

UNIVERSIDAD NACIONAL DE INGENIERÍA
FACULTAD DE INGENIERÍA ELÉCTRICA Y
ELECTRÓNICA



PROYECTOS SOBRE REDES DE NUEVA GENERACIÓN 3G Y
APLICACIONES PARA LA BANCA RURAL

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ANDY VALER BRAVO

PROMOCIÓN
2000-I

LIMA – PERÚ
2013

**PROYECTOS SOBRE REDES DE NUEVA GENERACIÓN 3G Y APLICACIONES PARA
LA BANCA RURAL**

A mis padres y familia por poner su entera
confianza en mí, aprendiendo de ellos que
nada es imposible y que con perseverancia se
llega siempre a la meta.
A todos mis amigos, quienes me brindaron su
apoyo incondicional y su sincera amistad..

SUMARIO

El objetivo de este trabajo es presentar el escenario tecnológico para implementación de redes corporativas implementando así servicios que van sobre una red de dato con tecnologías móviles 3G, voz sobre IP, administración, seguridad y redes inalámbricas.

El presente informe muestra la implementación realizada por una institución financiera donde se hace un despliegue de la solución a las zonas alejadas de la ciudad con tecnología 3G, se presenta el diseño de la arquitectura de red con la finalidad de entregar servicios financieros a las zonas rurales.

La tecnología utilizada para el desarrollo de este proyecto es de mucha utilidad por su facilidad de despliegue, su movilidad y bajo costo de planta externa.

El diseño y arquitectura de red se desarrolla a partir la consideración de poder contar con infraestructura del carrier que cuente con 3G y de equipos de comunicación con la misma tecnología.

Se muestra las especificaciones técnicas que deben de cumplir el equipo de comunicación que conecta con la red del carrier en 3G así como de los componentes de la red, se incluye el plan de trabajo establecido para la implementación de red propuesto en el ambiente productivo de la entidad bancaria.

Se describe las etapas de la implementación en la cual se hace un análisis de tráfico para la aplicación principal la cual entregará servicio en los lugares remotos, se incluye componentes de seguridad como alarmas, escenarios donde se requiere que la transacción se encripta a través de los dispositivos de comunicaciones, hasta llegar a la sede principal para completar la transacción generada desde la zonas rural.

ÍNDICE

INTRODUCCIÓN	1
CAPÍTULO I	3
MARCO TEÓRICO CONCEPTUAL	3
1.1 Antecedentes del problema (Marco histórico).....	3
1.2 Servicios, aplicaciones y su clasificación	5
1.2.1. Aplicaciones real – time.....	5
1.2.2. Aplicaciones non real – time	5
1.2.3. Requerimientos para los servicios a implementar	6
1.2.4. Sensibilidad de las aplicaciones.....	7
1.2.5. Clases de servicio.....	8
1.2.6. Multimedia.....	8
1.3 Redes y subredes	10
1.3.1 Direccionamiento IPv4	10
1.3.2 VLAN	11
1.3.3 SNMP: Simple Network Management Protocol.....	16
1.4 Seguridad	24
1.5 Firewall	24
CAPÍTULO II	25
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA	25
2.1 Descripción del problema	25
2.2 Objetivos del informe	25
2.3 Evaluación del problema.....	26
2.4 Limitaciones del informe	26
2.5 Síntesis del informe.....	26
CAPÍTULO III	28

DETERMINACIÓN DE LA NECESIDAD	28
3.1 Demanda potencial del servicio	28
3.2 Evaluación de la competencia	29
CAPÍTULO IV	30
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS	30
4.1 Introducción	30
4.2 Solución de la arquitectura de red	30
4.3 Costos y tiempos de ejecución	31
CONCLUSIONES Y RECOMENDACIONES	32
ANEXO	34
BIBLIOGRAFÍA	74

INTRODUCCIÓN

En mayo del año 2000, el Estado peruano entrega a concesión la tercera banda (Sistema de Comunicaciones Personales o PCS de 1900 Mhz) a Telecom Italia Mobile (TIM) el cual en enero de 2001 ingresa al Perú con tecnología GSM la cual busca ofrecer nuevos servicios como transmisión de datos y acceso inalámbrico a Internet a través de los teléfonos celulares y en los años 2004-2005: TIM comienza a sacar planes de datos, GPRS y EDGE a velocidades con tasas de 33.6kbps y 128kbps en descarga, respectivamente. Desde el 2007 a la fecha Claro, dispone del estándar UMTS (basado en GSM) para la banda ancha móvil (para luego pasar a HDSPA, HSPA+ la tecnología actual).

El objetivo de este trabajo es utilizar la alternativa de servicio de ancho de banda con la tecnología GSM/GPRS/3G existente en el estado peruano por medio del carrier móvil, proveedor de datos a utilizar en este trabajo. Para tener disponible este servicio es necesario contar con un equipo que realice el trabajo de poder enrutar el tráfico desde el cajero automático ubicado en un punto dentro del estado peruano (con cobertura de GPRS/EDGE/3G), de tal forma que se propone poder utilizar el equipo con características móviles y de router, como por ejemplo: Digi Transport GSM que es un Wireless WAN Gateway/Router (Ver ANEXO A: CATÁLOGO DE EQUIPOS Y ESPECIFICACIONES TÉCNICAS DEL EQUIPO MÓVIL), el equipo hace posible utilizar la tecnología disponible en el país de tal forma que la solución completa puede brindar movilidad, disponibilidad a bajo costo.

Se define como componente necesario para este proyecto al cajero automático utilizado por los bancos y PYMES el cual utiliza dinero electrónico con tarjetas de crédito y débito, el cajero automático con ayuda de la tecnología móvil es trasladado a las zonas rurales.

Para cumplir con todo lo expuesto, este informe se divide en seis capítulos, los cuales son descritos a continuación:

El capítulo I presenta el marco teórico, describiendo los antecedentes, se incluye también las bases teóricas para la tecnología utilizada en el presente trabajo, se hace hincapié a la teoría del equipamiento y el software, se incluye la normativa del sistema, sus definiciones y términos utilizados en este campo de la tecnología, se incluye un cálculo del impacto que tendrá los servicios adicionales sobre la red de datos.

El capítulo II presenta el planeamiento de ingeniería donde se incluye la descripción del problema, objetivos del trabajo, evaluación del problema, se incluye información de las limitaciones de la solución y finalmente se hace una síntesis del trabajo.

El Capítulo III presenta la determinación de la necesidad, basado en los proyectos con tecnología móvil aplicados a las zonas rurales del estado peruano.

Se describen los servicios a implementar sobre la red de la institución financiera y la red del carrier de servicio móvil, al igual que las aplicaciones y los requerimientos de éstas para que sean transmitidas sobre una red de datos móvil, se describe el análisis y capturas realizadas con un analizador de protocolos donde se muestra los tiempos y tramas de datos que reflejan el comportamiento del proceso del tráfico de datos del tipo transaccional.

El capítulo IV presenta la ingeniería del proyecto, las implementaciones, configuración y diseño de redes, así como también ajuste de la red para cada servicio a implementar y se dan las fórmulas para cálculo de ancho de banda y opciones para saber parámetros adecuados, seguidamente se describen los protocolos y estándares desarrollados.

En el capítulo V se presenta los costos asociados al proyecto en mención los cuales son calculados considerando costos de importación de equipos y costos operativos, se presenta la operación y mantenimiento, definiendo a detalle las actividades necesarias para que la operación del sistema sea óptima en cuanto sean factibles las actividades descritas.

Finalmente se da a conocer las conclusiones y recomendaciones que dan como resultado la buena práctica de implementar proyectos para aplicaciones en zonas rurales, de igual forma se incluye la bibliografía.

CAPÍTULO I

MARCO TEÓRICO CONCEPTUAL

Este capítulo se desarrolla con la finalidad de presentar de una manera clara y concisa los conceptos teóricos que son importantes para poder desarrollar el presente informe.

1.1 Antecedentes del problema (Marco histórico)

En la actualidad, las instituciones financieras tienen la necesidad de brindar a los usuarios finales servicios adicionales con aplicaciones que involucran proyectos sobre redes de nueva generación 3G y aplicaciones para la banca rural.

Acceder a servicios en las zonas rurales requiere llevar tecnología de transporte de datos a las localidades donde se consideran polos de desarrollo, donde los turistas y exportadores de productos forman parte del desarrollo de la población.

Primera Generación 1G: A comienzos de los 80's predominaba en el mundo la Telefonía celular analógica y sólo transmitiendo voz.

Cada país desarrolló su propio sistema, limitando su uso a solo dentro de sus fronteras y evitando de esta forma economías de gran escala y en la década de los 90's en la mayoría de estos países, los sistemas 1G fueron reemplazados por los que traían tecnología de segunda generación.

Segunda generación 2G: En los años 90's se da la necesidad del cambio de análogo a digital con el fin de optimizar el uso del espectro de radio frecuencia.

Coexisten 4 tecnologías 2G: GSM, CDMA, TDMA y PDC, a continuación se indican sus respectivos acrónimos:

GSM: Global System for Mobile Communication.

CDMA: Code Division Multiple Access.

TDMA: Time Division Multiple Access.

PDC: Personal Digital Cellular (JAPON)

Se muestra a continuación una distribución de estas tecnologías a nivel mundial.

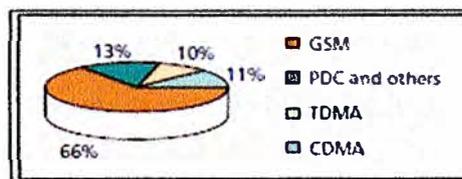


Fig.1.1: Mobile Standard global distribution

(Fuente: EMC: Agosto 2001)

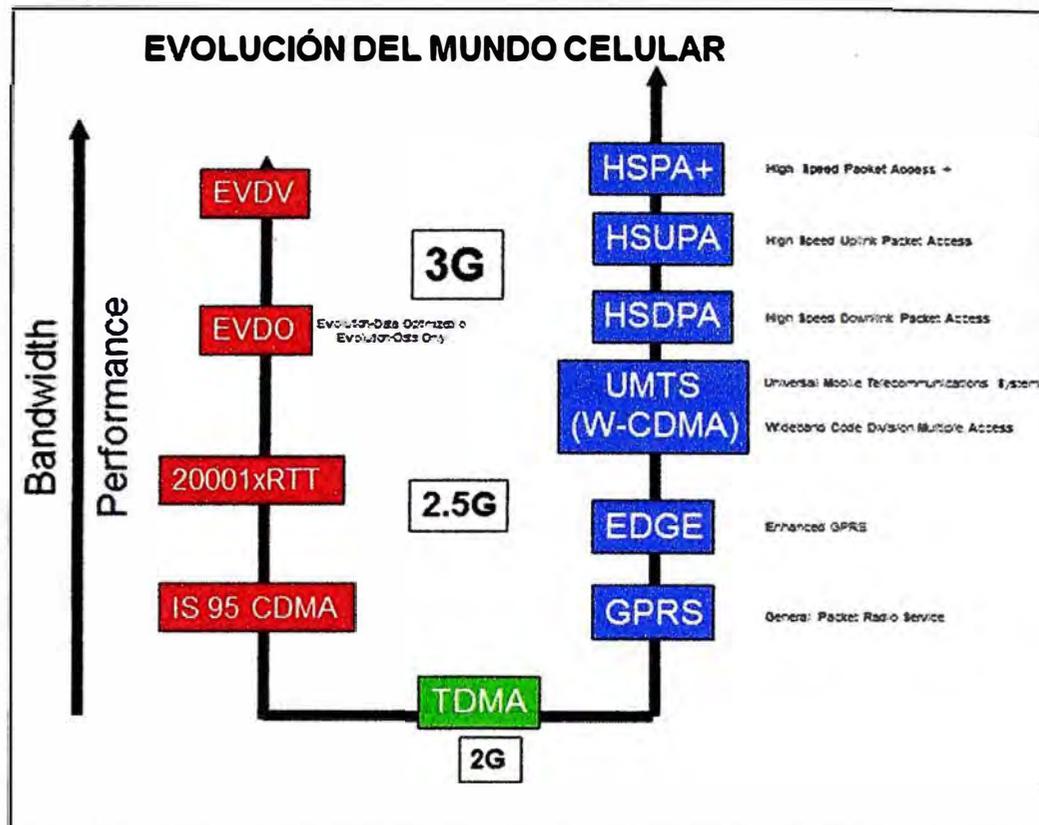


Fig1.2: Evolución del Mundo CELULAR

(Fuente: www.digi.com)

Segunda generación y media 2.5 G: Surgió como una tecnología intermedia debido al alto costo que ocasionaba la actualización de los sistemas 2G a 3G tanto en su infraestructura como en las limitaciones físicas que imponían los dispositivos de esta nueva tecnología 3G, en la tecnología 2.5G se desarrollaron por ejemplo:

GPRS: General Packet Radio Service: permitía sin mandar voz, transmitir información a través de una red de telefonía móvil.

EDGE: Enhanced Data rate GSM Evolution era un formato de modulación que ofrecía mayores velocidades de transmisión de data ocupando el mismo ancho de banda del GSM.

Tercera generación 3G: También es conocida como IMT 2000 (International Mobile Telecommunication), la necesidad de una nueva tecnología se hizo evidente, con la necesidad de más capacidad, nuevas frecuencias y velocidades más altas de transmisión en 3G, sistemas móviles de comunicación como GSM y CDMA convergen dando no solo voz sino también data.

Desafortunadamente el objetivo de tener un único estándar internacional no tuvo éxito y dos importantes sistemas propuestos para 3G han sido reconocidos por la International Telecommunication Union (ITU), UMTS tiene dos modos diferentes pero relacionados: CDMA direct spread: Wideband CDMA, también llamado FDD (Frequency division

duplex) y CDMA – TDD (Time - division duplex).

1.2 Servicios, aplicaciones y su clasificación

Para la definición de servicios a implementar en la red, primero clasificaremos las aplicaciones las cuales clasifican por su naturaleza como: Real – time y Non real – time, en la TABLA N°1.1 muestra un resumen de los tipos de aplicaciones definidas en el presente trabajo.

TABLA N° 1.1 – REQUERIMIENTOS DE LAS APLICACIONES

(Fuente: Elaboración propia)

	NON REAL TIME		REAL TIME		
	Teleproceso POS Chat Cajeros automáticos Telecomando Telecontrol	LAN to LAN Internet e - mail Browsing File Transfer Client/Server	Voz	Video Conferencia	Video
Throughput	1.2 a 9.6 K	1.2 K a 2 M	4 a 16 K	128 K	33.6 K a 34 M
Retardo	0.5 a 2 seg.	0.5 a 60 seg.	< 0.5 seg.	< 0.5 seg.	0.5 a 5 seg.
Jitter	insensible	insensible	sensible	sensible	sensible
Errores	insensible	insensible	tolerante	sensible	sensible

1.2.1. Aplicaciones real – time

La descripción para este tipo de aplicación es que no admiten retransmisión de paquetes ni control de flujo. Las cuales pueden ser: No interactivas e Interactivas.

a. Aplicaciones no interactivas: Admiten retardo pero no su variación: JITTER. Como por ejemplo: Música, video-streaming point – to – point o multicast, broadcasting de voz, música o video.

b. Aplicaciones interactivas: No admiten gran retardo, ni su variación (JITTER). Hay una respuesta entre dos o más entidades que se estén comunicando, como por ejemplo: Voz - Telefonía: Si hubiese algún retardo en la transmisión de la voz la conversación se va a ver afectada, llegando en algunos casos a ser inteligible, video - videoconferencia: Para este caso los recursos de red necesarios para la transmisión de video son mayores.

1.2.2. Aplicaciones non real – time

Este tipo de aplicaciones admite retransmisión de paquetes y control de flujo, como ejemplo de este tipo de aplicaciones podemos citar a los siguientes:

- Teleproceso, telecomando y telesupervisión.

- POS (Point of Sale).
- Correo electrónico (e-mail) y Chat.
- Transferencia de archivos, aplicaciones cliente – servidor.
- Browsing: Bases de datos, Web (hay una tendencia a multimedia con contenido real-time).
- Fax (fax-relay o store and forward).

1.2.3. Requerimientos para los servicios a implementar

Como se aprecia en el párrafo anterior las aplicaciones tienen ciertos requerimientos según su naturaleza. Para esto se tienen diversos parámetros que hay que tomar en cuenta cuando se va a diseñar o especificar una red multiservicio para que el usuario no tenga problemas al momento de hacer uso de dichos servicios

a. Ancho de banda (BW): El primer problema de mayor preocupación cuando se diseña una red es la limitación en el recurso de ancho de banda.

Por ejemplo: El ancho de banda necesario para video depende de la cantidad de: pixels, colores, cuadro por segundo y mecanismo de compresión.

Para el caso de tráfico de voz depende del codec y de las muestras de voz por paquete. Así mismo, el ancho de banda por llamada depende del medio de enlace de datos y del protocolo usado.

b. Retardo (Delay): El retardo es la cantidad de tiempo que toma la señal para salir del origen y llegar al destino. El retardo no afecta a la calidad, pero sí a la interacción.

El retardo siempre está presente, sólo que en una conversación telefónica convencional es tan pequeña que el oído humano no lo aprecia.

En los sistemas telefónicos convencionales, el retardo se debe principalmente a la demora en la propagación de la señal, evidente en transmisión vía satélite (250 milisegundos para un salto satelital a un satélite geoestacionario ubicado a 36,000 Km. de altitud).

Todo sistema digital tiene retardo debido al tiempo de procesamiento de las muestras digitales, especialmente si el tratamiento implica una compresión y descompresión digital hecha por procesadores digitales de señales (DSPs).

La voz requiere bajo retardo y poca variación del mismo.

A diferencia del tráfico de SNA requiere retardo mínimo para evitar el time – out de las sesiones, esto puede significar pérdida de conexión a nivel de aplicación aún cuando la conexión se restablezca.

c. Jitter (Variación del retardo): El jitter es la variación del tiempo de llegada entre paquetes. Es un problema que existe sólo en las redes de paquetes. Por ejemplo: En un ambiente de voz paquetizada, se espera que el origen envíe los paquetes a intervalos

regulares (por ejemplo: cada 20 ms). Estos paquetes de voz pueden verse retardados a través de la red de paquetes y no llegarán en los mismos intervalos regulares de tiempo a la estación receptora. La diferencia entre cuando el paquete es esperado y cuando ha sido recibido es el jitter.

d. Tasa de error de bits (BERT): Los errores de bits ocurren en los sistemas de transmisión digital debido a fallas de cableado, mal funcionamiento de equipos, niveles de señal débil, o varias otras razones. Los errores de bits se caracterizan porque son cambios ocasionales y no periódicos de la señal transmitida (por ejemplo un "0" reemplazado por un "1") y son usualmente medidos en términos de la tasa de error de bits (BER). Si el BER de un circuito es 10^{-6} , significa que hay un bit errado de cada millón de bits transmitidos.

En una red de paquetes, un único bit errado daña todo un paquete. En situaciones con alta tasa de pérdida de bits es muy importante reducir este valor ya que esto afecta a la aplicación. Los errores de bits son detectados, generalmente, con algoritmos de CRC (Cyclic Redundance Check) que confirman la integridad de la data de un paquete.

Por ejemplo: IPX (Novell) requiere baja tasa de error y TCP/IP descarta la ventana (Windows) completa si pierde un segmento.

Para redes de voz sobre IP, el campo CRC de la cabecera UDP es responsable de detectar errores de bit que pueden producirse por procesamiento de software en la estación receptora. El campo CRC en la cabecera UDP no es generalmente requerida para corregir errores de bit que ocurren a través de una línea de transmisión, debido a que la cabecera de la capa de enlace de datos usualmente incluye un campo CRC para este propósito.

e. Prioridad y Disponibilidad: La prioridad en cada Red puede cambiar en el tiempo para cada aplicación que corre sobre la red, para proveer la priorización apropiada sobre una red de datos congestionada, esta debe tener conocimiento de las características de las aplicaciones luego definir determinada prioridad.

Por ejemplo: Se suele definir prioridad a cierto tipo de tráfico para transacciones bancarias mientras que en otro lado de la red (ejemplo en un call center) se puede definir que el tráfico de voz tiene más prioridad que la data.

Mientras que definir la disponibilidad depende del contrato de nivel de servicio (SLA – Service Level Agreement). Por ejemplo, 10 minutos de caída: por año = 99.998%, por mes = 99.997%.

1.2.4. Sensibilidad de las aplicaciones

Debido a que las aplicaciones pueden tener diversos requerimientos, hay que saber cuál de ellos son los que van a afectar su performance.

El tráfico multimedia integra todas estas aplicaciones y requiere que la red respete la sensibilidad de cada una.

1.2.5. Clases de servicio

En la TABLA N° 1.2 se tiene una clasificación referencial de servicio por niveles. Puede variar según el proveedor del servicio. El costo de la clase de servicio es mayor a medida que las especificaciones son más estrictas.

TABLA N° 1.2 – CLASES DE SERVICIO

(Fuente: Elaboración propia)

Servicio/QoS	Gold/High	Silver/Medium	Bronze/Low
Web browsing	Incoming>6Kbps	Incoming<=6Kbps or Latency<500ms	Incoming<=2Kbps or Latency<800ms
	Latency<500ms		
File transfer	Bandwidth>20Kbps	Bandwidth<=20Kbps	Bandwidth<=5Kbps
e-mail	Bandwidth>100Kbps	Bandwidth<=100Kbps	Bandwidth<=2Kbps
VoIP	Bi-directional>5Kbps	Bi-directional<=5Kbps or Packet Loss<25% or Latency<700ms	Bi-directional<=2Kbps or Packet Loss>25% or Latency>=700ms
	Packet Loss<5%		
	Latency<150ms		
Video	Bi-directional>48Kbps	Bi-directional<=48Kbps or Packet Loss<=25% or Latency<500ms	Bi-directional<=4Kbps or Packet Loss>25% or Latency>=500ms
	Packet Loss<5%		
	Latency<300ms		

1.2.6. Multimedia

Multimedia es cualquier combinación de texto, arte gráfico, sonido, animación y video que llega a nosotros por computadora u otros medios electrónicos. Es un tema presentado con lujos de detalles. Cuando conjuga los elementos de multimedia - fotografías y animación deslumbrantes, mezclando sonido, vídeo clips y textos informativos - puede electrizar a su auditorio; y si además le da control interactivo del proceso, quedarán encantados. La multimedia se compone, como ya se describió, de combinaciones entrelazadas de elementos de texto, arte gráfico, sonido, animación y video.

a. Formatos de audio

- WAV (Audio pre-generado)
- MIDI (Musical Instrument Digital Interface): Interface digital para instrumentos musicales.
- MP3 (MPEG-1 Layer 3) Calidad CD con compresión de 10:1
- RealAudio (Realnetworks)

b. Formatos gráficos

- BMP (Bit Mapped): Mapa de bits.
- GIF (Graphics Interchange Format): Es un formato de archivos comprimidos de 8 bits, típicamente para una resolución de 256 colores.
- JPEG (Joint Photographic Expert Group): Es un formato de archivo y un algoritmo de compresión. Tiene un formato de compresión de 24 bits.
- DIB (Device Independent Bitmap)
- TIF (Tagged Information Format): Es usado para el intercambio de documentos entre aplicaciones y plataformas de computadoras.
- Vector Oriented
- WMF (Windows Metafile Format): Es un vector gráfico y es editable con muchas aplicaciones basadas en Windows tales como Office.
- VSD (Visio Standard Drawing): Es un formato basado en vectores que es editable con el programa Visio.
- PDF (Portable Document Format): Es un formato de documentos independiente de la plataforma, sistema operativo y aplicación, que permite la visualización, impresión y edición de documentos basados en PostScript sin requerir el uso de la aplicación nativa.

Los siguientes son términos que permiten especificar un formato gráfico:

- Graphic Format: pixel o vector imagen.
- Image Resolution: Es el número de pixels por unidad de área usado en una imagen.
- Pixel: Bloque básico para la construcción de una imagen o mapa de bits.
- Pixel Depth: El número de bits por imagen. La profundidad de pixels controla el número de tonos de gris que contiene una imagen.

c. Formatos de video, videoconferencia , fax , H323

c.1 Video:

- MPEG-1: 1 a 1.5 Mbps (calidad VHS)
- MPEG-2: 6 a 20 Mbps
- MPEG-4: (integración de video digital, gráficos interactivos y multimedia)
- AVI (Audio Video Interleave de Video for Windows, de Microsoft)
- Indeo 3.2: 200 a 300kbps (Intel)
- RealVideo: + 0 – 64 kbps (Realnetworks)
- Quicktime: (Apple)

c.2 Videoconferencia:

- Netmeeting, H.323, H.324, RTSP

c.3 Fax:

- G3, G4, T.30, T.38

1.3 Redes y subredes

1.3.1 Direccionamiento IPv4

Para poder entender el direccionamiento IP de toda una dirección IP está formada por 32 bits agrupados en 4 octetos, la notación decimal de una dirección IP podría ser por ejemplo: 172.19.32.4, su correspondiente notación binaria sería: 10101100 00010011 00100000 00000100, es única para cada equipo e indica el número de red y el host.

Se muestra de la forma siguiente:

TABLA N° 1.3 – NOTACIÓN DECIMAL Y BINARIA

(Fuente: Elaboración propia)

Decimal	172	19	32	4
Binaria	1010 1100	0001 0011	0010 0000	0000 0100

Explicaré el concepto de máscara donde aquellos bits que están a 1 en la máscara hacen referencia a los bits que en la dirección IP hacen referencia a la red y los que están a 0 hacen referencia a los bits que en la dirección IP hacen referencia al host, Por ejemplo, supongamos la siguiente máscara: 255.255.0.0, esa máscara en binario quedaría: 11111111 11111111 00000000 00000000

Se muestra de la forma siguiente:

TABLA N° 1.4 – NOTACIÓN DECIMAL Y BINARIA DE RED

(Fuente: Elaboración propia)

Decimal	255	255	0	0
Binaria	1111 1111	1111 1111	0000 0000	0000 0000

Donde los primeros 16 bits de la dirección IP hacen referencia a la red y los 16 bits a 0 al host.

Supongamos la IP de antes: 172.19.32.4 y que tenga máscara la de arriba. Eso quiere decir que 172.19 hace referencia a la red y 32.4 al host, a partir de ahora para indicar una dirección IP pondremos: 172.19.32.4/16 es decir pondremos la dirección IP /máscara donde el /16 es el número de bits a 1 en la máscara.

La dirección de red correspondiente a una dirección IP es aquella en que todos los bits correspondientes al host están a 0. Ejemplo: Supongamos la IP de antes con la misma máscara es decir 172.19.32.4/16, en formato binario: 10101100 00010011 00100000 00000100, la máscara es: 255.255.0.0 y en formato binario 11111111 11111111 00000000 00000000 donde el host corresponden los 16 últimos bits porque son los que están a 0, revisando la dirección IP y sus 16 últimos bits, es decir 00100000 00000100 se ponen a cero, nos quedaría la dirección IP así: 10101100 00010011 00000000 00000000 o lo que es lo mismo 172.19.0.0. Eso sería la dirección de Red.

Se muestra la dirección de red de la forma siguiente:

TABLA N° 1.5 – EJEMPLO DE NOTACIÓN DECIMAL Y BINARIA DE RED

(Fuente: Elaboración propia)

Decimal	172	19	0	0
Binaria	1010 1100	0001 0011	0000 0000	0000 0000

La dirección de broadcast correspondiente a una dirección IP es aquella en que todos los bits correspondientes al host están a 1, con los valores utilizados se mostraría de la siguiente manera: los 16 bits últimos de 0 se pone a 1 quedando la dirección IP así: 10101100 00010011 11111111 11111111 o sea 172.19.255.255. Eso sería la dirección Broadcast.

En la TABLA N°1.6 se muestra la dirección broadcast de la forma siguiente:

TABLA N° 1.6 – Dirección broadcast

(Fuente: Elaboración propia)

Decimal	172	19	255	255
Binaria	1010 1100	0001 0011	1111 1111	1111 1111

La 1ª dirección de una red es siempre la dirección de red y la última es la dirección de broadcast.

En la TABLA N°1.7 se muestra la dirección broadcast de la forma siguiente:

TABLA N° 1.7 – Dirección broadcast de red

(Fuente: Elaboración propia)

1ra dirección de red	172	19	0	0
.....				
.....				
.....				
Dirección broadcast	172	19	255	255

Para calcular el número de host (n) de una red sería de la forma siguiente: $2^n - 2$ donde n es el número de bits para el host en la máscara (es decir el número de bits a 0 en la máscara).

1.3.2 VLAN

Red de área local virtual y el estándar IEEE 802.1Q, para poder definir y abordar el concepto de VLAN, se realizará una breve descripción de lo que significa LAN (Local Address Network).

- Son redes donde se comparte el mismo dominio de difusión.
- Formados por uno o más segmentos LAN.
- Dispositivos físicamente conectados mediante cableado, repetidores, hubs, bridges o switches.

En la figura 1.3 mostramos un diagrama de red donde se identifica una LAN y se requiere de componentes en Capa3 para conversar con otra LAN en la misma red.

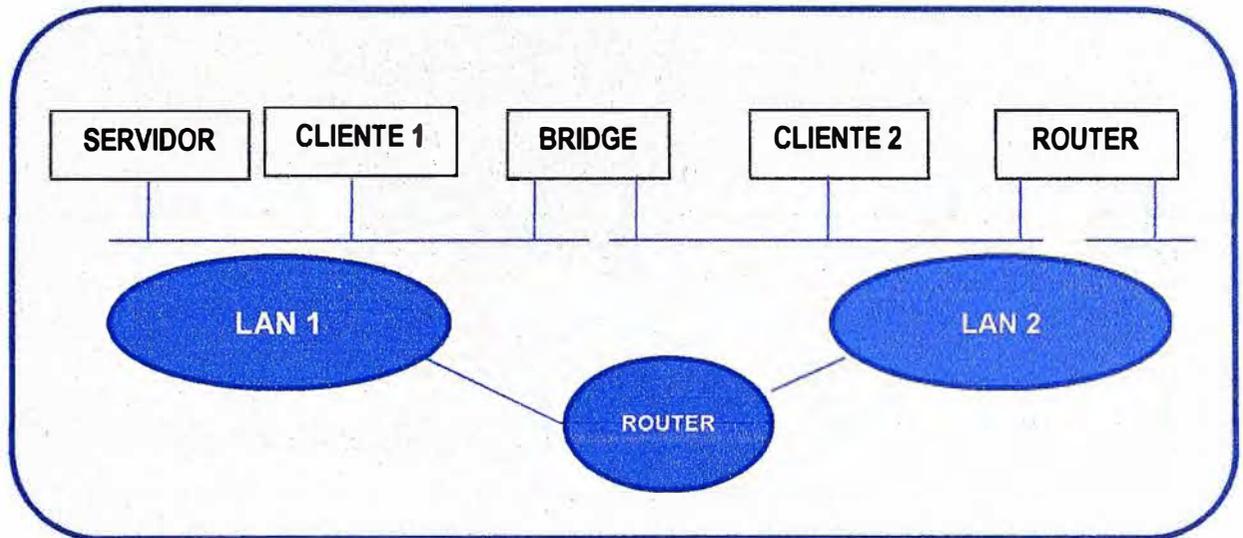


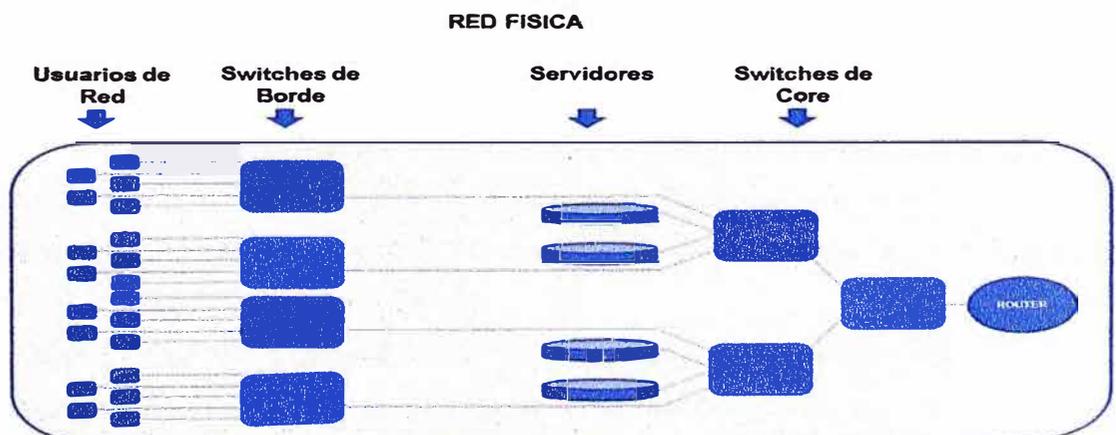
Fig.1.3: Diagrama de Red donde se identifica una LAN

(Fuente: Elaboración propia)

DESCRIPCIÓN DEL PROTOCOLO: LAN virtual (VLAN): Se refiere a un grupo de dispositivos lógicos de red en una o más redes de área local (LAN) que están configurado de manera que puedan comunicarse como si estuvieran conectados a la misma LAN, cuando en realidad se encuentra en un número de segmentos de LAN diferentes. Debido a que las VLAN se basan en lógica, en vez de conexiones físicas, son muy flexibles para la asignación de usuario / host ancho de banda de la gestión y los recursos optimización.

Se definen algunos conceptos de VLAN a continuación:

- Los miembros de la LAN están definidos por el administrador de la red "VIRTUAL".
- Tráfico multicast y broadcast alcanza únicamente miembros de la red.
- Independiente de situación geográfica y de donde se conecten los miembros.
- Separadas mediante el uso de routers.



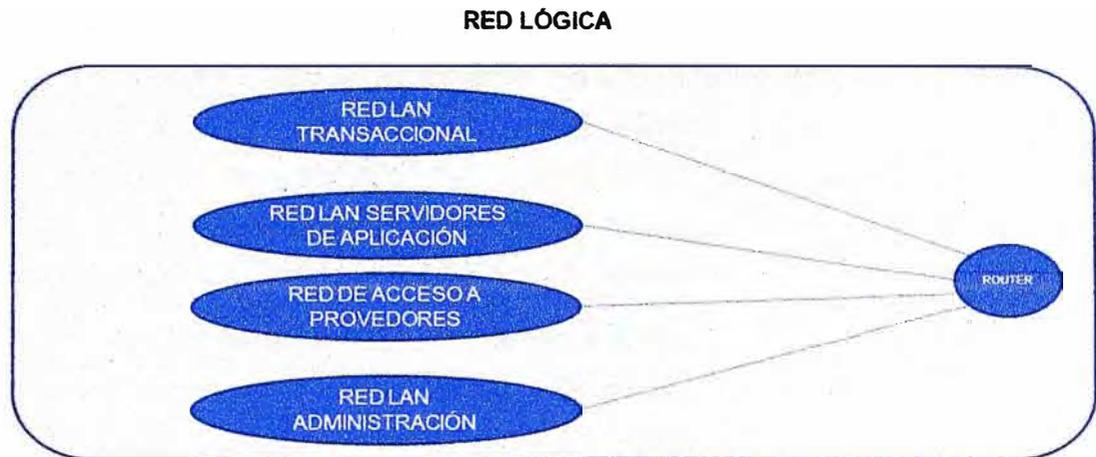


Fig.1.4: Concepto de VLAN identificando en la red de física y Lógica
(Fuente: Elaboración Propia)

Existen los siguientes tipos de redes LAN virtuales:

VLAN BASADO EN PUERTO: Cada puerto de switch es configurado con un access list especificando ser miembro de un set de VLAN.

Los miembros de la VLAN se especifican en base al puerto en el cual se encuentran conectados a los dispositivos de interconexión.

Requiere reconfigurar las VLANs si el usuario se mueve físicamente.

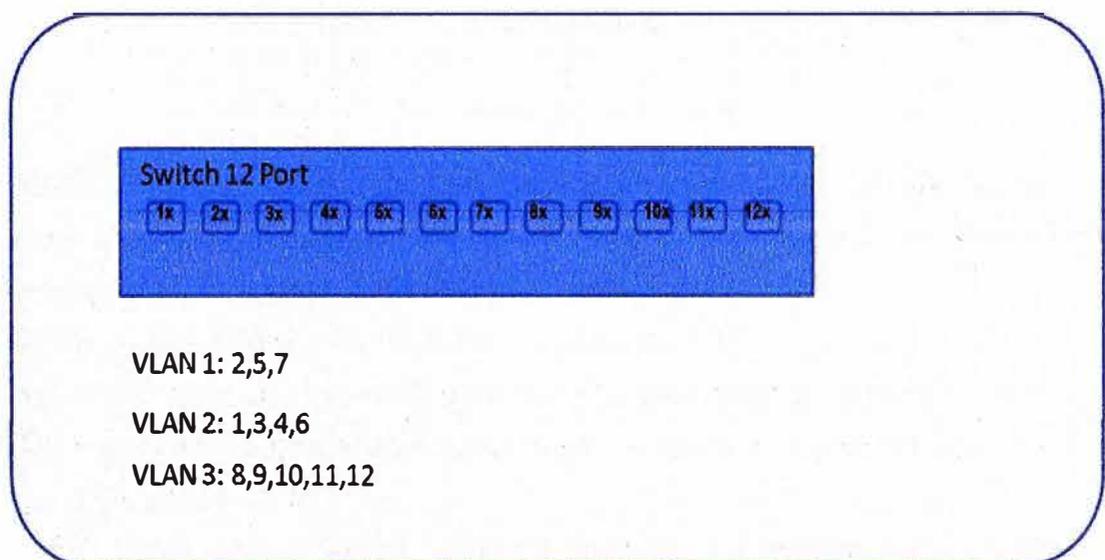


Fig.1.5: Ejemplo de VLAN basado en puerto
(Fuente: Elaboración Propia)

VLAN BASADO EN MAC: Un switch es configurado como access list mapeando de forma individual MAC addresses y su VLAN.

Los miembros de una VLAN dependen de la dirección MAC de las estaciones.

No requiere reconfiguración si las estaciones se mueven físicamente a puertos distintos.

Los miembros de la VLAN deben asignarse inicialmente.

Problemas cuando si existen decenas o cientos de usuarios.

Problemas para identificar a terminales que poseen varias direcciones MAC.

TABLA N°1.8 Ejemplo de VLAN basada en Mac

(Fuente: Elaboración propia)

VLAN	MAC
10	78:AC:C0:4A:A9:6A
11	00:04:2D:03:9F:9A
12	40:13:4A:F4:40:A8
13	00:19:2F:9F:F8:60
14	88:43:E1:AA:CB:C8
15	00:19:2F:9F:F8:60

VLAN BASADO EN PROTOCOLO NIVEL 2, 3, n: Un switch es configurado con una lista mapeando protocolo de capa 3 y el tipo de VLAN de esta forma filtrar el tráfico IP de las estaciones cercanas utilizando un protocolo determinado como el IPX.

Se muestra a continuación ejemplos:

VLANS NIVEL 2: Por tipo de protocolo: Basado en el campo tipo de protocolo del nivel 2

TABLA N°1.9 VLAN por tipo de protocolo

(Fuente: Elaboración propia)

VLAN	PROTOCOLO
2	IP
3	IPX

VLANS NIVEL 3: Direcciones de Subred: Basado en la cabecera de nivel 3, no tiene nada que ver con routing la cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece, requiere más retardo debido a procesamiento.

VLANS NIVEL n: Basados en otros niveles. Ej: VLAN para ftp.

ATM VLAN – Usa protocolo LAN Emulation (LANE) para asignar paquetes Ethernet en celdas ATM y entregarlos a su destino mediante la conversión de una dirección MAC de Ethernet en una dirección ATM.

IEEE 802.1Q: La especificación IEEE 802.1Q establece un método normalizado para etiquetar las tramas Ethernet con información de pertenencia a una VLAN. El estándar IEEE 802.1Q define el funcionamiento de VLAN donde los puentes que permiten la definición, operación y administración de topologías LAN virtual dentro de una infraestructura LAN puenteadas.

El estándar 802.1Q tiene como objetivo tratar el problema de los cómo romper las redes de gran tamaño en partes más pequeñas para transmitir y el tráfico de multidifusión no se agarra más ancho de banda necesario.

El estándar también ayuda a proporcionar un mayor nivel de seguridad entre segmentos de redes internas.

La clave para el IEEE 802.1Q para llevar a cabo las funciones anteriores está en sus etiquetas. 802.1Q compatibles con los puertos del switch se puede configurar para transmitir tramas etiquetadas y sin etiquetar. Un campo de etiqueta que contiene VLAN (y / o prioridad 802.1p) la información se puede insertar en una trama ethernet. Si un puerto tiene un dispositivo compatible con 802.1Q adjunta (como otro conmutador), estas tramas etiquetadas pueden llevar información perteneciente a la VLAN entre los switches, lo que deja que un switch abarca múltiples VLAN. Sin embargo, es importante para asegurar los puertos con y sin dispositivos compatibles con 802.1Q adjunta están configurados para transmitir tramas no etiquetadas. Muchas tarjetas de red para PCs e impresoras no son compatibles con 802.1Q. Si reciben un paquete marcado, no van a entender la VLAN etiquetada. Asimismo, la máxima longitud del frame ethernet para tramas etiquetadas se incrementó en 802.1Q (y también en, 802.3ac) de 1.518 a 1.522 bytes. Esto podría provocar que tarjetas con interfaz de red o más conmutadores dejen los frames marcados con etiqueta como "de gran tamaño".

ESTRUCTURA DEL PROTOCOLO: IEEE 802.1Q TAGGED FRAME FOR ETHERNET:

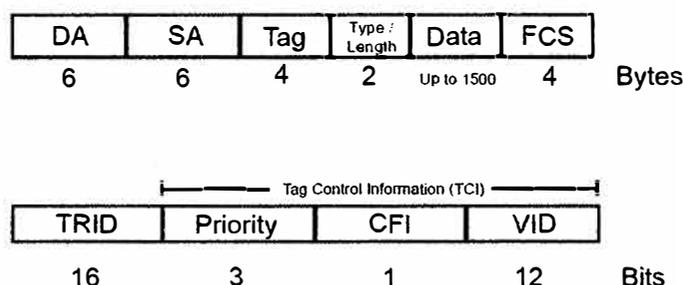


Fig.1.6: IEEE 802.1Q TAGGED FRAME FOR ETHERNET

(Fuente: Network Protocols Handbook, 4th Edition.)

TRID: Tag Protocol Identifier (Typically 0x8100 (default), 0x9100 or 0x9200)

PRIORITY: 802.1P priority levels (0 to 7)

CFI: Canonical Former Indicator 0=canonical MAC 1=non-canonical MAC

VID: Unique VLAN identifier (0 to 4095)

- TPID: Tag Protocol ID, valor definido de 8100 en hexadecimal. Cuando un cuadro tiene la EtherType igual a 8100, este cuadro lleva la etiqueta IEEE 802.1Q/802.1P.
- TCI: Tag Control Information este campo incluye la prioridad (3 bits), indica su forma canonica y Vlan ID.
- Priority: Define la prioridad del usuario, dando ocho niveles de prioridad, IEEE 802.1 define el funcionamiento de estos 3 bits (000 al 111) de prioridad de usuario.

- CFI: Canonical Format Indicator, Indicador de formato canónico siempre se fija en cero por conmutadores Ethernet. TPI se utiliza por razones de compatibilidad entre una red de tipo Ethernet y una red de tipo Token Ring.
- Si una trama recibida en un puerto de Ethernet tiene un conjunto TPI a 1, entonces ese marco no debe ser transmitido, como lo es para un puerto sin etiquetar.
- VID: VLAN ID es la identificación de la VLAN, que se utiliza básicamente por el estándar 802.1Q. Tiene 12 bits y permite la identificación de 4096 (2^{12}) VLAN. De los 4096 posibles VID, un VID de 0 se utiliza para identificar los marcos de prioridad y el valor 4095 (FFF) está reservado, por lo que las configuraciones máximas posibles de VLAN son 4.094.

A continuación se describe más definiciones de VLAN's:

Estándar internacional

Define VLANs de nivel 1 y 2 y niveles superiores.

Compatible con bridges y switches sin capacidad de VLAN.

Soporte de medio compartido y LANs conmutadas.

Soporte de configuración estática y dinámica.

Marcas genéricas: Cisco ISL: Inter Link Switch, 3COM Virtual LAN Trunking

1.3.3 SNMP: Simple Network Management Protocol

Descripción del Protocolo: Simple Network Management Protocol (SNMP). Es un protocolo estándar desarrollado para administrar nodos como: Servidores, estaciones de trabajo, routers, switches and hubs, etc. en una red IP. SNMP habilita la administración de los dispositivos (nodos de red) para administrar el performance de la red, buscar y solucionar problemas de red, es utilizado para planificar y gestionar su crecimiento.

El sistema de administración de red aprende con los traps y noticias de cambios de red que generan los nodos que están habilitados con SNMP.

Una red administrada por SNMP consiste en tres componentes clave: managed devices, agents, Network-Management systems (NMSs).

Un managed device es un nodo de red y contiene a un agent snmp el también reside en el administrador de la red, Managed devices colecta y almacena la información a administrar y hace que esta información esté disponible en el NMS utilizando SNMP.

Managed devices, algunas veces llama a los elementos de red, puede ser routers y access servers, switches and bridges, hubs, computadoras hosts o impresoras.

Un agente es un módulo de software de gestión de red que reside en un dispositivo gestionado. Un agente tiene conocimiento local de gestión de la información y traduce esa información en una forma compatible con SNMP.

Un NMS ejecuta aplicaciones que hacen control y monitoreo de dispositivos

gestionados. NMS proporcionan la mayor parte de los recursos de procesamiento y memoria necesarios para la gestión de la red. Uno o más NMS debe existir en cualquier red gestionada. El cuadro siguiente muestra la arquitectura SNMP.

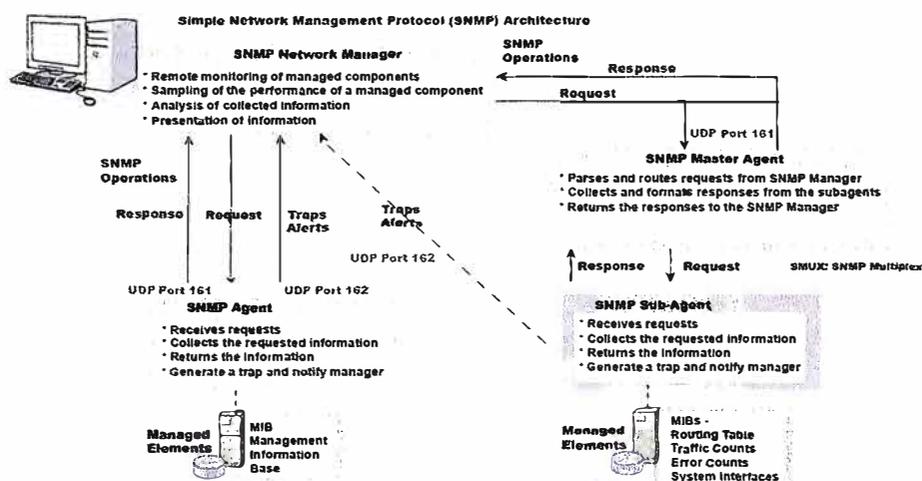


Fig.1.7: Simple Network Management Protocol (SNMP) Architecture
(Fuente: Network Protocols Handbook, 4th Edition.)

En la actualidad, hay tres versiones de protocolos de gestión de red simple definidos: SNMP v1, SNMP v2 y SNMP v3, La tabla siguiente proporciona el resumen de las operaciones y características de las diferentes versiones de SNMP.

TABLA N°1.10 Simple Network Management Protocol (SNMP) Características
(Fuente: Network Protocols Handbook, 4th Edition.)

SNMP V1	CARACTERÍSTICAS Y OPERACIONES BÁSICAS
Get	Usado por el NMS para recuperar el valor de uno o más instancias de objeto de un agente
GetNext	Usado por el NMS para recuperar el valor de la siguiente instancia del objeto en una tabla o una lista dentro de un agente
Set	Usado por el NMS para configurar los valores de la instancia de un objeto dentro de un agente.
Trap	Utilizado por los agentes para informar de forma asincrónica el NMS de un evento significativo.
SNMP V2	CARACTERÍSTICAS Y OPERACIONES ADICIONALES
GetBulk	Usado por el NMS para recuperar eficientemente grandes bloques de datos.
Inform	Permite a un NMS enviar trap de información a otro NMS y recibir entonces una respuesta.

SNMP V3	MEJORA DE LA SEGURIDAD
	Usuario basado en el modelo de seguridad (USM) para SNMP mensaje de seguridad
	View-based Modelo de Control de Acceso (VACM) para el control de acceso
	Configuración dinámica de los agentes SNMP utilizando Comandos Set de SNMP.

Para resolver los problemas de incompatibilidad entre las diferentes versiones de SNMP, RFC 3584 define las estrategias de coexistencia. SNMP también incluye un grupo de extensiones definidas por RMON, RMON 2, MIB, MIB2, SMI, OID, Enterprise OID.

Estructura del Protocolo SNMP: SNMP es un protocolo de aplicación, que está encapsulado en UDP. En general el mensaje SNMP es para todas las versiones y se muestra a continuación:

Versión	Community	PDU
---------	-----------	-----

TABLA N°1.11 Estructura del protocolo SNMP.

(Fuente: Network Protocols Handbook, 4th Edition.)

- **Versión:** SNMP versión number. Tanto el administrador como el agente deben utilizar la misma versión del SNMP. Los Mensajes que contienen diferentes números de versión se descartan sin más transformación
- **Community** – Nombre de comunidad utilizado para autenticar el administrador antes de permitir el acceso al agente
- **PDU (Protocol Data Unit)** -- Los tipos de PDU y formatos para SNMPv1, v2 y v3 se explican a continuación:

SNMPv1: Simple Network Management Protocol versión 1

Descripción del protocolo: Simple Network Management Protocol (SNMP) es un protocolo desarrollado para gestionar los nodos (servidores, estaciones de trabajo, routers, switches y hubs, etc.) de una red IP. SNMP permite a los administradores de red gestionar el rendimiento de la red, encontrar y resolver problemas de la red y el plan de crecimiento de la red. NMS aprende de los problemas recepcionando, recibiendo las notificaciones de cambio de los dispositivos de la red habilitados SNMP.

SNMPv1 es una simple petición / respuesta de protocolo. El sistema de gestión de red envía una solicitud, y logra respuestas retorno de los dispositivos. Este comportamiento se implementa mediante el uso de una de las cuatro operaciones de protocolo:

Get, GetNext, Set y Trap. La operación **Get** es utilizado por el NMS para recuperar el valor de una o más instancias de objeto de un agente.

Si el agente responde a la operación de **Get** no puede proporcionar valores para todas

las instancias del objetos en una lista, que no proporciona ningún valor.

La operación **GetNext** es utilizado por el NMS para recuperar el valor de la instancia del objeto siguiente en una tabla o una lista dentro de un agente. La operación en conjunto es utilizado por el NMS para establecer los valores de instancias de objetos dentro de un agente. La operación de captura es usada por los agentes para informar de forma asíncrona al NMS de un evento significativo.

Estructura del protocolo: SNMP es un protocolo de aplicación, que está encapsulado en UDP. En general el mensaje SNMP es para todas las versiones y se muestra a continuación:

Versión	Community	PDU
---------	-----------	-----

TABLA N°1.12 Estructura del protocolo SNMP v1.

(Fuente: Network Protocols Handbook, 4th Edition.)

- Versión -- Número de versión de SNMP. Tanto el manager y el agente debe utilizar la misma versión de SNMP. Mensajes que contienen diferentes números de versión se descarta sin más transformación
- Community -- Nombre de comunidad utilizado para autenticar el administrador antes de permitir el acceso al agente.
- PDU para SNMPv1 -- Hay cinco diferentes tipos de PDU: Get- Request, GetNextRequest, GetResponse, SetRequest, and Trap. Una descripción general de cada uno de estos campos se da a continuación.

En la TABLA N°1.13 se muestra el formato para GetRequest, GetNext Request, GetResponse y SetRequest PDU se muestra aquí.

PDU	type	Error	Error	Object 1,	Object 2,	...
	Request ID	status	index	value 1	value 2	

TABLA N°1.13 FORMATO DE GETREQUEST, GETNEXT REQUEST, GETRESPONSE, SETREQUEST, PDU.

(Fuente: Network Protocols Handbook, 4th Edition.)

- PDU type -- Especifica el tipo de PDU transmitidas: 0 GetRequest, 1 GetNextRequest, 2 GetResponse y SetRequest 3.
- Request ID -- Asociados SNMP peticiones con respuestas
- Error status --Indica una de un número de errores y tipos de error. Sólo la operación de respuesta fija este campo. Otras operaciones establezca este campo en cero.
- Error index -- Asocia un error con una instancia de objeto determinada. Sólo la operación de respuesta fija este campo. Otras operaciones establezca este campo en cero.

- Variable bindings --Sirve como el campo de datos de la PDU de SNMPv1. Cada enlace de variables asociadas a instancia de objeto particular con su valor actual (con la excepción de Get y GetNext requests, cuyo valor se ignora).

En la TABLA N°1.14 se muestra el formato de la PDU Trap se muestra a continuación.

PDU type	Enterprise	Agent Addr	Gen Trap	Spec Trap	Time Stamp	Obj 1, Val 1	Obj 1, Val 1	...
----------	------------	------------	----------	-----------	------------	--------------	--------------	-----

TABLA N°1.14 Formato de PDU.

(Fuente: Network Protocols Handbook, 4th Edition.)

- PDU type: Especifica el tipo de PDU (4=Trap).
- Enterprise: Identifica la gestión bajo cuya autoridad de registro ha sido definida el trap.
- Agent address: IP address del agente, utilizado para la identificación adicional.
- Generic trap type: Campo que describe el evento.
- Specific trap type: Se utiliza para identificar un trap no genérico cuando el tipo genérico de trap es la enterprise específica.
- Timestamp: Valor del objeto sysUpTime, que representa la cantidad de tiempo transcurrido entre la última (re-) inicialización y la generación de esa trap.

SNMPv2: Simple Network Management Protocol versión 2

Descripción del protocolo: Simple Network Management Protocol (SNMP) es un protocolo desarrollado para gestionar los nodos (servidores, estaciones de trabajo, routers, switches y hubs, etc.) de una red IP. SNMP permite a los administradores de red para gestionar el rendimiento de la red, encontrar y solucionar problemas de red, y un plan para el crecimiento de la red. NMS aprende de los problemas recepcionando, recibiendo las notificaciones de cambio de los dispositivos de la red habilitados SNMP.

SNMP versión 2 (SNMPv2) es una evolución de SNMPv1. El Get, GetNext, y las operaciones que se utiliza en SNMPv1 son exactamente los mismos que los utilizados en SNMPv2. Sin embargo, SNMPv2 añade y mejora algunas operaciones de protocolo. La operación Trap SNMPv2, por ejemplo: cumple la misma función que el utilizado en SNMPv1 pero utiliza un formato de mensaje diferente y está diseñado para sustituir el Trap SNMPv1 SNMPv2 también define dos nuevas operaciones: GetBulk e informar.

La operación GetBulk es utilizado por el NMS para recuperar eficientemente grandes bloques de datos, como por ejemplo varias filas en una tabla.

GetBulk llena un mensaje de respuesta con la mayor cantidad de datos que se solicitan como quepan. La operación Inform permite al NMS enviar información o trap a otra NMS y recibir entonces una respuesta. En SNMPv2, si el agente responde a las operaciones GetBulk no puede proporcionar valores para todas las variables en una lista, que proporciona resultados parciales.

Estructura del protocolo: SNMP es un protocolo de aplicación, que está encapsulado en UDP. En general en la TABLA N°1.15 se muestra el mensaje SNMP la cual es para todas las versiones y se muestra a continuación:

TABLA N°1.15 Formato del protocolo SNMP v2.

(Fuente: Network Protocols Handbook, 4th Edition)

Versión	Community	PDU
---------	-----------	-----

- **Versión:** Número de versión de SNMP. Tanto el manager y el agente debe utilizar la misma versión de SNMP. Mensajes que contienen diferentes números de versión se descarta sin más transformación
- **Community:** Nombre de comunidad utilizado para autenticar el administrador antes de permitir el acceso al agente.
- **PDU (Protocol Data Unit):** Los tipos de PDU y formatos son diferentes para SNMPv1, v2 y v3, que se explican en las secciones correspondientes.

Para SNMPv2, Get, GetNext, Inform, Response, Set y Trap PDU tiene en la TABLA N°1.13 se muestra el formato.

PDU type	Request ID	Error status	Error index	Object 1, value 1	Object 2, value 2	...
----------	------------	--------------	-------------	-------------------	-------------------	-----

TABLA N°1.16 Formato del Get, GetNext, Inform, Response, Set y Trap PDU.

(Fuente: Network Protocols Handbook, 4th Edition.)

- **PDU type:** Identifica el tipo de PDU transmitidas (Get, Get-Next, Inform, Response, Set, or Trap).
- **Request ID:** Asocia solicitudes SNMP con respuestas.
- **Error status:** Indica una de un número de errores y tipos de error. Sólo la operación de respuesta fija este campo. Otras operaciones establezca este campo en cero.
- **Error index:** Asocia un error con una instancia de objeto determinada. Sólo la operación de respuesta fija este campo. Otras operaciones establezca este campo en cero.
- **Variable bindings:** Sirve como el campo de datos (value 1, value 2...) del SNMPv2 PDU. Cada variable vinculante asocia una instancia de objeto determinada por su valor actual (con exclusión de Get y GetNext requests, para los cuales se omite el valor).

SNMPv2 Formato de GetBulk PDU, en la TABLA N°1.14 se muestra el formato correspondiente a la versión 2.

TABLA N°1.17 Formato de GetBulk PDU.

(Fuente: Network Protocols Handbook, 4th Edition.)

PDU	Request	Non	Max	Obj 1,	Obj 1,	...
-----	---------	-----	-----	--------	--------	-----

type	ID	repeaters	repetitions	Val 1	Val 1	
------	----	-----------	-------------	-------	-------	--

- PDU type: Identifica la PDU como una operación GetBulk.
- Request ID: Asocia solicitudes SNMP con respuestas.
- Non repeaters: Especifica el número de instancias de objeto en el campo de asignaciones de las variables que se deben recuperar no más de una vez desde el comienzo de la petición. Este campo se utiliza cuando algunos de los casos son objetos escalares con una sola variable.
- Max repetitions: Define el número máximo de veces que otras variables además de los especificados por el campo de repetidores no deben ser recuperados.
- Variable bindings: Sirve como el campo de datos (Obj 1, Obj 2 ...) de la PDU SNMPv2. Cada enlace de variables asociadas a instancia de objeto particular con su valor actual (con la excepción de Get y GetNext requests, cuyo valor se ignora).

SNMPv3: Simple Network Management Protocol versión 3

Descripción del protocolo: Simple Network Management Protocol (SNMP) es un protocolo desarrollado para gestionar los nodos (servidores, estaciones de trabajo, routers, switches y hubs, etc.) de una red IP. SNMP permite a los administradores de red para gestionar el rendimiento de la red, encontrar y solucionar problemas de red, y un plan para el crecimiento de la red. NMS aprende de los problemas recepcionando, recibiendo las notificaciones de cambio de los dispositivos de la red habilitados SNMP.

SNMP versión 3 (SNMPv3) añade capacidades de seguridad y configuración remota a las versiones anteriores. La arquitectura SNMPv3 presenta el modelo de seguridad basado en el usuario (USM) para la seguridad de los mensajes y la vista basada en el Modelo de Control de Acceso (VACM) para el control de acceso.

La arquitectura soporta el uso concurrente de seguridad diferente, control de acceso y los modelos de procesamiento de mensajes. Más específicamente:

SEGURIDAD

- Autenticación y privacidad.
- Autorización y control de acceso.

ADMINISTRACIÓN DEL FRAMEWORK

- Nombres de las entidades.
- Las personas y las políticas.
- Nombres de usuario y gestión de claves.
- Destinos de notificación.
- Las relaciones de proxy.
- Configurable de forma remota a través de operaciones de SNMP.

SNMPv3 también introduce la posibilidad de configurar dinámicamente el agente SNMP mediante los comandos SET de SNMP contra los objetos MIB que representan configuración del agente. Esta función permite la configuración dinámica de adición, eliminación y modificación de entradas de configuración de forma local o remota.

En la TABLA N°1.18 se muestra la estructura del protocolo para el formato del mensaje SNMPv3:

TABLA N°1.18 Estructura del protocolo SNMP v3
(Fuente: Network Protocols Handbook, 4th Edition.)

Msg Processed by MPM (Msg Processing Mode)					
Version	ID	Msg Size	Msg Flag	Security Model	
Msg Processed by USM (User Security Module)					
Authoritative Engine ID	Authoritative Boots	Authoritative Engine time	User Name	Authentication parameters	Privacy Parameter
Scoped PDU					
Context engine ID	Context name	PDU			

- Versión: snmv3(3).
- ID: Un identificador único que se utiliza entre dos entidades SNMP para coordinar los mensajes de solicitud y respuesta.
- Msg Size: El tamaño máximo de un mensaje en octetos apoyado por el emisor del mensaje.
- Msg Flags: Una cadena de octeto que contiene tres flags al menos con tres bits significativos: reportableFlag, privFlag, authFlag.
- Security Model: Es un identificador que indica qué modelo de seguridad fue usado por el remitente y por lo tanto que modelo de seguridad debe ser utilizado por el receptor para procesar este mensaje.
- AuthoritativeEngineID: El snmpEngineID es el motor SNMP que autoriza el intercambio de este mensaje. Por lo tanto, este valor se refiere a la fuente de un trap, response o report, y el destino de una Get, GetNext, GetBulk, Set o inform.
- AuthoritativeEngineBoots: El motor SNMP es el que autoriza al valor snmpEngineBoots a participar en el intercambio de mensajes.
- AuthoritativeEngineTime: El motor SNMP es el que autoriza al valor snmpEngineTime a participar en el intercambio de mensajes.
- User Name: El usuario (principal) en cuya parte el mensaje se intercambia.
- AuthenticationParameters: Nulo si la autenticación no está siendo utilizado para este intercambio. De lo contrario, este es un parámetro de autenticación.
- PrivacyParameters: Null si la privacidad no está siendo utilizado para este intercambio.

De lo contrario, este es un parámetro de privacidad.

- PDU (Protocol Data Unit): El tipo de PDU para SNMPv3 es el mismo para el SNMPv2.

1.4 Seguridad

La definición de la seguridad está referido al cumplimiento del estándar PCI DSS, el cual no es tópicamente a tratar en el presente capítulo sin embargo se recomienda que los equipos que están involucrados en la transacción soporten el PCI DSS.

1.5 Firewall

Los firewalls son dispositivos de red que restringen el acceso entre redes, para nuestro caso, el Firewall (FW) es un componente importante de la red para poder asegurar que el tráfico a través de la red sea seguro. En la actualidad, muchas empresas financieras emplean el firewall para restringir el acceso desde Internet a sus redes privadas, como se puede apreciar en el ANEXO C: DIAGRAMA ACTUAL DE RED.

CAPÍTULO II

PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

Este capítulo se desarrolla con la finalidad de presentar de una manera clara y concisa el escenario bajo el cual nace la motivación de este informe y a qué necesidad responde. Se definen también cuáles son los alcances y aportes del mismo. Finalmente se dedica un punto a la síntesis de este informe.

2.1 Descripción del problema

En la actualidad los costos de los enlaces de datos disponibles para las zonas alejadas de la ciudad o en zonas rurales como servicio de datos por fibra óptica, enlace en cobre, enlaces satelitales, etc., son costosos y hacen no viable la posibilidad de llegar con servicios financieros tipo cajeros automáticos, cajeros corresponsales, puntos de venta (POS) a las zonas rurales.

El presente informe presenta una alternativa adecuada para llegar con los servicios financieros a las zonas rurales los cuales aportan al desarrollo económico de la comunidad.

2.2 Objetivos del informe

Conocer las etapas relacionadas al proceso de implementación de los proyectos utilizando tecnología 2G/3G, descripción de los componentes de la solución.

Presentar un estudio de la topología, arquitectura de hardware requerido para que puedan operar en producción los terminales tipo cajero automático, cajero corresponsal, puntos de venta (POS).

Describir cómo se comporta el tráfico transaccional a través de la red móvil hasta llegar a los servidores de la institución financiera.

Desarrollar los lineamientos para que se pueda poner en producción un cajero automático en zona rural y que se haga posible la transacción bancaria en línea.

Proponer el diseño para la implementación del sistema en las distintas instituciones bancarias (privadas y del estado).

La evolución de la tecnología disponible servirá como base para desarrollar más aplicaciones basadas en la disponibilidad de más ancho de banda en los enlaces de

datos provistos por los carriers con servicios móviles de tipo 2G los cuales están avanzando con las nuevas tecnologías de 3G

2.3 Evaluación del problema

En el Perú, actualmente, existen poblaciones alejadas de la ciudad donde se requieren de servicios financieros, los cuales están siendo atendidos por instituciones como Bancos privados y del estado.

El presente trabajo describe completamente la interacción de la tecnología para llevar a los destinos alejados los sistemas como cajeros automáticos, cajeros corresponsal, puntos de venta, en donde la actividad económica de la localidad permita el desarrollo de la comunidad.

Desde la perspectiva del estado, su presencia sería notable pues permitirá aportar al desarrollo económico de estas comunidades.

Desde la perspectiva privada, se abre un abanico de oportunidades comerciales y una nueva forma de poder tener presencia en lugares donde la necesidad de utilizar cajeros automáticos, puntos de venta (POS) por la población, turistas y comerciantes acelere el desarrollo de la comunidad.

2.4 Limitaciones del informe

Este trabajo constituye una guía para aquellas personas que se encuentren investigando temas relacionados al desarrollo de las comunidades rurales con aporte de las tecnologías que puedan ser de utilidad al desarrollo del país.

Una de las limitaciones del sistema es que el ancho de banda de los servicios móviles permite únicamente tráfico transaccional para tener una buena experiencia con el servicio entregado.

A la medida que la tecnología evolucione y los carriers dispongan planes de crecimiento en las zonas rurales con tecnologías que hagan factible poder desplegar servicios más complejos y/o aplicaciones que requieran más anchos de banda será factible poder incrementar las aplicaciones que estas tecnologías entreguen a comunidades donde los accesos de red son muy escasos o no son factibles por las condiciones que presenta la geografía de las zonas donde se requiera llevar servicios o cajeros automáticos y/o puntos de venta (POS).

2.5 Síntesis del informe

Se exponen los fundamentos teóricos que permitan comprender los procesos involucrados en la transmisión de datos transaccionales sobre la red de datos móviles 2G/3G. Se presenta un análisis de la arquitectura de hardware y software de los equipos de datos para tráfico por tecnologías 2G/3G y se realiza un estudio de la topología implementada en una solución para la banca rural.

Finalmente, se propone un escenario de implementación con los lineamientos y recomendaciones a tener en cuenta en el proceso de implementación de la solución en la banca rural, para los servicios financieros.

CAPÍTULO III

DETERMINACIÓN DE LA NECESIDAD

Este capítulo presenta el potencial del servicio que se entrega en las zonas rurales, sobre todo en los puntos donde se desarrolla actividad económica con productores, turistas y exportadores e interacción con programas del gobierno.

3.1 Demanda potencial del servicio

En muchos países en desarrollo las finanzas rurales formales aún son muy débiles y la demanda real supera la oferta, y los servicios son inaccesibles para las poblaciones económicamente activas, poblaciones rurales y para personas que viven en áreas rurales. En el presente informe se propone una solución de llevar el sistema del cajero automático como un medio para que las zonas rurales se integren al sistema financiero del país, existen dudas respecto al potencial de los pobladores más pobres y de los residentes de áreas remotas para convertirse en clientes viables de servicios financieros supeditados al mercado.

El supuesto de que no hay una demanda real de servicios de microfinanzas entre los más pobres no parece ser realista. Pues igualmente, cerca del 7 por ciento de los clientes de Mi banco en Perú pertenece a la categoría de los más pobres (Welch y Devaney, 2003, <http://centerforfinancialinclusionblog.files.wordpress.com/2011/10/poverty-outreach-findings-mibanco-peru-spanish.pdf>). Los hogares más pobres presentan también una demanda real por facilidades seguras para realizar sus depósitos y/o transacciones.

Así mismo, a la fecha, el tráfico generado por las transacciones en los cajeros automáticos demandan una optimización del uso del ancho de banda disponible, puesto que no requieren de tasas altas de ancho de banda para que sea posible una transacción bancaria a través de las tarjetas de crédito y/o débito para estas transacciones, de tal forma que sea necesaria evaluar alternativas de soluciones para los enlaces que soportan este tipo de servicio.

Para el ANEXO B: ESTADÍSTICAS DE INEI Y OSIPTEL se presenta cuadros estadísticos de fuente INEI y OSIPTEL los cuales evidencian el número de población rural para los cuadros mostrados, detallando información de la población económicamente

activa y el cuadro LÍNEAS EN SERVICIO DE TELEFONÍA MÓVIL, POR EMPRESA, 2000 – 2010 muestra un consolidado a nivel nacional como es el crecimiento del número de líneas móviles a nivel nacional.

De la misma forma se muestra en el ANEXO B: ESTADÍSTICAS DE INEI Y OSIPTEL. La distribución de producción de los principales cultivos según departamentos al 2010.

3.2 Evaluación de la competencia

El consumo de ancho de banda que requiere una transacción demanda poder evaluar a los enlaces y tecnologías que puedan considerarse competencia, para esta solución nos lleva a analizar tipos de enlaces como: enlaces de Cobre, fibra, satelital, ISDN, los cuales para cada caso se hacen no factibles por la geografía de cada lugar donde se implementarían, tal es el caso de satélite si consideramos esta tecnología lo que hace no factible son los altos costos mensuales y por tener el enlace disponible bajo anchos de banda mínimos que ofrecen los carriers que prestan este tipo de servicio.

Para el caso de los enlaces de fibra óptica, por la geografía y distancia donde se encuentran la necesidad de poner servicios como cajero automático, cajeros corresponsal, puntos de venta, los costos altos de la fibra óptica, planta externa, obra civil versus el número volumen de transacciones que realizan en estas zonas alejadas hacen que esta tecnología de fibra óptica no sea factible poder implementar de igual forma sucede con los servicios con enlace con cobre.

CAPÍTULO IV

ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

4.1 Introducción

El análisis y presentación de resultados se enfoca en el diseño de la red interna donde se incluye el plan de numeración IP de la red de cajeros automáticos y el direccionamiento de las subredes ya que es la actividad más inmediata a realizar se muestra los distintos componentes que son añadidos a la red como cámaras de seguridad, se incluye el diseño de la red de puntos de Venta (POS)

4.2 Solución de la arquitectura de red

En el ANEXO C: DIAGRAMA ACTUAL DE RED, se muestra una red tradicional de servicios como cajeros automáticos, puntos de venta, video seguridad en los escenarios mostrados se puede apreciar que todos los sistemas cuentan con enlaces dedicados los cuales hacen que sea complejo y costoso poder llevar estos servicios a las zonas alejadas de la ciudad, las conexiones de red que se encuentran en los lugares remotos envían tráfico a través de la red del carrier que en su mayoría de los casos son enlaces con tecnología MPLS llegan a la sede principal para luego son autenticados por los sistemas de seguridad para llegar a los servidores centrales de cada aplicación.

En el ANEXO D: DISEÑO DE RED PARA SERVICIOS 3G, muestra el diseño de la red de cajeros automáticos la cual podrá ser implementada bajo los estándares de seguridad requeridos para esta solución, se muestra dos escenarios el primero es por circuito dedicado donde a la fecha los carrier proponen enlaces basados en arquitectura de red por MPLS donde se estima un ancho de banda basado en el tráfico cursado por cada cajero automático este tipo de enlace deberá ser del tipo MPLS donde se estima tráfico de datos y tráfico de video esencialmente.

De igual manera se muestra el diseño para cajeros automáticos por internet donde la institución financiera deberá contar con enlace internet por donde los componentes remotos (cajeros automáticos, equipo con soporte a 3G, sistemas de seguridad, sistemas de energía) deberán realizar tráfico hacia los servidores que se encuentran en la sede principal este tipo de tráfico deberá asegurar niveles de encriptación para cumplir con los estándares de seguridad para transacciones.

En el mismo ANEXO D: DISEÑO DE RED PARA SERVICIOS 3G de muestra los

circuito dedicado y por internet aplicaciones de puntos de venta y el sistema de video seguridad, este diseño de puede extender al resto de servicios que podrán ingresar a producción basados en la misma arquitectura.

En base a las consideraciones de diseño mencionadas en el punto anterior se muestra la arquitectura de red segmentada en el ANEXO D: DISEÑO DE RED PARA SERVICIOS 3G y en el ANEXO E: DIRECCIONAMIENTO IP se muestra el direccionamiento interno de los segmentos de red creados, así mismo, la VLAN a la cual pertenece cada uno de los segmentos.

4.3 Costos y tiempos de ejecución

En el ANEXO F: TABLA DE COSTOS, se muestra cuadros comparativos de costos los cuales son referenciales estos cálculos muestran que utilizando tecnología 3G es factible poder desplegar los cajeros automáticos así como los puntos de venta (POS), a través del territorio nacional, en el ANEXO G: DIAGRAMA DE GANTT se muestra los tiempos estimados para la implementación en las zonas alejadas del país donde exista cobertura de señal 3G.

CONCLUSIONES Y RECOMENDACIONES

1. En zonas rurales donde exista cobertura 3G por parte de los operadores locales ya es factible realizar una transacción a través de cajeros automáticos, puntos de venta (POS) permiten desarrollarse económicamente a las poblaciones del país.
2. Los ahorros en implementación de estos servicios para las zonas donde no hay factibilidad de poder llegar con enlaces de fibra óptica o cobre son importantes para poder hacer factible llevar servicios de cajero automático, y puntos de Venta como se muestra en el ANEXO F: TABLA DE COSTOS.
3. Es importante garantizar el consumo de tráfico consumido por los dispositivos móviles para el caso del equipo router con soporte a 3G, vigile el consumo e infórmese de cualquier anomalía en su factura.
4. A la fecha los operadores de celular ya se encuentran desplegando en muchas localidades alejadas de la ciudad servicio de 3G esto permite a las instituciones financieras y al estado poder desplegar sus servicios financieros y tener presencia para el caso del estado.
5. Es claro que la tecnología 3G brinda más servicios como a continuación describimos: video llamadas, video conferencias, TV móvil/monitoreo remoto, internet móvil, video streaming/video portal, capacidad simultanea de voz y datos, sin embargo el presente trabajo está basado esencialmente en brindar servicio financiero a través de las instituciones bancarias y el estado, para esto se propone implementar la red para cajeros automáticos, puntos de venta (POS) a través de la red 3G de los operadores locales.
6. Se recomienda la adquisición de nuevas plataformas tecnológicas, como es el caso del firewall de aplicaciones, dispositivos remotos en el caso del equipo terminal con soporte a tecnología 3G, se recomienda solicitar a los fabricantes un documento en donde detalle que su producto cumple con la norma de seguridad.
7. En el ANEXO D: DISEÑO DE RED PARA SERVICIOS 3G se muestra la solución de servicios 3G con integración utilizando internet para luego encriptar el trafico cursado esta posibilidad es utilizada para soluciones que demandan análisis de consumo de ancho de banda en bits por segundo dado que internet no garantiza ancho de banda en su totalidad, con esta conclusión se determina que los sistemas que cuentan con circuito

dedicado para la solución son escalables en el tiempo para que puedan implementarse otras tecnologías en el futuro.

8. Se recomienda la implementación del proceso de gestión de cambios en la infraestructura de red y los firewalls, provisión de equipos asociados al sim card.

9. Se recomienda la implementación del proceso de atención de eventos e incidencias con el cumplimiento de los estándares adecuados.

10. Es adecuado contar con especialistas que puedan determinar y analizar los eventos en los equipos donde se puedan ver log como niveles de señal, comportamiento del equipo en la zona geográfica donde está operando, información del número de celda.

11. La información que se pueda registrar del log de los equipos terminales con soporte 3G es importante pues permite llevar un historial de eventos y comportamiento de la zona geográfica donde opera el equipo terminal.

ANEXO A

CATÁLOGO DE EQUIPOS Y ESPECIFICACIONES TÉCNICAS DEL EQUIPO MÓVIL



EQUIPO ROUTER IP/3G
Digi TransPort® WR44 RR

1. ESPECIFICACIONES TÉCNICAS DEL EQUIPO

GSM/CDMA Gobi (U8):

GSM and CDMA supported on the same module via Gobi diversity;
UMTS/HSPA/HSPA+ (850/900/1700 AWS/1800/1900/2100 MHz with Rx Diversity);
EV-DO Rev A (800/1900 MHz with Rx Diversity); Transfer Rate (max): 5.76 Mbps Up,
14.4 Mbps Down.

Edge:

GPRS/EDGE Class 10; 850/900/1800/1900 MHz; Transfer rate (max): 236 Kbps
Up/Down.

Connector:

U8, L2, & L3 variants: 2 x 50 Ω SMA (Center pin: female); E1, Cx, Bx variants: 1 x 50
 Ω SMA (Center pin: female).

SIM Slots:

2.

Management (Cloud-based):

iDigi® Manager Pro™

Management (Local)

Web Interface via HTTP/HTTPS; CLI via serial port, Telnet, SSH.

Software:

Python, iDigi® Dia, Digi ESP™ development environment.

Input:

9 – 36 VDC

Consumption:

15W max, 8.5W typical.

DC Power Cord*

Locking barrel to bare wire or 4-pin connector to bare wire

AC Power Supply*

100-240 VAC 50/60 Hz; Option of standard temperature or extended temperature.

Dimensions (L x W x H):

WR44: (non-DSL variants): 5.7 in x 8.3 in x 1.6 in (145 mm x 210 mm x 40 mm)

WR44: (DSL variants): 5.7 in x 10.4 in x 1.6 in (145 mm x 264 mm x 40 mm)

Weight:

WR44: (non-DSL variants): 1.98 lb (0.9 kg) WR44: (DSL variants): 2.25 lbs (1 kg)

Status LEDs:

Power, 4x LAN, Wi-Fi, Serial/DSL, WWAN (Link, Act, SIM), 3x Signal strength

Operating Temperature:

WR44: (standard temp variants): 0° C to +60° C WR44: (extended temp variants)

Relative Humidity:

20% to 95% (non-condensing)

Ethernet Isolation:

1.5 kV RMS

GSM/UMTS:

PTCRB, NAPRD.03, GCF-CC, R&TTE, EN 301 511

Safety:

UL 60950, CSA 22.2 No. 60950, EN60950

Emissions/Immunity:

CE, FCC Part 15 Class B, AS/NZS CISPR 22, EN55024, EN55022 Class B

Protocols:

Same as Standard plus iDigi; Dynamic DNS client compatible with BIND9/No-IP/DynDNS

HTTP, HTTPS, FTP, SFTP, SSL, SMTP, iDigi SNMP, SNMP (v1/v2c/v3), SSH, Telnet and CLI for web management; remote management via software tool (option); SMS management, protocol analyzer, ability to capture PCAP for use with Wireshark; DynDNS

Security/Firewall/VPN:

RADIUS TACACS+, SSL, SSLv2, SSLv3, FIPS 197, L2TP, (5 tunnels included); IPSec with IKEv1, IKEv2, ISAKMP; DES, 3DES and AES up to 256-bit encryption; SCEP for X.509 certificates, Open VPN client and server, PPTP; IPSec/PPP/L2TP VPN Server support; Stateful inspection firewall with scripting; Content Filtering (via 3rd party).

Routing:

Bridging, NAT/NAT-Traversal, NAPT forwarding; PPP, PPPoE, GRE; IP Routing Protocol: PPP, GRE, RIP (v1 & v2) OSPF, SRI, BGP; IP Failover: VRRP, VRRP+TM; VLAN support; STP (Spanning Tree Protocol); Automatic failover/failback to second GSM network/Standby APN; Firmware upgradable to IPv6; iGMP routing (multicast); IP pass-through (advanced).

Specialty Protocol:

DHCP; RealPort®; Modbus UDP/TCP to serial; Legacy protocols (X.25 (including X0T), SNA/IP, TPAD and PAD); Protocol switch.

ANEXO B
ESTADÍSTICAS DE INEI Y OSIPTEL

**ESTIMACIONES Y PROYECCIONES DE LA POBLACIÓN ECONÓMICAMENTE ACTIVA
RURAL, SEGÚN SEXO Y EDADES QUINQUENALES, 2000 - 2015**

Sexo y Edad quinquenal	Población Económicamente Activa Rural				
	2000	2005	2010	2011	2015
Total	4,057,407	4,230,240	4,200,997	4,180,867	4,094,510
De 14 años	93,652	101,004	93,833	91,663	84,057
De 15 a 19 años	504,983	555,515	510,108	501,061	473,995
De 20 a 24 años	524,057	524,577	540,267	530,959	474,879
De 25 a 29 años	518,304	516,471	495,381	496,871	506,946
De 30 a 34 años	459,072	483,218	470,584	466,830	455,255
De 35 a 39 años	400,049	418,364	433,384	432,577	422,364
De 40 a 44 años	340,936	357,326	364,123	366,277	374,633
De 45 a 49 años	290,687	302,519	307,484	307,968	310,558
De 50 a 54 años	243,447	254,147	254,478	254,373	253,907
De 55 a 59 años	203,551	210,538	213,294	213,263	212,639
De 60 a 64 años	173,494	173,704	177,658	178,369	181,940
De 65 a 69 años	136,269	140,410	137,722	137,733	140,018
De 70 a 74 años	92,475	101,422	102,983	102,516	100,759
De 75 a 79 años	49,130	58,839	63,969	64,283	64,892
De 80 y más años	27,301	32,186	35,729	36,124	37,668

Fuente: INEI - Perú: Estimaciones y Proyecciones de Población Económicamente Activa, Urbana y Rural por Sexo y Grupos de Edad, según Departamento, 2000 - 2015 - Boletín Especial N° 20.

**ESTIMACIONES Y PROYECCIONES DE LA POBLACIÓN ECONÓMICAMENTE ACTIVA
RURAL, SEGÚN SEXO Y EDADES QUINQUENALES, 2000 - 2015**

Sexo y Edad quinquenal	Población Económicamente Activa Rural				
	2000	2005	2010	2011	2015
Hombres	2,394,666	2,441,998	2,406,709	2,396,145	2,350,530
De 14 años	53,180	58,014	54,208	52,841	48,043
De 15 a 19 años	308,651	329,092	296,239	290,688	273,811
De 20 a 24 años	334,207	318,158	318,833	313,144	280,264
De 25 a 29 años	316,079	309,945	293,589	294,011	298,044
De 30 a 34 años	271,229	282,503	276,211	274,139	266,552
De 35 a 39 años	231,835	239,912	249,920	250,227	247,210
De 40 a 44 años	193,996	201,271	207,130	209,168	217,577
De 45 a 49 años	164,581	169,495	172,210	172,998	177,136
De 50 a 54 años	136,640	140,782	141,557	141,636	141,801
De 55 a 59 años	114,189	115,360	117,243	117,396	117,487
De 60 a 64 años	97,445	95,353	96,219	96,642	98,764
De 65 a 69 años	76,429	76,821	74,446	74,381	75,340
De 70 a 74 años	51,999	55,564	55,659	55,343	54,174
De 75 a 79 años	28,044	32,079	34,369	34,506	34,743
De 80 y más años	16,162	17,649	18,876	19,025	19,584

Fuente: INEI - Perú: Estimaciones y Proyecciones de Población Económicamente Activa, Urbana y Rural por Sexo y Grupos de Edad, según Departamento, 2000 - 2015 - Boletín Especial N° 20.

**ESTIMACIONES Y PROYECCIONES DE LA POBLACIÓN ECONÓMICAMENTE ACTIVA
RURAL, SEGÚN SEXO Y EDADES QUINQUENALES, 2000 - 2015**

Sexo y Edad quinquenal	Población Económicamente Activa Rural				
	2000	2005	2010	2011	2015
Mujeres	1,662,741	1,788,242	1,794,288	1,784,722	1,743,980
De 14 años	40,472	42,990	39,625	38,822	36,014
De 15 a 19 años	196,332	226,423	213,869	210,373	200,184
De 20 a 24 años	189,850	206,419	221,434	217,815	194,615
De 25 a 29 años	202,225	206,526	201,792	202,860	208,902
De 30 a 34 años	187,843	200,715	194,373	192,691	188,703
De 35 a 39 años	168,214	178,452	183,464	182,350	175,154
De 40 a 44 años	146,940	156,055	156,993	157,109	157,056
De 45 a 49 años	126,106	133,024	135,274	134,970	133,422
De 50 a 54 años	106,807	113,365	112,921	112,737	112,106
De 55 a 59 años	89,362	95,178	96,051	95,867	95,152
De 60 a 64 años	76,049	78,351	81,439	81,727	83,176
De 65 a 69 años	59,840	63,589	63,276	63,352	64,678
De 70 a 74 años	40,476	45,858	47,324	47,173	46,585
De 75 a 79 años	21,086	26,760	29,600	29,777	30,149
De 80 y más años	11,139	14,537	16,853	17,099	18,084

Fuente: INEI - Perú: Estimaciones y Proyecciones de Población Económicamente Activa, Urbana y Rural por Sexo y Grupos de Edad, según Departamento, 2000 - 2015 - Boletín Especial N° 20.

LÍNEAS EN SERVICIO DE TELEFONÍA MÓVIL, POR EMPRESA, 2000 - 2010

Año	Total	Empresa			
		Telefónica Móviles 1/	Comunicaciones Móviles 1/	Nextel del Perú	América Móvil Perú 2/
2000	1 339 667	898 173	373 091	68 403	-
2001	1 793 284	1 087 152	430 282	110 248	165 602
2002	2 306 943	1 239 056	550 162	129 780	387 945
2010 a/	2 930 343	1 506 637	650 617	146 971	626 118
2004	4 092 558	2 124 776	680 493	184 895	1 102 394
2005	5 583 356	3 383 835	-	249 475	1 950 046
2006	8 772 479	5 058 497	-	345 354	3 368 628
2007	15 417 368	9 436 371	-	472 809	5 508 188
2008	20 951 834	13 114 150	-	659 879	7 177 805
2009	24 702 060	15 600 558	-	834 986	8 266 516
2010 a/	27 099 375	17 139 925	-	965 050	8 994 400

Nota: En 2009 y 2010, OSIPTEL está evaluando el tratamiento estadístico a los dispositivos USB de internet de banda ancha móvil. Mientras no se concluya dicha evaluación, el reporte periódico de líneas móviles en servicio incluirá a dichos USB de internet móvil que hayan sido contabilizados como líneas activas.

a/ Información a junio de 2010.

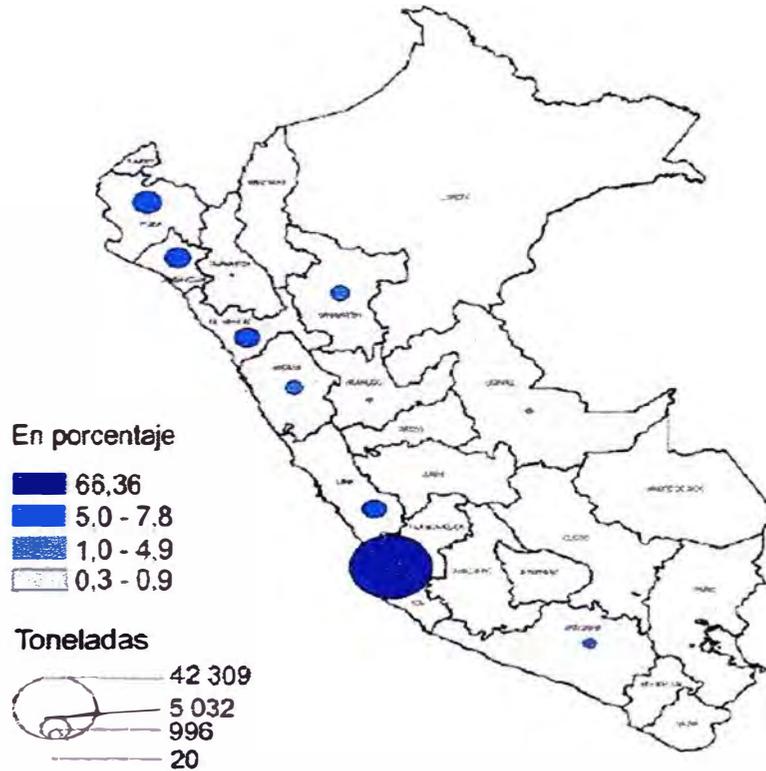
1/ En el año 2005 las empresas Telefónica Móviles y Bellsouth (Comunicaciones Móviles) se fusionaron.

2/ Hasta setiembre del 2005, cifras corresponden a TIM PERÚ S.A.C.

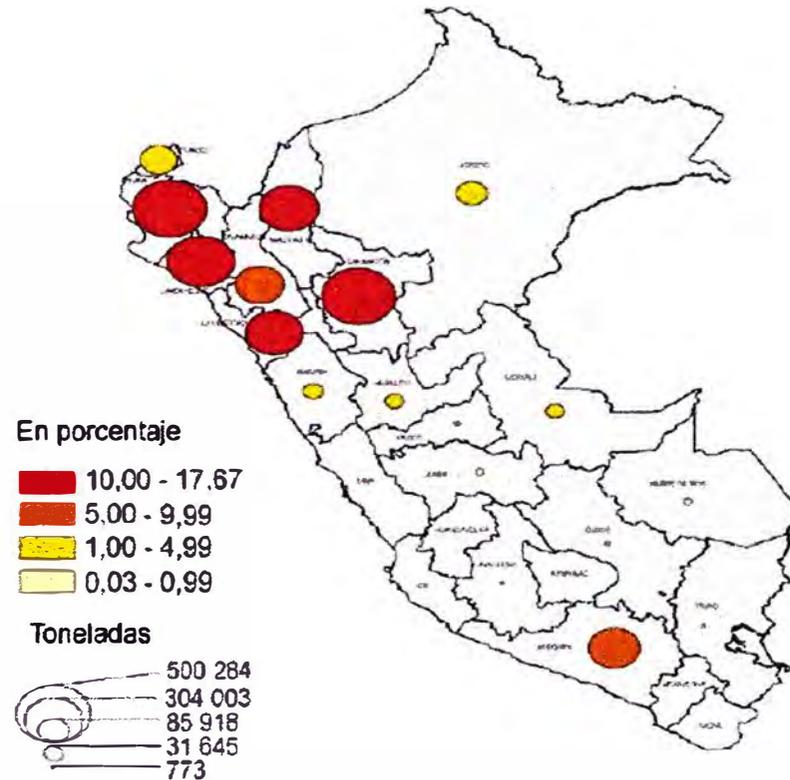
Fuente: Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).

PRODUCCIÓN DE LOS PRINCIPALES CULTIVOS, SEGÚN DEPARTAMENTO, 2010

Algodón rama



Arroz cáscara

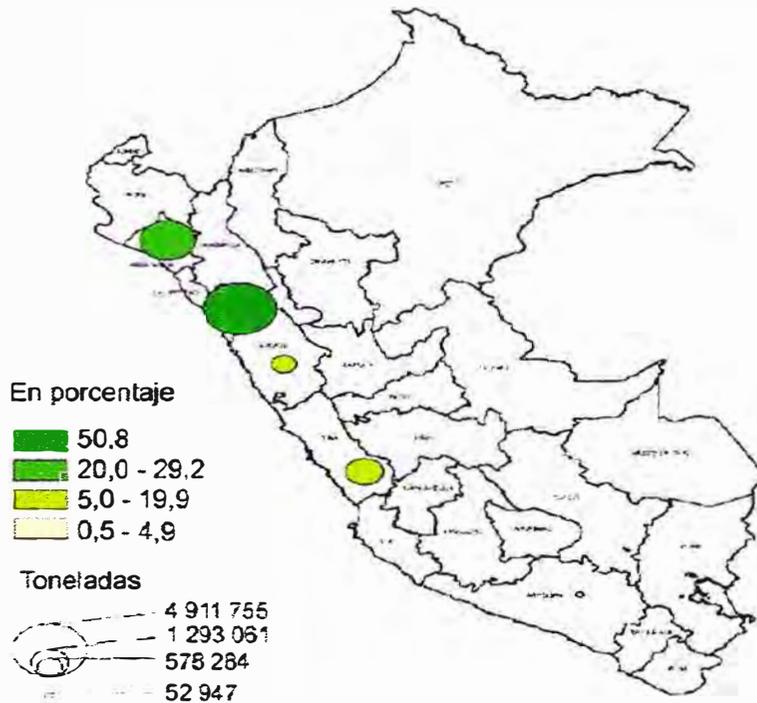


Fuente: Ministerio de Agricultura - Oficina de Estudios Económicos y Estadísticos - Unidad de estadística.

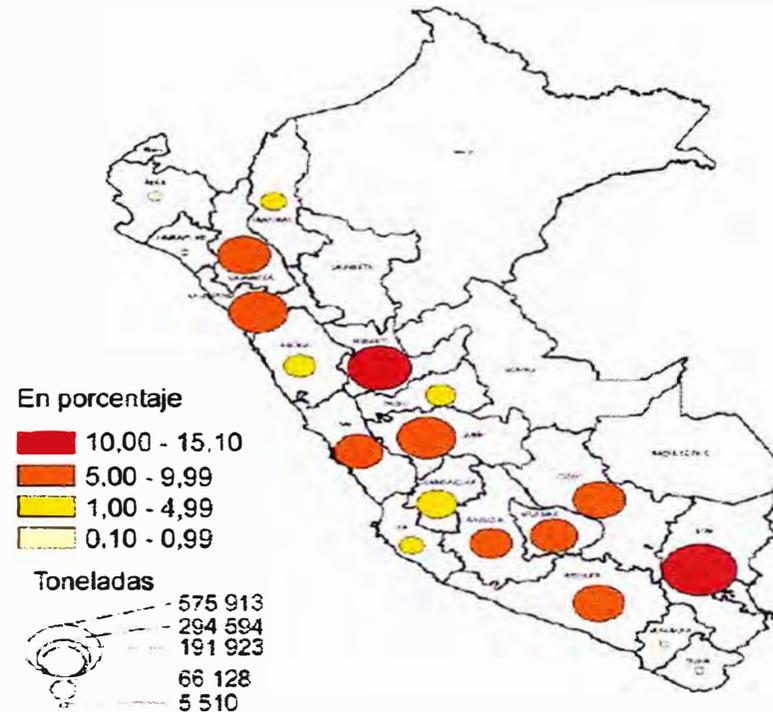
Elaborado: Instituto Nacional de Estadística e Informática - INEI

PRODUCCIÓN DE LOS PRINCIPALES CULTIVOS, SEGÚN DEPARTAMENTO, 2010

Caña de azúcar



Papa



Fuente: Ministerio de Agricultura - Oficina de Estudios Económicos y Estadísticos - Unidad de estadística.

Elaborado: Instituto Nacional de Estadística e Informática - INEI

ANEXO C
DIAGRAMA ACTUAL DE RED

DIAGRAMA DE RED ACTUAL PARA CAJEROS AUTOMÁTICOS

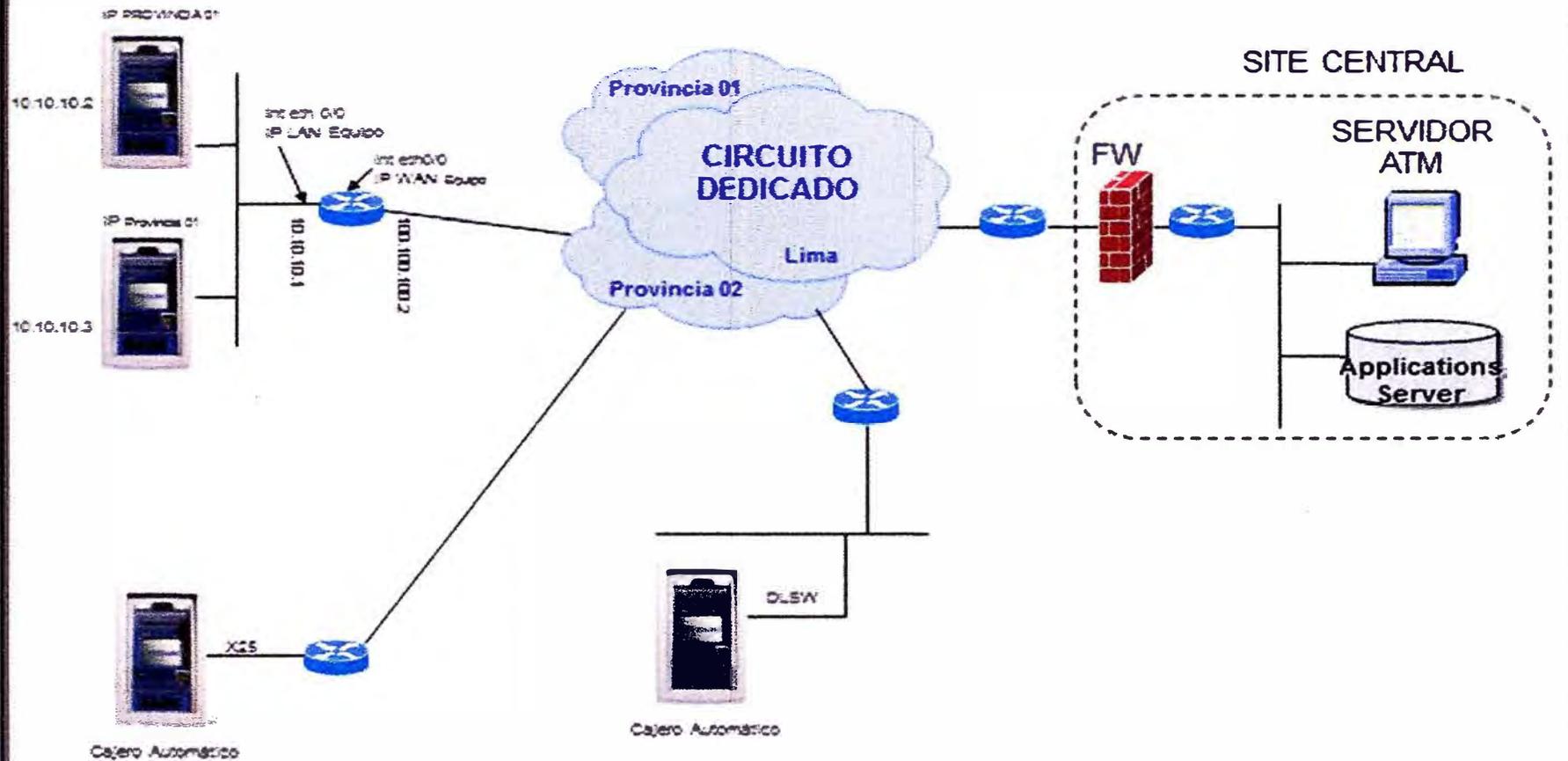


DIAGRAMA DE RED ACTUAL PARA POS

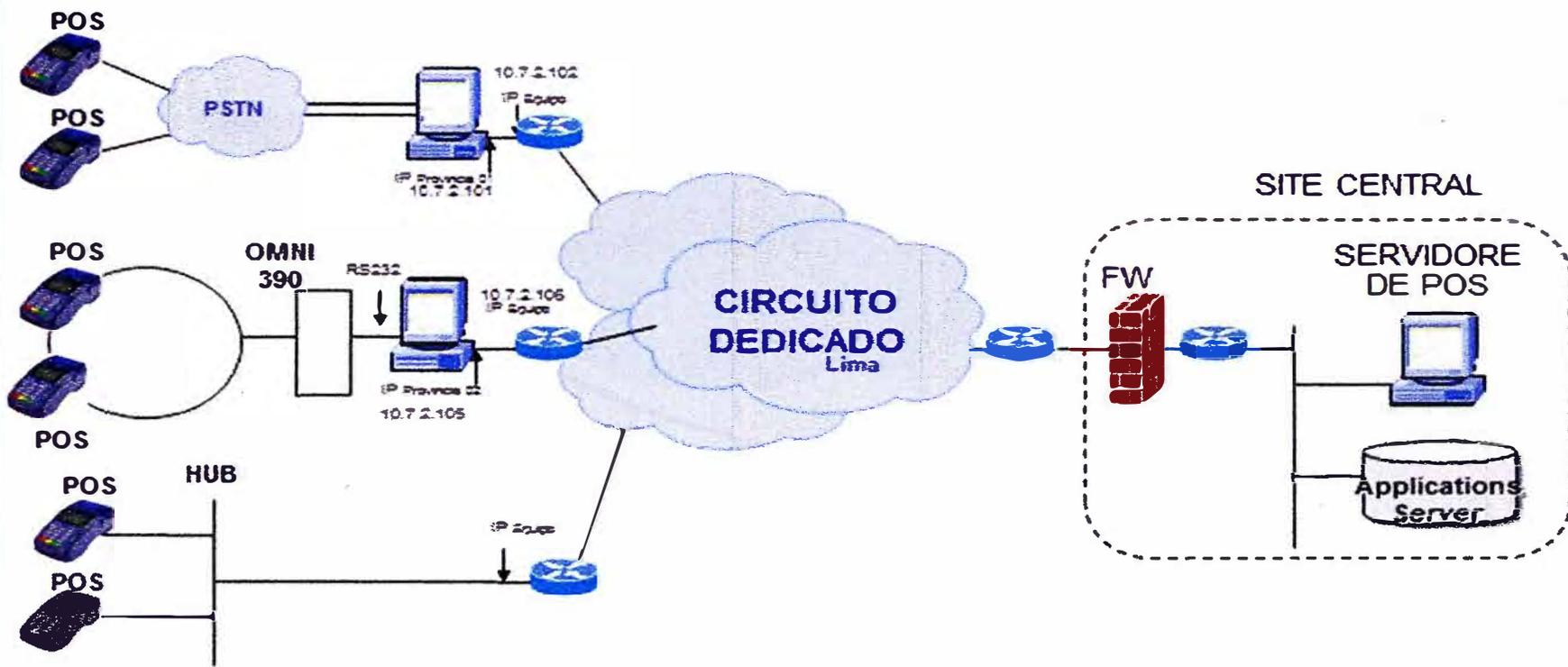
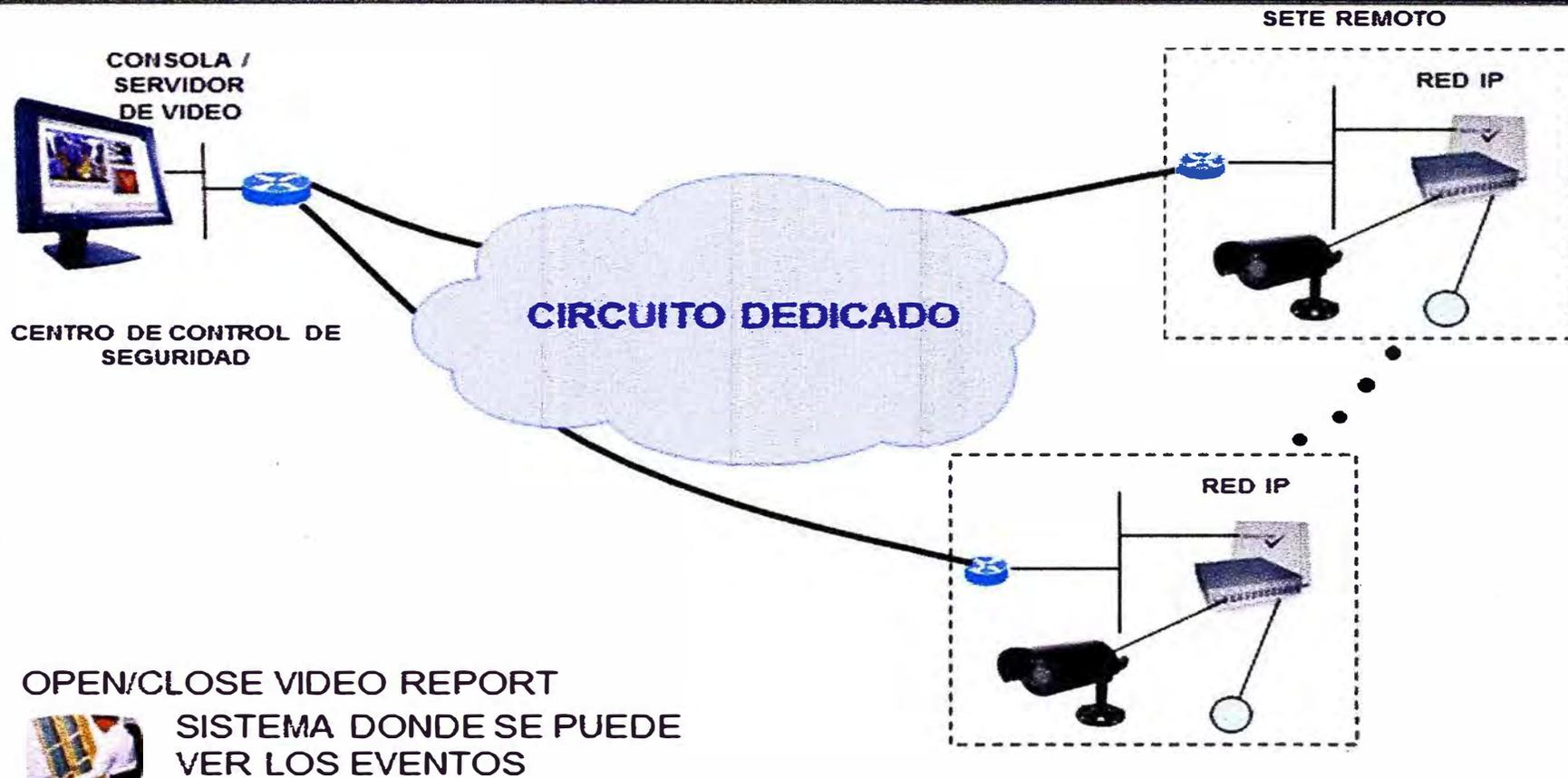
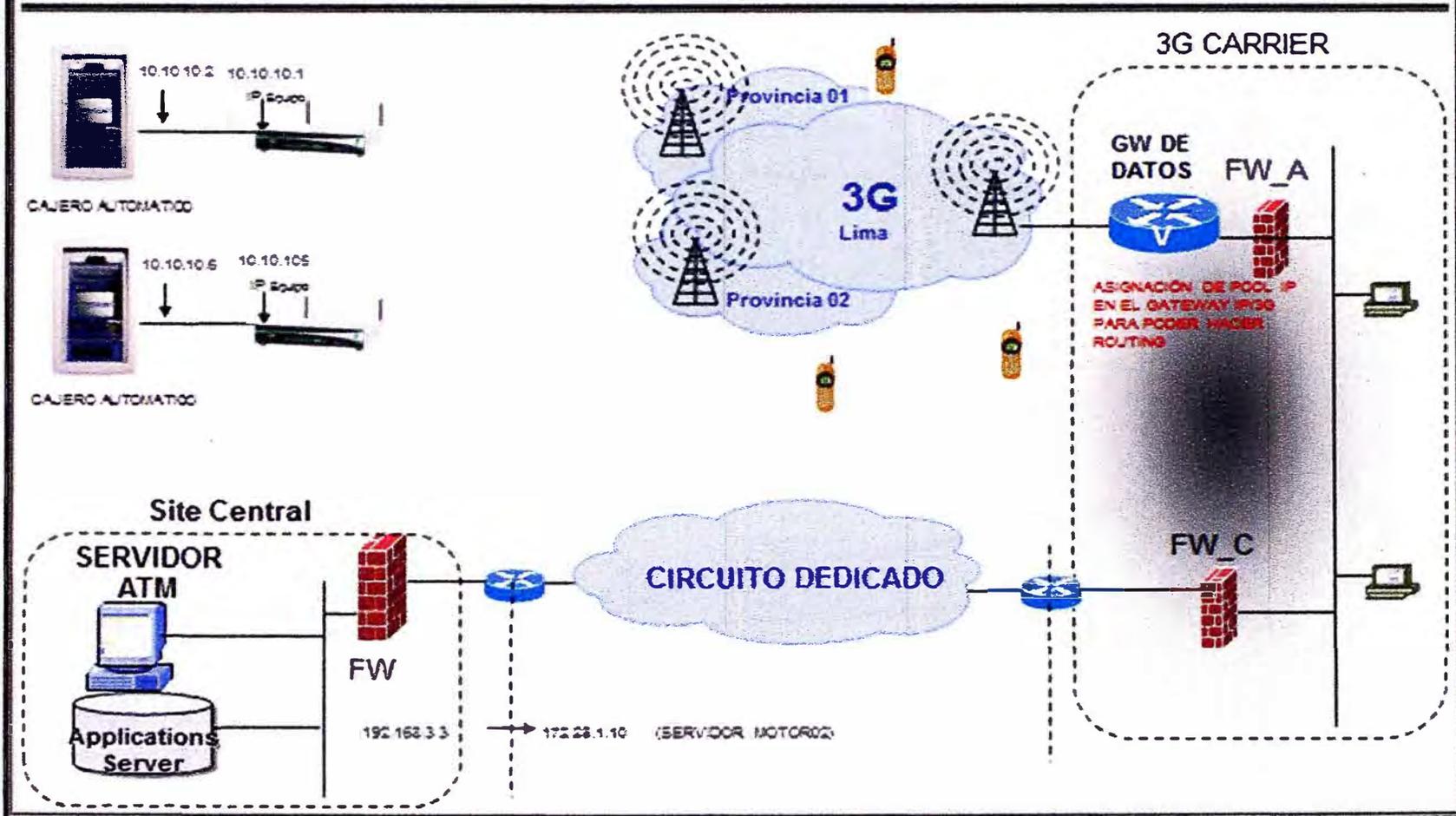


DIAGRAMA DE RED ACTUAL PARA EL SISTEMA DE SEGURIDAD Y MONITOREO REMOTO

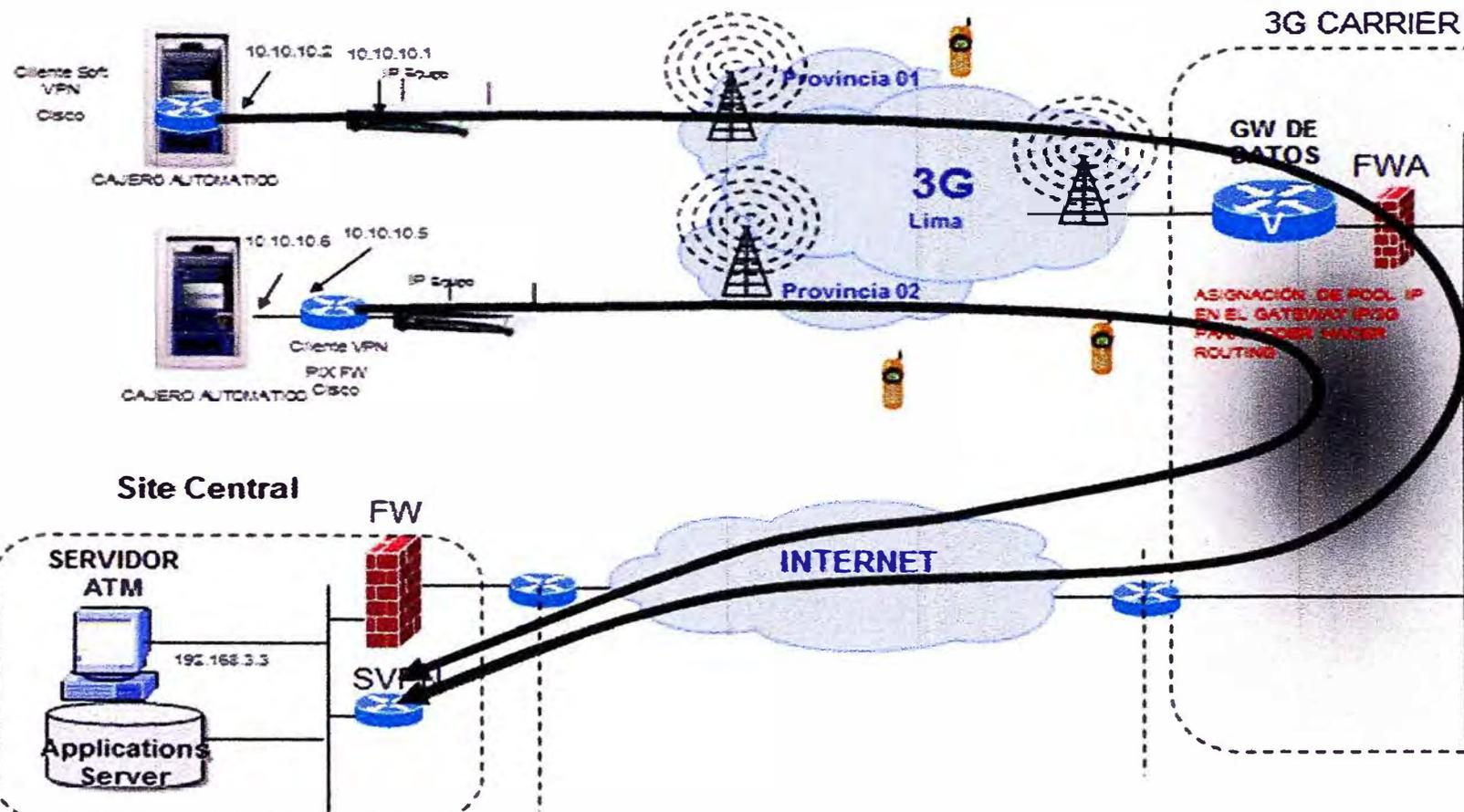


ANEXO D
DISEÑO DE RED PARA SERVICIOS 3G

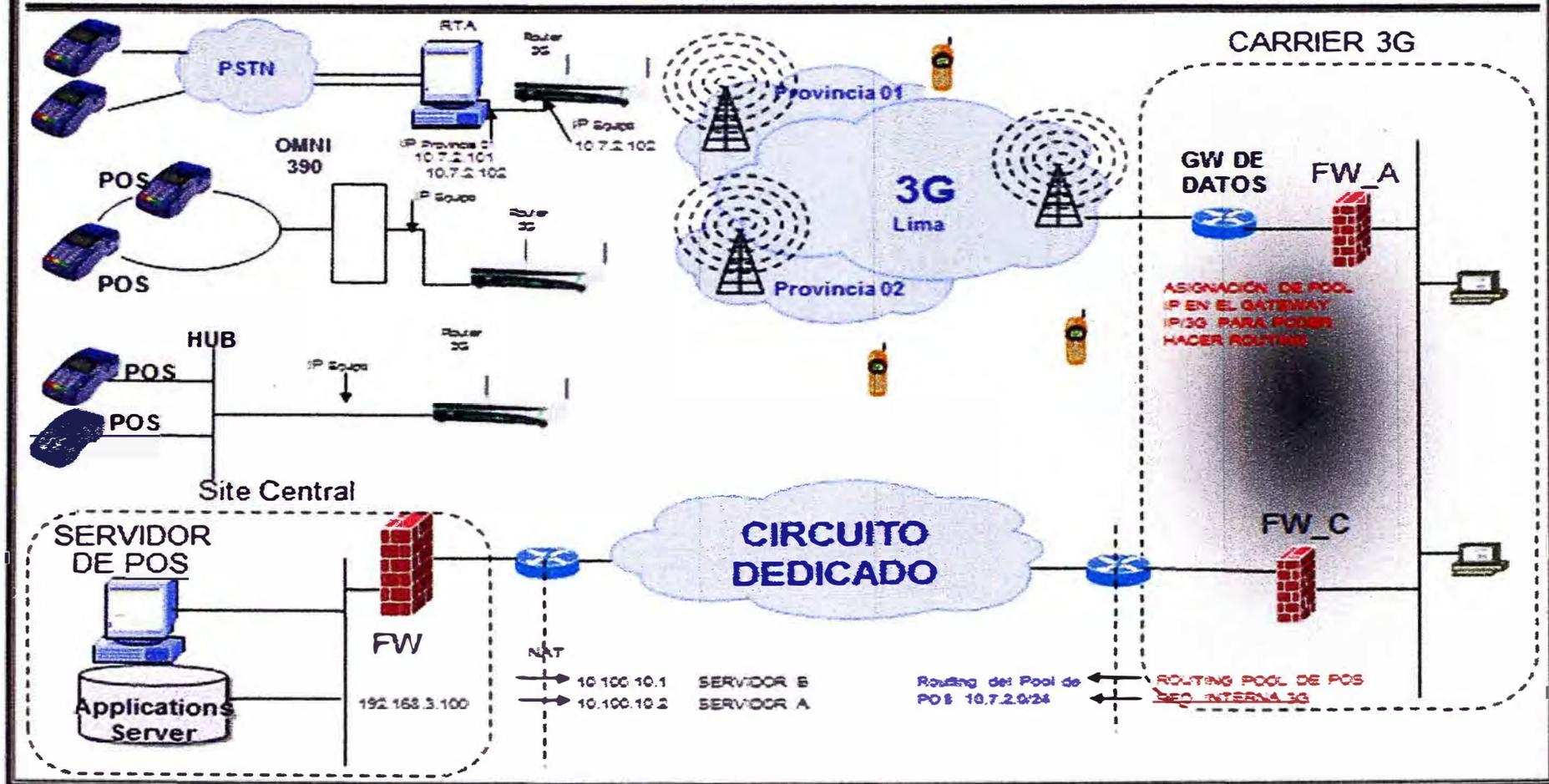
DISEÑO DE RED CON SERVIDOR IP VIA 3G POR CIRCUITO DEDICADO PARA CAJERO AUTOMÁTICO



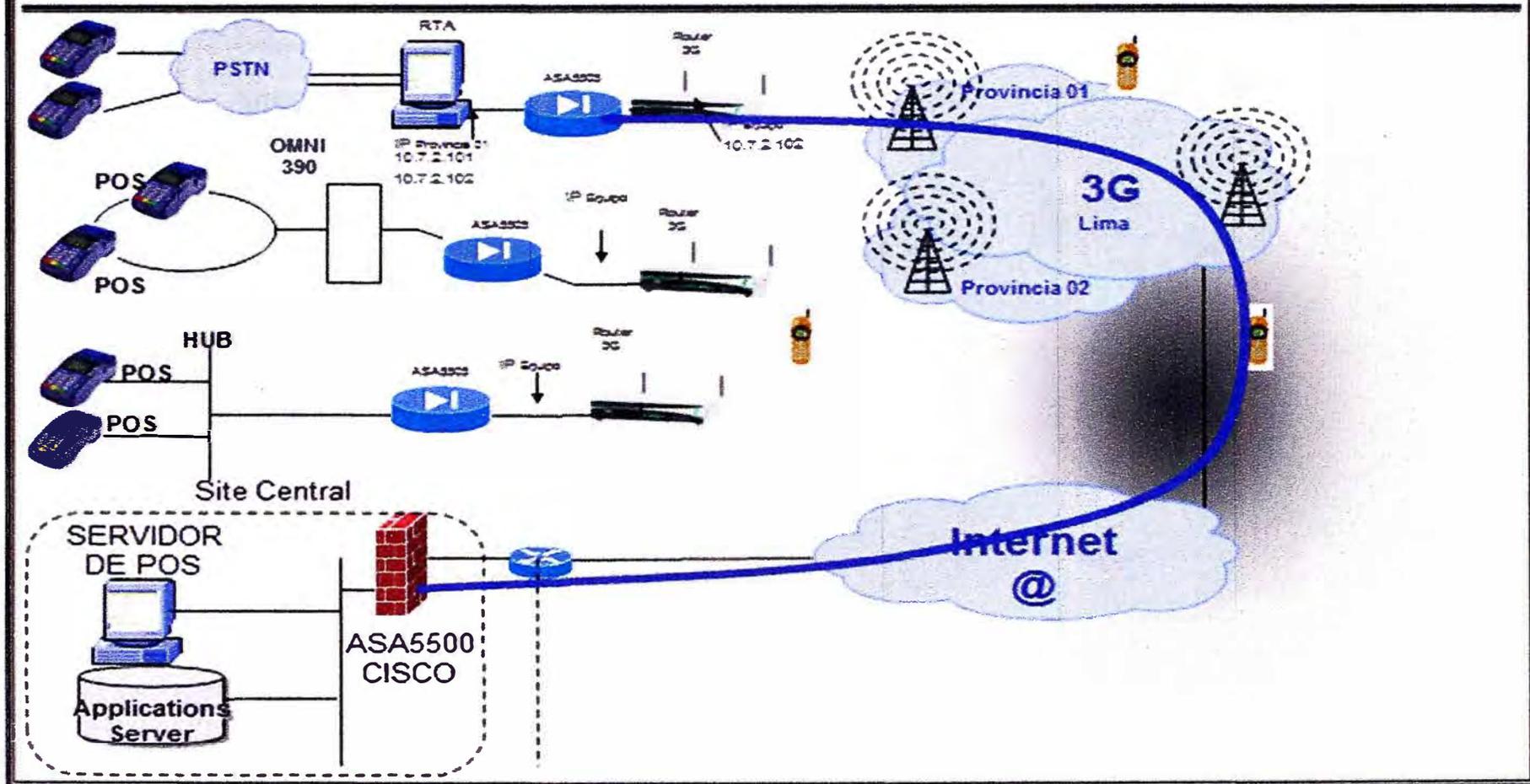
DISEÑO DE RED CON SERVIDOR IP VIA 3G CON VPN IPSEC VIA INTERNET PARA CAJERO AUTOMÁTICO



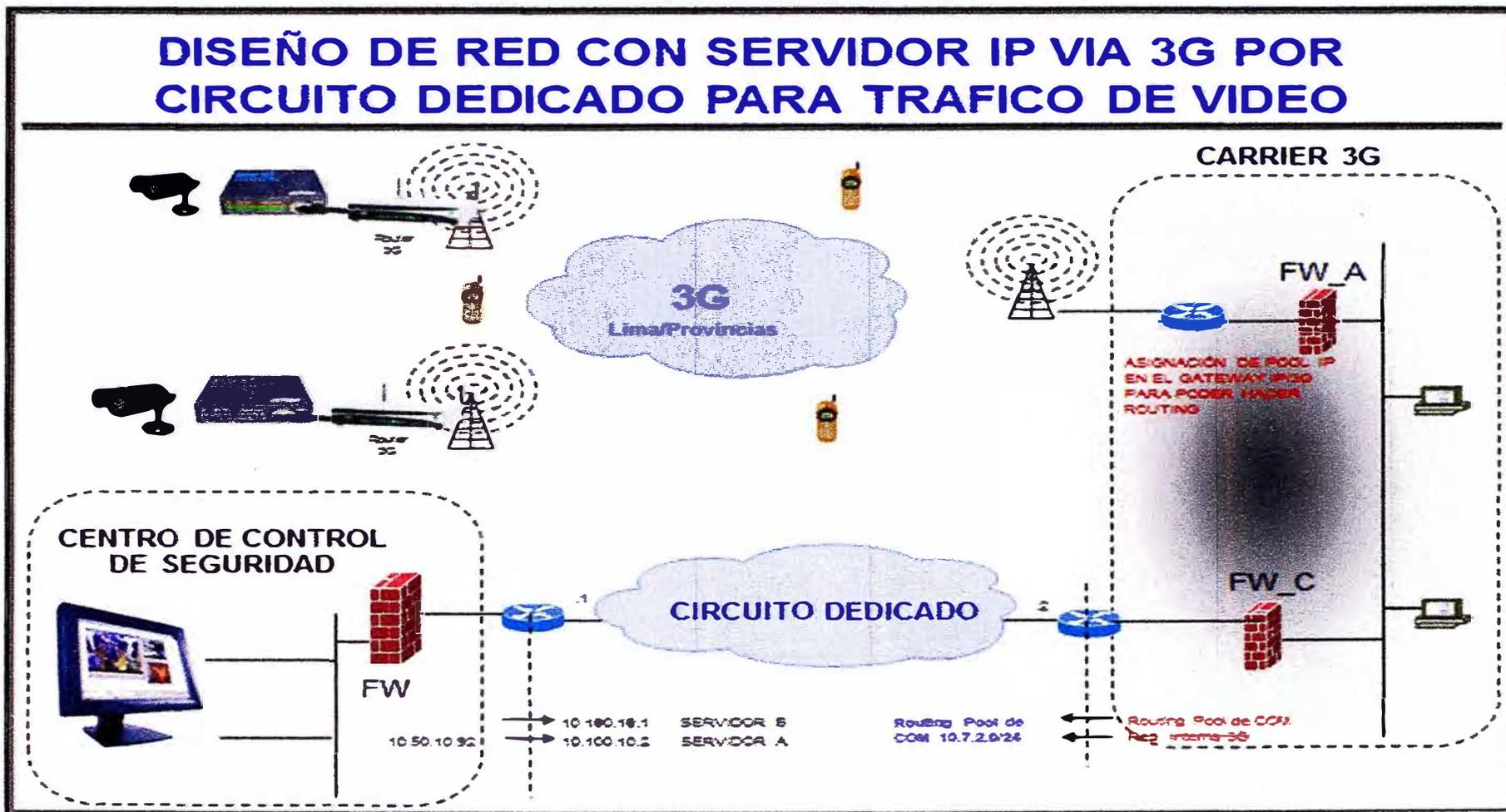
DISEÑO DE RED CON SERVIDOR IP VIA 3G POR CIRCUITO DEDICADO PARA POS



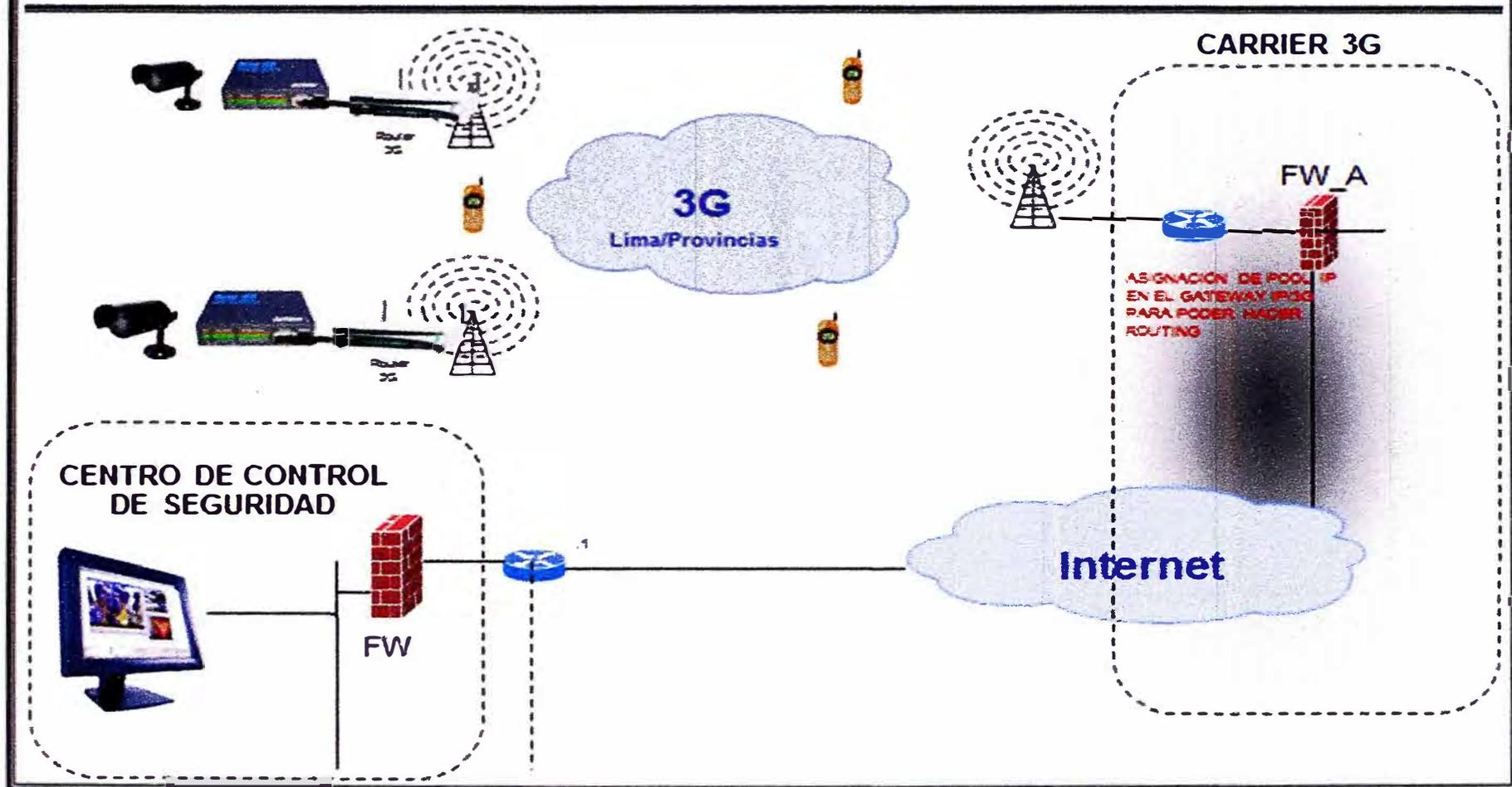
DISEÑO DE RED CON SERVIDOR IP VIA 3G CON VPN IPSEC VIA INTERNET PARA POS



DISEÑO DE RED CON SERVIDOR IP VIA 3G POR CIRCUITO DEDICADO PARA TRAFICO DE VIDEO



DISEÑO DE RED CON SERVIDOR IP VIA 3G POR VPN IPSEC VIA INTERNET TRAFICO DE VIDEO



ANEXO E
DIRECCIONAMIENTO IP

PLAN DE NUMERACIÓN IP PROPUESTO

Para la RED: 10.10.10.0/24

Tendríamos 252 Host disponibles para asignar a los Cajeros

Para la RED: 10.10.10.0/24

Tendríamos 64 Sub-redes de la forma siguiente:

Red 01: 10.10.10.0/30

Por ejemplo:

10.10.10.0 Net

10.10.10.1 ATM01

10.10.10.2 3G

10.10.10.3 Broadcast

Red 26: 10.10.10.100/30

Por ejemplo:

10.10.10.100 Net

10.10.10.101 ATM26

10.10.10.102 3G

10.10.10.103 Broadcast

Red 64: 10.10.10.252/30

Por ejemplo:

10.10.10.252 Net

10.10.10.253 ATM64

10.10.10.254 3G

10.10.10.255 Broadcast

ANEXO F
TABLA DE COSTOS

SERVICIO DE DATOS CARRIER 01

Condiciones Generales para el equipamiento de esta solución

1. Costos*:

CARRIER 01 - SERVICIO DE DATOS IP

Bandwith: 128k

PVC Punto a Punto : \$350 (Mensual)

Equipo: Cisco1605 : \$62.85 (Mensual)

Costo de instalación** : \$935

Tiempo de instalación* : 35 días Después del pago de la instalación

** : costo por el punto a punto..

* : En días Útiles, Una vez verificadas las facilidades técnicas y stock disponible

Tiempo de contrato : 1 año.

Para un Punto a Punto el costo total es :

Sede Principal : 350(m) + 935(u) + 62.85 (m) (Dollar)

Sede Remota : - (m) + - (u) + 62.85 (m) (Dollar)

***Referenciales a la fecha 08/06/05**

SERVICIO DE DATOS CARRIER 02

Condiciones Generales para el equipamiento de esta solución

2. Costos*:

CARRIER 02 - SERVICIO DE DATOS IP

Bandwidth: 128k

PVC Punto a Punto : \$175.5 (Mensual)

Equipo: Modem : \$60 (Mensual)

Equipo Cisco1721 : \$ 24*86 = \$ 2064 (a 24 meses por contrato)

Costo de instalación** : \$710 (Conex. a la Red e install. de la Pta inc. Router)

Tiempo de instalación* : Por Confirmar

** : Una vez verificadas las facilidades técnicas y stock disponible.

* : En días Útiles

Tiempo de contrato : Libre (excepto el Router que puede variar de 1 año o 2 años)

Para un Punto a Punto el costototal es:

Sede Principal : 500(u) + 100 (u) + 110 (u) + 175.5 (m) + 60 (m) + 86*24 (Dollar)

Sede Remota : 500 (u) + 100 (u) + 110 (u) + 175.5 (m) + 60 (m) + 86 *24 (Dollar)

*Referenciales a la fecha 08/06/05

SERVICIO DE DATOS CARRIER 03

Condiciones Generales para el equipamiento de esta solución

3. Costos*:

CARRIER 03 - Servicio de Datos

Bandwith: 128k

clearchannel con calidad de servicio : \$280 (Mensual)

Equipo: Cisco1601 ó Cisco3810 : \$50 (Mensual)

Costo de instalación** : \$800

Tiempo de Instalación* : 10 días

** : Costo por Punto.

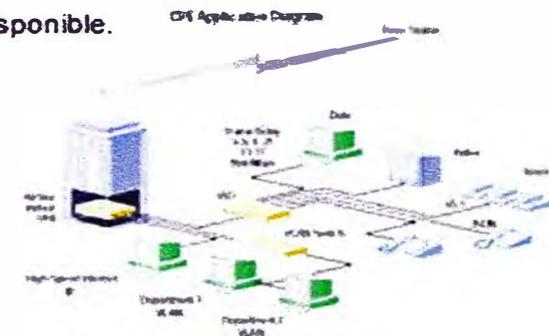
* : En días Útiles. Una vez verificadas las facilidades técnicas y stock disponible.

Tiempo de contrato : 1 año.

Para un Punto a Punto el costo total es:

Sede Principal : 280(m) +50(m)+800(u) (Dollar)

Sede Remota : 280(m) +50(m)+800(u) (Dollar)



*Referenciales a la fecha 08/06/05

SERVICIO DE DATOS CARRIER 3G

Condiciones Generales para el equipamiento de esta solución

4. Costos*:

CARRIER 3G - Servicio de Datos por 3G

Bandwidth: Para 3G y disponibilidad

(definida por el equipo Terminal CPE).

: S/.175 (Mensual) ilimitado

: S/.35 (Mensual) 5Mbps

Equipo: Equipo3G

: \$1000 (Costo Único)

Costo de instalación**

: \$0

Tiempo de instalación*

: 2 días

** : Costo por Punto.

* : En días Útiles, Una vez verificadas las facilidades técnicas y stock disponible

Tiempo de contrato*

: a definir el tiempo.

Para este servicio el costo total es:

Sede Remota : $54.4 (<> \text{Soles } 175)(m) + 1000.00(u) + 0.00 (m) (\text{Dollar})$

*Referenciales a la fecha 08/06/05

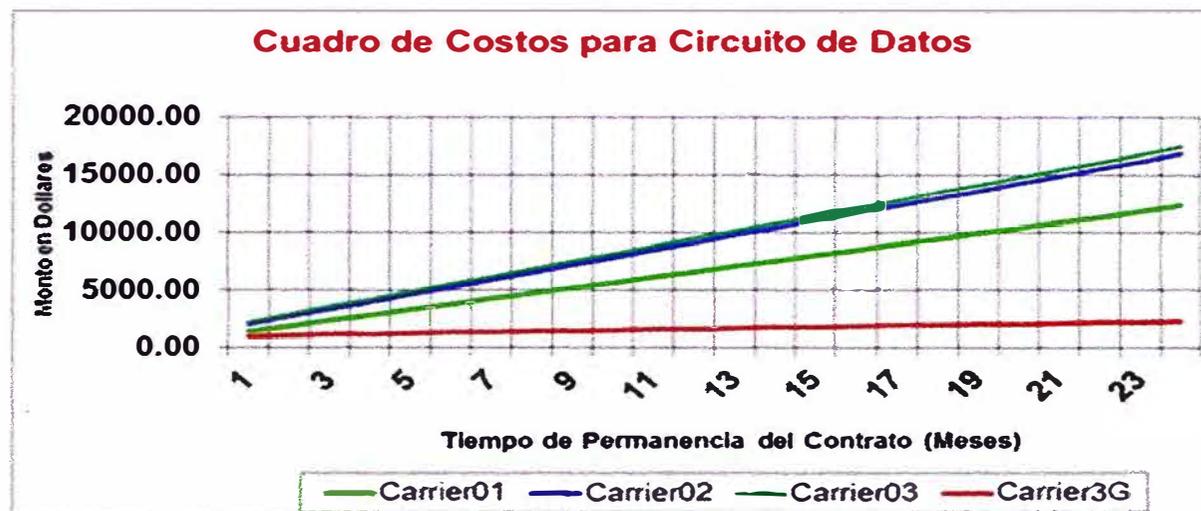
RESUMEN DE COSTOS A 128kbps VS 3G*

TIEMPO MESES	CARRIER 01 **	CARRIER 02**	CARRIER 03**	3G CARRIER**	TIEMPO MESES	CARRIER 01**	CARRIER 02**	CARRIER 03**	3G CARRIER**
1	1410.70	2063.00	2260.00	1054.69	13	7119.10	9779.00	10180.00	1710.94
2	1886.40	2706.00	2920.00	1109.38	14	7594.60	10422.00	10840.00	1765.63
3	2362.10	3349.00	3580.00	1164.06	15	8070.50	11065.00	11500.00	1820.31
4	2837.80	3992.00	4240.00	1218.75	16	8546.20	11708.00	12160.00	1875.00
5	3313.50	4635.00	4900.00	1273.44	17	9021.90	12351.00	12820.00	1929.69
6	3789.20	5278.00	5560.00	1328.13	18	9497.60	12994.00	13480.00	1984.38
7	4264.90	5921.00	6220.00	1382.81	19	9973.30	13637.00	14140.00	2039.06
8	4740.60	6564.00	6880.00	1437.50	20	10449.00	14280.00	14800.00	2093.75
9	5216.30	7207.00	7540.00	1492.19	21	10924.70	14923.00	15460.00	2148.44
10	5692.00	7850.00	8200.00	1546.88	22	11400.40	15566.00	16120.00	2203.13
11	6167.70	8493.00	8860.00	1601.56	23	11876.10	16209.00	16780.00	2257.81
12	6643.40	9136.00	9520.00	1656.25	24	12351.80	16852.00	17440.00	2312.50

*Referenciales a la fecha 08/06/05

**Costo expresados en Dólares americanos

CUADRO COMPARATIVO



Observación:

- Par el caso de CARRIER 01 el contrato es de 12 meses.
- Par el caso de CARRIER 02 el contrato es Libre (Excepto el router que esta cotizado a 24 meses).
- Par el caso de CARRIER 03 el contrato es de 12 meses.
- Los valores de la tabla son aproximados y se tendría que validar con una nueva propuesta del proveedor de servicios.

ANEXO G
DIAGRAMA DE GANTT

Id	Nombre de tarea	Duración	mes				
			1	2	3	4	5
1	PROYECTO 3G PARA ZONAS RURALES	81 días	[Barra de proyecto que cubre los meses 1, 2, 3, 4 y 5]				
2	Gestión de importación de equipos	61 días	[Barra de tarea que cubre desde el inicio hasta el inicio de mes 4]				
3	Solicitar los equipos a fábrica	1 día	[Punto de hito en el inicio]				
4	Trasferencia Bancaria al extranjero	2 días	[Barra de tarea que cubre los primeros 2 días]				
5	Confirmación de fábrica disponibilidad de equipos	1 día	[Punto de hito al final de los 2 días]				
6	Equipos disponibles en fábrica	18 días	[Barra de tarea que cubre los primeros 18 días]				
7	Traslado prioritario por avión	4 días	[Barra de tarea que cubre los días 18-22]				
8	Agente de aduanero para el trámite	2 días	[Barra de tarea que cubre los días 22-24]				
9	Permiso de internamiento	3 días	[Barra de tarea que cubre los días 24-27]				
10	Aduanas	2 días	[Barra de tarea que cubre los días 27-29]				
11	Pago de impuestos	2 días	[Barra de tarea que cubre los días 29-31]				
12	Equipos disponibles en aduanas para ser recojidos	2 días	[Barra de tarea que cubre los días 31-1 de mes 2]				
13	Entrega de equipos en almacén del proveedor	1 día	[Punto de hito al inicio de mes 2]				
14	Revisión de equipos para validar su estado antes de entregar al cliente	3 días	[Barra de tarea que cubre los días 1-3 de mes 2]				
15	Análisis de tráfico	20 días	[Barra de tarea que cubre desde el inicio de mes 3 hasta el inicio de mes 4]				
16	Análisis de aplicaciones	10 días	[Barra de tarea que cubre los primeros 10 días de mes 3]				
17	Análisis de tráfico de alarmas	10 días	[Barra de tarea que cubre los días 10-20 de mes 3]				
18	Entrega de equipos y configuración	20 días	[Barra de tarea que cubre desde el inicio de mes 4 hasta el inicio de mes 5]				
19	Entrega de equipos al cliente	3 días	[Barra de tarea que cubre los primeros 3 días de mes 4]				
20	Configuración de equipos	5 días	[Barra de tarea que cubre los días 3-8 de mes 4]				
21	Carga de firmware	5 días	[Barra de tarea que cubre los días 8-13 de mes 4]				
22	Instalación de sim card provisionado	5 días	[Barra de tarea que cubre los días 13-18 de mes 4]				

Proyecto: PROYECTOS SOBRE REDES DE NUEVA GENERACIÓN 3G
Y APLICACIONES PARA LA BANCA RURAL
Fecha: dom 03/02/13

Tarea		Resumen inactivo	
División		Tarea manual	
Hito		Sólo duración	
Resumen		Informe de resumen manual	
Resumen del proyecto		Resumen manual	
Tareas externas		Sólo el comienzo	
Hito externo		Sólo fin	
Tarea inactiva		Fecha límite	
Hito inactivo		Progreso	

Id	Nombre de tarea	Duración					
			mes 1	mes 2	mes 3	mes 4	mes 5
23	Prueba de operación y enrutamiento del equipo	2 días					
24	Implementación de la solución	63 días					
25	planificación de la solución	3 días					
26	Etapa Carrier	60 días					
27	Habilitación de enlace dedicado entre el carrier y la institución Financiera	45 días					
28	Provisión de SIM Card (IP fijo, tráfico internet habilitado, APN customizado)	15 días					
29	Etapa Institución financiera	21 días					
30	Elaboración de la topología de red para el ingreso del nuevo tráfico	7 días					
31	Revisión del plan de numeración de la solución	3 días					
32	Configuración de las redes en los distintos dispositivos de comunicaciones de la red del cliente	10 días					
33	Revisión de las redes de los servidores de aplicación y seguridad	1 día					
34	Etapa site remoto	6 días					
35	Planta externa y montaje del cajero automático	3 días					
36	Instalación del equipo y conexión de red	1 día					
37	Pruebas de conectividad	1 día					
38	Pruebas de transacción	1 día					
39	Validación de conexión de aplicación	1 día					
40	Puesta en producción del servicio	1 día					

Proyecto: PROYECTOS SOBRE REDES DE NUEVA GENERACIÓN 3G
Y APLICACIONES PARA LA BANCA RURAL
Fecha: dom 03/02/13

Tarea		Resumen inactivo	
División		Tarea manual	
Hito		Sólo duración	
Resumen		Informe de resumen manual	
Resumen del proyecto		Resumen manual	
Tareas externas		Sólo el comienzo	
Hito externo		Sólo fin	
Tarea inactiva		Fecha límite	
Hito inactivo		Progreso	

Id	Nombre de tarea	Duración					
			mes 1	mes 2	mes 3	mes 4	mes 5
41	Documentación	5 días					
42	Elaboración de informe	5 días					
43	Cierre del proyecto (Firma de acta de servicio)	1 día					
44	Soporte post implementación (garantía de implementación)	30 días					

Proyecto: PROYECTOS SOBRE REDES DE NUEVA GENERACIÓN 3G
 Y APLICACIONES PARA LA BANCA RURAL
 Fecha: dom 03/02/13

Tarea		Resumen inactivo	
División		Tarea manual	
Hito		Sólo duración	
Resumen		Informe de resumen manual	
Resumen del proyecto		Resumen manual	
Tareas externas		Sólo el comienzo	
Hito externo		Sólo fin	
Tarea inactiva		Fecha límite	
Hito inactivo		Progreso	

ANEXO H
GLOSARIO DE TÉRMINOS

ATM: Conocido en el medio local como cajero automático. El cajero automático es una máquina expendedora usada para extraer dinero utilizando una tarjeta de crédito o débito.

Administrador de red: Personal responsable de administrar la red dentro de una entidad. Entre las responsabilidades generalmente se incluyen, a modo de ejemplo, la seguridad, las instalaciones, las actualizaciones, el mantenimiento y la supervisión de la actividad de la red.

Aplicación: Incluye todos los programas o grupos de programas de software adquiridos y personalizados, así como también las aplicaciones internas y externas.

Aplicación Web: Una aplicación a la que generalmente se accede mediante un explorador web o a través de servicios Web. Las aplicaciones web pueden estar disponibles a través de Internet o en una red privada e interna.

Base de datos: Formato estructurado que permite organizar y mantener información de fácil recuperación. Algunos ejemplos simples de base de datos son las tablas y las hojas de cálculo.

BPI: Acrónimo de banca por Internet.

Broadcast: Transmisión de un paquete que será recibido por todos los dispositivos en una red.

BERT: Tasa de error de bits.

BMP: Mapa de bits o Bit Mapped.

CAPEX: Significa "los gastos de capital", gasto de capital es la cantidad de dinero gastado por una empresa para mejorar, adquirir, mantener incluyendo tangibles depreciables de los activos físicos por el plazo de duración.

CRC: Cyclic Redundancy Check.

CDMA: Wideband Code-Division Multiple-Access.

DMZ: Abreviatura de zona desmilitarizada, viene del término en inglés "demilitarized zone". Subred física o lógica que proporciona una capa de seguridad adicional a la red privada interna de una organización.

DSP: Digital Signal Processing.

EDGE: Enhanced Data rate GSM Evolution.

Enmascaramiento: Técnica empleada para ocultar valores en pantalla o impresos mediante el empleo de asteriscos o algún símbolo similar.

FDD: Frequency division duplex.

Firewall: Dispositivo de red empleado para bloquear el acceso no autorizado de redes no confiables hacia una red confiable, permitiendo al mismo tiempo comunicaciones autorizadas.

FW: Dispositivo de red empleado para bloquear el acceso no autorizado de redes no confiables hacia una red confiable, permitiendo al mismo tiempo comunicaciones autorizadas.

FTP: Acrónimo del protocolo de transferencia de archivos. Protocolo de red que se utiliza para transferir datos de una computadora a otra mediante un red pública, como Internet. En general, se considera que FTP es un protocolo inseguro, porque permite enviar contraseñas y contenido de archivos sin protección y en texto simple.

Gateway de datos: Es un dispositivo de comunicaciones que es capaz de interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

GPRS: General Packet Radio Service.

Host: Es el término empleado para identificar un nodo de red como por ejemplo una computadora o laptop.

HTTP: Acrónimo del protocolo de transferencia de hipertexto. Protocolo abierto de Internet que permite transferir o transmitir información en Internet.

HTTPS: Acrónimo del protocolo de transferencia de hipertexto a través de una capa de conexión segura. HTTP seguro que proporciona autenticación y comunicación cifrada en Internet diseñado para comunicaciones que dependen de la seguridad, tales como los inicios de sesión basados en la web.

ICMP: Acrónimo del protocolo de mensajes de control de Internet. Es el encargado de control y notificación de errores del protocolo IP.

IMT 2000: International Mobile Telecommunication 2000.

IP: Acrónimo del protocolo de Internet. Protocolo de capas de red que contiene información sobre direcciones y algunos datos de control, y permite el ruteo de paquetes. IP es el protocolo primario de capas de red en la suite de protocolos de Internet.

IPv4: Versión 4 del protocolo IP.

IPSec: Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete.

LAN: Acrónimo de red de área local.

Multicast: Envío de la información en una red a múltiples destinos simultáneamente.

MPLS: Multi-Protocol Label Switching, Conmutación Multi-Protocolo mediante Etiquetas, es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031

OPEX: Es el costo de la ejecución de los servicios de TI. Frecuentemente se trata de pagos. Por ejemplo, el costo de personal, el mantenimiento de hardware o el consumo eléctrico.

PCI DSS: Norma de seguridad que deben cumplir las organizaciones que procesan, transportan o almacenan datos de titulares de tarjeta.

PCI SSC: Es el acrónimo del comité PCI Security Standards Council, el cual es un foro mundial abierto destinado a la formulación, la mejora, el almacenamiento, la difusión y la aplicación permanentes de las normas de seguridad para la protección de datos de cuentas.

POS: Equipo terminal de transacción utilizado para hacer pagos con tarjeta de crédito es llamado punto de venta o point of sale.

SAN: Acrónimo de red de área de almacenamiento.

Servidor Web: Computadora con un programa capaz de aceptar pedidos HTTP de clientes web y brindar respuestas HTTP (en general, páginas web).

Server APP: Servidor donde se encuentra la aplicación para entregar servicios transaccionales.

Servidor ATM: Servidor donde se encuentra las aplicaciones de los cajeros automáticos, los cuales por medio de una conexión TCP pueden conectar estableciendo así una conexión para realizar transacciones.

Servidor POS: Servidor donde se encuentra las aplicaciones de los POS, los cuales por medio de una conexión TCP pueden conectar estableciendo así una conexión para realizar transacciones.

Servidor de Video: Servidor donde se encuentra las aplicaciones cliente servidor de la solución de video seguridad.

SFTP: Acrónimo del protocolo de transferencia segura de archivos.

SLA: Service level agreement.

SNMP: Simple Network Management Protocol.

SMTP: Acrónimo del protocolo simple de transferencia de correo, es empleado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

Switch: Dispositivo digital de lógica de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI.

TDD: Time - division duplex.

TCP: Acrónimo del protocolo de control de transmisión. Lenguaje comunicativo o protocolo básico de Internet.

UDP: Acrónimo del protocolo de datagramas de usuario. Proporciona una sencilla interfaz entre la capa de red y la capa de aplicación sin ofrecer garantías para la entrega de sus mensajes.

UMTS: Universal mobile telecommunications system

VLAN: Abreviatura de LAN virtual o red de área local virtual. Red de área local lógica que se extiende más allá de una sola red física de área local.

WAN: Acrónimo de red de área amplia. Red informática que abarca un área amplia, a menudo parte de un sistema con cobertura en toda una región o empresa.

BIBLIOGRAFÍA

- [1] INEI - Perú: "Estimaciones y Proyecciones de Población Económicamente Activa, Urbana y Rural por Sexo y Grupos de Edad, según Departamento, 2000 - 2015 - Boletín Especial N° 20".
- [2] Cisco System, "Internet Edge Solution Overview"
- [3] Fabián Garzón Garzón, "Evolución en la seguridad de medios de pago"
- [4] Cisco Systems, "Cisco IT, Case Study Service Oriented Network Architecture".
- [5] Office of Technology Services Security Management Division, "Network Architecture Standard".
- [6] Vanesa Gil Laredo, "PCI DSS Compliance- Payment Card Industry Data Security Standard".
- [7] Braintree Payment Solutions, "PCI DSS Compliance Overview".
- [8] SNMP is defined by IETF (<http://www.ietf.org>) with a group of RFCs shown in the reference links.
- [9] SNMPv1 is defined by IETF (<http://www.ietf.org>) in RFC 1157 plus a few supporting RFCs shown in the reference links.
- [10] SNMPv2 is defined by IETF (<http://www.ietf.org>) in RFC 1441 originally plus by a group of supporting and updating RFCs shown in the list below.
- [11] SNMPv3 is defined by IETF (<http://www.ietf.org>) in RFC 3411 plus a group of supporting RFCs shown in the reference links.
- [12] Korhonen, Juha. Introduction to 3G Mobile Communications. United states of America, Norwood, MA: Artech house, 2001
- [13] RFC 3031 MPS: <http://www.ietf.org/rfc/rfc3031.txt>