Mercado Sudamericano de Servicios de *Roaming* Internacional: Obstáculos técnicos y oportunidades

Documento preparatorio para el segundo GTE

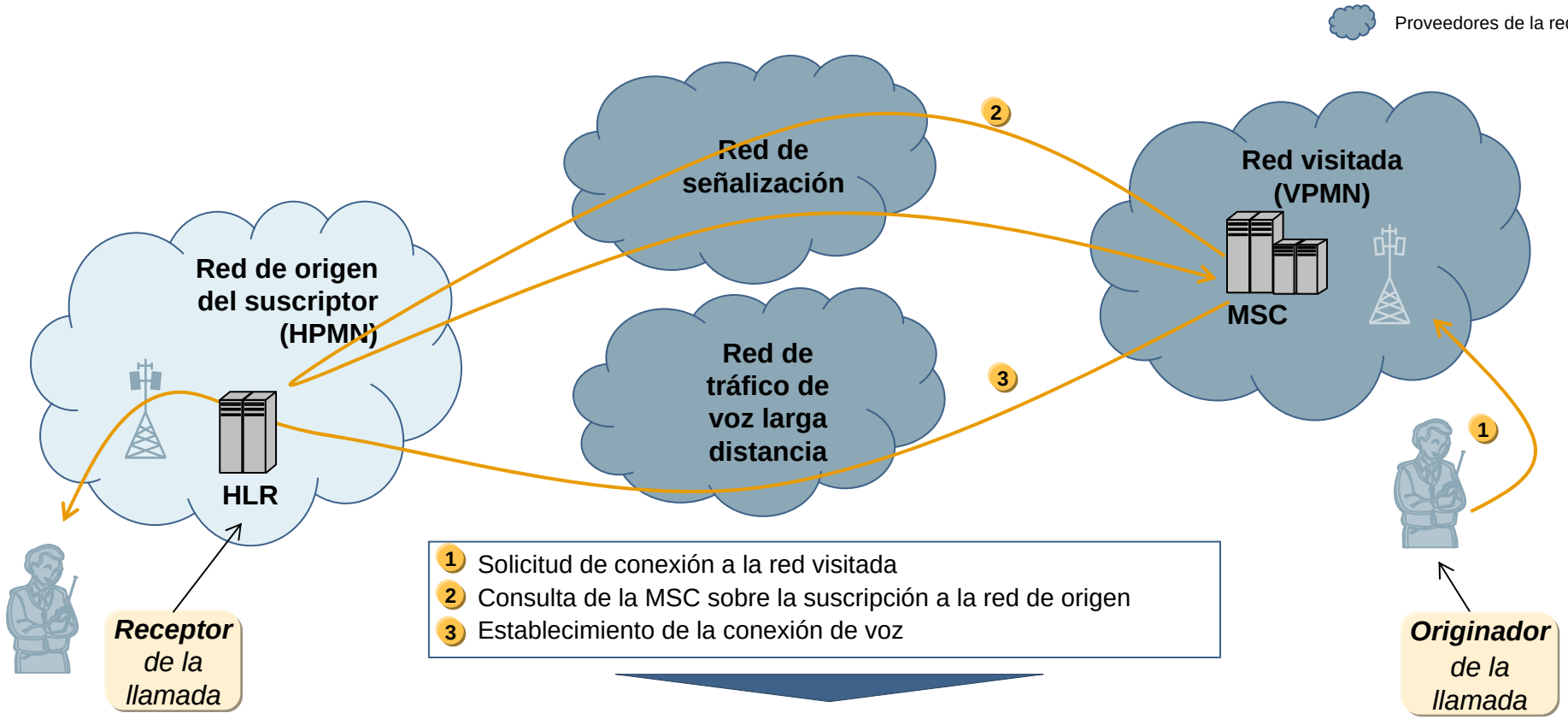
Cusco, mayo de 2009

Contenido del documento

- **Larga distancia**
- Roaming prepago
- Roaming fronterizo
- Fraude
- Iniciativas a discutir

El servicio de voz de roaming internacional requiere (entre otros) de un proveedor de señalización y de un proveedor de larga distancia internacional (LDI)

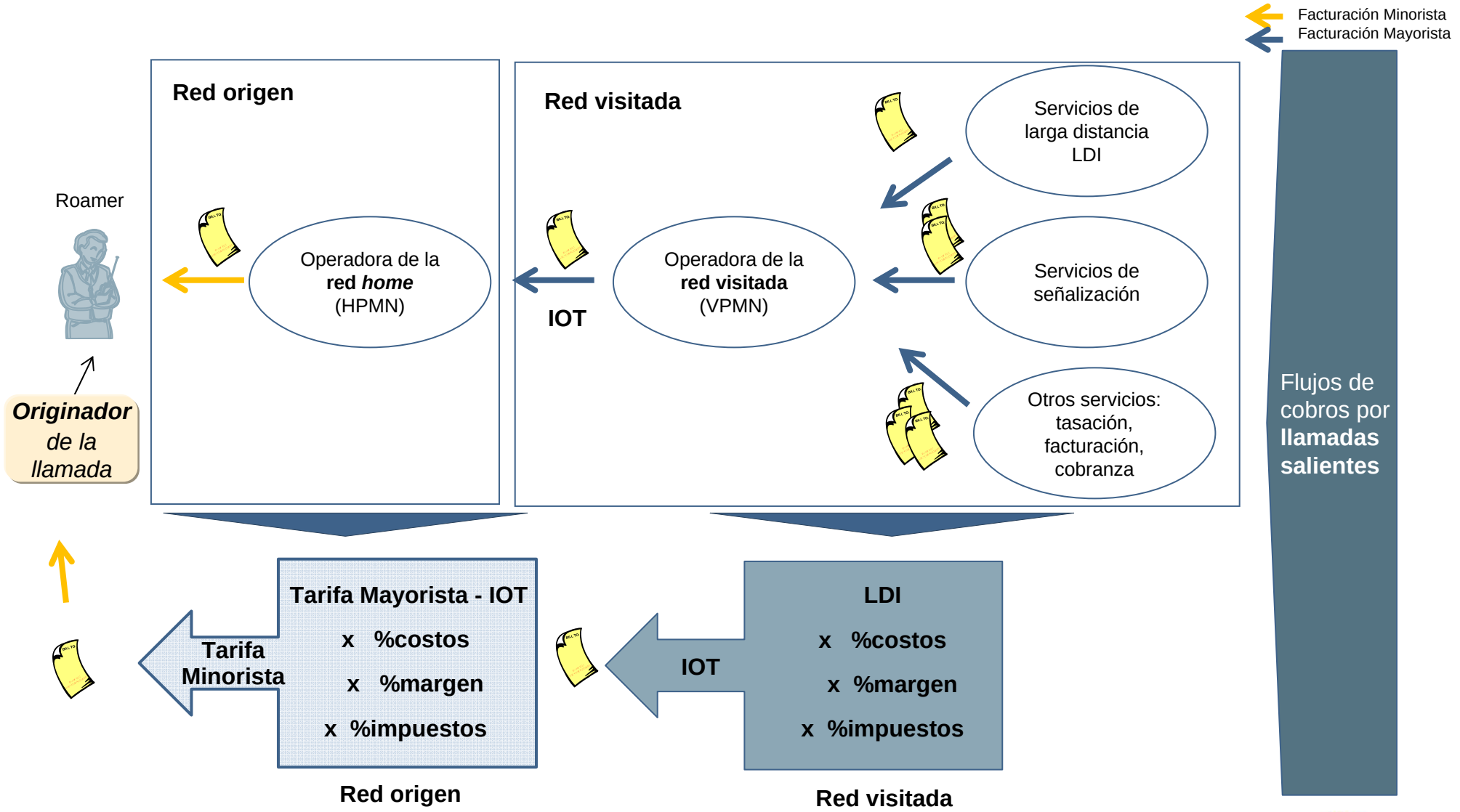
CONCEPTUAL



- Las llamadas al país de origen representan el porcentaje más alto de las llamadas realizadas por el roamer.
- Entre los costos más importante de estas llamadas se encuentra el costo de larga distancia internacional que se paga a los *carriers* de interconexión.
- Suramérica representa solo el 3% del tráfico internacional dejando a la región en una no conveniente posición para la negociación de tarifas.

Fuente: GSMA

Las tarifas mayoristas de roaming (IOT) incluyen los costos del proveedor de LDI así como otros costos y los impuestos locales

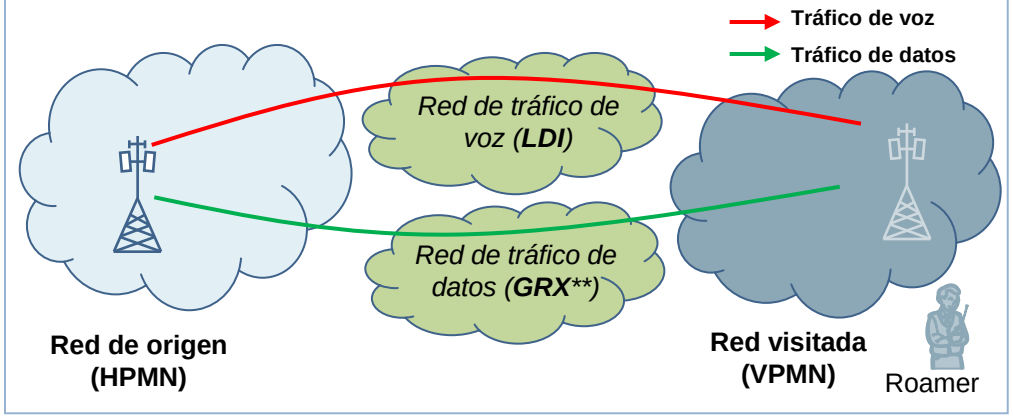


*Inter Operator Tariffs

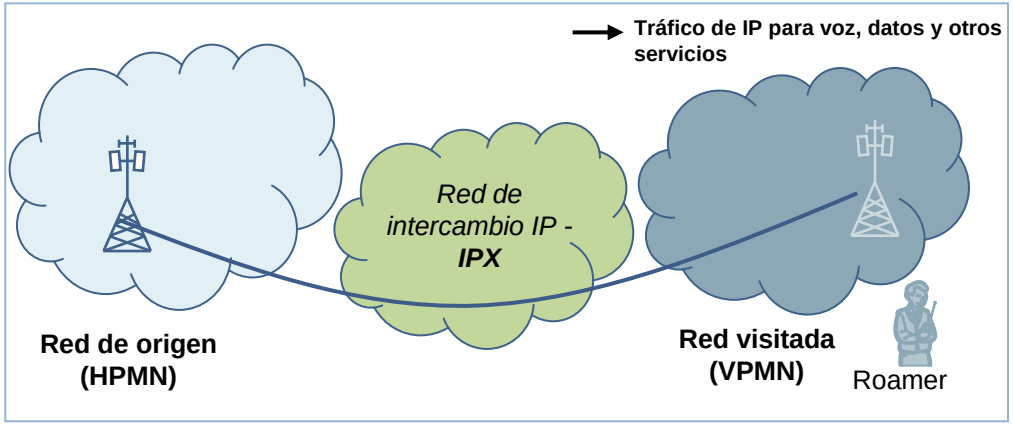
Actualmente las operadoras de *roaming* deben utilizar redes y proveedores diferentes para la entrega del tráfico de voz y datos. La propuesta de NGN*** de la GSMA es la iniciativa IPX

IPX: Redes de Nueva Generación

Situación actual: Tráfico de voz y datos separado



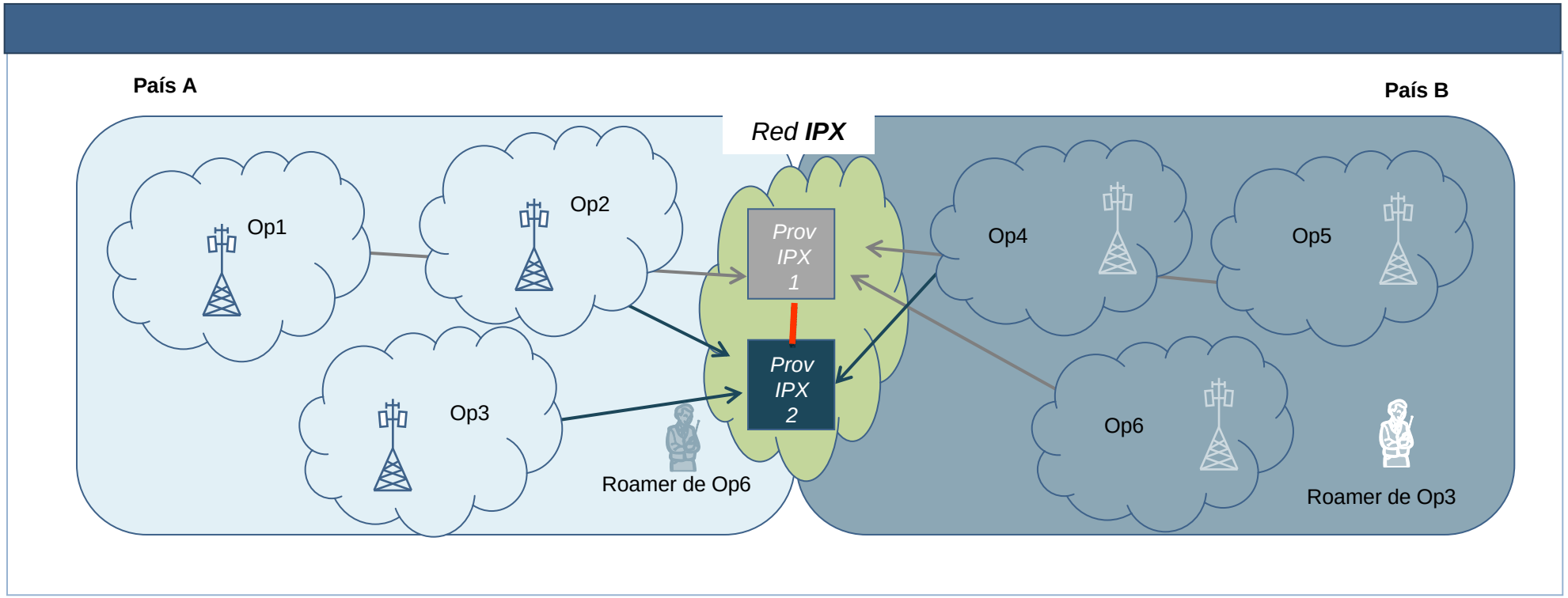
Redes de Nueva Generación (NGN): Intercambio IP – IPX*



- La GSMA ha lanzado la iniciativa IPX como una red de nueva generación basada sobre transporte IP
- La iniciativa ha finalizado exitosamente su etapa de pruebas para los servicios de voz básicos (la videoconferencia no se encontró dentro de este ensayo)
- La GSMA alienta a los operadores suramericanos de iniciar los ensayos en la región
- La regulación de la convergencia es un desafío que las reguladores deben enfrentar

*IPX = IP eXchange
** GRX = GPRS eXchange
*** NGN Next Generation Nettworks

Los proveedores de servicios IPX deben estar interconectados entre sí (peering) de manera de asegurar la conectividad entre todos los operadores conectados a diferentes proveedores.



- Los roamers pueden llamar o recibir llamados de los diferentes operadores.
- Cuando el roamer se comunica con un usuario de otro operador utiliza alguno de los puntos de *peering* establecidos entre proveedores.

*IPX = IP eXchange
** GRX = GPRS eXchange
*** NGN Next Generation Nettworks

Contenido del documento

- Larga distancia
- **Roaming prepago**
- Roaming fronterizo
- Fraude
- Iniciativas a discutir

Existe una baja disponibilidad de *roaming* prepago en la región siendo pocas las operadoras que ofrecen este servicio

0 2
1 3 o más

Número de operadores del país de origen que ofrecen el servicio de *roaming* prepago al país visitado

País de origen	Países visitados											
	AR	BO	BR	CH	CO	EC	GY	PY	PE	SU	UY	VE
AR			1	1				1			2	
BO												
BR	2											
CH	3 o +	2	2		2	2		1	1		2	2
CO												
EC												
GY	3 o +	2	3 o +	2	2			2	2	2	2	1
PY	1										1	
PE												
SU			3 o +	1	1		1		1			
UY	1											
VE	3 o +	2	3 o +	2	2	1		2	1	1	2	

TIM Brasil tiene servicio prepago con 15 países

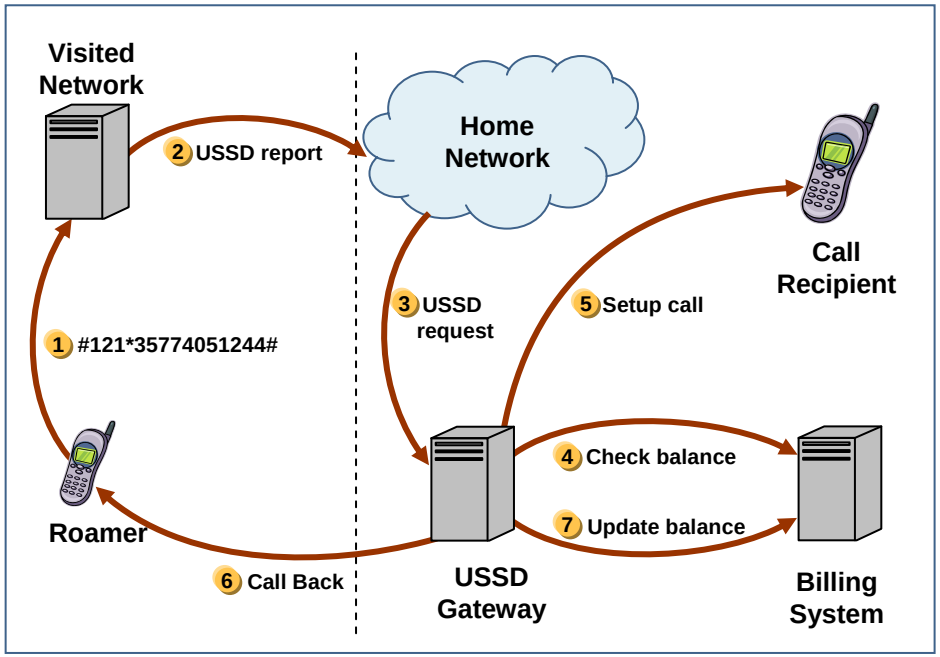
Sólo servicio para transferencia de Datos

*En un ~**69**% de los casos no hay ningún acuerdo prepago*

*La cobertura de roaming prepago actualmente se encuentra limitada a algunas regiones de mayor flujo turístico reflejando la **falta de desarrollo de este componente en Sudamérica***

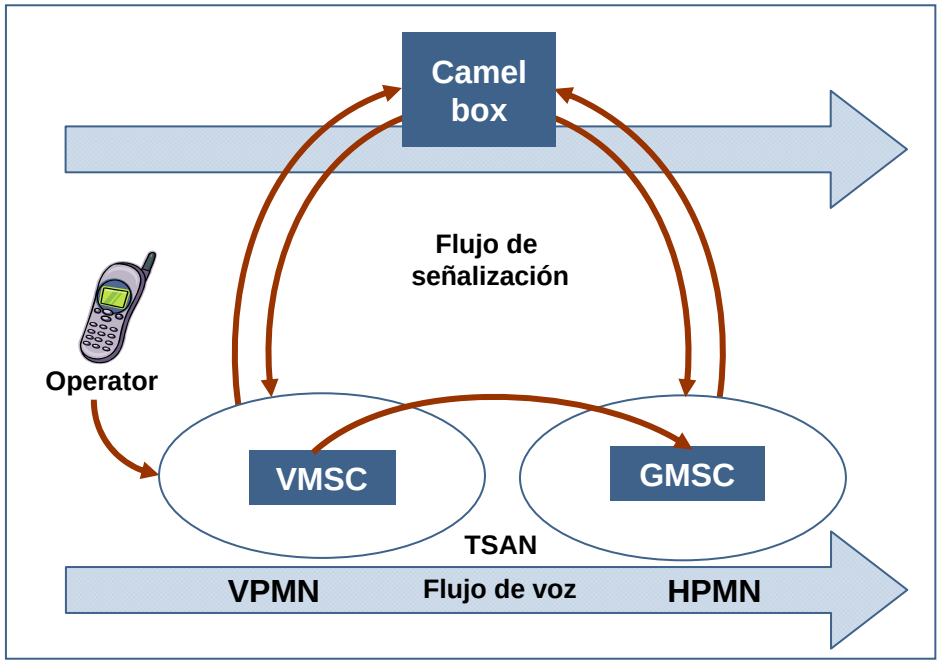
Existen dos métodos más comunes para la implementación de *roaming* prepago: USSD *Callback* y CAMEL,...

USSD (*Unstructrued Supplementary Services Data*) Callback



- Capacidad de los terminales GSM asociado con servicios de mensajería pero sin la capacidad de *store and forward*
- Utilizado para transmitir información sobre canales de señalización GSM, enviando información sobre saldos disponibles para subscriptores prepago

CAMEL (*Customised Applications for Mobile Enhanced Logic*)

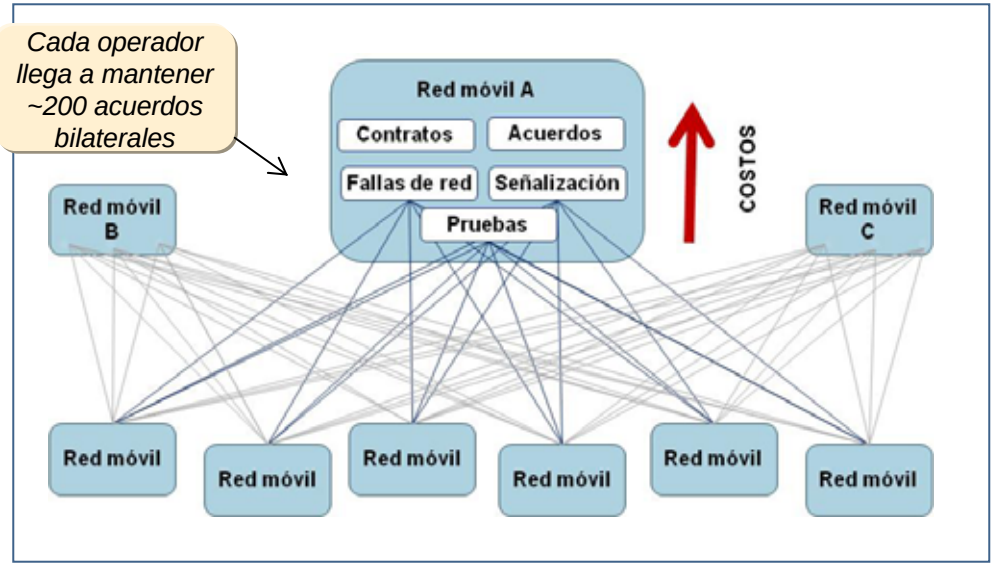


- CAMEL es una especificación de ETSI* para Redes Inteligentes (IN) en tecnología GSM
- Existen 5 fases del patrón:
  - Fase II: permite *roaming* prepago de voz y SMS**
  - Fase III a V: aumentan el acceso a servicio de datos prepagos

* *European Telecommunication Standartization Institute*
** El roaming de SMS prepago requiere *patchs* complementarios al CAMEL II
Fuente: Análisis del equipo de trabajo

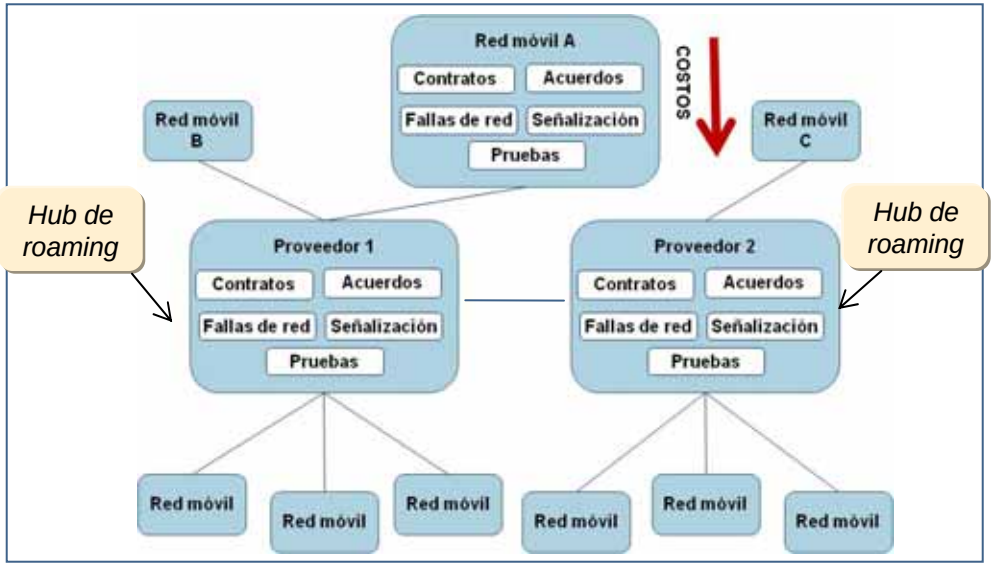
Existen dos métodos para implementar CAMEL: CAMEL bilateral y CAMEL hubbing

Esquema de acuerdos bilaterales



- Actualmente los operadores establecen acuerdos bilaterales por cada relación con un operador de *roaming*.
- Esto conlleva un importante esfuerzo para establecer este relacionamiento uno-a-uno

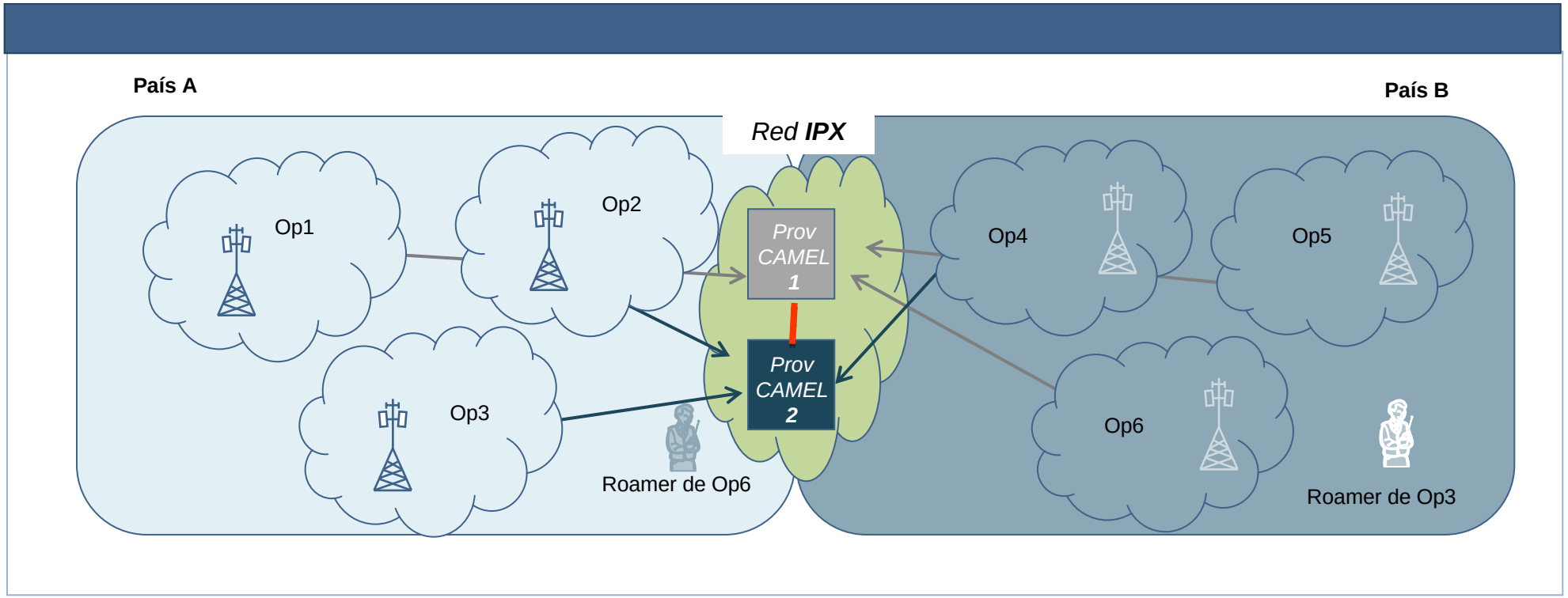
Esquema de conectividad abierta (OC)



- Los proveedores de redes de conectividad abierta actúan como centro - hubs- de las relaciones de roaming.
- Los operadores clientes conectados a un hub de roaming tienen acceso a la relación con los operadores del mismo hub y de los otros hubs

- *El objetivo de la iniciativa de conectividad abierta – OC – de la GSMA es proveer a los subscriptores de un **servicio global de roaming GSM**.*
- ***Reducir los costos de lanzamiento** con un nuevo operador y ayudar a tener una mejor cobertura permitiendo que los **acuerdos de roaming** puedan realizarse **con los hubs** en lugar de con cada uno de los operadores móviles*

Los proveedores de servicios CAMEL OC deben estar interconectados entre sí (peering) de manera de asegurar la conectividad entre todos los operadores conectados a diferentes proveedores.

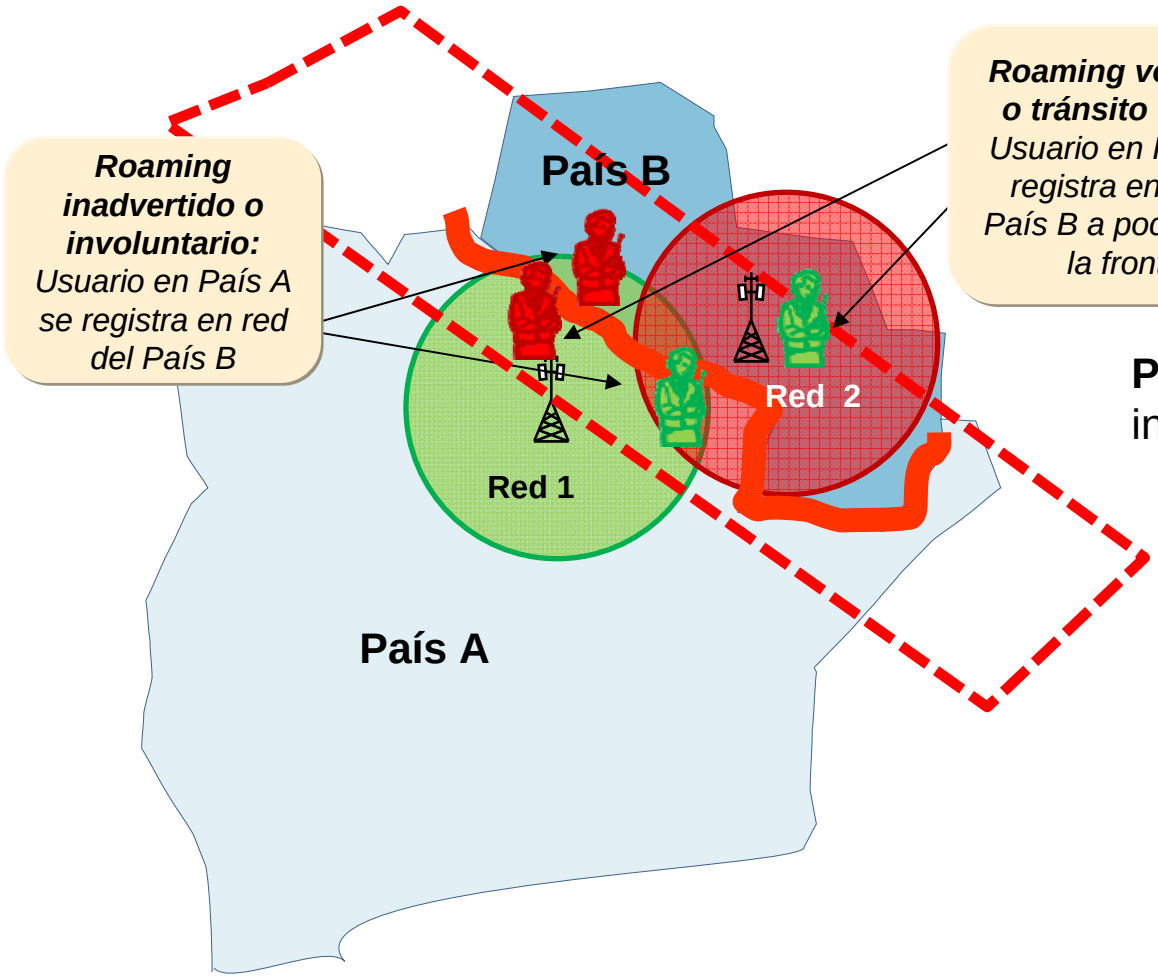


- Los roamers pueden llamar o recibir llamados de los diferentes operadores.
- Cuando el roamer se comunica con un usuario de otro operador utiliza alguno de los puntos de *peering* establecidos entre proveedores.
- Existen numerosos proveedores de estos servicios con la solución funcionando.
- No se requiere inversión inicial.

Contenido del documento

- Larga distancia
- Roaming prepago
- **Roaming fronterizo**
- Fraude
- Iniciativas a discutir

En zonas fronterizas, el servicio de roaming enfrenta el desafío de evitar el uso del servicio en forma inadvertida y promover el uso del servicio como integración de economías.



Roaming inadvertido o involuntario: *Usuario en País A se registra en red del País B*

Roaming voluntario o tránsito vecinal: *Usuario en País B se registra en red del País B a pocos km de la frontera*

Las poblaciones fronterizas de Sudamérica abarcan un 4% de la población total (~16 Mn de personas)

Potenciales Soluciones: para evitar el involuntario y promover el tránsito vecinal

- **Operadores:**
  - **Técnicas**: solucionar problemas de señalización
  - **Comerciales**: comunicar mejor la modalidad de uso, bonificación de casos, tarifas especiales, crear promociones con tarifas especiales en las zonas de fronteras
- **Regulatorios**: regulación y control sobre roaming inadvertido para protección del usuario, promover el tránsito vecinal

En zonas fronterizas, el servicio de roaming enfrenta el desafío de evitar la activación del servicio en forma inadvertida para usuarios que no cruzaron la frontera

Áreas clave		Problemática	Potenciales soluciones
Técnicas	**Superposición de cobertura**	Por aspectos técnicos no es posible limitar la cobertura de RF dentro de las fronteras del país Principal causa del *roaming* fronterizo	Coordinar entre Asociaciones de reguladores o las operadores para limitar el alcance de las frecuencias radiales
Comerciales	**Tarifas**	Facturación automática de tarifas a nivel internacional en vez de locales	Eliminar los cargos de *roaming* Cambiar el sistema de facturación en estos casos especiales
Información al consumidor		Cliente posee limitado conocimiento sobre cargos de *roaming* Centros de atención al cliente lejos de fronteras Representantes poco capacitados en *roaming* Mala atención de problemas-desatención	SMS de bienvenida Campañas de marketing para educar Mejor capacitación y conocimiento en los centros de atención al cliente

Una solución más abarcativa debería considerar

- Definir regiones especiales en fronteras para que las llamadas en esas regiones reciban tratamientos acordes y tarifas especiales
- Controlar *roaming* fronterizo utilizando un software especial, si bien esta opción está limitada a grandes operadoras por su elevado costo

En la experiencia internacional existen casos donde la resolución de los problemas de superposición de cobertura creó oportunidades para crear zonas fronterizas con tratamiento especial para el roaming

	Problema	Actor de intervención	Solución
USA-México	Superposición de cobertura apalancada por la costa geográfica En la frontera criticidad a partir de los últimos años con el cruce de usuarios móviles en ciudades fronterizas	Operadoras	Determinaron zonas especiales donde se aplican tarifas especiales mayoristas entre los operadores Dejando las tarifas minoristas y atención al cliente a cada operador
Irlanda del norte	Mucha superposición de coberturas por las características geográficas	Asociación de regulación	Eliminación de los cargos por *roaming* internacional en ambos lados de la frontera

Contenido del documento

- Larga distancia
- Roaming prepago
- Roaming fronterizo
- **Fraude**
- Iniciativas a discutir

El fraude causa pérdidas significativas para las operadoras (3 a 5% de los ingresos) donde el ~24% suceden en situación de *roaming*

- *Se estima que el fraude causa pérdidas de 3 a 5% de los ingresos totales de operadoras de telecomunicaciones*
- *~24% de pérdidas con fraude suceden en situación de roaming*

Fraudes más comunes en situación de *roaming*

Tipos de Fraude	Casos de fraude más comunes	
	Fraude	**Descripción**
Proceso • Procesos de negocio ineficientes o mal diseñados	• **Suscripción**	• Uso de identidad falsa o robada para obtener acceso a servicios móviles (ej: llamadas telefónicas, datos y *m-commerce*)
	• **Llamadas a número *premium rate* o IRSF** (*International Revenue Share Fraud*)	• Llamadas destinadas a servicios con tarifación diferenciada: - Números *premium rate* (900) - Destinos internacionales con alto coste (ej: naciones en pequeñas islas) - Rangos de numeración de servicios de satélite
	• **Robo de Tarjetas**	• Robo de tarjetas SIM y su posterior activación
	• **Fraude de reventas**	• Ventas falsas para inflar la comisión sobre ventas
Técnica • Fallos técnicos en la configuración, diseño o arquitectura de las redes o terminales de comunicación	• **Clonación**	• Copia de las tarjetas SIM y de los IMEI (*International Mobile Equipment Identities*)
	• ***Hacking***	• Invasión de sistemas inseguros para explorar o vender facilidades de telecomunicaciones
	• **Pirateo**	• Copia de contenidos protegidos por copyright (ej: música, vídeos)
Interna • Generados por personal de las compañías por: - Protocolos permisivos - Seguridad deficiente	• **Créditos falsos de prepago**	• Activación falsa o múltiples reactivaciones de créditos de prepago
	• **Remoción de CDR**	• Remoción de *Call Detail Records* (CDR) de los ciclos de facturación

El proveedor del servicio premium usualmente participa del fraude con el llamador

Frecuente robo de tarjetas de prueba para los escenarios de roaming

Fuentes: CITEL/IIRSA; Billingworld Berlin privacy group, Informa Telecom , GSMA

IMOBIX VALUE PARTNERS IIRSA

El mayor riesgo de fraude en *roaming* es debido a la demora en el intercambio de informaciones entre operadoras.

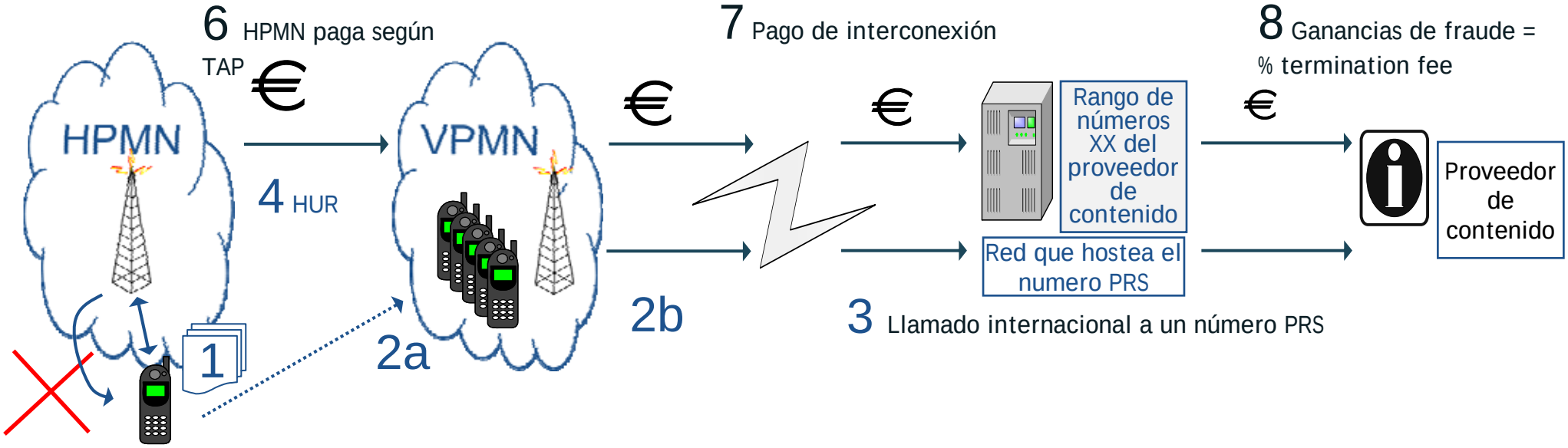
○ Bajo
● Alto

Fraudes más comunes en *roaming*		Frecuencia	Fragilidades específicas al *roaming*	Posibles acciones de combate
Fraudes de procesos	• De suscripción • Llamadas a número *premium rate* o IRSF • Robo de Tarjetas		• **Cambio de CDRs** entre operadoras para llamadas en *roaming* **demoran hasta 24 horas** • **Algunos departamentos anti-fraude no trabajan en los fines de semana** • **Heterogeneidad de las redes VPMN y HPMN** dificulta la integración de sistemas de prevención, detección y respuesta automática	• **Cambio rápido de informaciones sobre usuarios**, especialmente con patrones de alto uso • **Operación anti-fraude 7x24** • **Lista negras** con números *premium rate* o IRSF sospechosos
Fraudes técnicos	• Clonación de tarjetas		• **Más comunes para terminales CDMA y TDMA cuando entran en *roaming* analógico** (AMPS)	• Utilización de **técnicas de encriptación** • **Obligación de protección PIN** (*Personal Identification Number*)
	• Bypass		• No es específico del roaming	• Utilización de herramientas de detección de bypass.

- **Para combatir los fraudes de procesos es clave el cambio inmediato de informaciones** entre las operadoras
- Los **fraudes técnicos por clonación son cada vez menos frecuentes en Sudamérica** por el avance de GSM, aunque el bypass es una de las mayores preocupaciones de los operadores.

Fuentes: Billingworld Berlin privacy group, Informa Telecom, GSMA

El mecanismo del fraude organizado (IRSF*) implica la participación de 3 entidades fraudulentas que comparten la ganancia



1 "Usuario" compra SIM con intenciones de fraude (utiliza normalmente por algunos meses)

2 (a) SIM de "Usuario" son enviadas al exterior para un cómplice y

(b) típicamente realiza llamadas non-stop utilizando SIM gateways para números nacionales premium o para otros países de tarifas de terminación caras (> 5-10€/min)

3 La llamada es ruteada vía una o mas operadoras de larga distancia para un B-party number (proveedor de contenido)

4 Cuando el uso del IMSI llega al limite del HUR la VPMN informa a la HPMN por email en 36 horas.

5 La HPMN revisa manualmente las alarmas HUR alerts y suspende los IMSI relevantes. Y el "usuario" nunca va pagar la cuenta.

6 La HPMN tiene que pagar para el VPMN los encargos de roaming enviados en los archivos TAP.

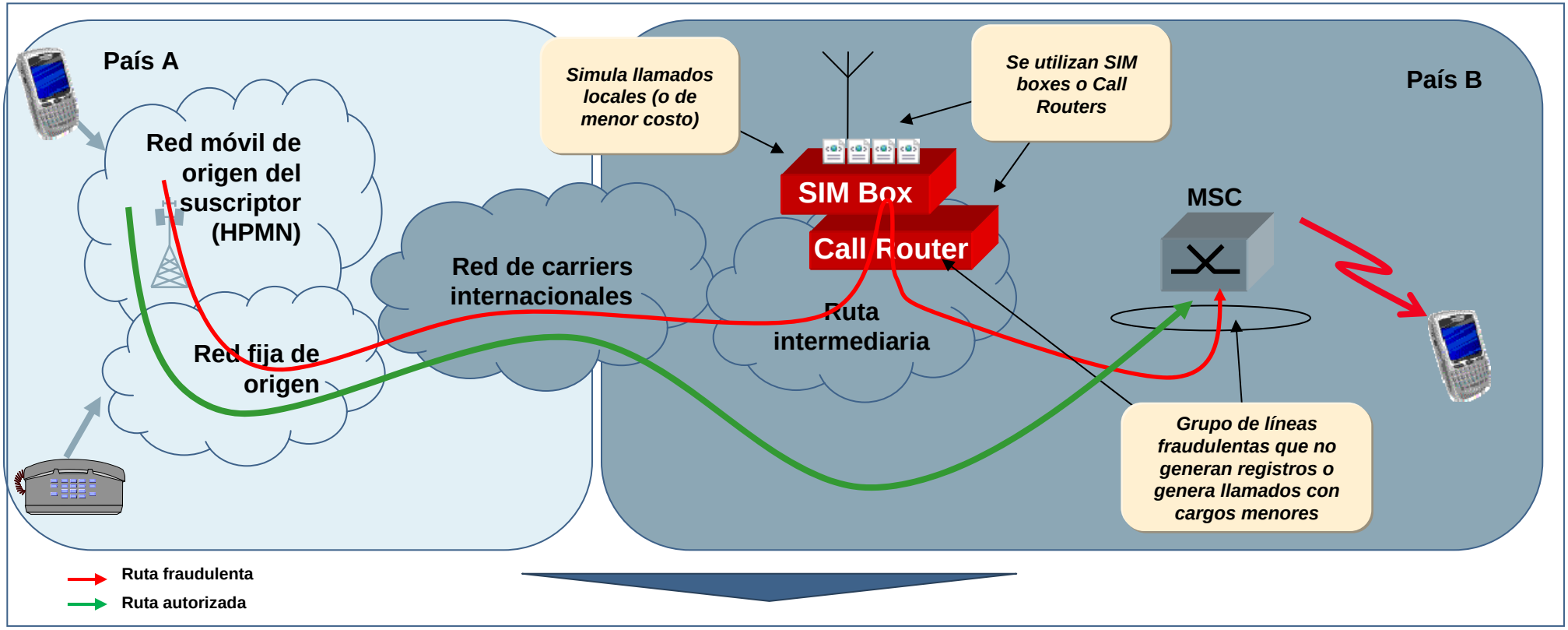
7 La VPMN paga a las operadoras de larga distancia los costos de interconexión, y esta paga a la operadora donde la llamada fue terminada.

8 La operadora que termino la llamada paga un porcentual para el content provider de la llamada.

* International Revenue Share Fraud

El uso de rutas fraudulentas para la transmisión del tráfico de voz (bypass) es un fraude que suele generar serios problemas de calidad como ser la pérdida del CLI

Bypass o uso de rutas fraudulentas de tráfico

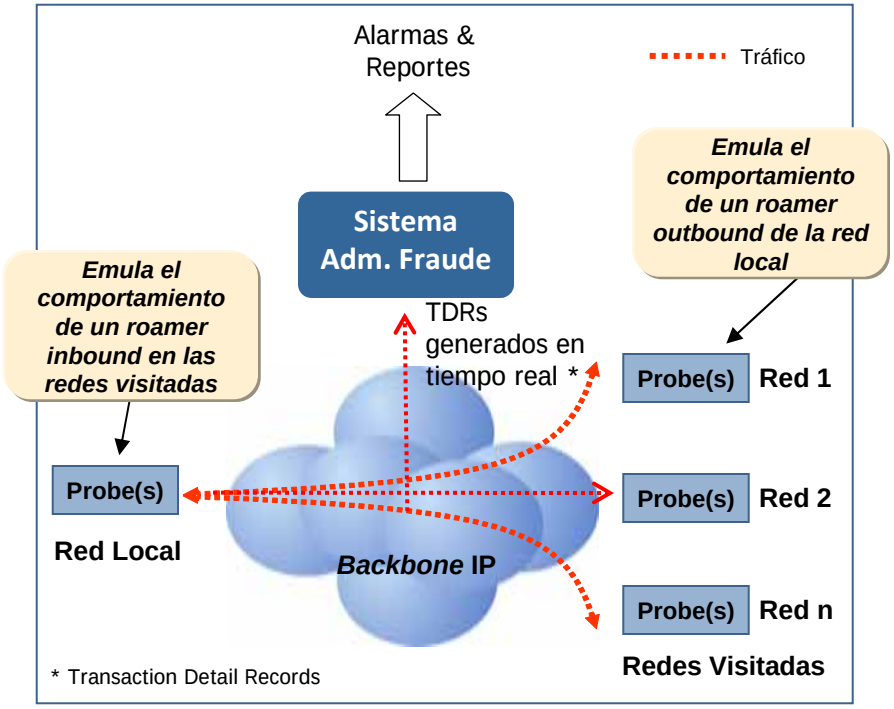


- Un llamado vía una ruta normal cuesta ~€ 0,8 (0,5 originación y 0,3 terminación)
- En el caso de Bypass una llamada vía VoIP cuesta ~€ 0,15 (0,05 terminación). El operador en el país B pierde un **83% del ingreso** (0,3-0,05)
- Una llamada fijo-móvil cuesta ~€ 0,25 (0,15 originación y 0,1 terminación). Un bypass genera una pérdida de (0,1 – 0,05) es decir una **pérdida del 50%.**

Equipos llamados probes permiten emular el comportamiento de los usuarios y detectar en forma no intrusiva el caso del bypass u otros fraudes de tipo interno

Funcionamiento

- Cada par de *probes* (o sondas de prueba) puede **emular el comportamiento entre dos subscriptores móviles** en distintos lugares del mundo.
- Las plataformas no son intrusivas, por lo tanto, pueden instalarse sin requerir autorización de los diferentes operadores.
- Permite a un operador capturar el tráfico de sus *roamer* en el exterior y el de los *roamers* de sus socios en su red, en tiempo real.



Las regulaciones anti-fraude son poco frecuentes y suelen enfocarse en procedimientos y políticas anti-fraude

NO EXAHUSTIVO

País	Regulación de anti-fraude	Disposiciones	
		Obligación de implementar procedimientos/políticas anti-fraude	**"Criminalización" de los actos de fraude en telecomunicaciones**
Argentina	• **Ley No 25.891 de 2004 (conocida como "Ley Blumberg")**	✓ • Cambio diario de lista negra de terminales robadas o hurtadas entre operadoras y la entidad reguladora	✓ • Represión con prisión para aquellos que cometen fraude
Brasil	• **Resolución Anatel N° 410 de julio de 2005 – Reglamento General de Interconexión**	✓ • Procedimientos anti-fraude en los contractos de interconexión	
Colombia	• **Circular Externa Conjunta N° 011 de 2001 de la Superintendencia de Industria y Comercio** • **Resolución CRT N° 1732 de 2007**	✓ • Política anti-fraude para los operadores fijos y móviles ✓ • Manejo confidencial de los datos de usuarios y lista negra de terminales	
Ecuador	***Ley Reformatoria al Código Penal No. 99-38 mediante la cual se reforma el artículo 422 , publicada en el Registro Oficial No. 253 del 12 de agosto de 1999***	✓ • Exige estar legalmente facultado mediante concesión o licencia para prestar servicios de telecomunicaciones	✓ • Represión con prisión para aquellos que cometen fraude con dos a 5 años

- Sin embargo, **los operadores sudamericanos adoptan procedimientos anti-fraude entre ellos formalizados en sus acuerdos de interconexión,** mismo cuando no existen regulaciones impositivas
- **Las regulaciones que criminalizan los actos específicos de fraude en telecomunicaciones son muy raras**, porque si considera que tales actos son previstos en la legislación criminal general

Fuente: Página Web de los reguladores, Análisis del equipo de trabajo

Contenido del documento

- Larga distancia
- Roaming prepago
- Roaming fronterizo
- Fraude
- **Iniciativas a discutir**

¿Que medidas regulatorias pueden promoverse para resolverse los problemas planteados?

Larga distancia internacional	• **Utilizar redes IP de Nueva Generación** para cursar directamente el tráfico entre operadores. Utilizar redes de proveedores IPX o construir redes propias. Regular la liberación de licencias. • **Evitar rutas fraudulentas** que aumentan los precios y bajan la calidad. Ver Fraude.
Roaming prepago	• **Impulsar el *roaming* prepago regional** a través de modelos de conectividad abierta que eliminan la inversión inicial requerida.
Roaming fronterizo	• **Crear zonas de tránsito vecinal** con tratamiento local de las llamadas. Regular las pautas de funcionamiento entre operadores. • **Disminuir los inconvenientes de roaming involuntario** a través de regulación y control específico.
Fraude	• **Evitar rutas fraudulentas** a través de controles y reglamentación específica. Evitar la evasión de impuestos por parte de los gobiernos y de ingresos por parte de los operadores.
Otras…	• **Transparentar la calidad de los servicios** a través del control específico de la calidad de las señales en frontera, el uso de rutas autorizadas, la calidad del servicio en general.