

Réflexions sur :
Connexion OutOfBand mobile sécurisée

Laurent FACQ

facq@u-bordeaux.fr

Directeur Technique & Responsable Sécurité



www.reaumur.net

REseau Aquitain des Utilisateurs des Milieux Universitaire et de Recherche

Version du 4/20/05 07:39:11 am

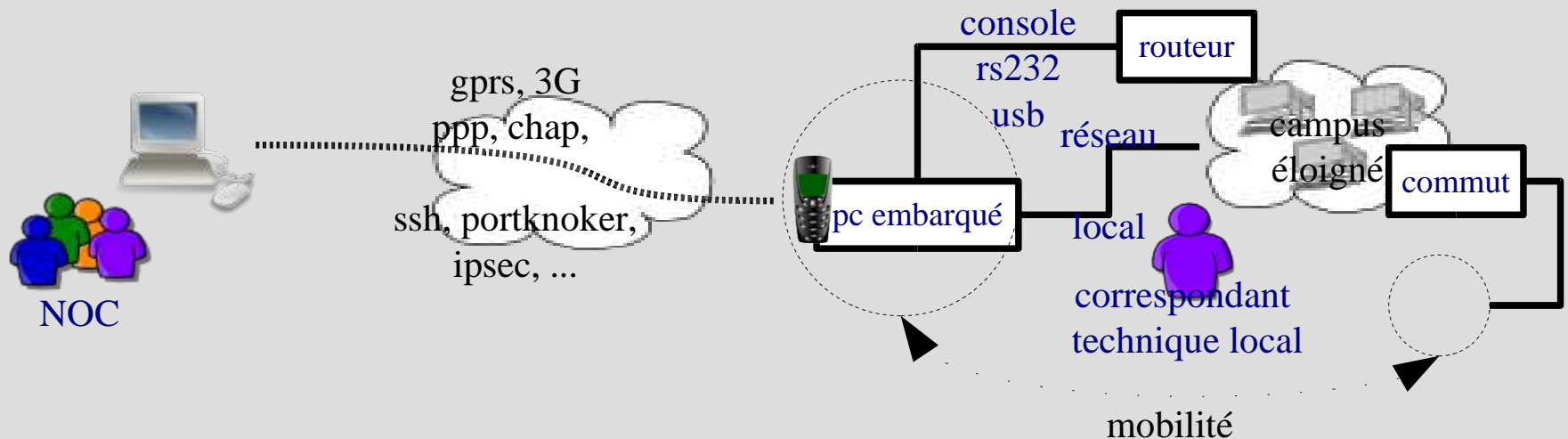


Contexte

- REAUMUR : Un réseau régional Aquitain enseignement recherche, qui s'étend sur plusieurs sites sur plusieurs campus éloignés
(<http://www.reaumur.net>)
 - Une équipe d'ingénieur centralisée
 - Des correspondants techniques présent sur chaque campus
 - En cas de problème, ou simplement pour mettre à jour les équipements réseau en toute sécurité, un déplacement sur place est indispensable => délais et coûteux en temps de transport.
 - Des connexions OutOfBand permanente sur chaque équipement distant, répartis sur le campus distant, ne se justifient pas ou ne sont pas toujours possible simplement.
- Idée : un système de connexion OutOfBand mobile sur chaque campus distant pouvant être déplacé sur demande au correspondant local afin de donner accès à n'importe quel équipement du campus en port console et réseau local.

Objectif

- Boitier de prise de main à distance sur équipements réseaux ayant les caractéristiques suivantes :
 - équipement mobile
 - “OutOfBand” via le port console et via réseau local
 - connexion sans fil (type téléphonie mobile)
 - totalement sécurisé sur la partie sans fil au niveau applicatif (authentifié, chiffré)
 - utilisant des logiciels libres (linux, ppp, ssh, ipsec...)
 - sur mini pc embarqué sans disque (type soeckris)





Exemple de procédure mise à jour de firmware a distance

1. demander la mise en place du boitier
2. vérifier que l'outofband fonctionne bien et se trouve raccordé au bon équipement
3. par précaution : charger le firmware sur le boitier via le réseau (et non via la connexion sans fil)
4. faire la mise à jour via le réseau classique
5. en cas de problème
 1. se connecter en out of band
 2. si besoin, recharger le firmware via outofband en utilisant celui sauvegardé au préalable



Divers

- En temps normal, le boitier est raccordé au réseau local du campus et sur le port console de l'équipement d'accès du site
 - permet de contrôler en permanence le bon fonctionnement du boitier
 - permet d'intervenir en OutOfBand sur le site distant pour diagnostique en cas de rupture de la liaison principale.



A voir...

- Existence de solutions satisfaisantes ?
- Un téléphone mobile peut-il se faire appeler pour une connexion data (gprs...) ?
- Existence de contrat téléphonie mobile moins cher pour réception d'appel data uniquement ?