP:
  - Ne devrait avoir que des loopbacks de routeurs, adresses de liens point-à-point de backbone WAN, et des adresses réseau de n'importe quels LAN ayant une IGP qui s'exécute sur eux.
  - Fortement recommandé d'utiliser l'authentification inter-routeur.
  - Utilisez une récapitulation inter-zone si possible.

Protocoles de routage: Plus de recommandations IGP

- Pour affiner davantage la taille de la table IGP, considérez :
  - L'utilisation de “ip non numéroté” sur les liens client point-à-point – économise le transport de ce /30 dans l'IGP
    - (Si le point-à-point client / 30 est nécessaire à des fins de surveillance, alors mettez ceci dans iBGP)
  - Utiliser des adresses contiguës pour des liens WAN de backbone dans chaque zone - puis regrouper en zone backbone
  - Ne pas résumer les adresses loopback du routeur - comme l’iBGP en a besoin (pour le next-hop)
  - Utilisez iBGP pour transporter tout ce qui ne contribue pas au processus de routage IGP

Protocoles de routage: Recommendations iBGP

- iBGP doit transporter tout ce qui ne contribue pas au processus de routage IGP
  - Table de routage Internet
  - Adresses affectées aux clients
  - Liens point-à-point client
  - Des pools de réseaux commutés, LAN passive, etc.

Protocoles de routage: Plus de recommandations iBGP

- Caractéristiques évolutives d'iBGP:
  - Utilisez une authentification voisine
  - Utilisez des groupes de pairs pour accélérer le processus de mise à jour et l'efficacité de la configuration
  - Utilisez les communautés pour faciliter le filtrage
  - Utilisez la hiérarchie réflectrice de routes
    - Paire de réflecteur de route par PoP (clusters superposées)

La sécurité

La sécurité

- Sécurité de l'Infrastructure FSI
- Sécurité du réseau FSI
- La sécurité n'est pas une option!
- Les FSI doivent:
  - se protéger
  - aider à protéger leurs clients de l'Internet
  - protéger l'Internet de leurs clients
- Les diapositives qui suivent sont des recommandations générales
  - Faire plus de recherche sur la sécurité avant de déployer un réseau

Sécurité de l'Infrastructure FSI

- Sécurité du routeur
  - Noms d'utilisateur, mots de passe, filtres vty, TACACS+
  - Désactiver telnet sur vtys, utilisez uniquement SSH
  - Les filtres vty ne devraient permettre que l'accès NOC, aucun accès extérieur
  - Voir Essentials IOS pour les pratiques recommandées pour les FSI

Sécurité du réseau FSI

- Déni d’attaques de service
  - par exemple: “smurfing”
  - voir http://www.denialinfo.com
- Filtrage efficace
  - Frontières de réseau - voir Cisco ISP Essentials
  - Connexions clients statiques - Unicast RPF sur **chacun** d'eux
  - Centre d’opération de réseau
  - Réseau d'entreprise ISP – derrière un pare-feu

Filtrage de route Ingress & Egress

Vos clients ne doivent envoyer aucun paquet IP vers l'Internet avec une adresse source autre que celle que vous leurs avez alloué!

La gestion hors bande

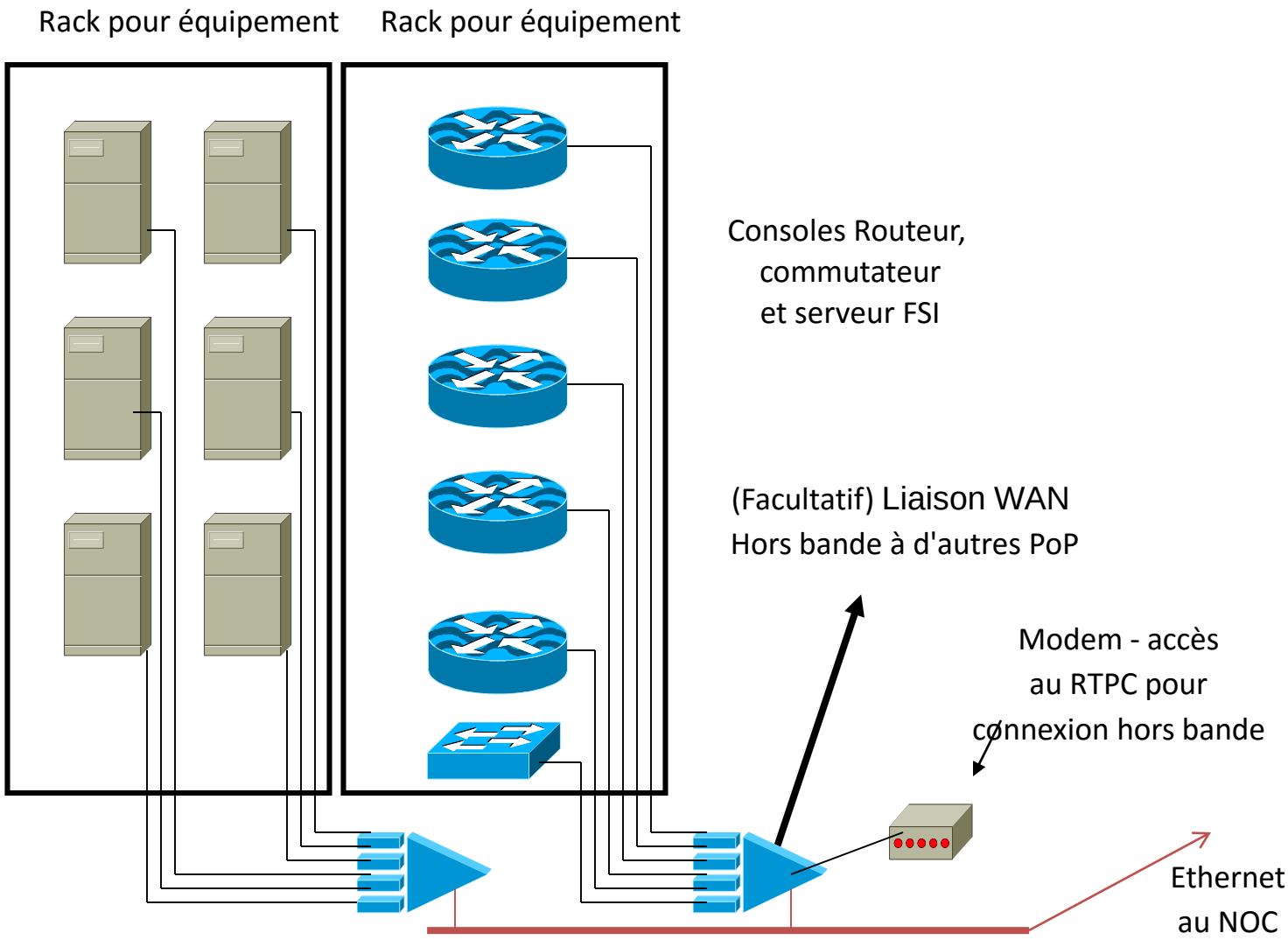
La gestion hors bande

- **Pas facultatif !**
- Permet l'accès à l'équipement du réseau en cas de défaillance
- Assure une qualité de service aux clients
  - Minimise les temps d'arrêt
  - Minimise les temps de réparation
  - Facilite les diagnostics et débogage

La gestion hors bande

- Exemple OoB – serveur d'accès :
  - modem relié afin de permettre au NOC de se connecter
  - ports de console de tous les équipements réseau connectés aux ports série
  - Le lien LAN et/ou WAN se connecte au coeur du réseau, ou via un lien de gestion distinct au NOC
- Un accès de contrôle à distance complet en toutes circonstances

Réseau Hors Bande



La gestion hors bande

- Exemple OoB - collecte de statistiques :
  - Les routeurs sont activés pour NetFlow et syslog
  - Les données de gestion sont sensibles à la congestion/échec
  - Assure l'intégrité des données de gestion en cas de défaillance
- Des informations à distance complètes en toutes circonstances

Laboratoire d'essai

Laboratoire d'essai

- Conçu pour ressembler à une PoP typique
  - Exploité comme un PoP typique
- Utilisé pour tester de nouveaux services ou de nouveaux logiciels dans des conditions réalistes
- Permet la découverte et la résolution de problèmes potentiels avant qu'ils font leur apparition sur le réseau

Laboratoire d'essai

- Certains FSI dédient des équipements au laboratoire
- D’autres FSI “achètent en avance” afin que les équipements de laboratoire d’aujourd'hui deviennent des équipements PoP de demain
- D’autres FSI utilisent du matériel de laboratoire comme “pièces de rechange” en cas de défaillance matérielle

Laboratoire d'essai

- Vous ne pouvez pas vous permettre un laboratoire d’essai?
  - Mettez de côté un routeur et un serveur de rechange pour l'essai de nouveaux services
  - Ne jamais essayer du nouveau matériel, des logiciels ou des services directement sur le réseau réel
- Tous les grands FSI aux Etats-Unis et en Europe disposent d'un laboratoire d’essai
  - Il s'agit d'une considération sérieuse

Considérations opérationnelles

Considérations opérationnelles

Pourquoi concevoir le meilleur réseau du monde quand vous n'avez pas pensé aux bonnes pratiques opérationnelles qui devraient être mises en œuvre?

Considérations opérationnelles Maintenance

- Ne jamais travailler sur le réseau réel, même si la modification semble triviale
  - Mettre en place des périodes de maintenance qui sont connues par vos clients
    - par exemple Mardi de 4 h à 7 h, jeudi de 4 h à 7 h
- Ne jamais faire de la maintenance un vendredi
  - A moins que vous ne vouliez travailler tout le weekend à travailler!
- Ne jamais faire de la maintenance un lundi
  - A moins que vous ne vouliez travailler tout le weekend à faire des préparatifs

Considérations opérationnelles Soutien

- Faire la différence entre le soutien aux clients et le centre d'opérations du réseau
  - Le service de soutien aux clients résout les problèmes des clients
  - Le NOC traite les problèmes liés au backbone et à l'Internet
- L'équipe d'ingénierie de réseau sert de dernier recours
  - Ils conçoivent le réseau de prochaine génération, améliorent la conception de routage, mettent en œuvre de nouveaux services, etc.
  - Ils ne doivent pas et n'ont pas à faire du soutien!

Considérations opérationnelles Communications du NOC

- Le NOC devrait connaître les coordonnées des NOC équivalents des fournisseurs et des pairs en amont
- Ou bien envisager l'adhésion au système INOC-DBA
  - Système téléphonique Voix sur IP utilisant SIP
  - Fonctionne sur Internet
  - www.pch.net/inoc-dba pour plus d'informations

Conception de réseaux FSI

Résumé

Résumé de la conception FSI

- KEEP IT SIMPLE & STUPID ! (KISS)
- Simple est élégant, est évolutif
- Utilisez la redondance, la sécurité et la technologie pour rendre la vie plus facile pour vous-même
- Par-dessus tout, assurez la qualité de service pour vos clients

GRAND DUCHY OF LUXEMBOURG
Ministry of Foreign Affairs

Directorate for Development Cooperation

European Union Africa
Infrastructure Trust Fund

Conception de réseaux FSI

Conception de réseaux évolutive

Internet Society™