Déploiement sécuritaire de la téléphonie IP

Simon Perreault

Viagénie

{sip,mailto}:simon.perreault@viagenie.ca

http://www.viagenie.ca

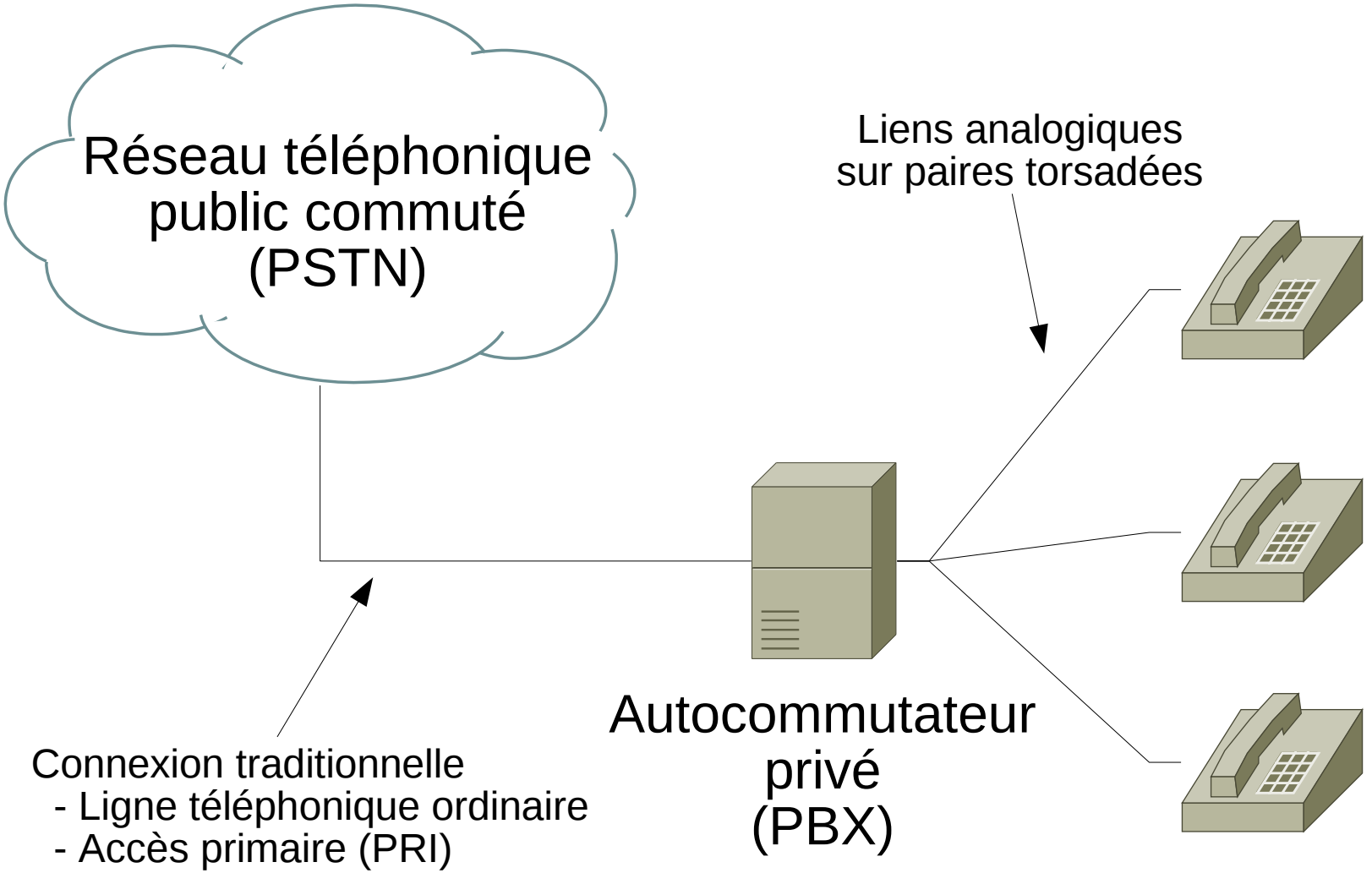
À propos du conférencier

- Consultant en réseautique et VoIP chez Viagénie
- Co-auteur du port de Asterisk à IPv6 (voir http://www.asteriskv6.org)
- Auteur du port de FreeSWITCH à IPv6 (intégré depuis version 1.0.1)
- Auteur de Numb, un serveur STUN/TURN (voir http://numb.viagenie.ca)
- Co-auteur de la spécification TURN-TCP de l'IETF
- Participation à AstriCon, ClueCon, SIPit, IETF, etc.
- Développé plusieurs applications VoIP sur mesure

Plan

- Retour sur la téléphonie traditionnelle
- Introduction à la téléphonie sur IP
- Scénarios de déploiement
  1. Remplacement du système téléphonique traditionnel
  2. Accès au PSTN via IP
  3. Interconnexion de succursales
  4. Télétravail / Itinérance
- Déploiements typiques
- Conclusion

Téléphonie traditionnelle



Caractéristiques de la téléphonie traditionnelle

- Centralisation
- Fiabilité
  - Avez-vous déjà vécu une panne de téléphone?
- Pierre angulaire de la sécurité: le contrôle du réseau
- Écouter une conversation
  - Technologie simple
  - Accès au réseau
- Changement d'identité (*caller ID*) possible avec ISDN
- Déni de service

La Téléphonie IP

Ce que ce n'est pas

- Téléphonie IP ≠ Téléphonie Internet
  - IP est seulement un protocole de réseau.
  - IP peut être utilisé en vase clos.
- Skype, MSN, etc.
  - Protocoles propriétaires, secrets et non normalisés
  - Faible disponibilité de matériel
  - Mode d'utilisation différent de la téléphonie traditionnelle
- La même chose, en moins cher
  - Technologie radicalement différente
  - Les scénarios de déploiement vont du semblable à l'incomparable.

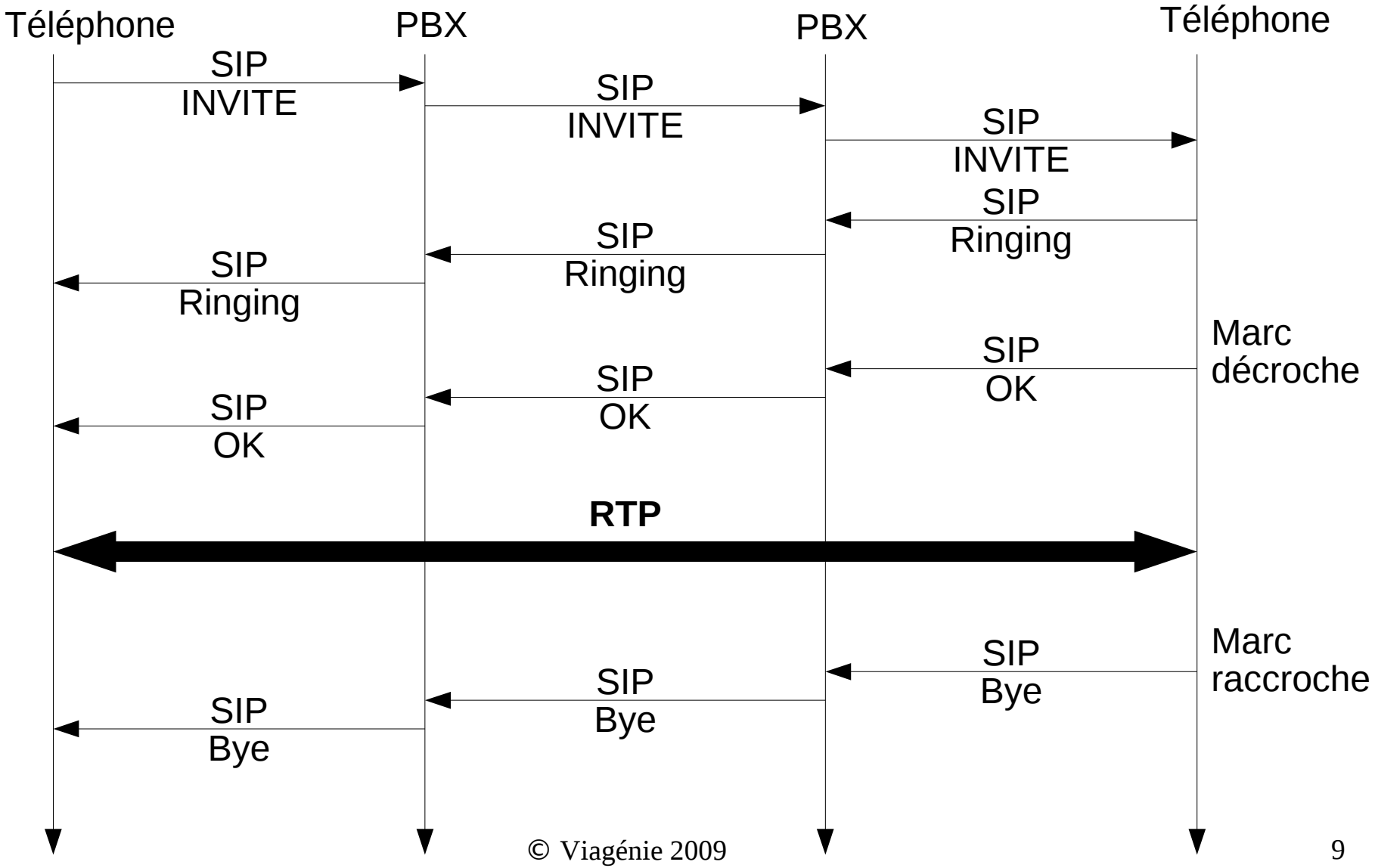
SIP (*session initiation protocol*)

- Inspiré de HTTP et SMTP

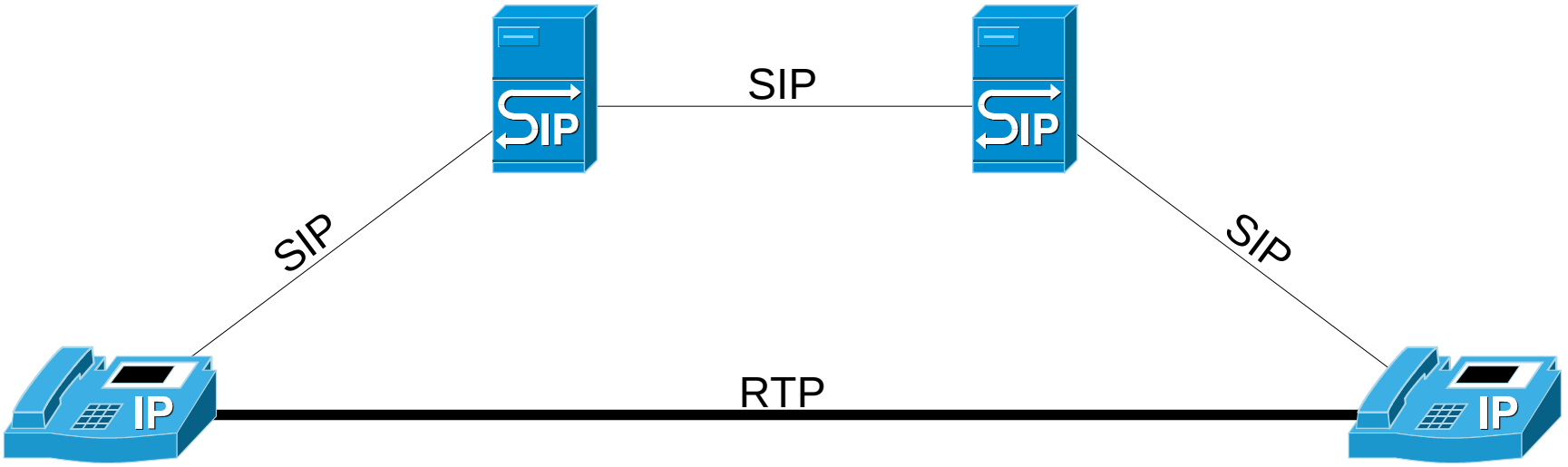
```
INVITE sip:4185551234@bell.ca SIP/2.0
Via: SIP/2.0/UDP ringo.viagenie.ca;branch=z9hG4bKnashds8
Max-Forwards: 70
To: Marc Blanchet <sip:4185551234@bell.ca>
From: Simon Perreault <sip:simon.perreault@viagenie.ca>;tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE
Contact: <sip:simon@pc33.viagenie.ca>
Content-Type: application/sdp
Content-Length: 142
```

- Séparation de la signalisation du contenu média
  - SIP établit la session.
  - Média transporté sur UDP avec le *real-time transport protocol* (RTP)
    - Voix, vidéo, texte, etc.

Exemple SIP



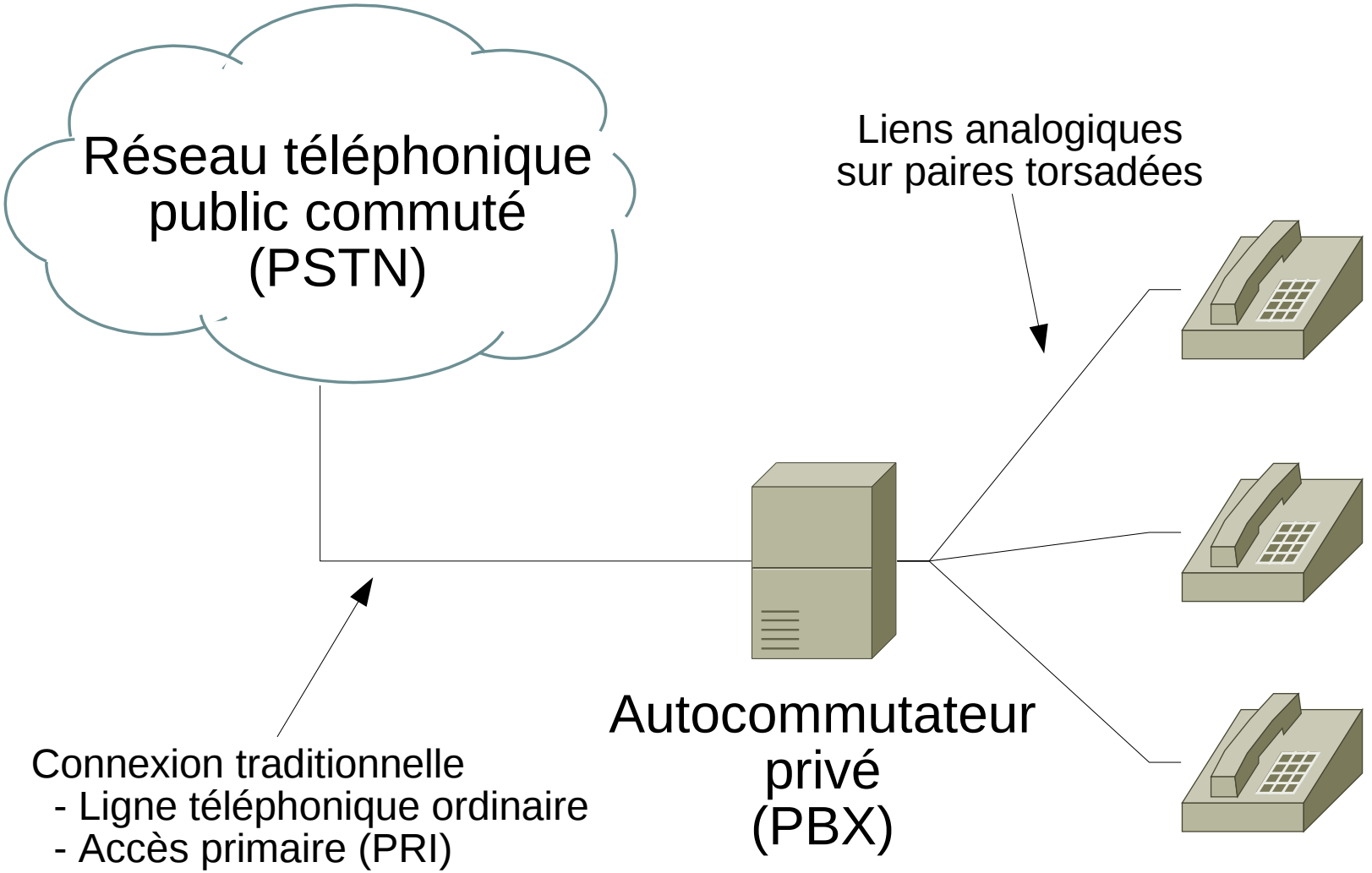
Exemple SIP



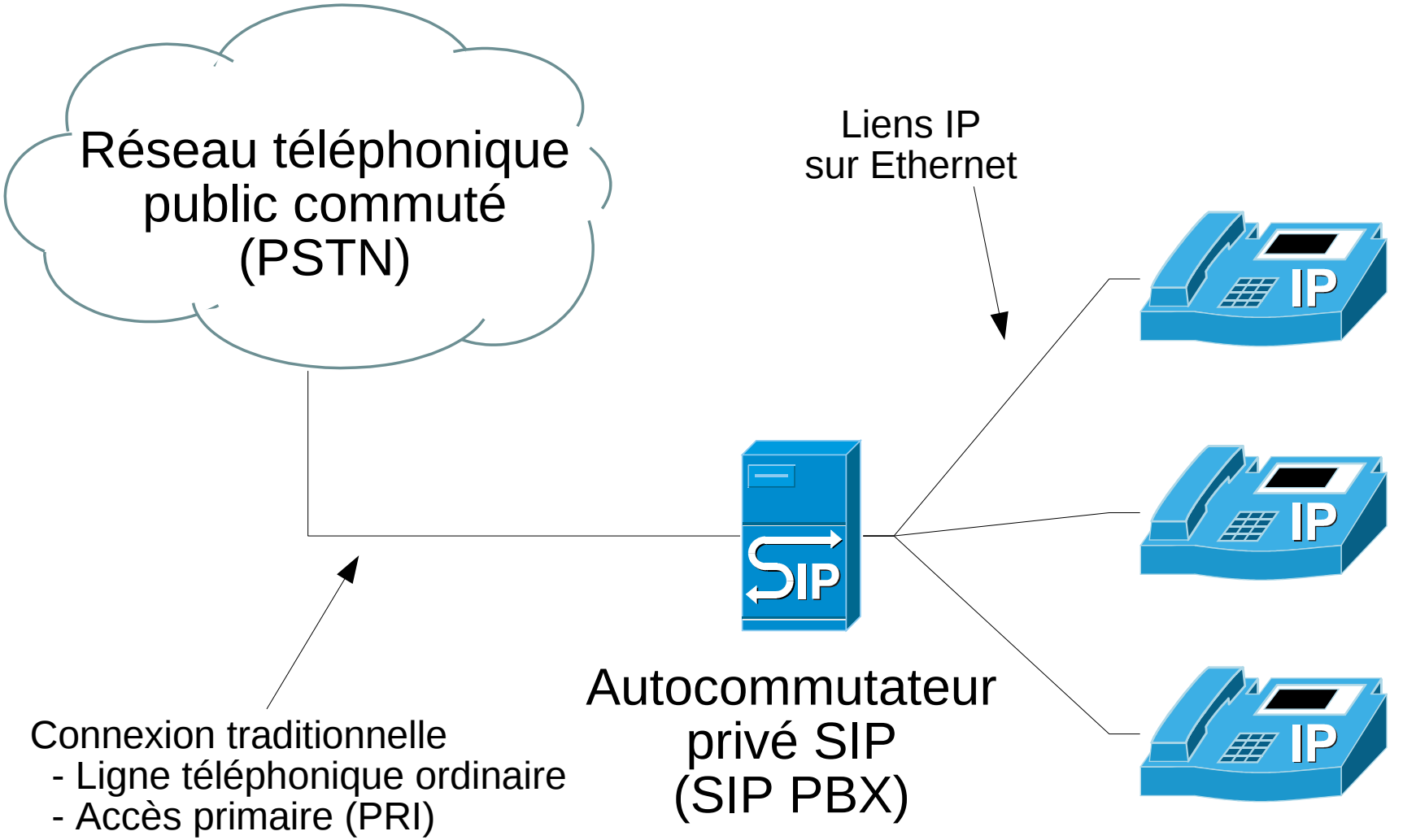
Scénarios de déploiement

1. Remplacement du système téléphonique traditionnel

Situation initiale



Migration à la téléphonie IP



Remplacement du système téléphonique traditionnel

- Changements:
  - Installation de téléphones SIP
  - Remplacement du câblage des téléphones
  - Remplacement du PBX
- On conserve:
  - Lien au PSTN

Nouvelles caractéristiques de sécurité

- Liens numériques entre PBX et téléphones
  - Intercepter une conversation: accès au réseau.
  - Nouvelle possibilité: chiffrement
    - Rend l'interception impossible.
    - Le téléphone et le PBX doivent le supporter.
      - De nos jours, ce n'est pas encore certain. Il faut vérifier.
    - Interception toujours possible...
      - ...sur le PSTN.
      - ...à l'autre bout de la connexion.
    - TLS pour SIP (signalisation) [RFC3261]
    - SRTP pour RTP (média) [RFC3711]
      - Algorithme AES

Nouvelles caractéristiques de sécurité

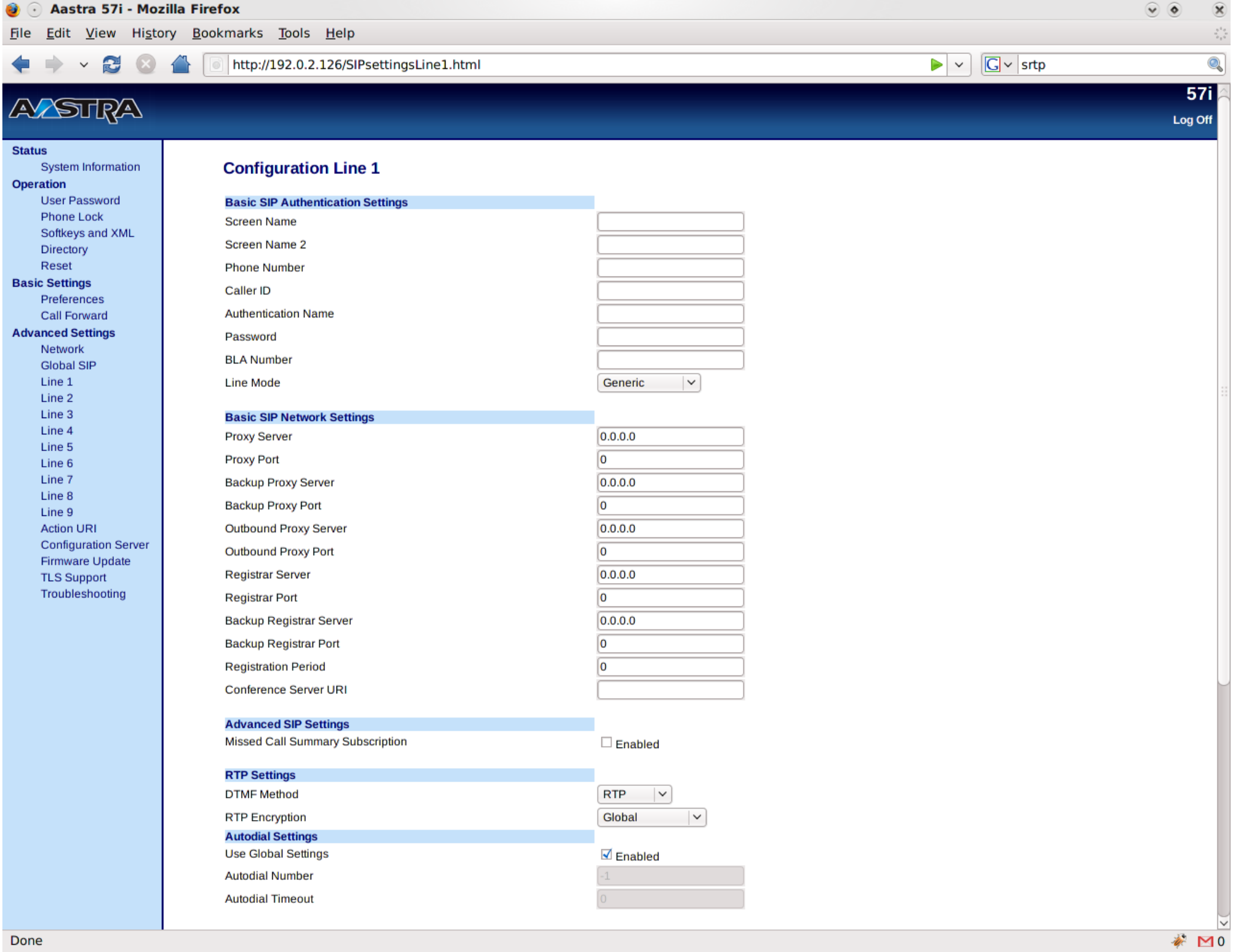
- L'identité est associée au téléphone (ou même à un utilisateur en particulier).
  - La prise réseau n'a pas d'importance.
  - Nouvelle possibilité: mobilité
    - Déplacement d'appareil
    - Assignation dynamique d'identité

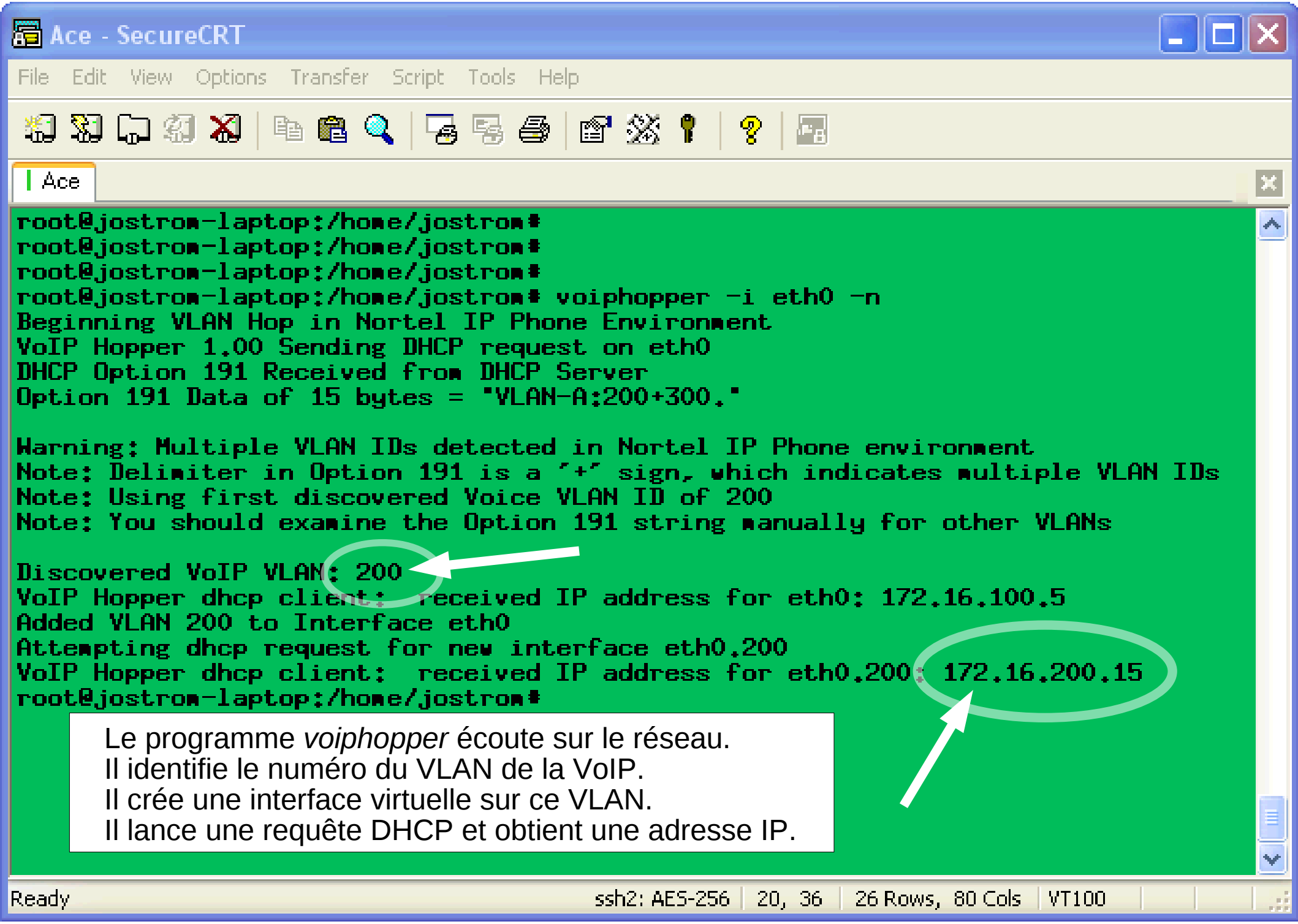
Nouvelles caractéristiques de sécurité

- Pour usurper une identité:
  ١. Outils ⇒ Préférences...
  ٢. Entrer le nom voulu.
  ٣. Cliquer sur OK.
- Nouvelle possibilité: identité cryptographique
  - Rend impossible l'usurpation d'identité.
  - Le téléphone et le PBX doivent le supporter.
    - De nos jours, encore moins répandu que le chiffrement.
  - Ne garantit pas l'identité émise sur ou reçue du PSTN.
  - TLS pour SIP [RFC3261]
  - Rien pour RTP (voir développements courants)

Nouvelles caractéristiques de sécurité

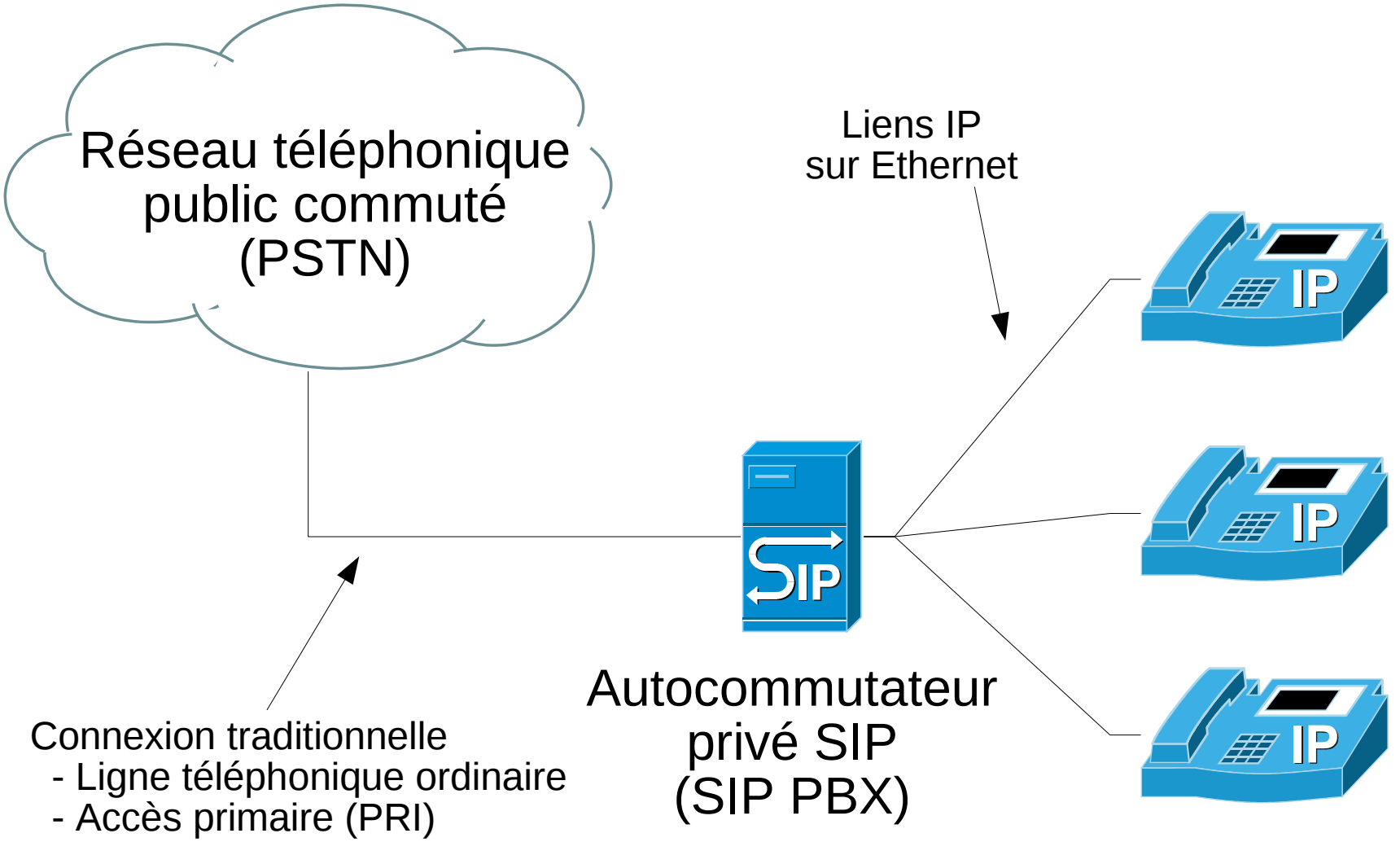
- Chaque téléphone est un ordinateur
  - Mots de passe
    - Administrateur
    - Usager
  - Adapter règles de pare-feu
    - Trafic interne seulement
  - VLAN séparé
    - Isoler et limiter les interactions
    - Faciliter la QoS
- Chaque téléphone est un serveur web


Aastra 57i - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.0.2.126/SIPsettingsLine1.html
srtp
AASTRA
57i
Log Off
Status
System Information
Operation
User Password
Phone Lock
Softkeys and XML
Directory
Reset
Basic Settings
Preferences
Call Forward
Advanced Settings
Network
Global SIP
Line 1
Line 2
Line 3
Line 4
Line 5
Line 6
Line 7
Line 8
Line 9
Action URI
Configuration Server
Firmware Update
TLS Support
Troubleshooting
Configuration Line 1
Basic SIP Authentication Settings
Screen Name
Screen Name 2
Phone Number
Caller ID
Authentication Name
Password
BLA Number
Line Mode
Generic
Basic SIP Network Settings
Proxy Server
0.0.0.0
Proxy Port
0
Backup Proxy Server
0.0.0.0
Backup Proxy Port
0
Outbound Proxy Server
0.0.0.0
Outbound Proxy Port
0
Registrar Server
0.0.0.0
Registrar Port
0
Backup Registrar Server
0.0.0.0
Backup Registrar Port
0
Registration Period
0
Conference Server URI
Advanced SIP Settings
Missed Call Summary Subscription
Enabled
RTP Settings
DTMF Method
RTP
RTP Encryption
Global
Autodial Settings
Use Global Settings
Enabled
Autodial Number
-1
Autodial Timeout
0
Done
0

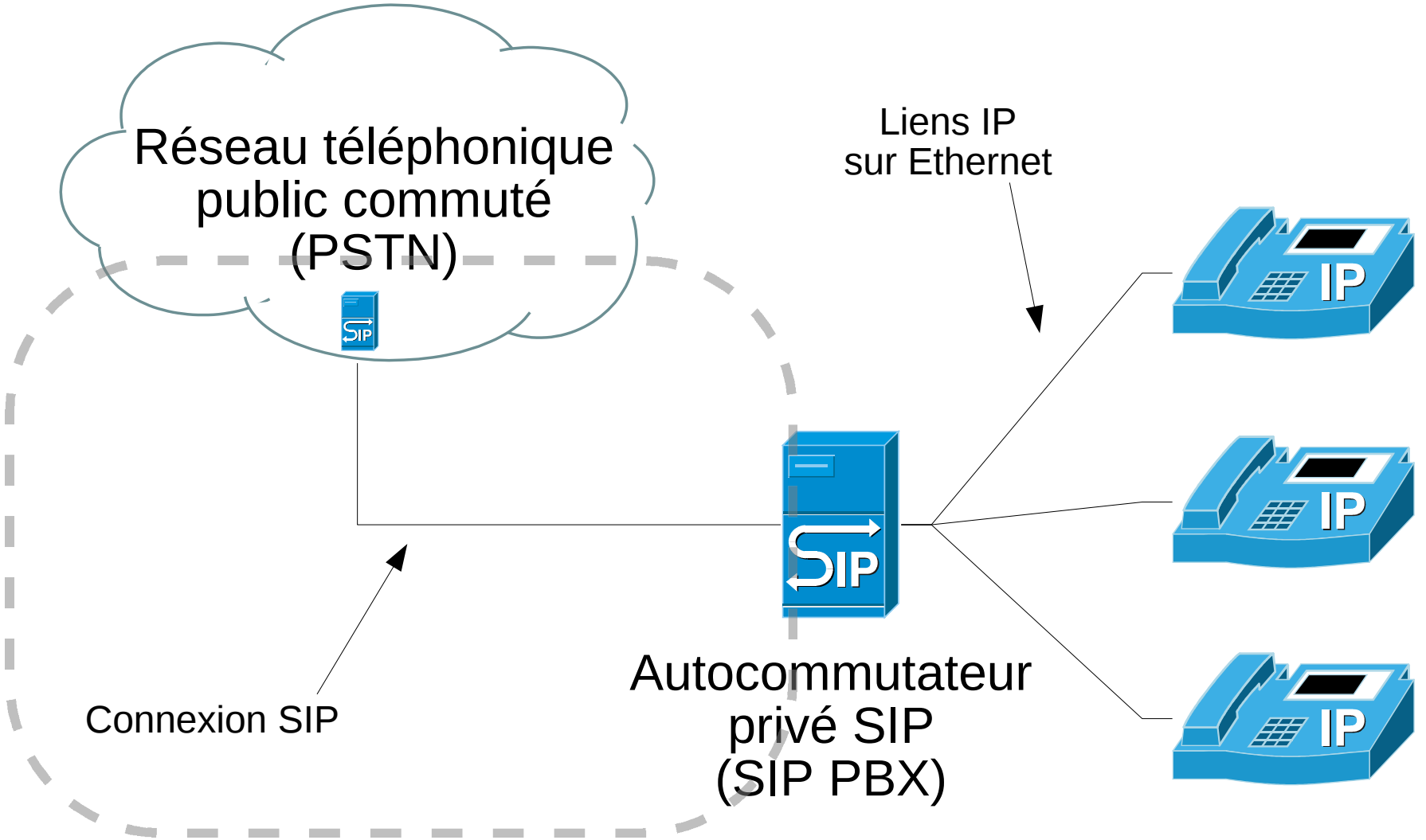

Ace - SecureCRT
File Edit View Options Transfer Script Tools Help
Ace
root@jostrom-laptop:/home/jostrom#
root@jostrom-laptop:/home/jostrom#
root@jostrom-laptop:/home/jostrom#
root@jostrom-laptop:/home/jostrom# voiphopper -i eth0 -n
Beginning VLAN Hop in Nortel IP Phone Environment
VoIP Hopper 1.00 Sending DHCP request on eth0
DHCP Option 191 Received from DHCP Server
Option 191 Data of 15 bytes = "VLAN-A:200+300,"
Warning: Multiple VLAN IDs detected in Nortel IP Phone environment
Note: Delimiter in Option 191 is a '+' sign, which indicates multiple VLAN IDs
Note: Using first discovered Voice VLAN ID of 200
Note: You should examine the Option 191 string manually for other VLANs
Discovered VoIP VLAN: 200
VoIP Hopper dhcp client: received IP address for eth0: 172.16.100.5
Added VLAN 200 to Interface eth0
Attempting dhcp request for new interface eth0.200
VoIP Hopper dhcp client: received IP address for eth0.200: 172.16.200.15
root@jostrom-laptop:/home/jostrom#
Le programme voiphopper écoute sur le réseau.
Il identifie le numéro du VLAN de la VoIP.
Il crée une interface virtuelle sur ce VLAN.
Il lance une requête DHCP et obtient une adresse IP.
Ready
ssh2: AES-256
20, 36
26 Rows, 80 Cols
VT100

2. Accès au PSTN via IP

Situation initiale



Accès au PSTN via IP



Accès au PSTN via IP

- Changements:
  - Le PBX ne "traduit" plus entre l'analogue et le numérique.
    - Allègement de la charge
    - Diminution des coûts en matériel
  - Réutilisation de la connexion IP
    - Diminution des coûts en abonnement téléphonique
- On conserve:
  - Tout le réseau interne

Nouvelles caractéristiques de sécurité

- Fiabilité du lien IP
  - **En général** moins fiable qu'un lien téléphonique
  - Nouvelle possibilité: redondance
    - Obtenir plusieurs liens IP de fournisseurs différents
    - Transition automatique lors de panne
- Fiabilité du lien SIP
  - Nouvelle possibilité: redondance partielle
    - Obtenir plusieurs liens SIP de fournisseurs différents
    - Numéros différents
    - Transition automatique lors de panne (appels sortants seulement)

Nouvelles caractéristiques de sécurité

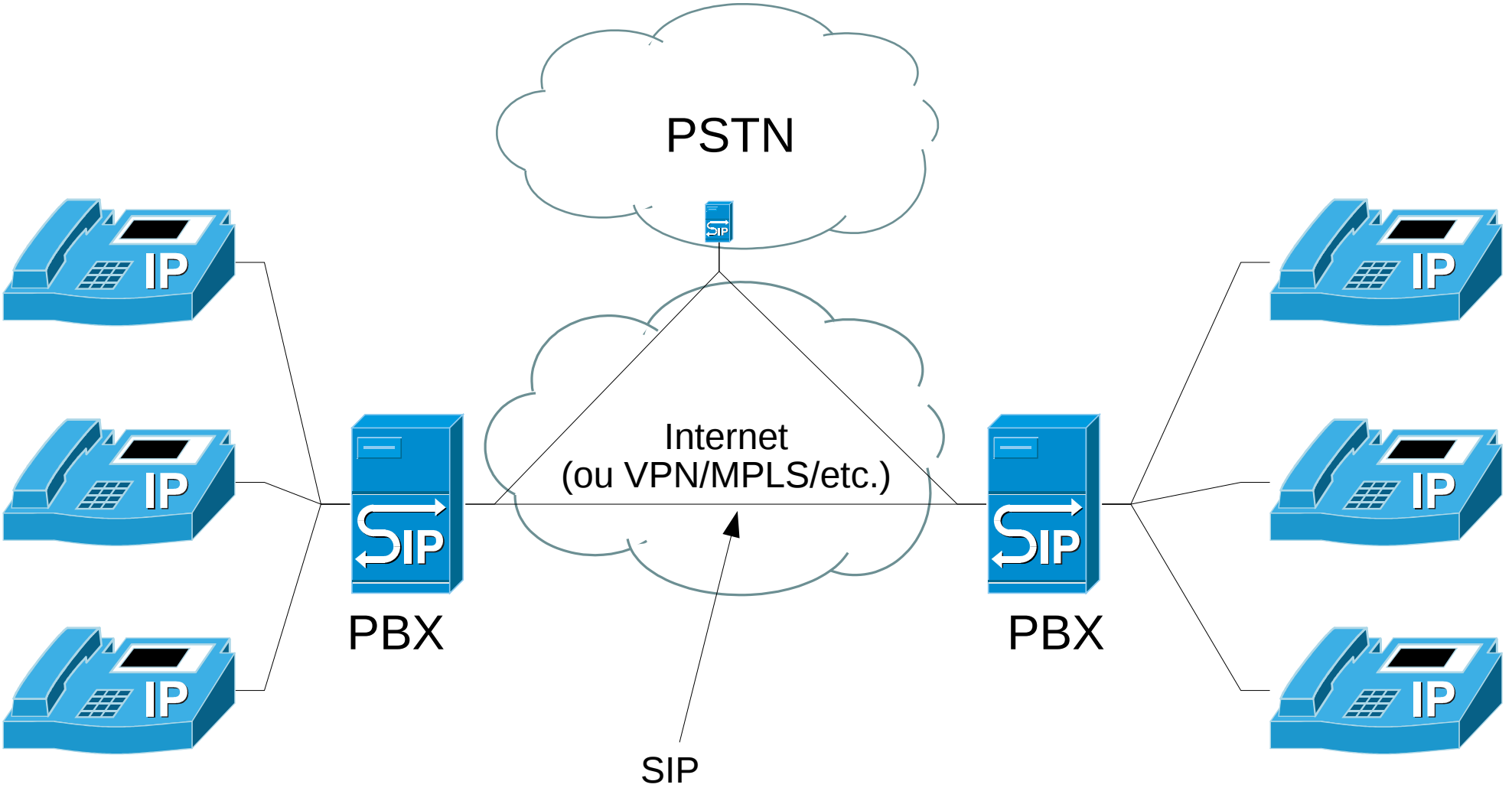
- Interception de communication
  - Requiert accès au réseau (difficile)
  - Nouvelle possibilité: chiffrement
    - Doit être supporté par le fournisseur et le PBX.
    - Protection limitée à SIP, pas PSTN
    - Confiance en votre fournisseur

Nouvelles caractéristiques de sécurité

- Déni de service (DoS)
  - Nom de lignes SIP grand ou illimité
    - Dépend de la capacité du fournisseur
  - Saturer le lien IP
    - Difficile à prévenir
  - Rendre le PBX hors fonction
    - Nouvelle possibilité: redondance
      - Plusieurs PBX
      - Transition automatique en cas de panne
  - Couper le fil

3. Interconnexion de succursales

Interconnexion de succursales



Interconnexion de succursales

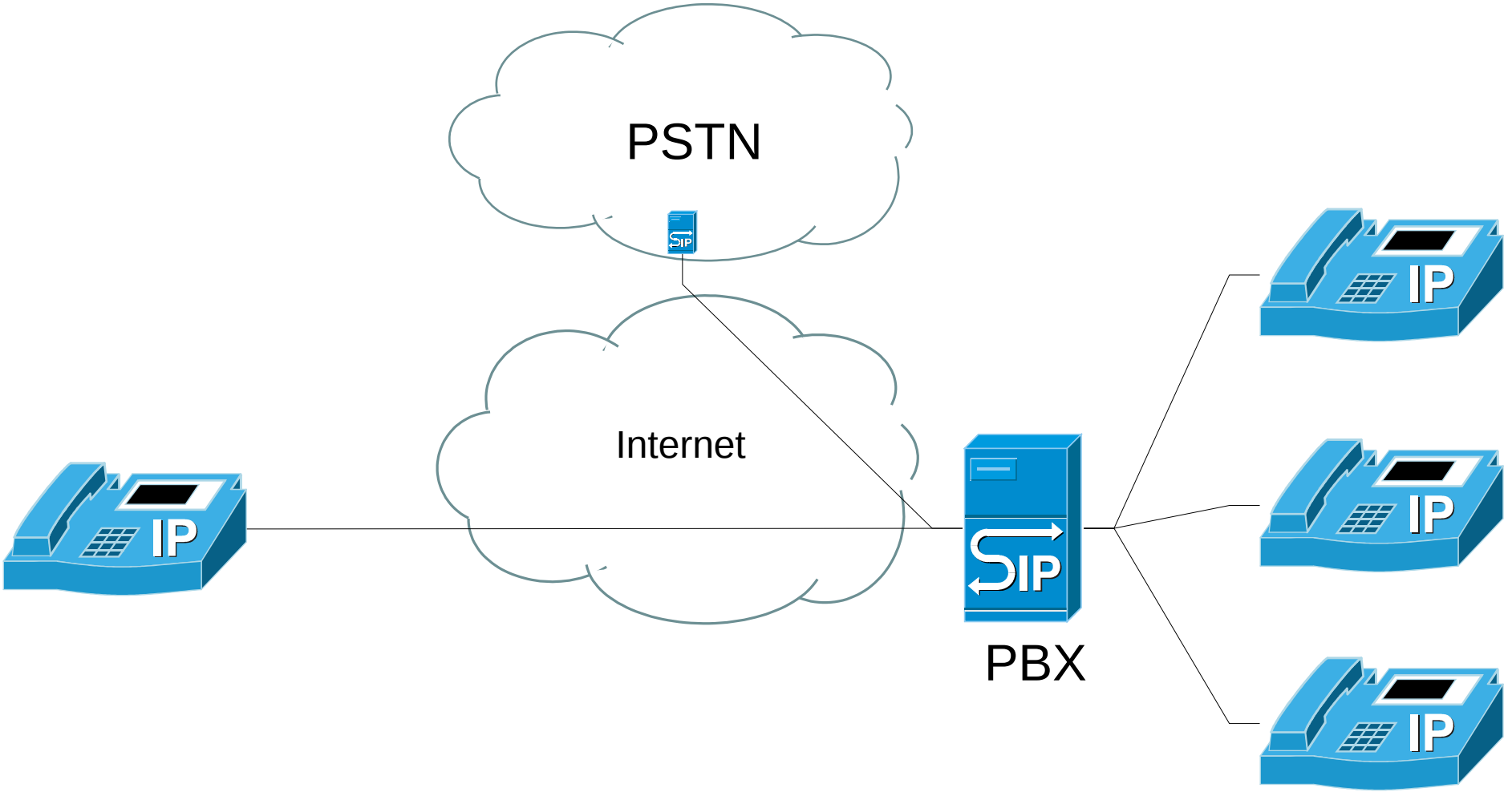
- Changements:
  - Lien SIP établi entre PBX
    - Élimination des coûts d'appels téléphoniques pour appels entre succursales
    - Contrôle total

Nouvelles caractéristiques de sécurité

- Chiffrement du lien inter-succursale
  - Les PBX doivent le supporter
  - VPN peut être une option
    - Attention à la quantité de trafic
    - Augmente la latence
- Nouvelle possibilité: chiffrement de bout en bout
  - Seuls les téléphones doivent le supporter
  - Diminution importante de la charge sur VPN ou PBX
- Nouvelle possibilité: identité cryptographique
  - L'intégrité de l'identité peut être assurée pour les appels à l'intérieur de l'entreprise.

4. Télétravail / Itinérance

Télétravail / Itinérance



Télétravail / Itinérance

- Changements:
  - Lien entre téléphone et PBX via Internet
    - Mobilité
    - Diminution des coûts pour appels externes
    - Élimination des coûts pour appels internes

Nouvelles caractéristiques de sécurité

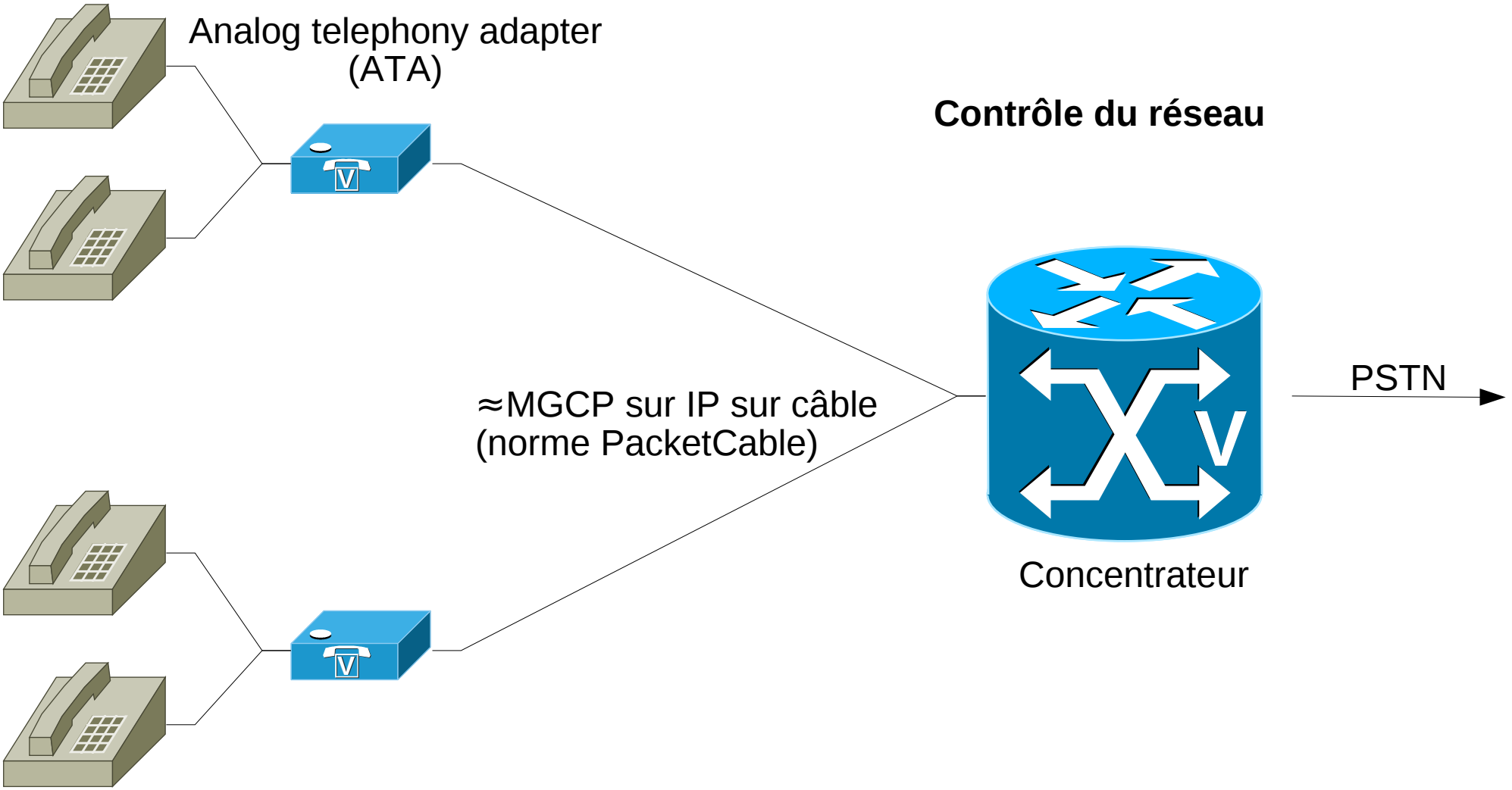
- Connexion établie à partir de n'importe où
  - Règles de pare-feu assouplies
  - PBX devient accessible de l'extérieur
    - Système dédié et isolé
- Interception de communications
  - Point d'accès quelconque
    - À la maison
    - Café Internet
    - Espion en mission chez le compétiteur
    - ...

Nouvelles caractéristiques de sécurité

- Sécurisation de la connexion
  - VPN peut être une option
    - Attention à la quantité de trafic
    - Augmente la latence
  - Chiffrement et identité cryptographique
    - Doivent être supportés par le client SIP et le PBX

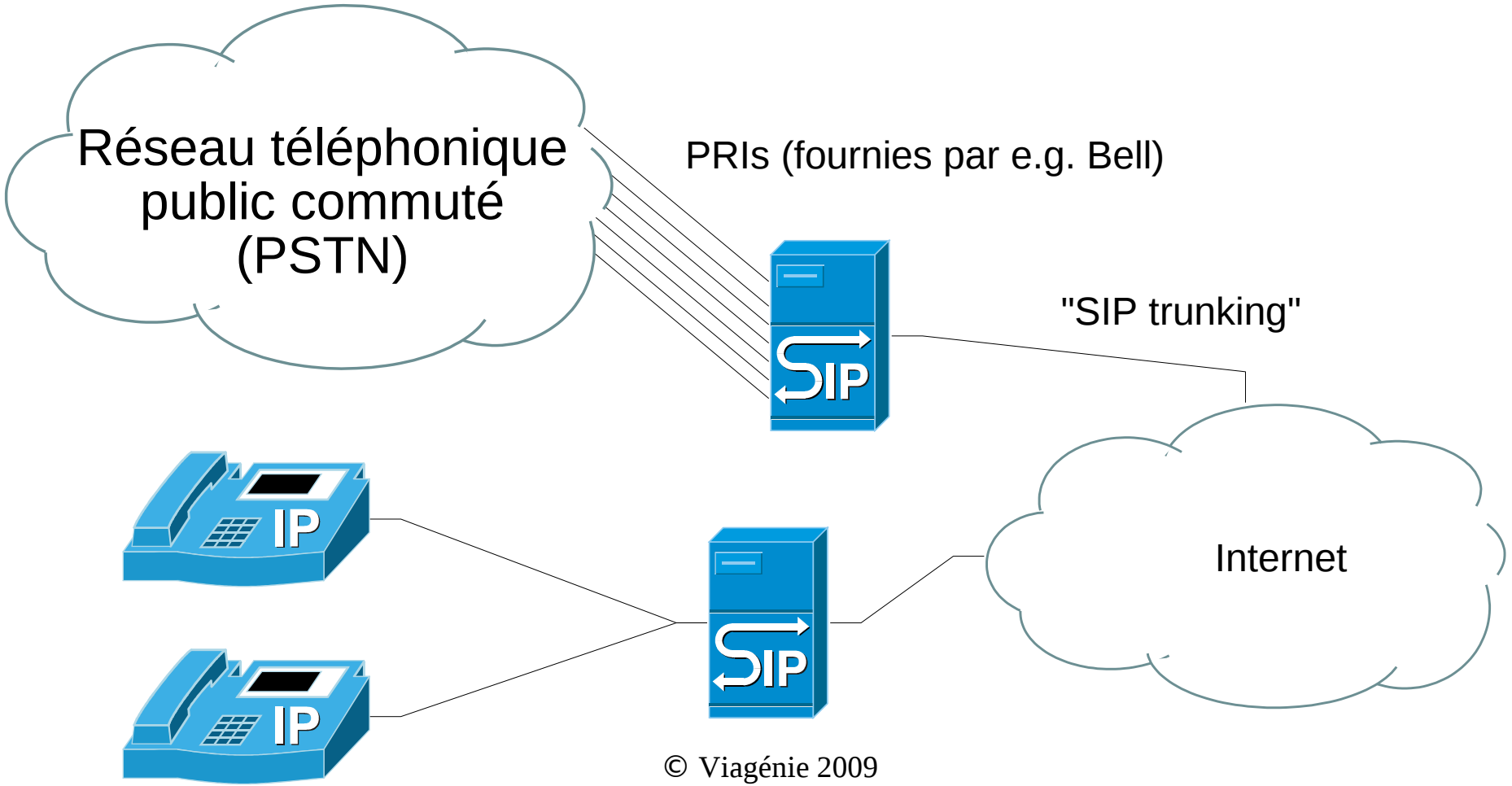
Déploiements typiques

Câblodistributeur



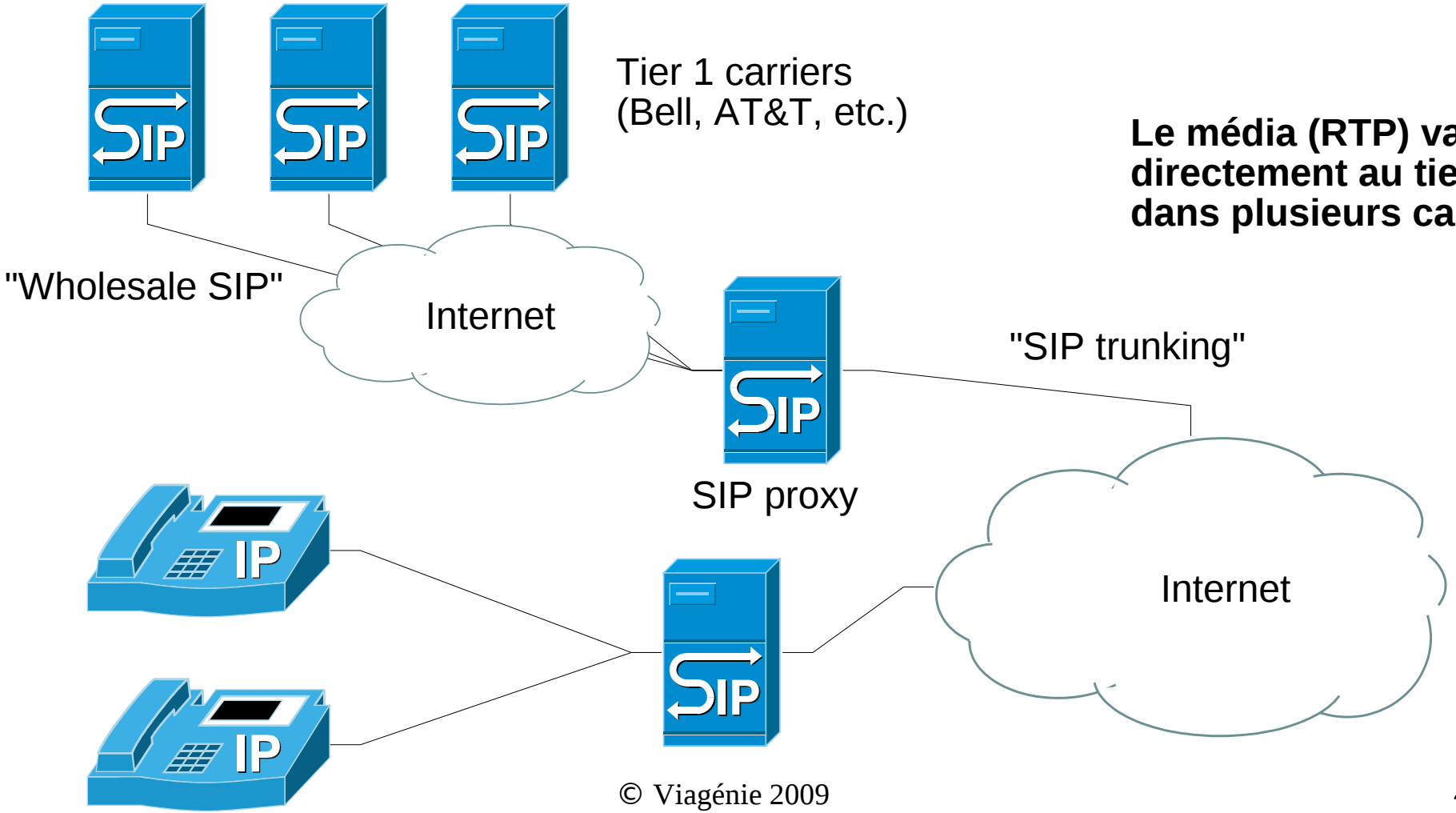
ITSP (*Internet Telephony Service Provider*)

- Exemple: Unlimitel.ca et bien d'autres



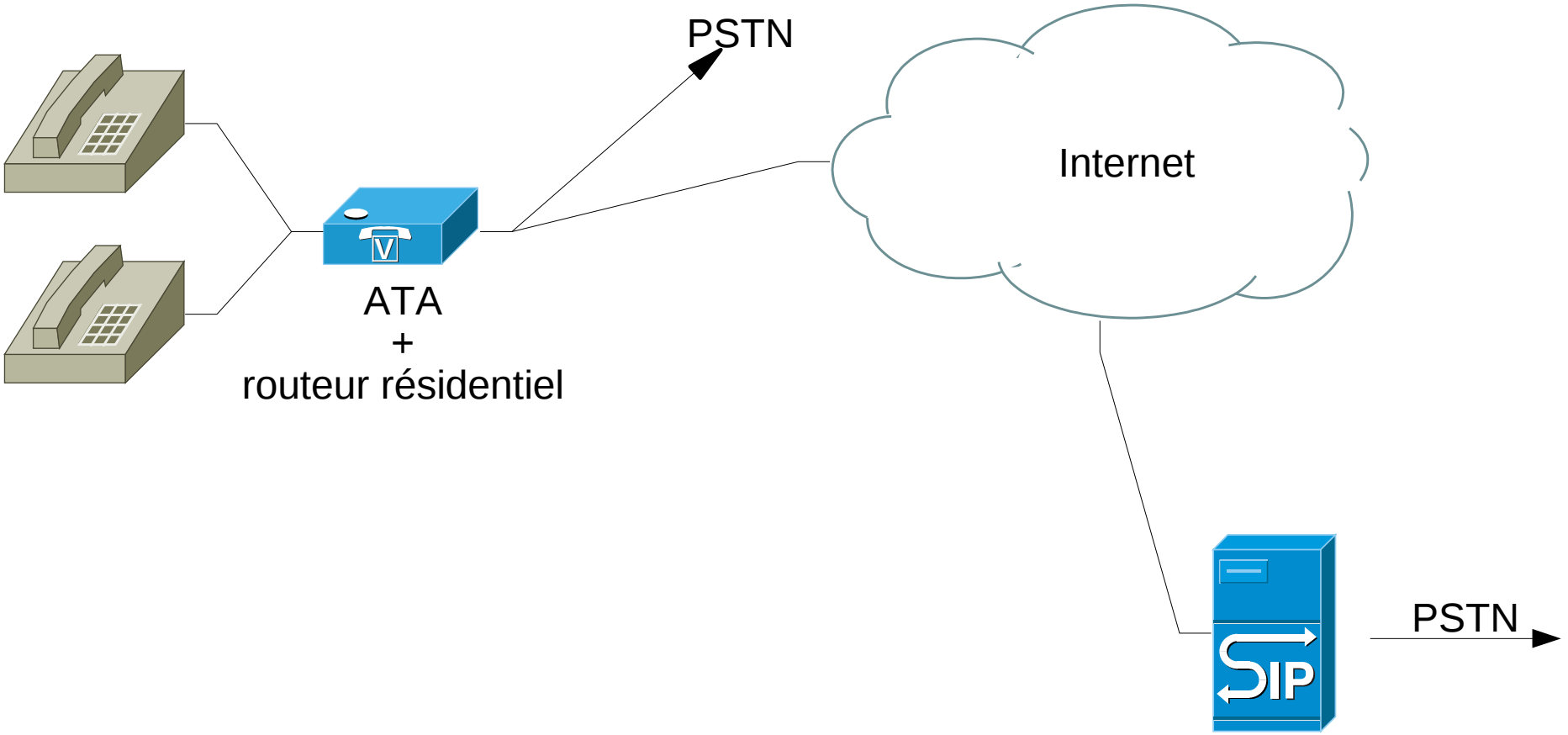
ITSP avec SIP en amont

- Exemples: Flowroute.com, VoIP.co.uk, etc.



"Internet Telephony"

- Exemples: Ooma, Vonage, etc.



Développements courants

- Identité crytpo. du média
  - Les relais posent un problème.
  - Document de travail: [draft-wing-sip-identity-media]
- Groupe de travail P2PSIP
  - Un protocole de réseau pair-à-pair sans serveur central.
  - La sécurité est un défi de taille!
- Groupe de travail GEOPRIV
  - Information géographique (longitude, latitude, rue, ville, pays, etc.)
  - Comment décider du niveau de précision? À qui fournir l'information?
- ZRTP
  - Protocole pour échange de clés SRTP "in-band" (pas dans SIP).
  - Document de travail: [draft-zimmermann-avt-zrtp-15]
- DTLS-SRTP
  - Alternative à ZRTP qui utilise TLS sur UDP.
  - Document de travail: [draft-ietf-avt-dtls-srtp-07]

Conclusion

- La téléphonie traditionnelle comporte des risques, que l'on accepte souvent sans même y penser.
- La téléphonie IP modifie ces risques.
  - Nouvelles fonctionnalités = Nouveaux risques
  - Possibilités
    - Redondance plus facile
    - Cryptographie (TLS pour SIP, SRTP pour média)

Questions?

{sip,mailto}:simon.perreault@viagenie.ca

Références:

- [RFC3261] J. Rosenberg *et. al.*, "SIP: Session Initiation Protocol", juin 2002.
- [RFC3711] M. Baugher *et. al.*, "The Secure Real-time Transport Protocol (SRTP)", mars 2004.
- C. Stredicke, "Why VoIP security matters", *Communication News*, août 2007.
- VoIP Security Alliance, *http://www.voipsa.org*

Cette présentation est disponible à http://www.viagenie.ca/publications/