

Déploiement d'une solution de téléphonie IP dans un campus (4 200 postes)

Loïc PASQUIET



PLAN



- ◆ Présentation du projet : contexte, ...
- ◆ Le projet : sa mise en oeuvre
- ◆ Premier bilan / architecture : les composants



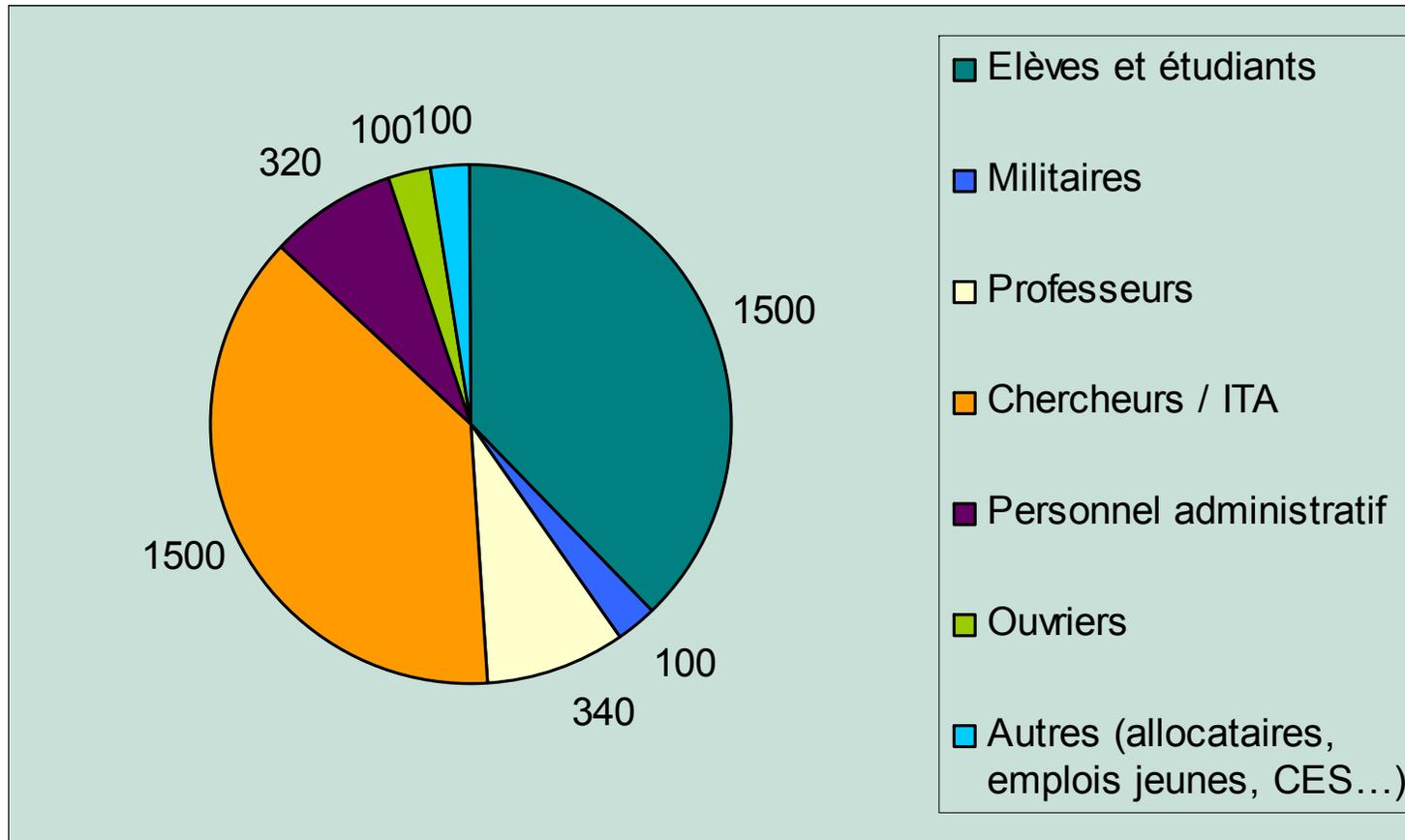
PLAN ... suite



- ◆ La sécurité : les éléments retenus
- ◆ Quelques mécanismes du fonctionnement



Présentation du projet (1)



- . Un réseau informatique récent interconnectant tous les postes de travail
- . Un réseau téléphonique de 4200 postes

~ 4000 personnes



Le projet : sa mise en œuvre (1)

Etude d'opportunité et schéma directeur

➤ Appel d'offres sur performances (PFD)

➤ Maquettage sur deux mois

➤ Mise au point du CCTP

➤ Choix de l'intégrateur-constructeur

SECURITE

- Postes IP
- Vlans
- Niveau 3
- Redondances



Le projet : sa mise en œuvre (2)

Présentation des scénarios étudiés

- **Scénario 1 : tout en technologie voix sur IP (ToIP)**
- **Scénario 2 : tout en technologie numérique conventionnel (TCO)**
- **Scénario 3 : mixte (Résidents en TCO, ERA en ToIP)**

**Le comité exécutif de l'École a choisi
le scénario 1 : le tout IP**



Elements financiers

- Un budget prévisionnel pour la ToIP comparable aux investissements de 1990
- Couvre l'architecture (voix/data), les 4200 postes, les prestations et la maintenance
- 300 euros par abonné dont 100 euros de poste



Le projet : sa mise en œuvre (3)

- 2005 : système pour 1600 postes et 600 postes en production,
- 2006 : les 1000 résidents actuels,
- 2007 : extension du système à 4200 postes et équipement de la recherche (1600 postes),
- 2008 : équipement enseignement et administration (1000 postes)

=> arrêt PABX



Premier bilan (1)

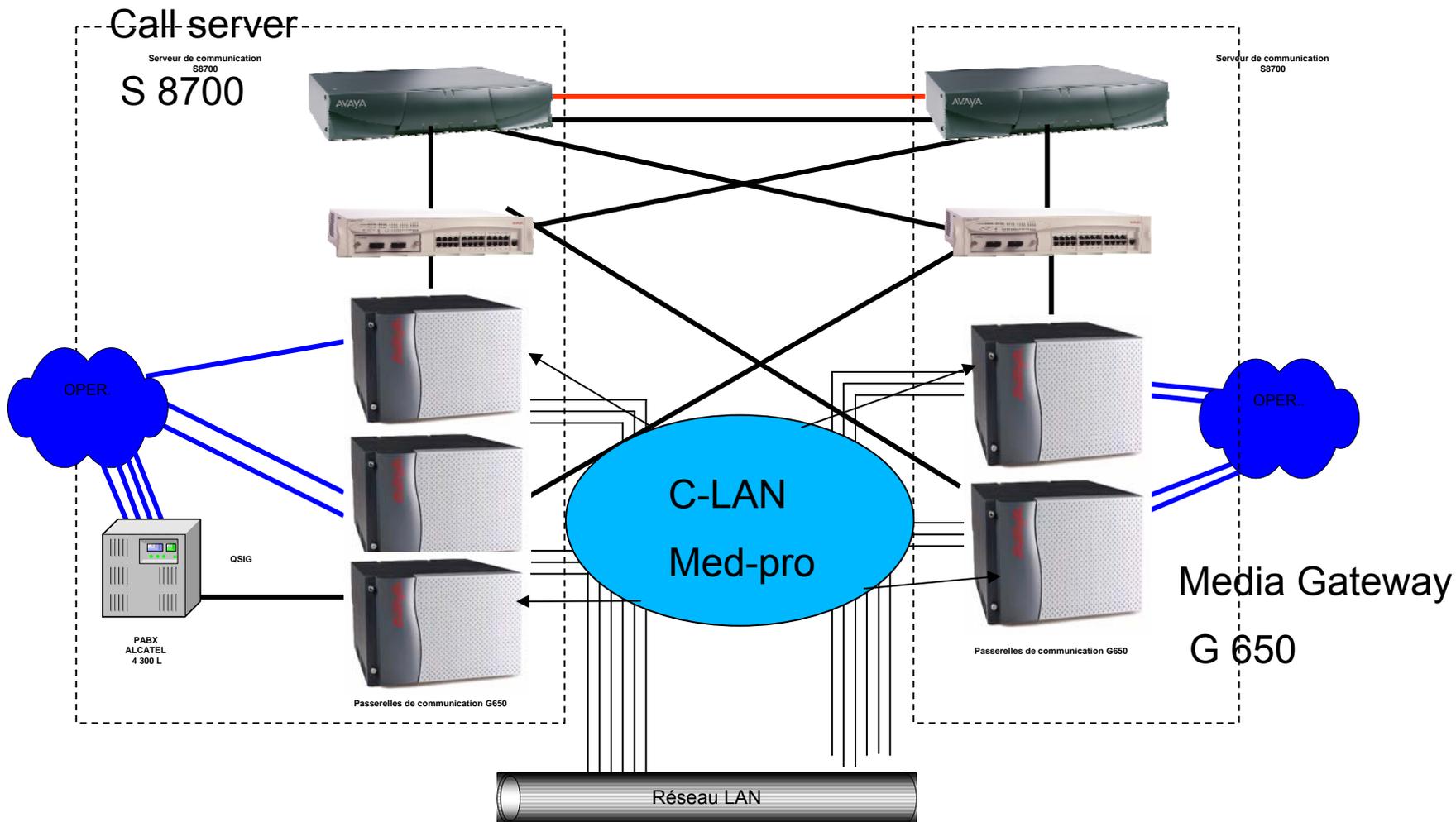
Quelques éléments ...

- 2 salles télécoms redondantes
- Architecture du transport de la voix séparée
- 600 postes en production, 1600 à l'été
- Interconnexion QSIG à renforcer
- Audit externe ToIP favorable
- Régions téléphoniques



Premier bilan : architecture ToIP (2)

Configuration cible 4 200 Postes IP



La sécurité (1)

- Garantir la continuité de service par la mise en place d'une protection contre:
 - Les défaillances de liens physiques ou d'équipements
 - Les attaques
 - La dégradation de la qualité de service (QoS)
- Empêcher les écoutes téléphoniques

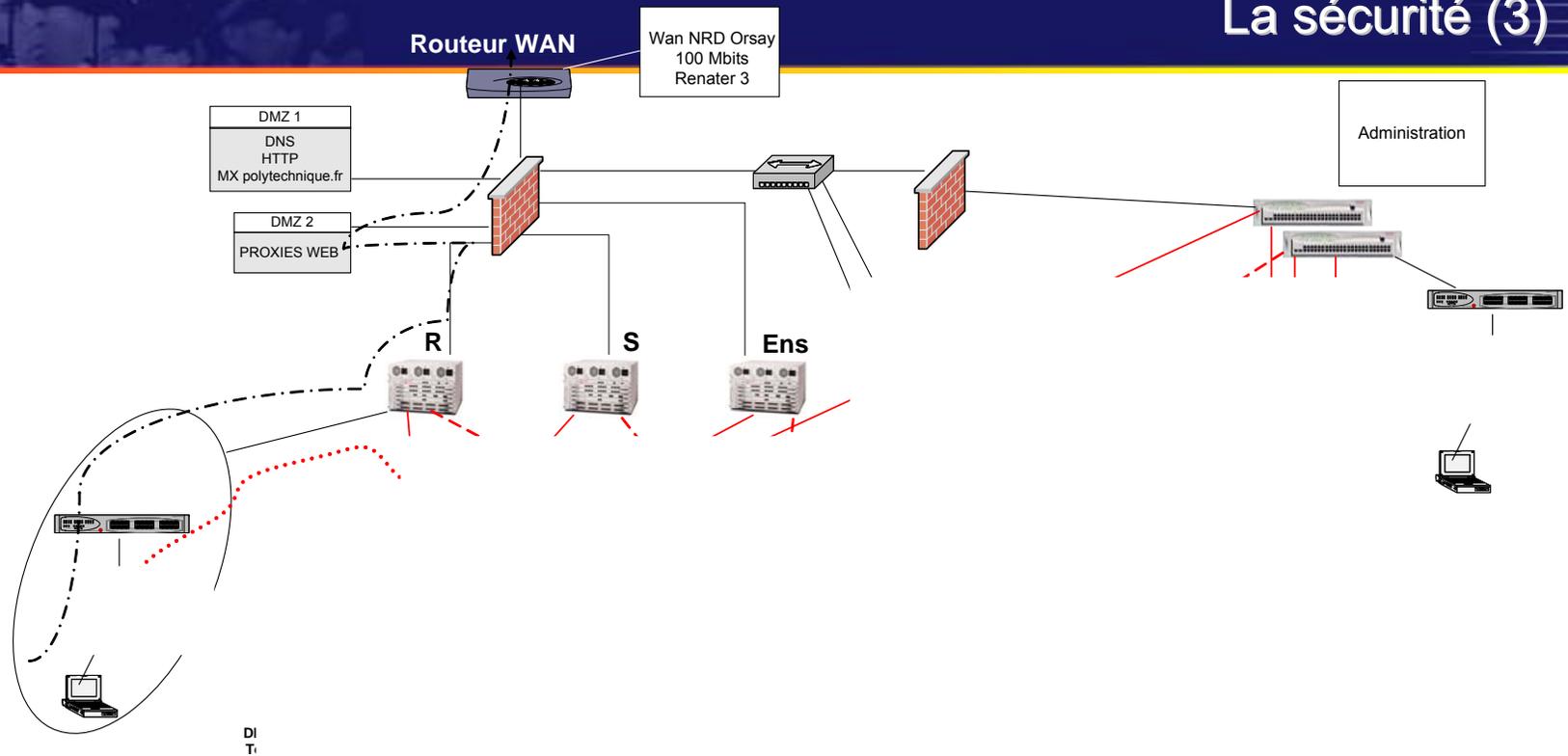


- Secours électrique (onduleurs dans tous les locaux techniques)
- 802.3af (alimentation par la prise RJ45)
- Redondance des call servers
- Redondance des passerelles par défaut des téléphones : **VRRP**
- Redondance des liens optiques : **EAPS**



Schéma du réseau voix / données

La sécurité (3)

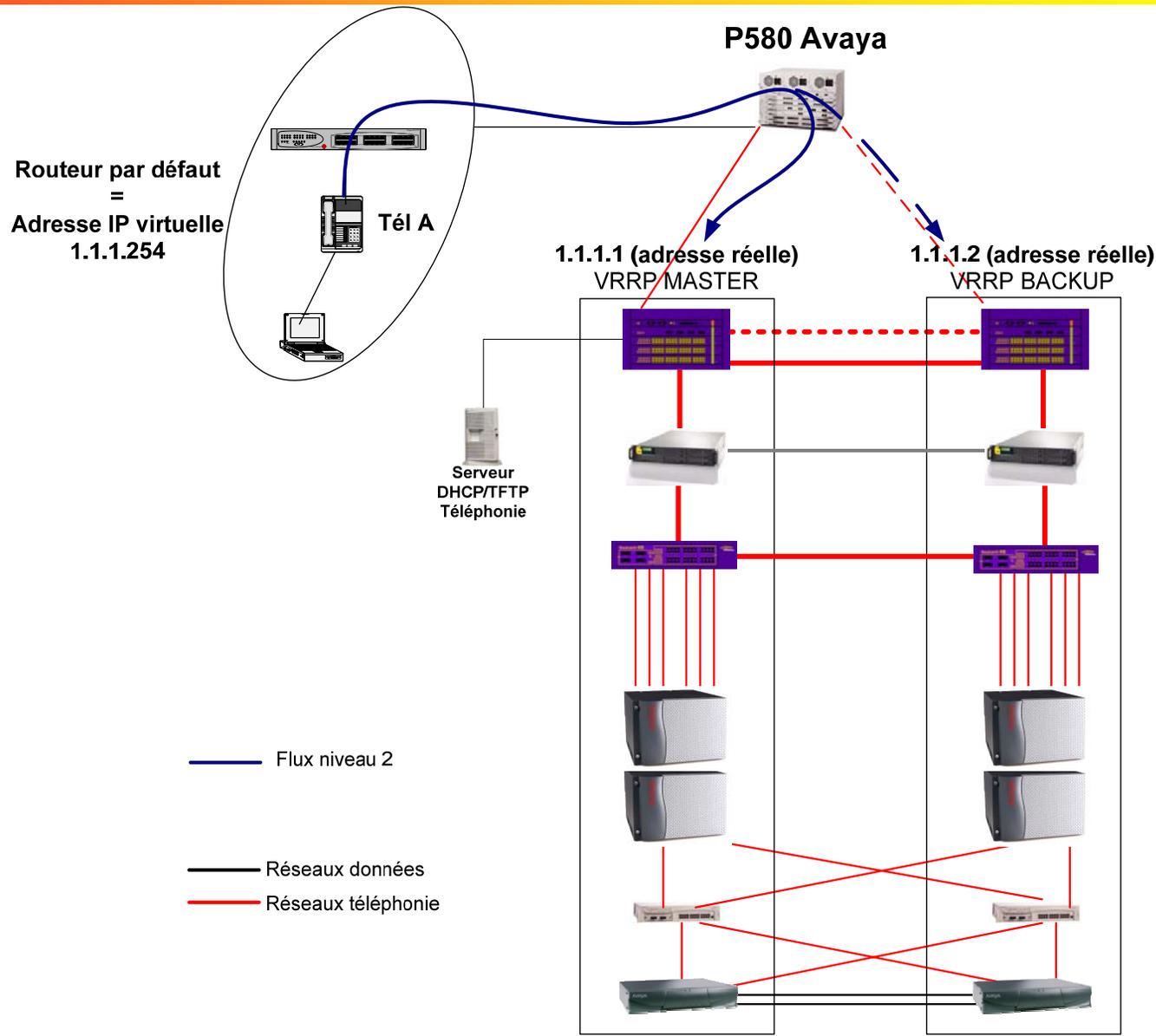


— Réseaux données
— Réseaux téléphonie



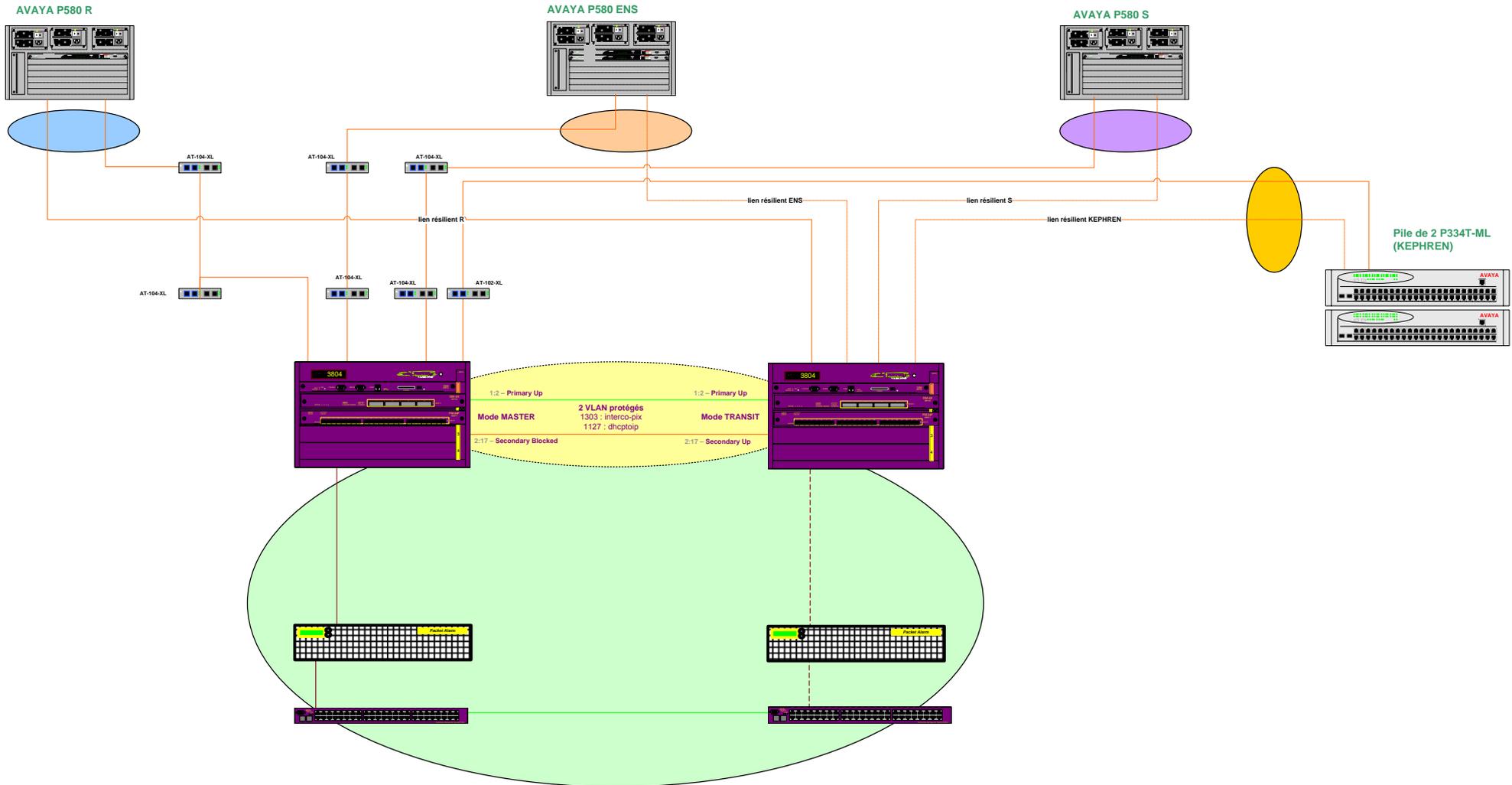
Redondance du routeur par défaut VRRP (RFC 2338)

La sécurité (4)



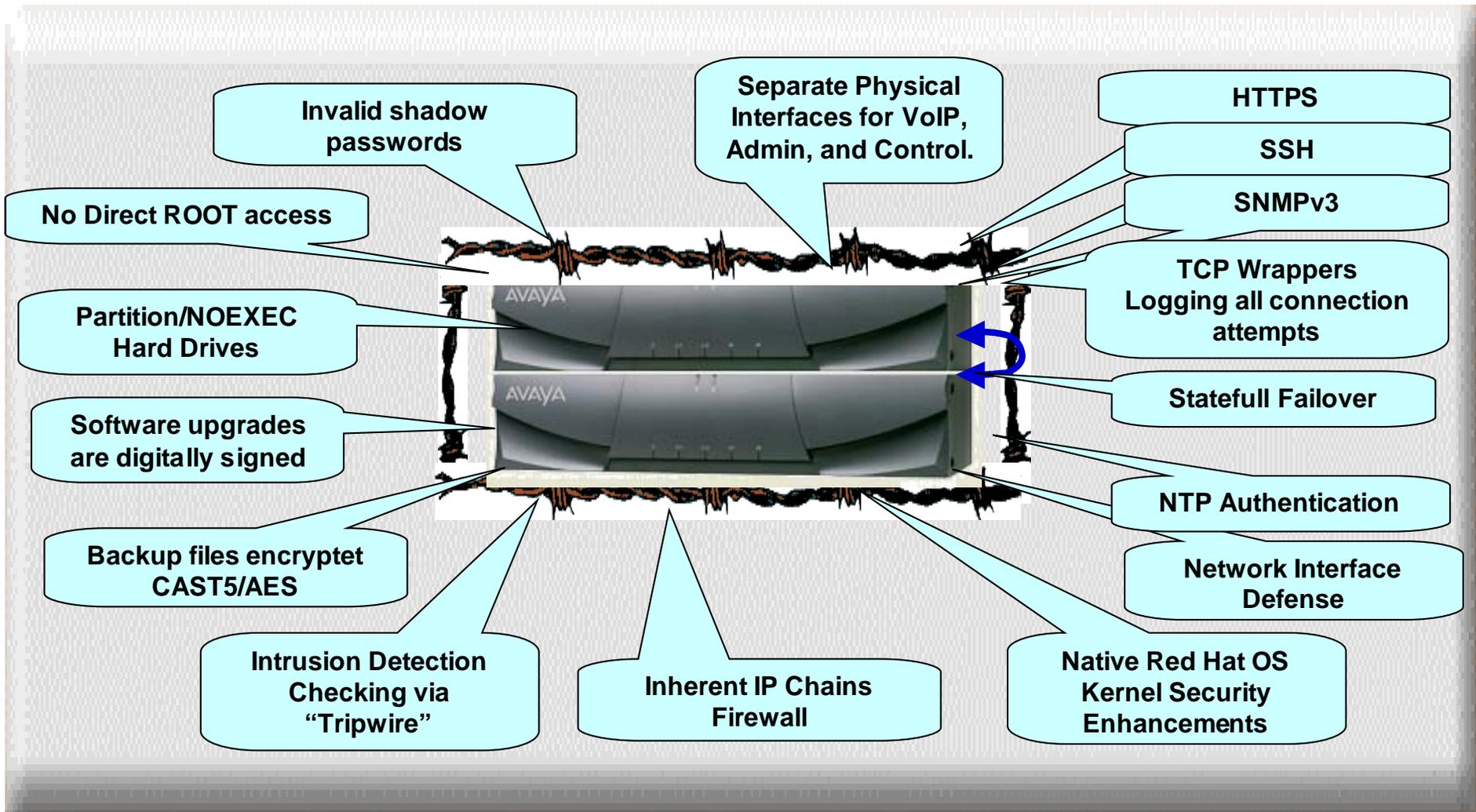
Boucles EAPS (RFC 3619) : convergence <50ms

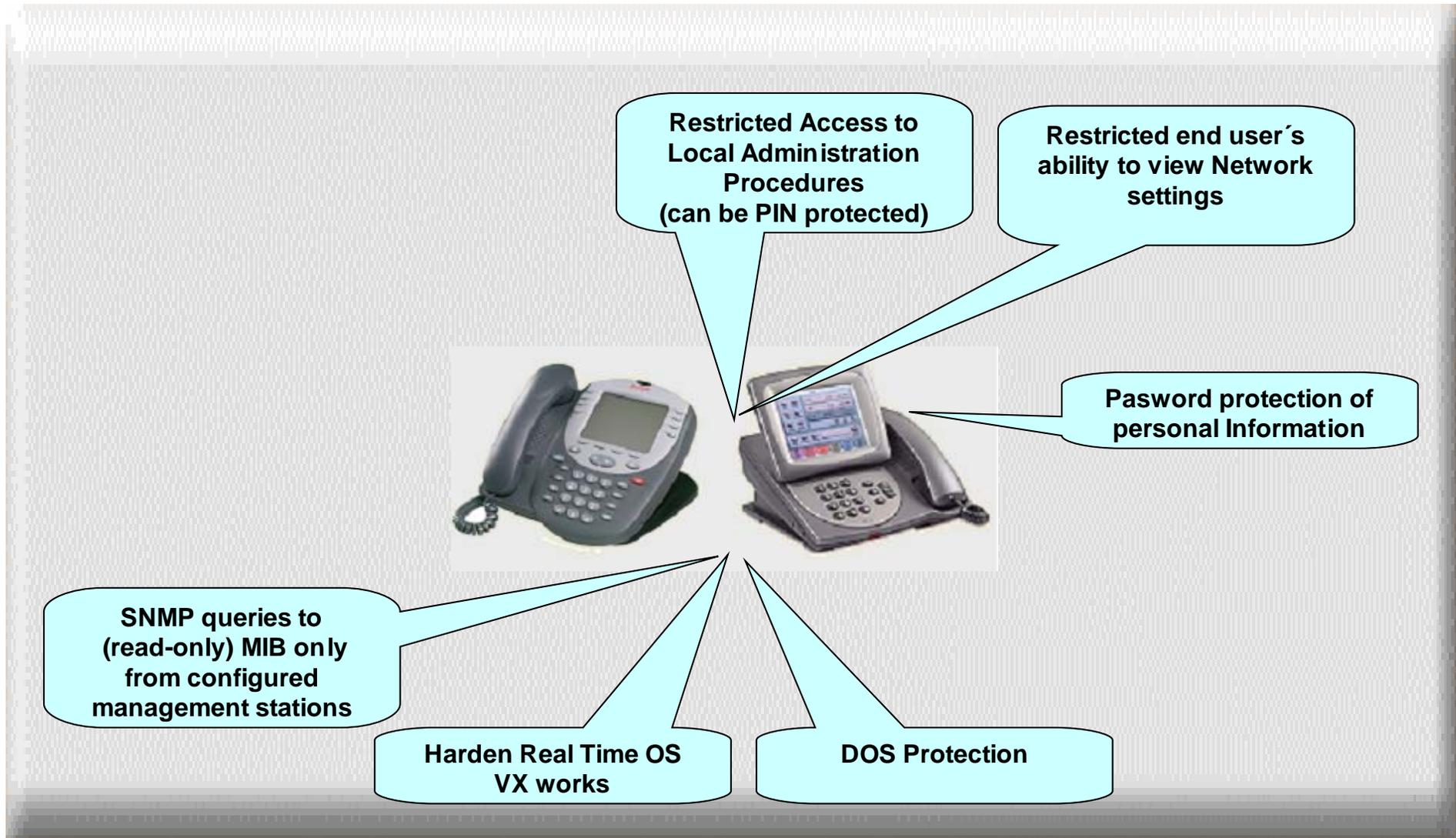
La sécurité (5)



- Code téléphonique renforcé
- Séparation des VLAN voix/données
- Quadruplet de protection (@MAC-PORT-VLAN-IP), 802.1x (été 2006)
- Sonde Intrusive Packet Alarm, filtrage L4
- Call Servers avec unix épuré
- Bus TDM entre G650 et CallServer (pas de trafic IP possible)
- Régions téléphoniques « étanches »



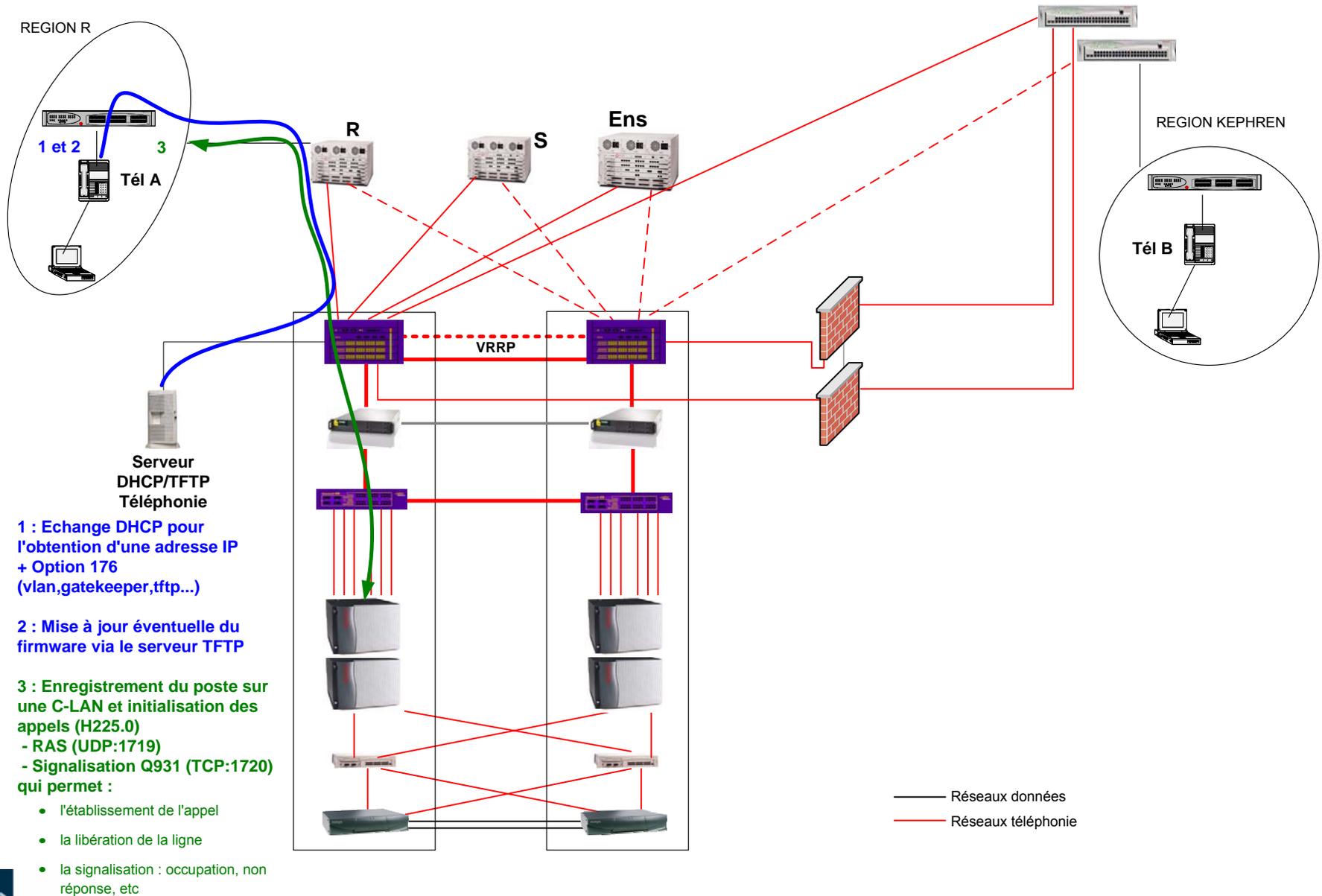




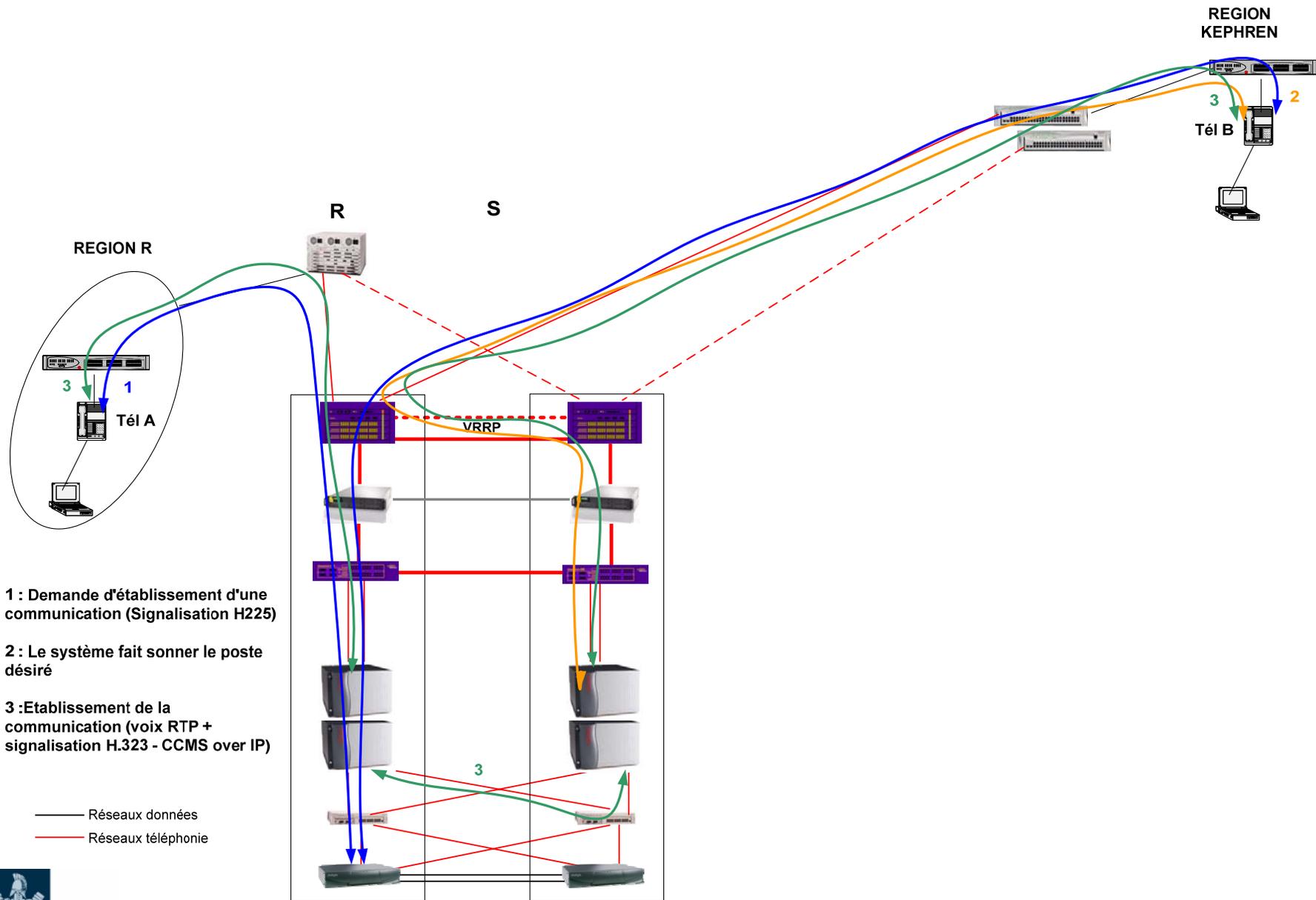
- Chiffrement du payload des packets RTP (contenant de la voix numérisée)
- AEA (Advanced Encryption Algorithm)
RC4-104 bits
- AES réduit de 25% le nombre de communications simultanées assuré par un même codec...
...mais plus le cas bientôt.



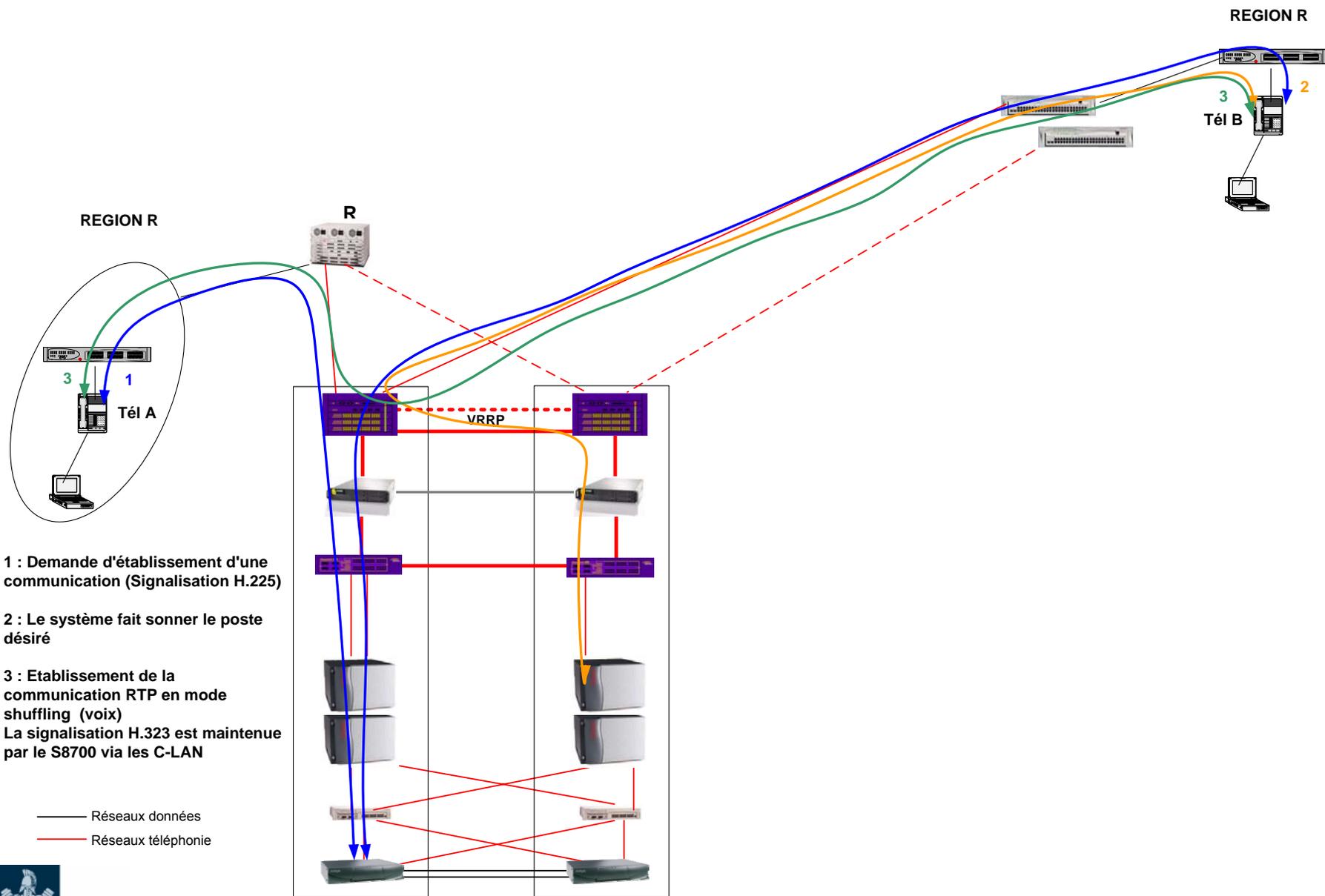
Les mécanismes : démarrage ... (1)



Les mécanismes : communication Inter-Régions (2)



Les mécanismes : communication Intra-Régions (IP-IP) (3)



Bibliographie

- Security Alliance de la voix sur IP.
<http://www.voipsa.org>, crée fin 2004.
- National Institute of Standards and Technology, Special publication 800-58, Security Considerations for Voice over IP Systems, January, 2005
<http://csrc.nist.gov/publications/drafts/>.
- <http://www.avaya.com/gcm/master-usa/en-us/resource/assets/applicationnotes/av-iptel-imp-gd-cm21-0804.pdf>
- <http://www.afutt.org>



DES QUESTIONS ?

