Services RENATER
www.renater.fr/services

09/06/2011 – CAPITOUL

Simon.Muyal@renater.fr

Réseau

QoS
Multicast
IPv4
L3VPN
L2VPN
Lambda 10GE
IPv6
Circuits
DNS
Allocation IP

Voix et images

Gatekeeper
H323
ToIP
MCU
IPBX
EVO

Middleware

Fédération Education-Recherche
Edugain

Mobilité

Eduspot
eduroam
Wi-Fi
802.1X

Sécurité

CERT
Anti-spam
Anti-virus
Certificats serveurs
Certificats de personne
TCS

Réseau

QoS

Multicast

IPv4

L3VPN

L2VPN

IPv6

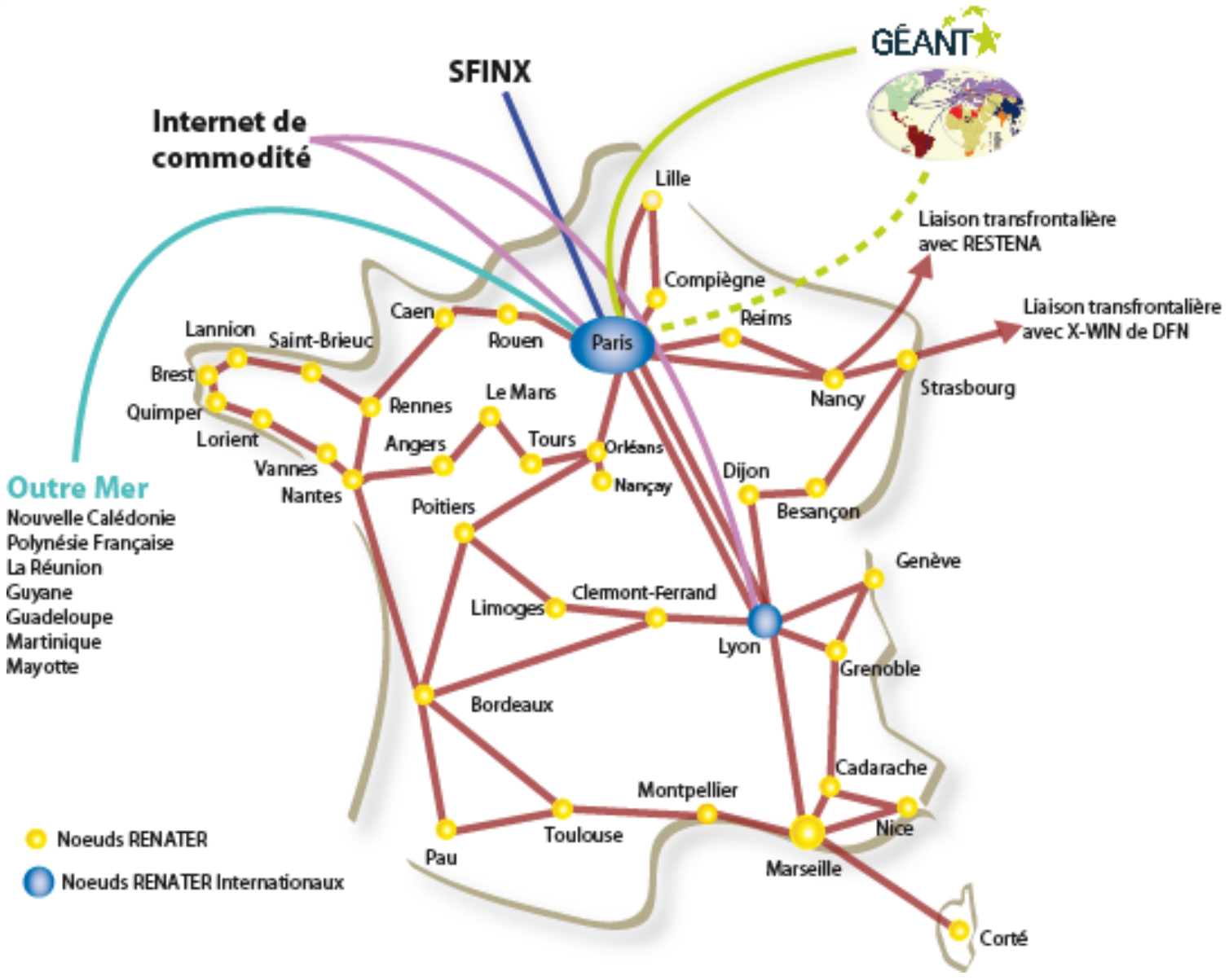
Lambda 10GE

DNS

Allocation IP

Circuits

Le réseau RENATER



Spécifications d'interconnexion IP

Pré-requis techniques pour se raccorder au réseau

RENATER

Interfaces de raccordement

- Interfaces Ethernet uniquement
  - 10/100/1000 TX (RJ45)
  - GE SX (fibre multimode)
  - GE LX (fibre monomode)
  - 10GE LR (fibre monomode)

  → Faire remonter les besoins spécifiques

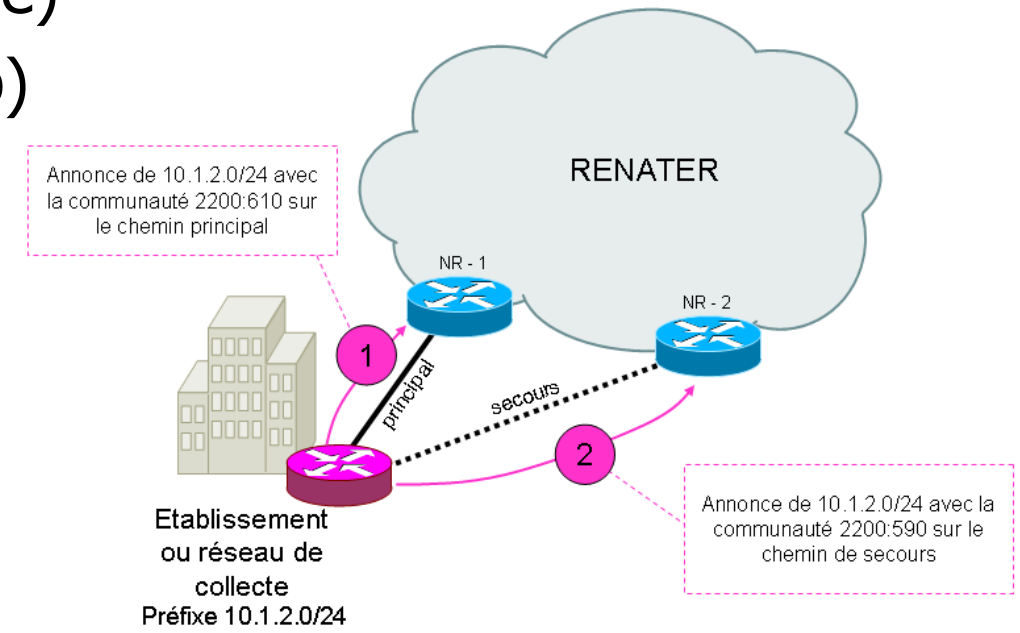
- Configuration en « trunk » recommandée
  - Permet ensuite d'activer des services sur des VLANs dédiés

Protocole de routage

- Un seul protocole BGP
  - Pas de routage statique sur RENATER
  - Le GIP RENATER peut
    - Allouer des numéros d'AS (privés)
    - Fournir des configurations de base
  - RENATER = AS2200
- Annonces en IPv4
  - RENATER annonce au choix:
    - Route par défaut (0.0.0.0/0 + préfixe backbone RENATER)
    - Routes des usagers RENATER + route par défaut (4000 routes environ)
    - Full routing (300 000 routes environ → doit être justifié)
  - Le site annonce ses préfixes en agrégeant
    - RENATER n'accepte que les annonces validées dans l'agrément
    - Détails sur l'importance de l'agrément vus plus tard
- Les autres services réseau (IPv6...) se basent aussi sur BGP

Communautés BGP

- http://www.renater.fr/bgp
- Communautés prédéfinies
  - 2200:610 (primaire)
  - 2200:590 (backup)



IPv6

- http://www.renater.fr/ipv6
- Déployé en natif sur RENATER
- Des services commencent à être disponibles en IPv6 (ex: Google)
  - Assurez-vous que votre déploiement IPv6 n'est pas moins performant que votre déploiement IPv4
- Comment bénéficier du service?
  - Faire une demande de préfixe IPv6 à support-adressesip@renater.fr
  - Faire une demande de routage IPv6 via SAGA
- Consiste à
  - Déployer un VLAN pour l'interconnexion IPv6 avec RENATER
  - Configurer un peering BGP IPv6 et annoncer son préfixe

Multicast IPv4

- http://www.renater.fr/multicast
- Faire une demande au support technique de RENATER
  - support-reseau@renater.fr
- Consiste à
  - Activer l'address-family « ipv4 multicast » sur le peering BGP existant
  - Activer PIM-SMv2 pour IPv4 sur l'interface IPv4 de raccordement
  - *ASM: Mettre en place un point de rendez-vous (RP) et déployer 2 peerings MSDP vers RENATER pour l'annonce des sources actives*

Multicast IPv6

- Très simple à activer sur une connexion IPv6 existante
  - utilisation d'un seul VLAN pour l'unicast et le multicast
- Faire une demande au support technique de RENATER
  - support-reseau@renater.fr
- Consiste à
  - Activer l'address-family « ipv6 multicast » sur le peering BGP existant
  - Activer PIM-SMv2 pour IPv6 sur l'interface IPv6 de raccordement
  - *ASM: Embedded-RP (RFC3956) recommandé + configuration de RP statiques si besoins*

Demande de modification de routage

www.renater.fr/routage

Importance de l'agrément

- Le routage configuré n'est que le reflet de ce qui est dans l'agrément !
- Pour changer son point de raccordement au réseau RENATER une modification d'agrément est nécessaire sur SAGA
- C'est le point de départ pour toute demande de modification de la connexion réseau (traçabilité)
- Configurations générées automatiquement à partir des agréments
  - Assurez-vous que tous vos préfixes sont bien déclarés

Service de circuits

www.renater.fr/vpn

Les circuits

- Plusieurs types
  - Point-à-point
  - Multipoint-à-multipoint

- Basés sur différentes technos
  - L2VPN MPLS
  - L3VPN MPLS
  - VLAN

  } Jusqu'à 1Gbit/s

  - 10GE / lambda dédié

  } 10 Gbit/s

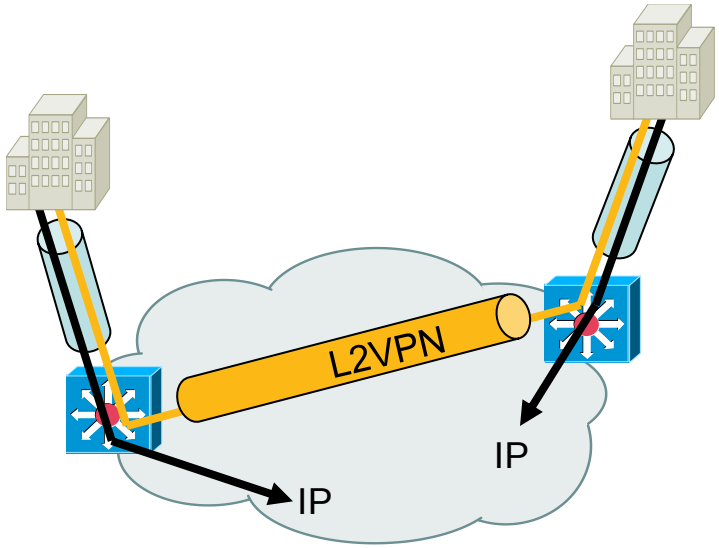
  - ...

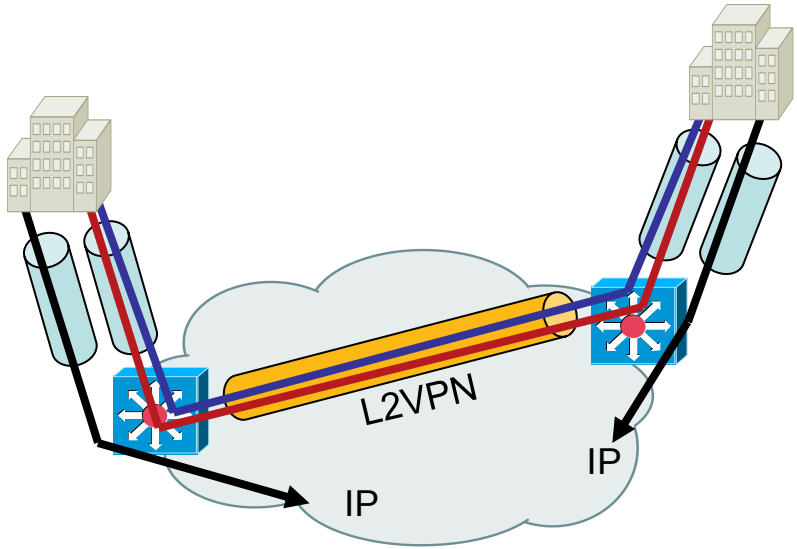
➔ **Le choix du type de circuit se fait par le GIP RENATER selon les besoins exprimés**

➔ **Formulaire en ligne pour les demandes de circuits (ou VPN) http://www.renater.fr/vpn**

L2VPN (interco Ethernet entre deux établissements)

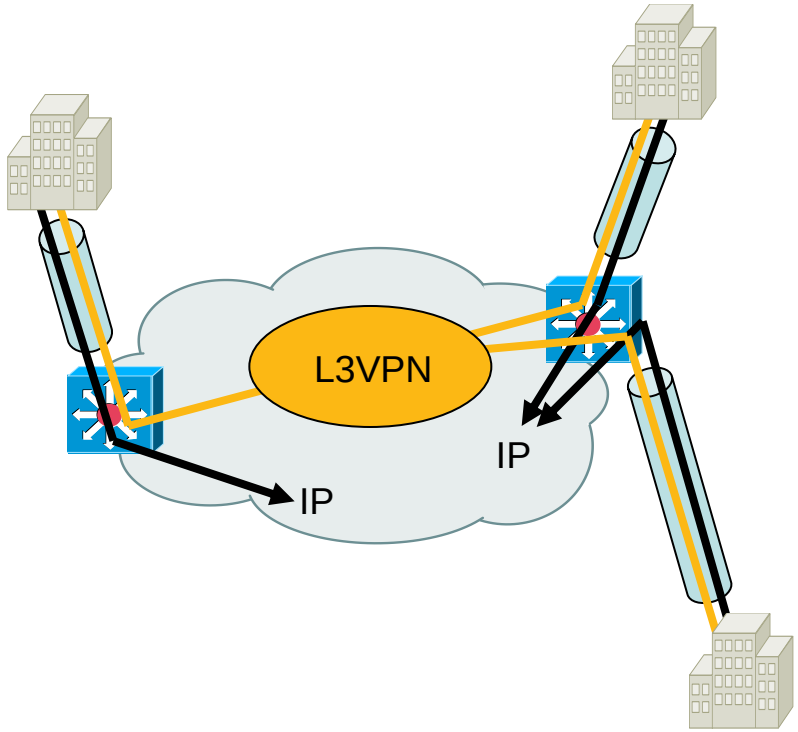
- VLAN à VLAN
  - Un seul port
  - Un seul VLAN transporté
  - QinQ par le site pour transporter plus de VLANs
- Port à Port
  - Un port nécessaire pour le VPN
  - Transport de tous les VLANs





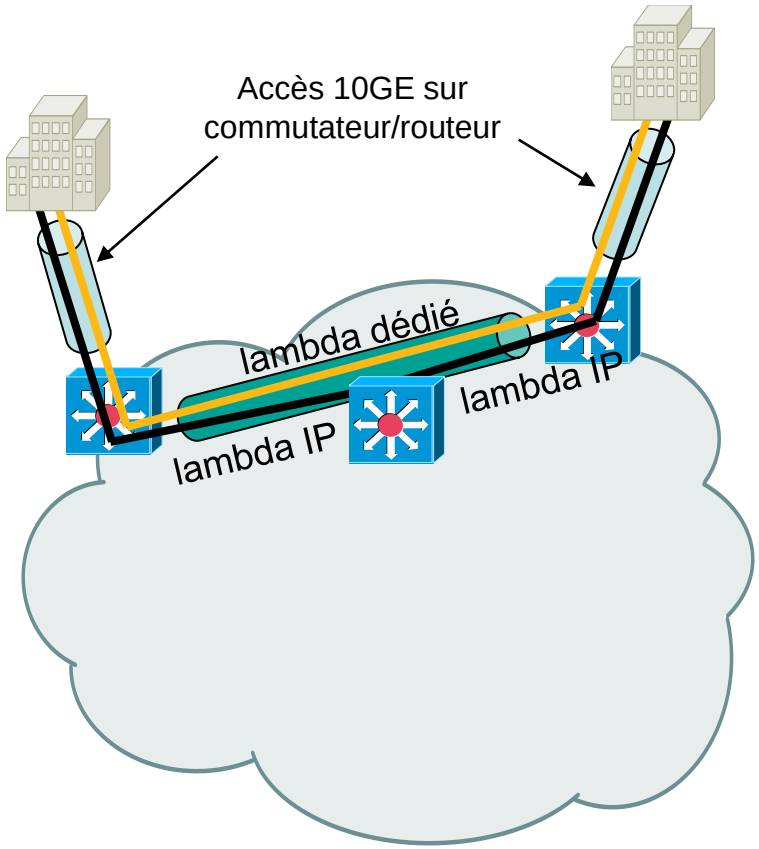
L3VPN (interco IP entre plusieurs établissements)

- Possibilité routage IP privées
- BGP pour routage RENATER<->site
  - Pas de filtrage sur les annonces
  - Nombre de préfixes limité
- IPv6 et multicast pas supportés
  - IPv6 et IPv4 multicast en cours d'intégration
- Troubleshooting simplifié
  - NOC-RENATER a la visibilité du routage



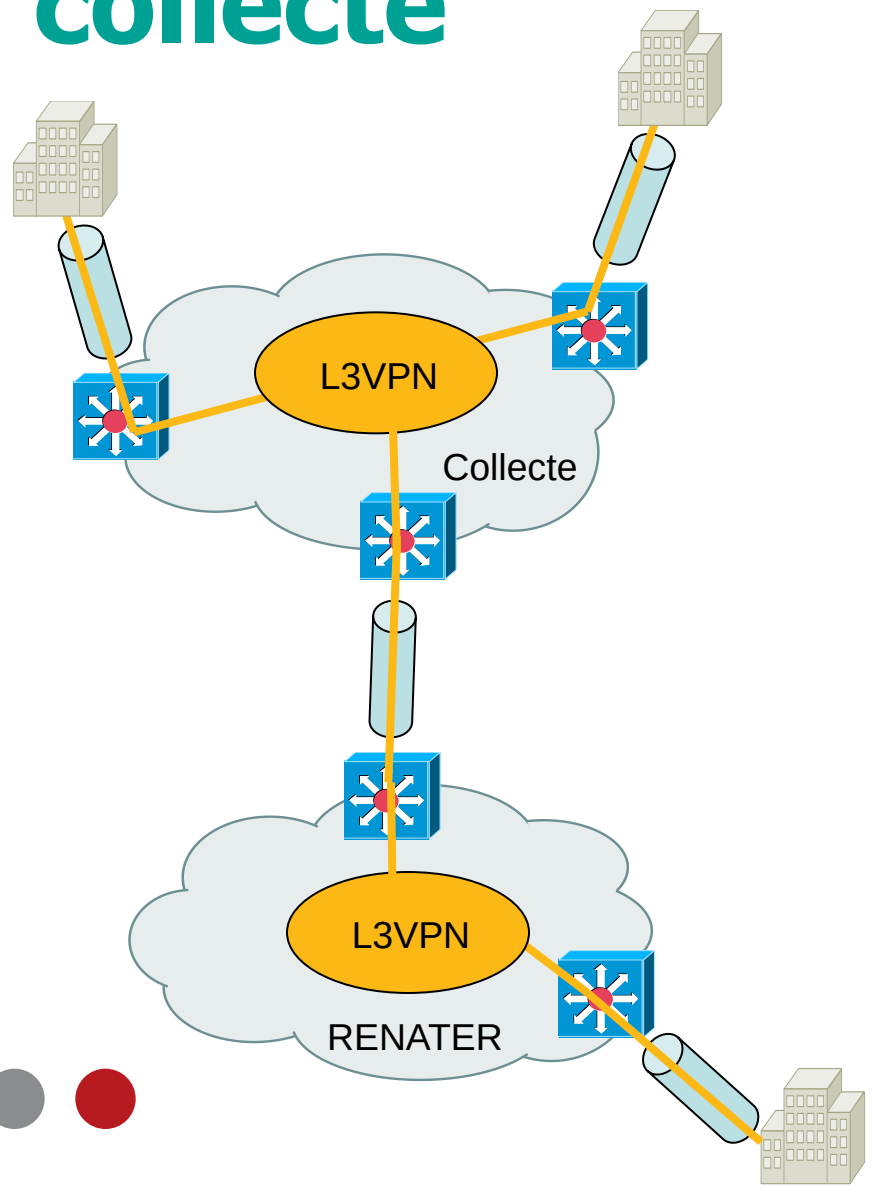
10GE / lambda

- VLAN vers VLAN
- L'interface de raccordement reste sur le commutateur routeur
  - Métrologie
  - Plus de flexibilité
- VLAN commuté sur 10GE dédié
  - L'interface d'accès peut aussi être utilisée pour l'accès IP
- Pour des projets de recherche nécessitant le très haut débit



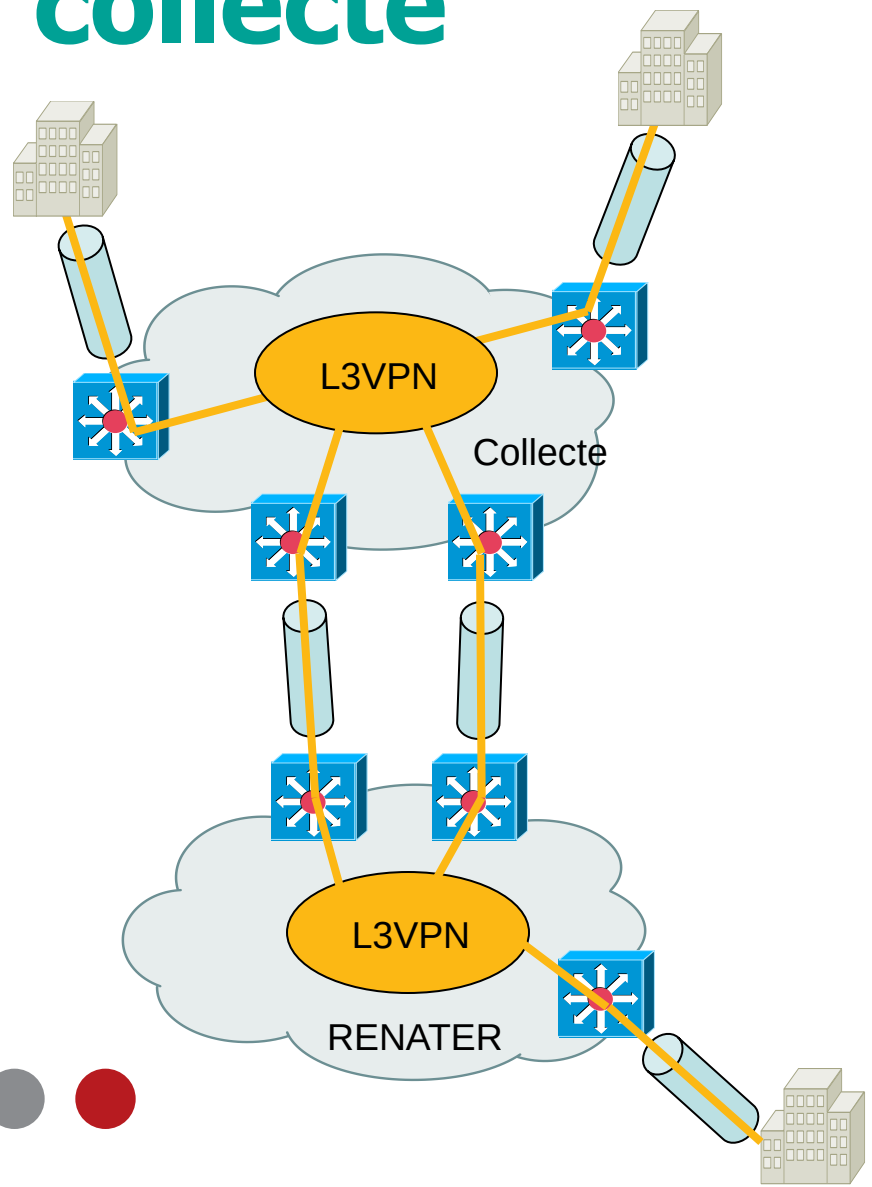
Prolongation des circuits sur la collecte

- Un circuit sur RENATER est fait entre interfaces de raccordement (ou VLANs)
- Nécessité de le prolonger sur le réseau de collecte
- Interconnexion simple de circuits
- Technologie éventuellement différentes
- Collaboration indispensable entre établissements, collectes, RENATER



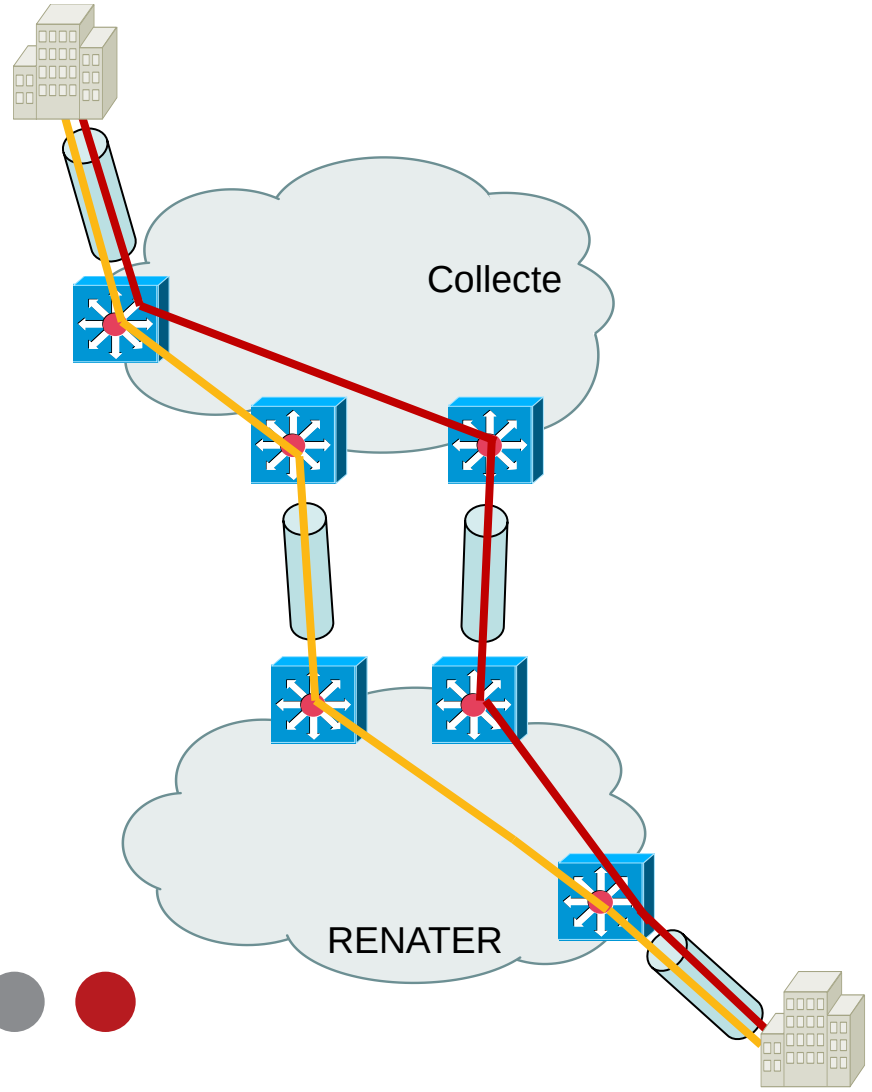
Prolongation des circuits sur la collecte

- Un circuit sur RENATER est fait entre interfaces de raccordement (ou VLANs)
- Nécessité de le prolonger sur le réseau de collecte
- Interconnexion simple de circuits
- Technologie éventuellement différentes
- Collaboration indispensable entre établissements, collectes, RENATER



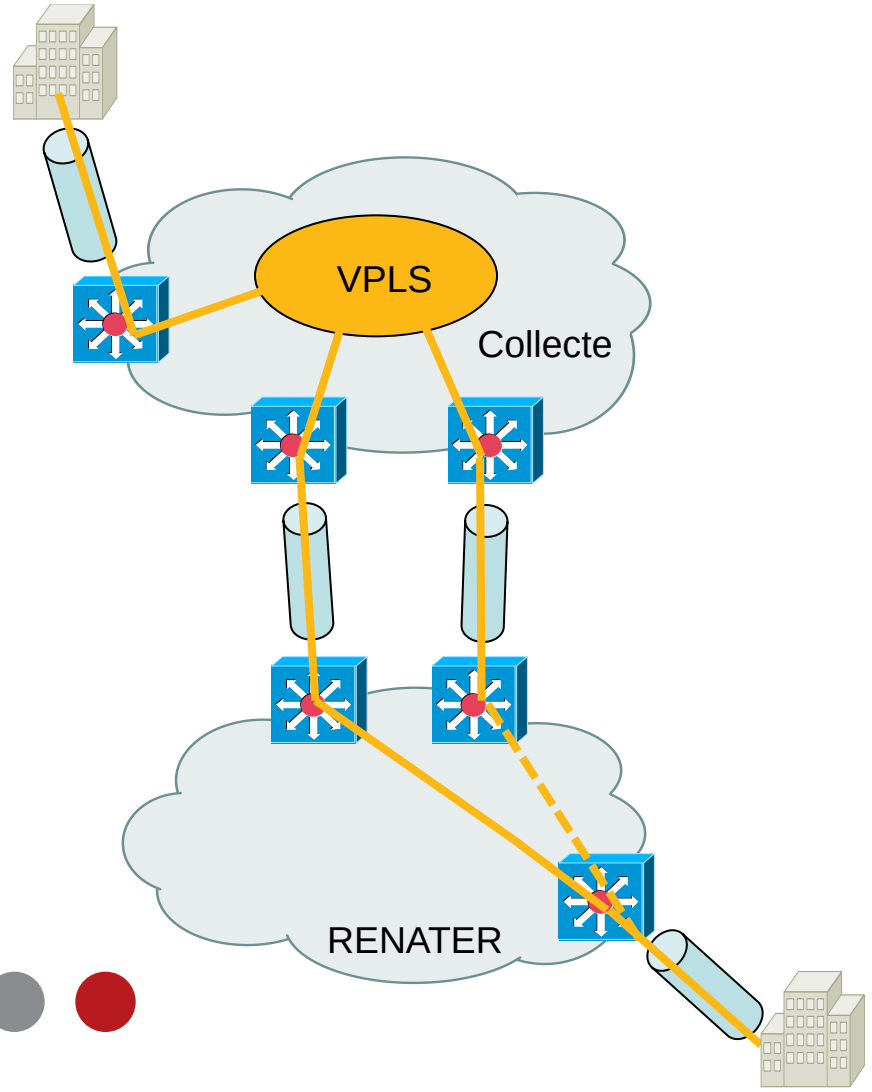
Prolongation des circuits sur la collecte

- Possible aussi pour VPN de niveau 2
- Complexité pour la redondance
- Pas de VPLS sur RENATER
- Possibilité de backuper les VPN point a point



Prolongation des circuits sur la collecte

- Possibilité également de prolonger un VPLS
- Possibilité de configuration d'un L2VPN de backup sur RENATER pour protéger l'accès



QoS

www.renater.fr/qos

QoS

- La QoS n'est activée qu'en cas de congestion

  ➔ L'absence de QoS ne signifie pas une mauvaise qualité de service
- Réingénierie de la QoS sur RENATER en cours
  - Ouverture premium à tous
  - QoS en accès des sites
  - Quelques corrections

Les classes

Classe	DSCP	Usage	Limitation
Premium	46 (ef)	Voix sur IP (téléphonie)	10% max
BBE	34 (af41)	Vidéo Applications critiques	10% max
BE	Tous les autres DSCP	Tout	Pas de restrictions
LBE	8 (cs1)	Scavenger	Pas de restrictions

Allocation d’adresses

www.renater.fr/adressesip

Adresses IP

- Le GIP attribue les préfixes IPv4 et IPv6 pour ses utilisateurs
- Formulaires disponibles en ligne
  - www.renater.fr/adressesip
- Le GIP RENATER alloue les préfixes en suivant les règles définies par le RIPE NCC
  - Formulaire assez « indigeste »
  - Mais procédure loin d'être insurmontable!
- Besoin d'aide ?
  - support-adressesip@renater.fr

Délégation de zone inverse

- En parallèle de l'allocation de préfixes IPv4 et IPv6
  - RENATER vous délègue la zone inverse pour les préfixes IP qui vous sont attribués
- Formulaire en ligne
  - www.renater.fr/zi
  - support-dns@renater.fr

Noms de domaines

www.renater.fr/domaine

Noms de domaines

- Le GIP RENATER ouvre les noms de domaines en .fr pour ses utilisateurs
  - le GIP signe une convention avec l'AFNIC qui est le Registre du .fr
- Gestion de la zone .prd.fr
- Actions stratégiques du GIP RENATER
  - Membre du CA AFNIC
  - Participe aux Comités de Concertation des Bureaux d'Enregistrement

Ouverture des noms de domaines

- Lettre d'engagement et annexe technique à remplir par les utilisateurs et à retourner au GIP RENATER
  - Service inclus dans la prestation RENATER pour les établissements sous tutelle
  - Service facturé 75€ pour les établissements sous contrat (1er nom gratuit)
- Validation des aspects administratifs puis techniques
- RENATER fait l'intermédiaire avec l'AFNIC
- Pour les noms en .prd.fr, RENATER gère directement la zone DNS

Voix et images

MCU

EVO

ToIP

IPBX

H323

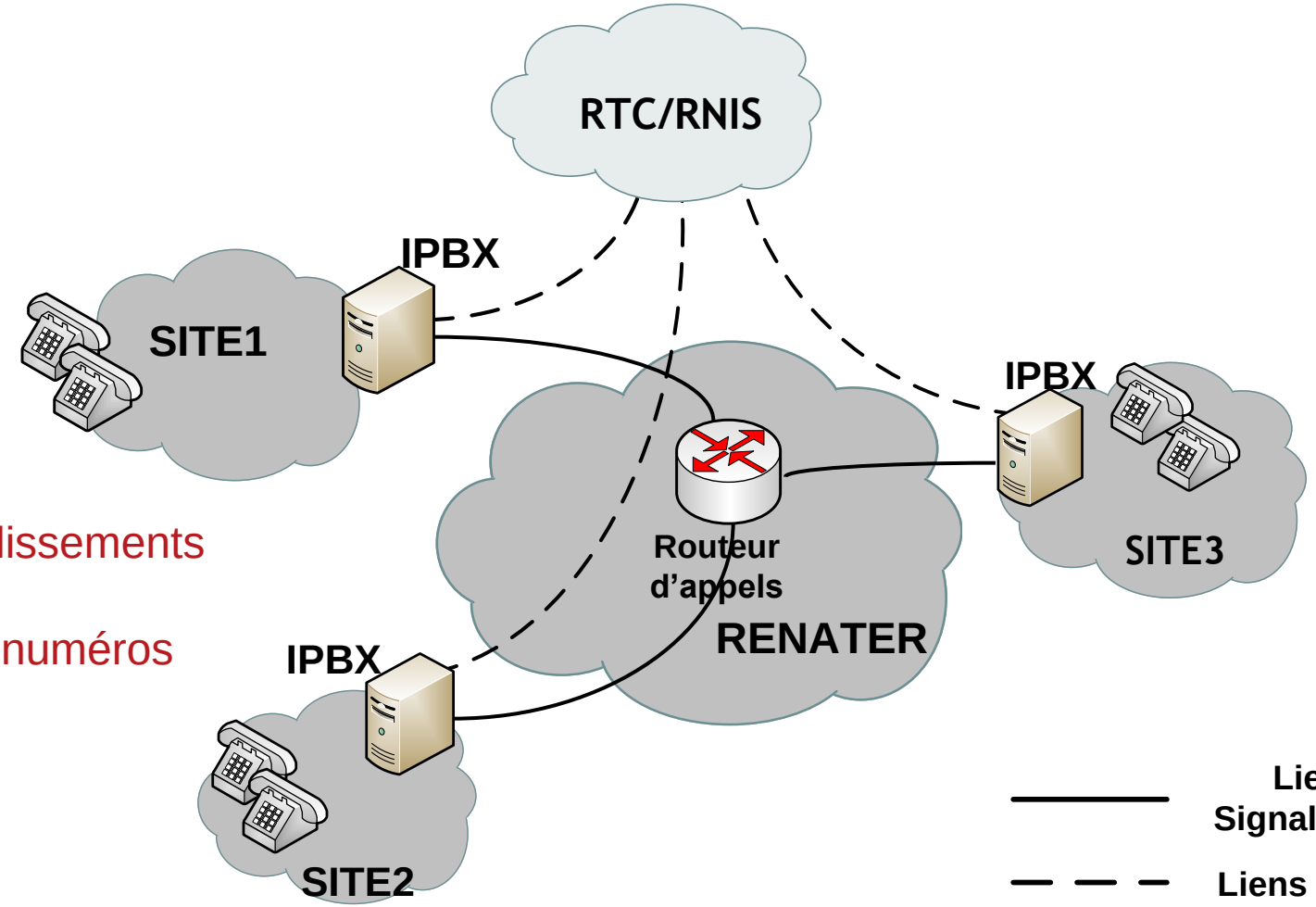
Gatekeeper

EVO

- Enabling Virtual Organizations
- Visioconférence sur poste de travail
  - Multi-participants
  - Outils de web-collaboration (partage de fichiers, écran…)
- 4 réflecteurs sur RENATER (inc. UPMC)
- Support technique

- **www.renater.fr/evo**
  - Création du compte utilisateur
  - Téléchargement du client « Koala »
  - Pré-configuration optimisée pour RENATER

ToIP



~15 établissements

25 000 numéros

ToIP

- Les informations à fournir pour se connecter au service :
  - Le nom DNS du proxy SIP du site
  - Les plages de SDA utilisées par le site
  - Le site doit justifier qu'il est bien « propriétaire » de ces SDA
  - La demande doit émaner du correspondant technique du site
- **www.renater.fr/toip**

- Tableau de bord disponibles tous les mois

Routage des appels

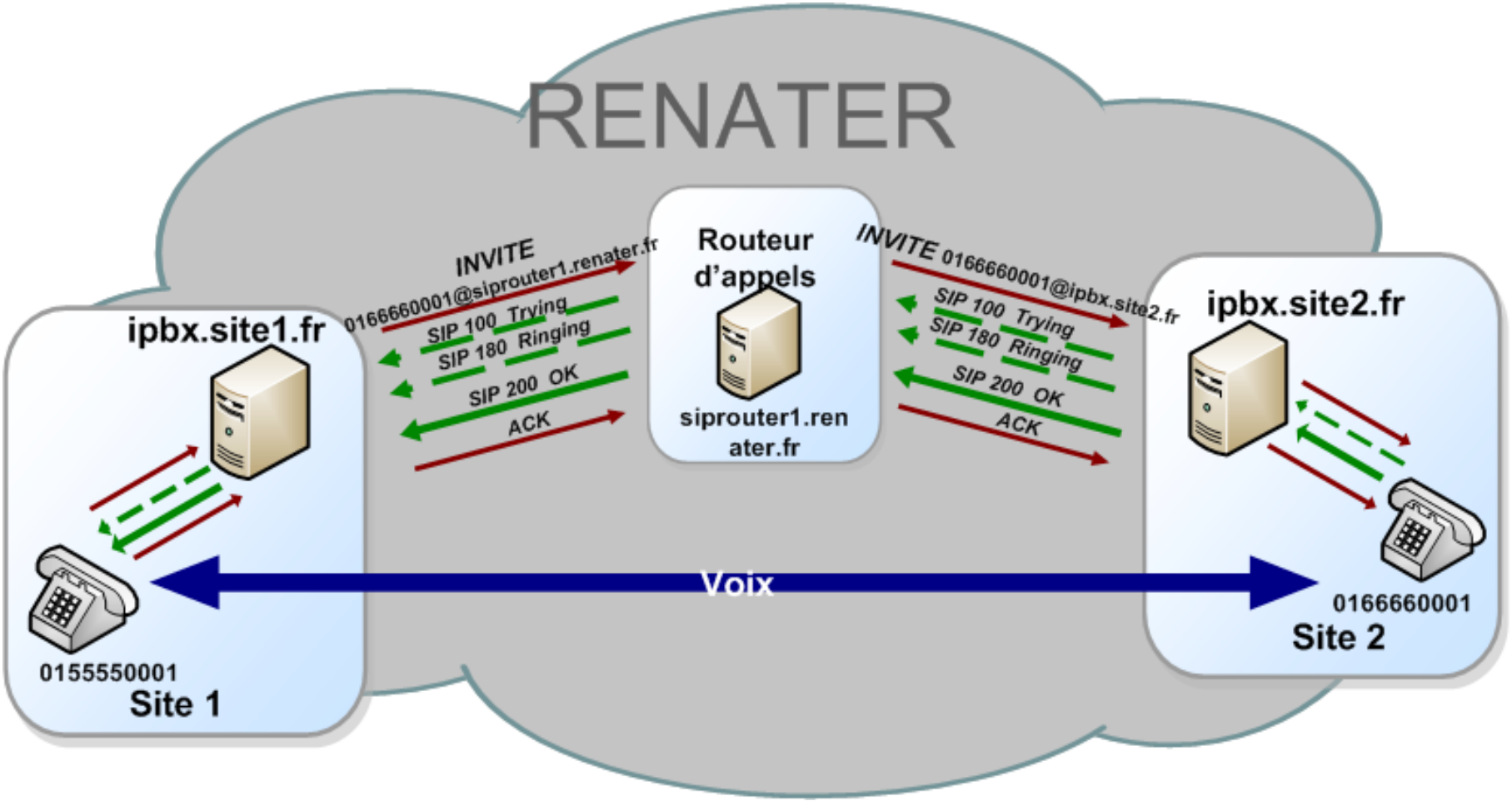
- Principe:
  - Proxy SIP au niveau du site
  - 2 routes à configurer au niveau du proxy SIP:
    - une route principale vers le routeur d'appels de RENATER ;
    - une route secondaire vers l'opérateur du lien RTC/RNIS.

  - Cette configuration simple au niveau du site permet de garder un accès de secours et de basculer vers celui-ci si nécessaire.

- 3 cas de figure se présentent:
  - Le numéro appelé est raccordé au service pilote ET **le site est joignable**
  - Le numéro appelé est raccordé au service pilote ET **le site n'est pas accessible**
  - Le numéro appelé n'est pas raccordé au pilote

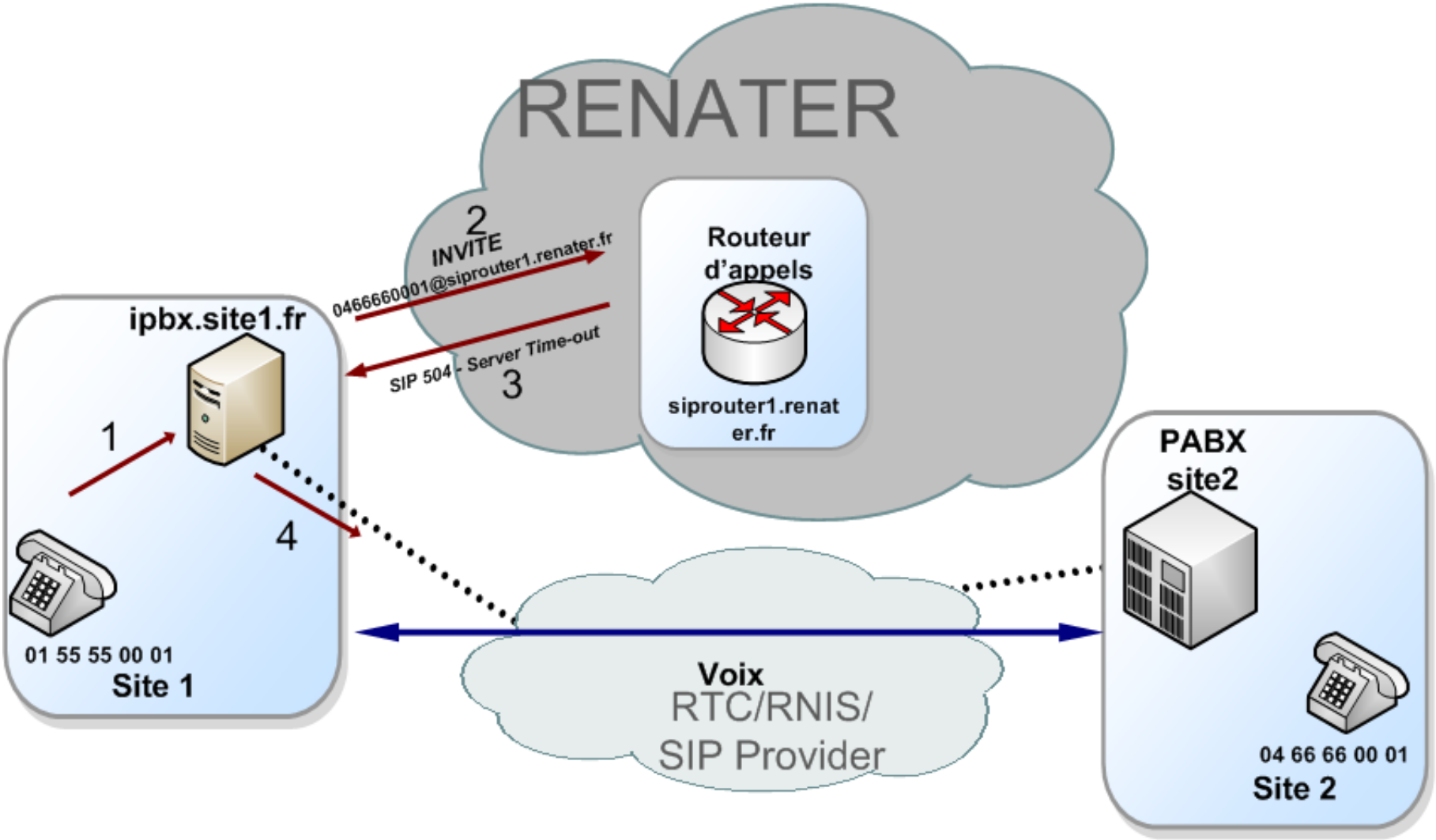
Routage des appels (1)

Le site appelé est raccordé au pilote et joignable



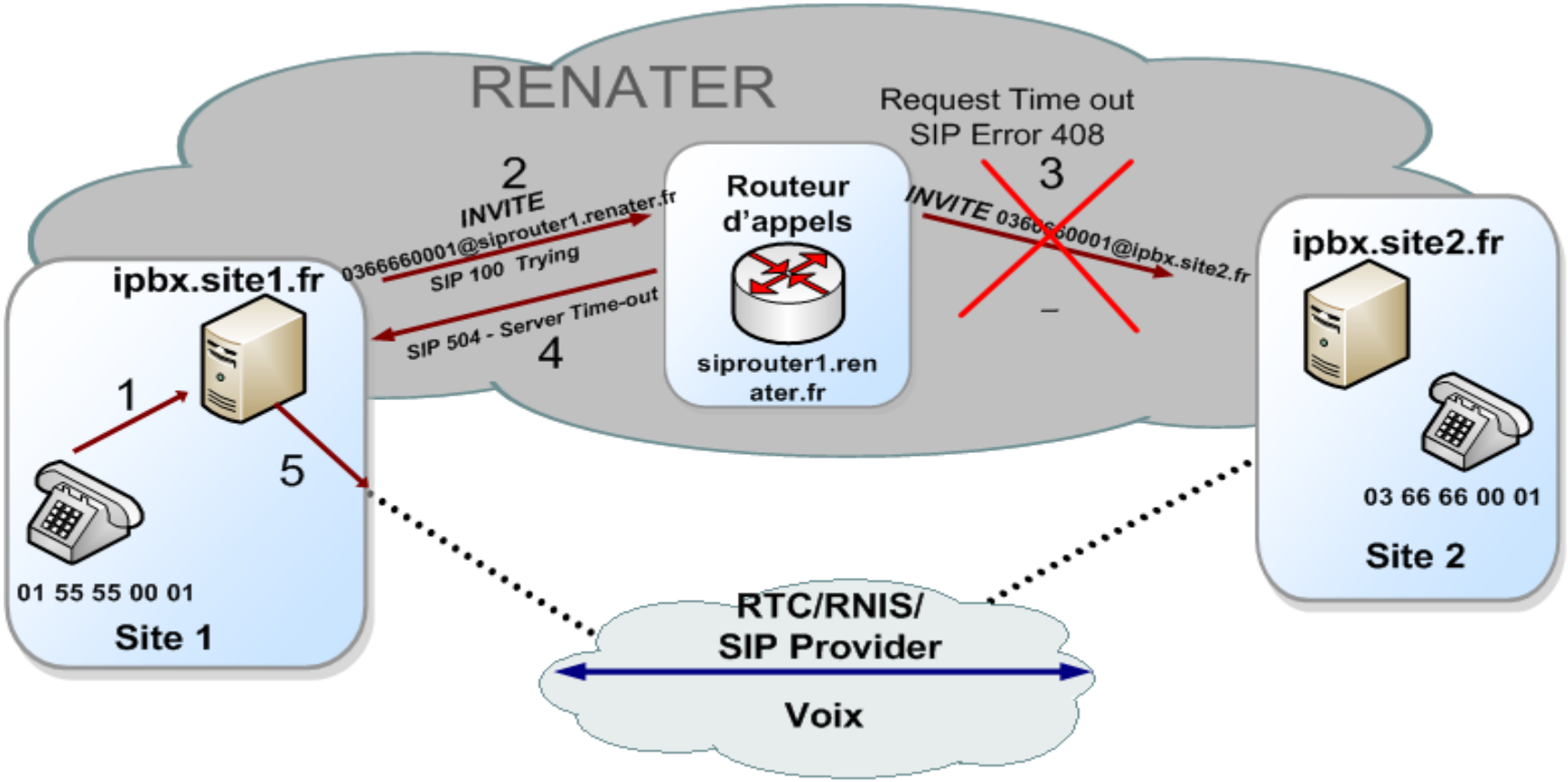
Routage des appels (2)

Le site appelé n'est pas raccordé au pilote

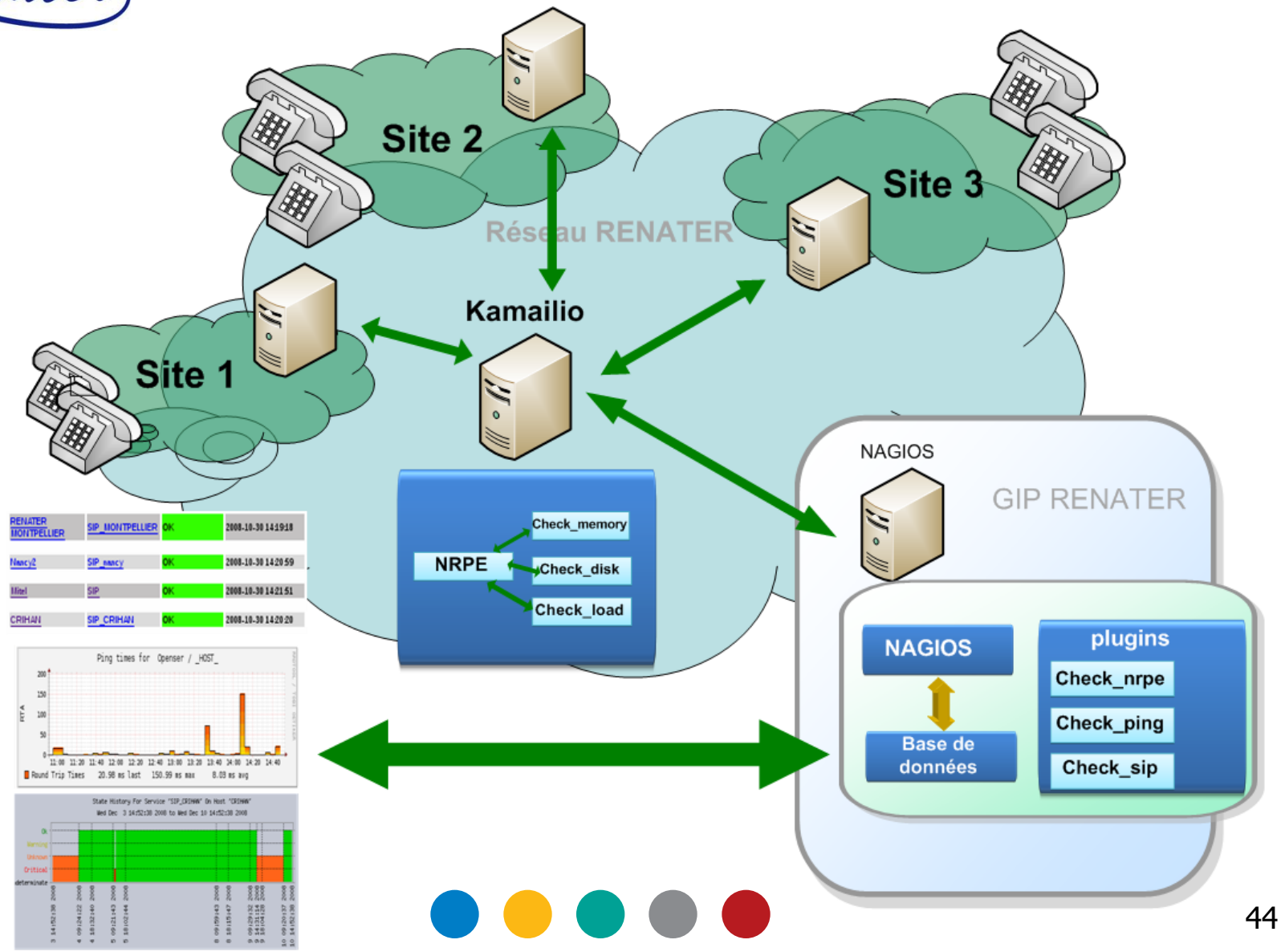


Routage des appels (3)

Le site appelé est raccordé au pilote mais il est injoignable



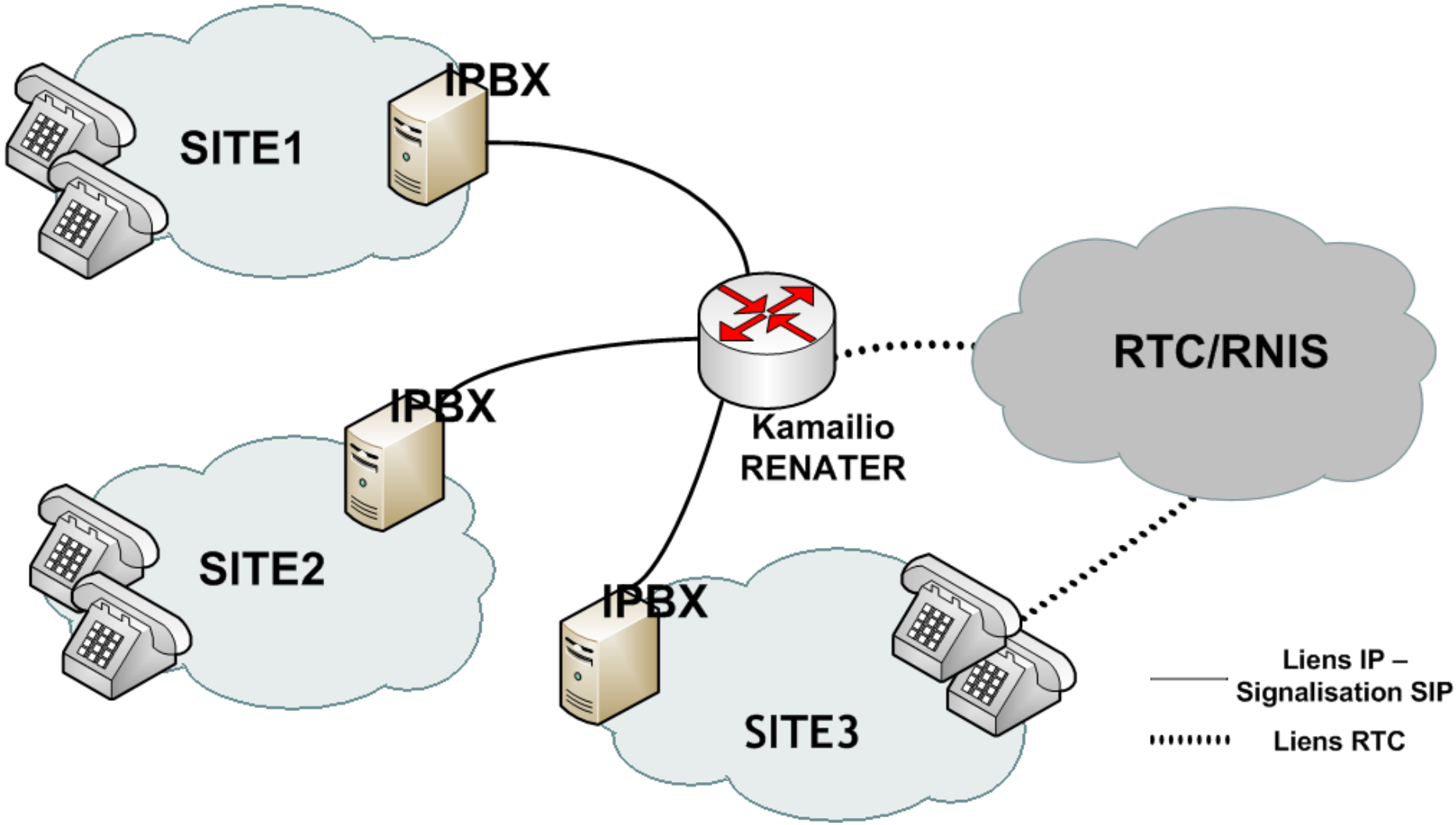
Supervision du service pilote



La comptabilisation des appels

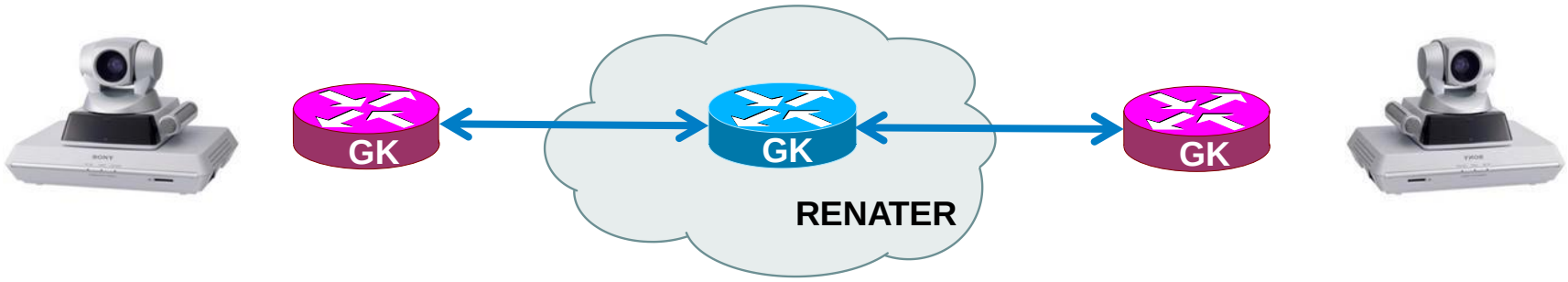
- Solution permettant de faire :
  - des statistiques sur les appels (réussis et échoués)
  - le suivi de ces statistiques dans le temps
  - l'agrégation des statistiques pour connaître l'usage du service pour chaque site.
- Solution basée sur:
  - Le module *ACC* de *Kamailio*
  - *Couplé avec freeRadius* et *MySQL*
- Une interface web développée en interne permet de visualiser ces informations

Mutualisation des accès téléphoniques



H323

- Interconnexion de gatekeepers H323
  - Numérotation E164
  - Pour les salles de visio H323



- **www.renater.fr/h323**

H323

- Pont de visioconférence
  - Upgrade du MCU de l'IN2P3
    - Cofinancement INRA / RENATER / INSERM
  - Pont largement utilisé dans la communauté
  - Outil de réservation du pont de visioconférence
  - http://rms.in2p3.fr

Middleware

SAML

Edugain

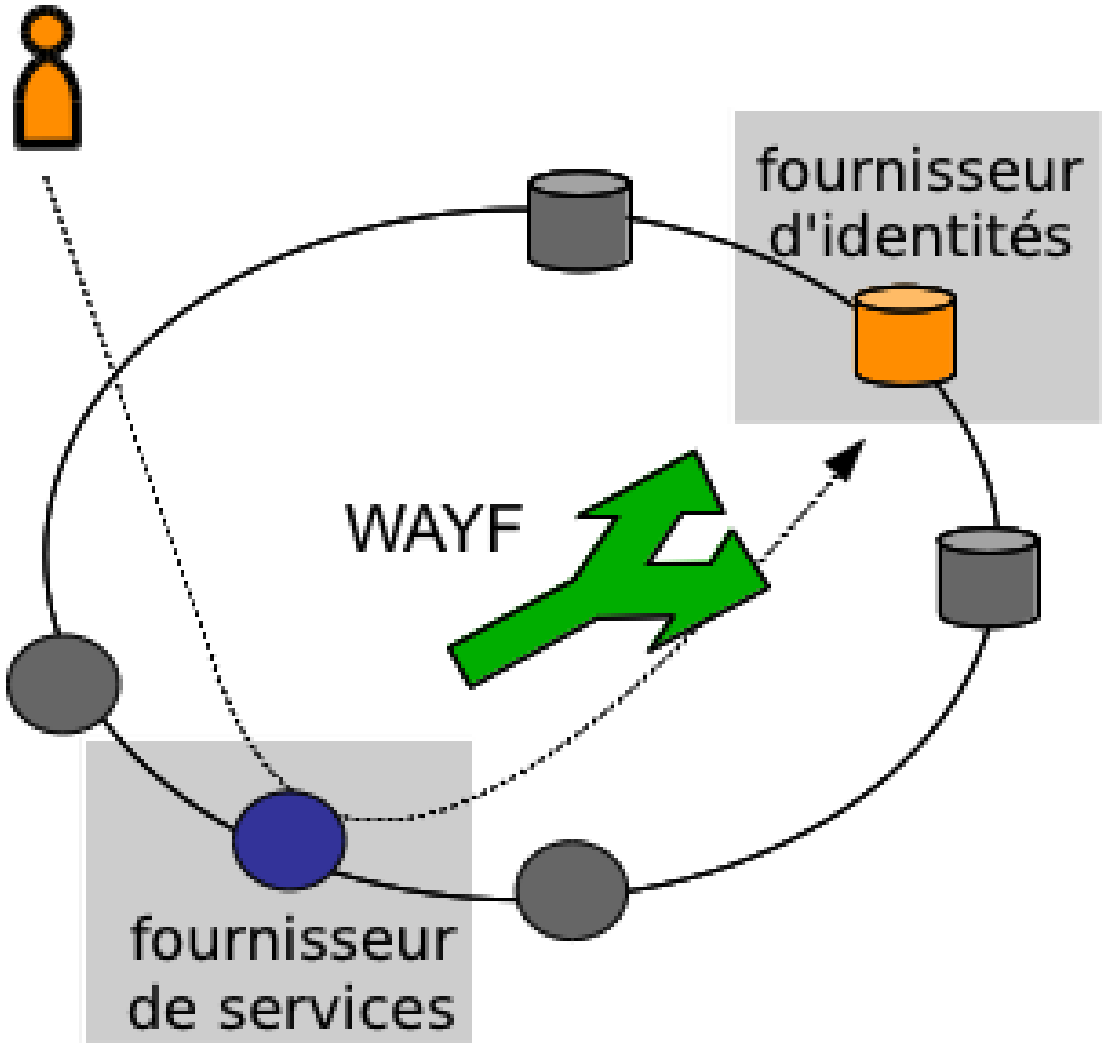
Shiboleth

Fédération Education-Recherche

La Fédération Education-Recherche

- **Infrastructure nationale**
- Basé sur une **authentification web**
- Mécanismes de **fédération d'identités**
- Utilisant le logiciel **Shibboleth**
- Implémente le protocole **SAML**

Fédération / comment ça marche ?



Fédération / deux rôles

- Fournisseur d'identités (IdP)
  - Service d'authentification web
  - Une instance par établissement
- Fournisseur de services (SP)
  - Consomme des identités
  - En amont d'une application/service
  - N instances par établissements

Fédération / Qui l'utilise ?

- En France
  - 98 fournisseurs d'identités
  - 136 ressources enregistrées
  - Des ressources locales pas enregistrées

- Dans d'autres pays
  - https://federation.renater.fr/docs/autres_federations
  - Interopérables mais pas encore connectées

Fédération / Les usages

https://services-federation.renater.fr/liste?action=view_all&type=sp&federation=renater

- Ressources documentaires
- E-learning
- Accès Wi-Fi
- Applications métier mutualisées
- Applications nationales
- Extranet
- Distribution de logiciels
- …

Fédération / comment s'inscrire ?

- Activer le service fédération auprès de RENATER
  - Via SAGA
  - Déclaration de deux contacts fédération
  - Mise à jour de l'agrément RENATER
- Inscription technique
  - D'un IdP ou d'une ressource
  - Déclaration des informations techniques
  - Validation et diffusion

Fédération / formation et support

- Formation
  - Supports et vidéo sur le site web
  - Formations régulières

- Support
  - Site web www.renater.fr/federation
  - Liste federation-utilisateurs@cru.fr
  - fed-contact@ml.renater.fr

Mobilité

Eduspot

eduroam

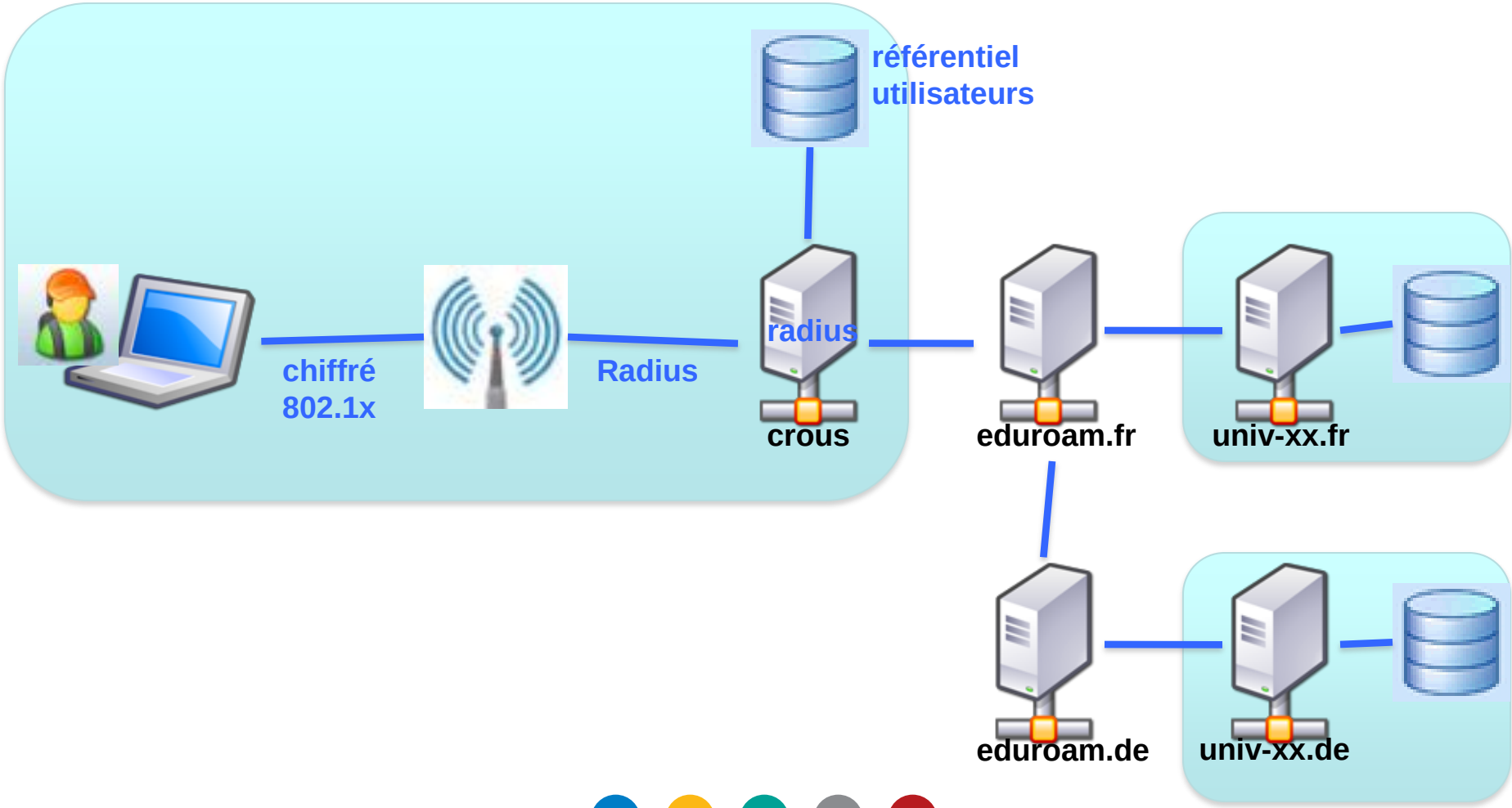
Wi-Fi

802.1X

eduroam pour l'utilisateur

- C'est une connexion Wi-Fi
  - Sécurisée (802.1x)
  - Utilisable dans son établissement d'origine
  - Utilisable dans d'autres établissements
  - Utilisable à l'étranger
  - Saisie de son login habituel
  - Configuration initiale du poste utilisateur

eduroam / comment ça marche ?

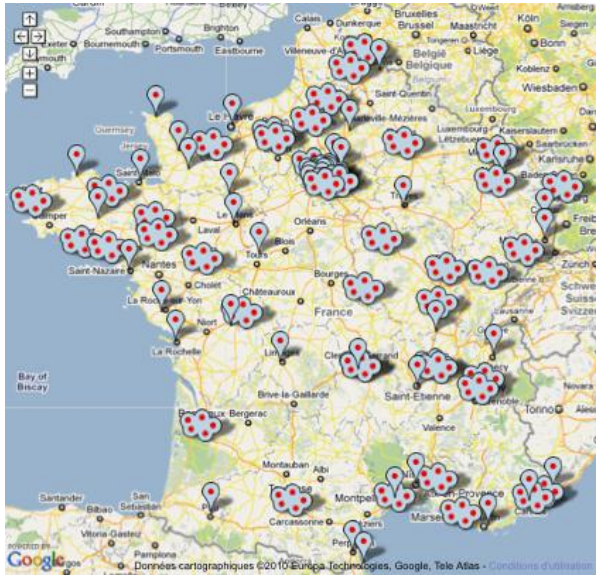


eduroam / qui fait quoi ?

- Infrastructure internationale
  - **Europe**, USA, Canada, Asie
  - Serveur radius racine
  - Organisation financée par Geant
- eduroam.fr
  - Opéré par le CRU, pour RENATER
  - Un serveur radius proxy national (+backup)
- Les établissements
  - Opèrent un serveur radius pour leurs utilisateurs
  - Proposent des points d'accès Wi-Fi

eduroam / qui l'utilise ?

- 129 établissements français membres
  - 283 sites déclarés
  - Plus de 100.000 logins inter-etab fin 2010
- Europe
  - 36 pays couverts
  - 800+ org membres
  - 3000 sites déclarés



eduroam / comment participer ?

- Partie administrative
  - Activer le service mobilité auprès de RENATER
    - SAGA
  - Déclarer un contact eduroam
  - Signature charte eduroam
    - => Mise à jour agrément RENATER
- Partie technique
  - Un serveur Radius connecté au proxy national
  - Publier le SSID « eduroam »
  - Offrir pages web et support aux utilisateurs
  - Déclarer les sites couvertes + protocole chiffrement

Eduspot / pourquoi ?

- eduroam ne répond pas à 100% des besoins

- Situation selon les établissements
  - eduroam pour tout le monde
  - eduroam pour enseignants et personnel
  - Pas d'eduroam

Eduspot / objectif

- Projet récent du CRU
  - Complémentaire de eduroam
- Objectif
  - Bonnes pratiques pour mettre en œuvre des portails captifs
  - Authentification utilisant la Fédération Education-Recherche
  - Un SSID national

Renater eduroam.fr / WiFi eduspot

	eduroam	eduspot
Sécurité	Flux radio chiffré (802.1x)	Flux radio non chiffré
Authentification	EAP / Radius (via proxies éventuellement)	Fédération d'identités (échange direct utilisateur⇔IdP)
Configuration	Configuration du poste utilisateur	Aucune (lancement navigateur)
Contraintes architecture	Serveur radius + raccordement au proxy	Portail + white list + SP Shibboleth
Ergonomie	Transparent (modulo profil standard)	Pas de configuration du poste. Plusieurs clics. Partage session ENT
Couverture	Internationale (arbre)	Nationale (cercle de confiance)
Comptes invités	Envisageable	Envisageable

Sécurité

CERT

Anti-spam

Anti-virus

Certificats serveurs

Certificats de personne

TCS

Certificats serveurs

- Délivrance de certificats reconnus par les navigateurs
- Un document à signer: lettre d'engagement TCS
- Application en ligne https://tcs.renater.fr
  - Saisir la lettre d'engagement
  - Faire les demandes de certificats
  - Révoquer les certificats
- Service inclus dans la prestation RENATER
  - Pas de coûts pour les usagers

CERT RENATER

- Publication des dernières vulnérabilités
  - Veille
  - Coordination avec les autres CERT
- Détection des attaques sur RENATER
  - A partir d'outils de métrologie
  - Déclenchement éventuel d'actions de mise en sécurité
- Assistance aux contacts sécurité
- Traitement de requêtes
- www.renater.fr/securite
  - certsvp@renater.fr
  - +33 1 53 94 20 44

Support et Contacts

www.renater.fr/support

Contacts administratifs

- www.renater.fr/support

- Suivi administratif de votre agrément (signature, modifications diverses, demande de compte SAGA…)

  agrement@renater.fr

  Mme Hoinville-Antonini : 04 67 16 38 25

  Mme Gomes : 04 67 16 38 23

  Mme Pierne : 04 67 16 38 22

Contacts techniques

- www.renater.fr/support

- Opération de votre connexion (incidents, maintenances...)
  - NOC-RENATER
  - noc-renater@noc.renater.fr
  - 0800 77 47 95
- Demandes de changement techniques
  - GIP RENATER – SSU – Suivi des Services aux Usagers
  - support-reseau@renater.fr
  - 01 53 94 20 40

Des forums d'usagers

- www.renater.fr/support

- Anti-spam - antispam-forum@ml.renater.fr
- Certificats - tcs-forum@ml.renater.fr
- EVO - evo-forum@ml.renater.fr
- Fédération - federation-utilisateurs@cru.fr
- H323 - h323-forum@ml.renater.fr
- Messagerie électronique - smtp-fr@cru.fr
- Multicast - multicast@ml.renater.fr
- Réseau - ip@services.cnrs.fr
- ToIP - toip-forum@ml.renater.fr

www.renater.fr/support