(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 796 473**

(51) Int. CI.:

H04L 12/715 (2013.01)
H04L 29/06 (2006.01)
H04L 12/707 (2013.01)
H04L 12/703 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.04.2016 PCT/IB2016/000531**

(87) Fecha y número de publicación internacional: **13.10.2016 WO16162749**

(96) Fecha de presentación y número de la solicitud europea: **07.04.2016 E 16727220 (2)**

(97) Fecha y número de publicación de la concesión europea: **06.05.2020 EP 3281368**

(54) Título: **Sistema de red que tiene interfaces virtuales y un módulo de enrutamiento para una red virtual**

(30) Prioridad:

07.04.2015 US 201562144293 P
22.04.2015 US 201562151174 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.11.2020

(73) Titular/es:

UMBRA TECHNOLOGIES LTD. (100.0%)
Suite 2006 20th Floor, Hua Qin International Building, 340 Queen's Road Central
Hong Kong 100015, CN

(72) Inventor/es:

ORE, CARLOS EDUARDO;
SAINT-MARTIN, THIBAUD AUGUSTE BERNARD JEAN y
RUBENSTEIN, JOSEPH E.

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de red que tiene interfaces virtuales y un módulo de enrutamiento para una red virtual

Esta solicitud reivindica prioridad a la Solicitud Provisional de Estados Unidos No. 62/144.293 archivada el 7 de abril, 2015 y la Solicitud Provisional de Estados Unidos No. 62/151.174 archivada el 22 de abril, 2015.

Campo de la descripción

La presente descripción se refiere generalmente a redes, y más particularmente, a la construcción automática de interfaces virtuales (VIF) y estructuras de VIF que actúan como puntos de enganche para múltiples túneles de red. Las VIF permiten el desplazamiento en el tiempo y operaciones intensivas de recursos tal como enrutamiento hacia arriba al VIF que son típicamente aplicadas a túneles.

Antecedentes de la descripción

Los seres humanos son capaces de percibir retrasos de 200ms o más ya que es el tiempo de reacción humano promedio típico a un evento. Si la latencia es demasiado alta, los sistemas en línea tales como clientes delgados de servidores basados en la nube, gestión de relaciones con cliente (CRM), planificación de recursos de empresa (ERP) y otros sistemas tendrán un rendimiento pobre y pueden incluso dejar de funcionar debido a tiempos acabados. La alta latencia combinada con alta pérdida de paquetes puede hacer una conexión inutilizable. Incluso si los datos pasan, en un cierto punto demasiada lentitud resulta en una experiencia de usuario (UX) pobre y en algunas instancias el resultado puede ser negación de los usuarios a aceptar esas condiciones en efecto que interpreta servicios entregados de manera pobre como inútiles.

Para abordar algunos de estos problemas, varias tecnologías han sido desarrolladas. Una de tales tecnologías es optimización de WAN, que normalmente implica un dispositivo hardware (HW) en el borde de una red de área local (LAN) que construye un túnel a otro dispositivo HW de optimización de WAN en el borde de otra LAN, que forma una red de área extensa (WAN) entre ellas. Esta tecnología asume una conexión estable a través de los dos dispositivos conectados entre sí. Un optimizador de WAN se esmera en comprimir y asegurar el flujo de datos a menudo resultando en una ganancia de velocidad. El impulsor comercial para la adopción de la optimización de WAN es ahorrar en el volumen de datos enviados en un esfuerzo para reducir el coste de la transmisión de datos. Las desventajas de esto son que a menudo es punto a punto y puede luchar cuando la conexión entre dos dispositivos no es buena y hay poco o ningún control sobre el camino del flujo del tráfico a través de Internet entre ellos. Para abordar esto, los usuarios de optimizadores de WAN a menudo optan por ejecutar sus WAN sobre una línea MPLS o DDN u otro circuito dedicado que resulta en un gasto añadido y de nuevo normalmente implicando una conexión punto a punto fija y rígida.

Enlaces directos tales como MPLS, DDN, Circuitos Dedicados u otros tipos de conexiones punto a punto fijas ofrecen calidad de conexión y garantías de Calidad de Servicio (QoS). Son caras y a menudo toman un tiempo significativamente largo para instalarlos debido a que necesitan dibujar líneas físicas desde un POP en cada lado de la conexión. La topología punto a punto trabaja bien cuando se conectan desde dentro de una LAN a los recursos de otra LAN a través de esta WAN conectada directamente. Sin embargo, cuando la puerta de enlace (GW) a Internet general está ubicada en la LAN de un extremo, digamos en la sede corporativa, entonces el tráfico desde la LAN remota de un país subsidiario puede ser enrutado a Internet a través de la GW. Una ralentización ocurre a medida que el tráfico fluye a través de internet de vuelta a los servidores en el mismo país que la sucursal. El tráfico debe entonces ir desde la LAN a través de la WAN a la LAN donde la GW está ubicada y entonces a través de Internet de vuelta a un servidor en el país de origen, entonces de vuelta a través de internet a la GW, y entonces de vuelta a la línea dedicada al dispositivo de cliente dentro de la LAN. En esencia se duplica o triplica (o peor) el tiempo de tránsito global de lo que debería tomar una fracción pequeña de la latencia global para acceder a este sitio cercano. Para superar esto, la conectividad alternativa de otra línea de internet con configuración apropiada cambia y los dispositivos añadidos pueden ofrecer tráfico local a internet, en cada extremo de tal sistema.

Otra opción para crear enlaces de WAN desde una LAN a otra LAN implica la construcción de túneles tales como IPSec u otros túneles de protocolo entre dos enrutadores, cortafuegos, o dispositivos de borde equivalentes. Estos son normalmente encriptados y pueden ofrecer compresión y otra lógica para intentar mejorar la conectividad. Hay poco o ninguno control sobre las rutas entre los dos puntos ya que dependen en la política de varios jugadores intermedios en internet que llevan su tráfico sobre su red o redes y son pares a otros portadores y/o operadores de red. Los cortafuegos y enrutadores, conmutadores y otros dispositivos de varios suministradores de equipos tienen opciones de creación de túneles construidas en su firmware.

Mientras que la conectividad de la última milla ha mejorado vastamente en los años recientes todavía hay problemas con la conectividad de larga distancia y rendimiento debido a problemas relacionados con la distancia, limitaciones de protocolo, pares, interferencias, y otros problemas y amenazas. Como tal, existe una necesitad para servicios de optimización de red seguros que se ejecutan por encima de las conexiones de internet estándar.

Compendio de la descripción

La presente invención está dirigida al tema en cuestión como se describe por las reivindicaciones anexas.

Breve descripción de los dibujos

Para facilitar una comprensión más completa de la presente descripción, se hace referencia ahora a los dibujos que acompañan, en los cuales elementos iguales son referenciados con numerales o referencias iguales. Estos dibujos no deberían interpretarse como limitación de la presente descripción, sino que pretenden ser solo ilustrativos.

La FIG. 1 ilustra el hinchado de paquete para paquetes de transporte IP cuando se añaden cabeceras a los datos en varias capas.

La FIG. 2 ilustra el hinchado de paquetes de datos y cabeceras en cada una de las siete capas del modelo OSI.

La FIG. 3 muestra un diagrama de bloques que representa la resolución del localizador de recursos uniforme (URL) a través de la búsqueda en un sistema de nombre de dominio (DNS) de internet para enrutar desde el Equipo (cliente) a la dirección IP numérica del Equipo (servidor).

La FIG. 4 ilustra una ecuación para calcular producto de retraso de ancho de banda (BDP) para un segmento de conexión o camino que tiene en cuenta varios atributos de conectividad.

La FIG. 5 ilustra el camino de flujo del tráfico dentro de un dispositivo de punto extremo (EPD).

La FIG. 6 ilustra un túnel encima de todo (OTT) creado encima de una conexión de internet ordinaria.

La FIG. 7 ilustra una interfaz virtual para túneles encima de todo (OTT) creados encima de una conexión de internet ordinaria.

La FIG. 8 es un diagrama de flujo que describe cómo determinar el mejor punto de ingreso egreso (EIP) para que el tráfico fluya a través de una red virtual global (GVN) a internet.

La FIG. 9 ilustra el esfuerzo colaborativo entre varios módulos, mecanismos, tecnologías y otros componentes de la GVN.

La FIG. 10 ilustra las operaciones de capa uno, capa 2, y capa 3 de una red virtual global (GVN).

La FIG. 11 es un diagrama de flujo de Enrutamiento Inteligente Avanzado (ASR) dentro de una red virtual global (GVN).

La FIG. 12 es un diagrama de flujo de las varias rutas disponibles a través de una GVN desde un origen a un destino.

La FIG. 13 ilustra la unión de varios segmentos de red diferentes en un camino extremo a extremo.

La FIG. 14 ilustra un salto entre dos segmentos de red.

La FIG. 15 ilustra problemas potenciales que pueden ocurrir dentro de un dispositivo en un salto entre dos segmentos de red.

La FIG. 16 ilustra el ciclo de vida de un túnel.

La FIG. 17 ilustra la relación e interacciones entre un dispositivo de punto extremo (EPD), un servidor de control central (SRV_CNTRL), y un servidor de punto de acceso (SRV_AP) cuando se construye un túnel entre el EPD y el SRV.

La FIG. 18 ilustra la organización lógica de interfaces e interfaces virtuales dentro de un dispositivo de punto extremo (EPD) para soportar múltiples túneles.

La FIG. 19 es un diagrama de flujo que describe la lógica de algoritmos que potencian el enrutamiento inteligente avanzado (ASR) dentro de una red virtual global (GVN).

La FIG. 20 ilustra la funcionalidad de una interfaz virtual VIF con un camino de tráfico y las ventanas que ofrece.

La FIG. 21 es un diagrama de flujo que describe el algoritmo que gobierna cuando el flujo de tráfico debería ser conmutado desde un túnel a otro túnel.

La FIG. 22 ilustra la estructura lógica de dos interfaces virtuales (VIF) conectadas secuencialmente a lo largo de un camino.

La FIG. 23 ilustra el tiempo requerido para procesar varios túneles (TUN) e interfaces virtuales (VIF).

La FIG. 24 ilustra la estructura lógica de múltiples VIF dispuestas secuencialmente dentro de un camino de tráfico entre el tráfico entrante y otro tráfico.

La FIG. 25 ilustra la estructura lógica de tres interfaces virtuales y sus varios túneles a tres regiones diferentes.

La FIG. 26 ilustra líneas de tiempo para operaciones relacionadas con varios túneles (TUN) e interfaces virtuales (VIF).

La FIG. 27 es un diagrama de flujo que describe el algoritmo que gobierna el proceso de toma de decisiones o si hay que conmutar o no desde una interfaz virtual a otra interfaz virtual.

La FIG. 28 ilustra la estructura lógica de tres interfaces virtuales y sus varios túneles a tres regiones diferentes.

La FIG. 29 es un diagrama de flujo que describe el algoritmo que gobierna la destrucción ordenada de una interfaz virtual (VIF).

La FIG. 30 ilustra cómo un túnel encriptado protege datos.

La FIG. 31 ilustra la seguridad ofrecida por un túnel envuelto en otro túnel.

La FIG. 32 ilustra un túnel envuelto y tapado.

La FIG. 33 ilustra un codificador de byte de 8 bits en dos dispositivos de puerta de enlace.

La FIG. 34 ilustra tres fases de codificación diferentes para bytes codificados de bit de un CAP.

La FIG. 35 ilustra un túnel interno a través de una serie de envolturas y entonces un CAP.

La FIG. 36 ilustra tráfico de túnel cortafuegos a cortafuegos durante un fallo de túnel.

La FIG. 37 ilustra tráfico de túnel cortafuegos a cortafuegos durante un fallo de túnel.

La FIG. 38 ilustra tráfico de túnel cortafuegos a cortafuegos durante un fallo de túnel.

La FIG. 39 ilustra el enlace de dos o más redes de área local (LAN) en una red de área extensa (WAN).

La FIG. 40 ilustra la importancia de una lista de disponibilidad de servidor y cómo las direcciones IP y rangos son asignados para varios dispositivos.

La FIG. 41 ilustra múltiples flujos únicos paralelos entre dispositivos.

La FIG. 42 ilustra múltiples flujos no únicos paralelos entre dispositivos.

La FIG. 43 ilustra el marco lógico y la estructura algorítmica para el modo de tiempo tormentos (SWM).

La FIG. 44 ilustra múltiples túneles entre dispositivos dentro de una red virtual global (GVN) sobre múltiples regiones.

La FIG. 45 ilustra problemas potenciales con cuellos de botella a través de un salto entre dos segmentos de red.

La FIG. 46 ilustra la organización y reporte de información en el SRV_CNTRL.

La FIG. 47 es un diagrama de flujo que describe la lógica usada para pruebas de túneles.

La FIG. 48 ilustra la ejecución de pruebas de túneles paralelas para medir latencia, ancho de banda, pérdida de paquetes, y otros factores.

La FIG. 49 ilustra la ejecución de pruebas de conectividad sin interferir con el uso de túnel de usuario actual.

La FIG. 50 ilustra la interacción entre tres dispositivos que colaboran en el proceso de la construcción de túneles.

La FIG. 51 ilustra las relaciones entre varias tablas de bases de datos usadas para almacenar información de conectividad.

La FIG. 52 ilustra los requisitos para información única por túnel para evitar colisiones.

La FIG. 53 es un diagrama de flujo que ilustra el flujo lógico usado para asignar un puerto a una dirección IP usada para construir un túnel.

La FIG. 54 es un diagrama de flujo que describe una estructura para una serie de pruebas de varios puertos de una dirección IP.

La FIG. 55 es un diagrama de flujo que muestra la lógica al respecto de la gestión de relaciones de pares entre dispositivos.

La FIG. 56 ilustra los pasos usados en el establecimiento y posterior ejecución de pruebas de túneles.

La FIG. 57 ilustra un punto extremo virtual (VEP) extendido en la nube.

La FIG. 58 ilustra la unión de un nombre de dominio a un punto extremo virtual (VEP) dinámico.

La FIG. 59 ilustra el enrutamiento de tráfico para un dominio.gTLD para entrar en una red virtual global (GVN) a través del punto de ingreso egreso (EIP) óptimo.

La FIG. 60 ilustra un registro de dispositivos de punto extremo (EPD) y dispositivos de punto extremo personales (PEPD) que pueden ser ubicados y alcanzados a través de un dominio.gTLD.

La FIG. 61 ilustra dispositivos que pueden ser alcanzados a través de un subdominio de un dominio de nivel superior global.

La FIG. 62 ilustra un método para usar una interfaz de usuario gráfica (GUI) que se ejecuta en un buscador en un Dispositivo de Cliente para gestionar información de punto extremo virtual.

La FIG. 63 ilustra cómo el enrutamiento de subdominios.dominios.gTLD puede aprovecharse del enrutamiento inteligente avanzado (ASR) en una red virtual globa (GVN).

La FIG. 64 muestra un diagrama de bloques de tecnología usada por y habilitada por una red virtual global (GVN).

La FIG. 65 ilustra algunos módulos de sistema y componentes para un dispositivo de punto extremo EPD, servidor de control central SRV_CNTRL, y un servidor de punto de acceso SRV_AP.

La FIG. 66 ilustra algunos módulos de sistema y componentes para un dispositivo de punto extremo EPD, servidor de control central SRV_CNTRL, y un servidor de punto de acceso SRV_AP.

La FIG. 67 ilustra algunos módulos de sistema y componentes para un dispositivo de punto extremo EPD, servidor de control central SRV_CNTRL, y un servidor de punto de acceso SRV_AP.

Descripción detallada

Una GVN ofrece servicios de optimización de red seguros a clientes encima de su conexión a internet estándar. Esto es una vista general de las partes constituyentes de una GVN así como una descripción de tecnologías relacionadas que pueden servir como elementos de la GVN. Los elementos de la GVN pueden operar de manera independiente o dentro del ecosistema de una GVN tal como mediante el uso del marco de trabajo de la GVN para sus propios propósitos, o puede ser desplegada para mejorar el rendimiento y eficiencia de una GVN. Esta vista general también describe cómo otras tecnologías pueden beneficiarse de una GVN tanto como en un despliegue único mediante el uso de algunos o todos los componentes de una GVN, o que podría ser rápidamente desplegada como un mecanismo independiente encima de una GVN existente, que usa sus beneficios.

Un software (SW) basado en red privada virtual (VPN) ofrece privacidad a través de un túnel entre un dispositivo de cliente y un servidor de la VPN. Estos tienen una ventaja de encriptación y en algunos casos también compresión. Pero aquí otra vez hay poco o ningún control sobre cómo el tráfico fluye entre el cliente de la VPN y el servidor de la VPN así como entre el servidor de la VPN y un servidor del equipo, cliente del equipo u otros dispositivos en el destino. Estos son a menudo conexiones punto a punto que requieren que se instale software de cliente por dispositivo que usa la VPN y alguna capacidad técnica para mantener la conexión para cada dispositivo. Si un punto de egreso del servidor de la VPN está cerca a través de un camino de comunicación de calidad al servidor de equipo destino o cliente de equipo entonces el rendimiento será bueno. Si no, entonces habrá lentitud apreciable en el rendimiento y descontento desde una perspectiva de usabilidad. A menudo un requisito para un usuario de VPN es tener una desconexión de un servidor de VPN y reconectar a otro servidor de VPN para tener calidad o acceso local a contenido desde una región versus el contenido desde otra región.

Una Red Virtual Global (GVN) es un tipo de una red informática encima de todo (OTT) de internet que proporciona servicios de red seguros globales que usan una malla de dispositivos distribuidos sobre el mundo enlazados de manera segura entre ellos por túneles avanzados, que colaboran y se comunican a través de Interfaz de Programa de Aplicación (API), replicación de Base de Datos (DB), y otros métodos. El enrutamiento del tráfico en la GVN es siempre a través del mejor camino de comunicación gobernado por Enrutamiento Inteligente Avanzado (ASR) desarrollado por sistemas automáticos que combinan constructores, gestores, probadores, análisis algorítmico y otras metodologías para adaptar a las condiciones cambiantes y aprender en el tiempo a configurar y reconfigurar el sistema.

La GVN ofrece un servicio para proporcionar conectividad concurrente segura, fiable, rápida, estable, precisa y enfocada encima de todo (OTT) de una o más conexiones ordinarias de Internet. Estos beneficios son logrados a través de la compresión del flujo de datos que transita múltiples conexiones de túneles envueltos, disfrazados y encriptados entre el EPD y servidores de punto de acceso (SRV_AP) cercanos al EPD. La calidad de la conexión entre el EPD y el SRV_AP es constantemente monitorizada.

Una GVN es una combinación de Dispositivo de Punto Extremo (EPD) de hardware (HW) con software (SW), bases de datos (DB) y otros módulos automáticos instalados del sistema de la GVN tal como Mecanismo de Interfaz de Programación de Aplicación Neutral (NAPIM), gestor de canal posterior, gestor de túnel, y más características que conectan el EPD a dispositivos de infraestructuras distribuidas tal como servidor de punto de acceso (SRV_AP) y servidor central (SRV_CNTRL) dentro de la GVN.

Los algoritmos analizan continuamente el estado de la red actual mientras tienen en cuenta tendencias finales más rendimiento histórico de largo plazo para determinar la mejor ruta que pueda tomar el tráfico y cual es el mejor SRV_AP o serie de servidores SRV_AP para empujar el tráfico a través. La configuración, camino de comunicación y otros cambios se hacen de manera automática y sobre la marcha con mínima o ninguna interacción de usuario o intervención requerida.

El Enrutamiento Inteligente Avanzado en un EPD y en un SRV_AP asegura que el tráfico fluye a través del camino más ideal desde el origen al destino a través de una “Tercera Capa” tan simple como sea posible de la GVN. Esta tercera capa es vista por los dispositivos clientes conectados a la GVN como un camino de internet normal pero con un número de saltos más bajo, mejor seguridad y en la mayoría de los casos menor latencia que el tráfico que fluye a través de internet ordinario al mismo destino. La lógica y automatización operan en la “segunda capa” de la GVN donde el software de la GVN monitoriza y controla de manera automática el enrutamiento subyacente y construye interfaces virtuales (VIF), múltiples túneles y uniones de caminos de comunicación. La tercera y segunda capas de la GVN existen encima de la “primera capa” operacional de la GVN que interactúa con los dispositivos de la red de Internet subyacente.

La nube dese una perspectiva técnica y de red se refiere a dispositivos o grupos o matrices o agrupaciones de dispositivos que están conectados y están disponibles a otros dispositivos a través de internet abierto. La ubicación física de estos dispositivos no es de importancia significativa ya que a menudo tienen sus datos replicados sobre múltiples ubicaciones con entrega hacia/desde el servidor más cercano hacia/desde el cliente que solicita que usa la red de entrega de contenido (CDN) u otra tecnología para acelerar la conectividad que mejora la experiencia de usuario (UX).

Además del tema más amplio de abordar los problemas de calidad de servicio (QoS) relacionados con la conectividad de red que mejora el rendimiento general y mejora la experiencia de usuario, dos características principales son que una GVN permite la extensión de un borde de red en la nube. De manera adicional, el EPD actúa como un puente entre la red más amplia y una red de área local (LAN) que trae elementos de la nube como una extensión del nodo local en el borde de la LAN. La GVN también permite la construcción automática de interfaces virtuales (VIF) y estructuras de VIF que actúan como puntos de enganche para múltiples túneles. Estas VIF permiten el desplazamiento de operaciones intensivas en tiempo y recursos tales como enrutamiento hacia arriba al VIF que son típicamente aplicados a túneles.

La FIG. 1 ilustra el hinchado de paquete para paquetes de transporte IP cuando se añaden cabeceras a los datos en varias capas. En la Capa de Aplicación 1-L04, la carga de datos tiene un tamaño inicial como se indica por Datos 1-D4. El tamaño del paquete es indicado por Tamaño Paquete 1-PBytes. En la siguiente capa, Capa de Transporte 1-L03, el Tamaño Paquete 1-PBytes tiene el tamaño original de los datos 1-D4 que es igual a Datos UDP 1-D3. Además incluye hinchado de Cabecera UDP 1-H3. En la siguiente capa, Capa de Internet 1-L02 la carga del cuerpo Datos IP 1-D2 es una combinación de 1-D3 y 1-H3. Aumenta 1-PBytes por la Cabecera IP 1-H2. En la Capa de Enlace 1-L01, Datos de Trama 1-D1 es una combinación de 1-H2 y 1-D2. Además aumenta 1-PBytes por la Trama de Cabecera 1-H1 y Trama de Pie 1-F1.

La FIG. 2 ilustra el hinchado de paquete de datos y cabeceras en cada una de las siete capas del modelo OSI. Los datos originales 2-D0 crecen en cada nivel de la Capa 7 OSI de Aplicación 2-L7 con la adición de cabeceras tales como Cabecera 2-H7. En cada capa subsecuente abajo desde la capa 7 a la capa 1, la capa de datos es una combinación de la capa de nivel superior anterior de Datos y Cabecera combinados. El hinchado de paquete total en un modelo OSI en la Capa OSI Física 2-L1 es denotada mediante 2-PBytes de Tamaño de Paquete.

La FIG. 3 muestra un diagrama de bloques que representa la resolución del localizador de recursos universal (URL) a través de la búsqueda en un sistema de nombre de dominio (DNS) de internet para enrutar desde el Equipo (cliente) a la dirección IP numérica del Equipo (servidor). Una solicitud de contenido o empuje desde un cliente (C) 101 de equipo a un servidor (S) 301 de equipo como archivos o flujos o bloques de flujos de datos en la dirección de la flecha 001. La respuesta 002 de entrega de contenido desde el equipo S al equipo C como archivos o flujos o bloques de datos. El dispositivo 101 cliente de equipo en la relación Cliente-Servidor (C – S) hace una solicitud para acceder a contenido desde un equipo S remoto o envía datos a un equipo S remoto a través de un localizador de recursos universal (URL) u otra dirección alcanzable de red.

La conexión desde el cliente de equipo a internet está marcada como P01 – la conexión desde el cliente 101 al POP 102 que se enfrenta directamente o puede ser localizado en una red de área local (LAN) que entones conecta a internet a través de un punto de presencia (POP) puede ser referida como la conexión de última milla. El punto de presencia (POP) 102 que representa la conexión proporcionada desde un punto extremo por un proveedor de servicio de internet (ISP) a internet a través de su red y sus interconexiones. Si el URL es un nombre de dominio más que una dirección numérica, entones este URL es enviado a un servidor 103 de sistema de nombre de dominio (DNS) donde el nombre del dominio es traducido a una IPv4 o IPv6 u otra dirección con propósito de enrutamiento.

El tráfico desde el cliente 101 al servidor 301 es enrutado a través de Internet 120 que representa el tránsito entre POP (102 y 302) que incluye pares, red de retorno, u otros tránsitos de red de frontera.

La conexión P02 desde POP 102 al DNS 103 para ubicar una dirección numérica desde un localizador de recursos universal (URL) para obtener la dirección IPv4 u otra dirección numérica del servidor objetivo puede ser directamente accedida desde el POP 102, o a través de Internet 120. La conexión P03 desde el POP 102 de un ISP a Internet 120 puede ser única o múltiple. Hay una conexión P04 desde Internet 120 al POP 302 enfrentado a internet del ISP o del centro de datos de internet (IDC). La conexión P05 desde el POP 302 del servidor al equipo 301 puede ser directa o a través de múltiples saltos.

Las búsquedas desde nombre a dirección numérica a través de sistemas de nombres de dominios es un estándar en Internet hoy y asume que el servidor de DNS es íntegro y que sus resultados son actuales y son de confianza.

La FIG. 4 ilustra una ecuación para calcular producto de retraso de ancho de banda (BDP) para un segmento de conexión o camino que tiene en cuenta varios atributos de conectividad. A mayor distancia entre dos puntos y/o otros factores que aumentan la latencia impacta la cantidad de datos que la línea puede absorber de manera ciega antes de que el dispositivo emisor reciba un mensaje de vuelta desde el dispositivo receptor sobre si fue capaz de aceptar o no el volumen de datos.

En breve, el cálculo de BDP puede representar una medida de cuántos datos pueden llenar una tubería antes de que el servidor sepa que está enviado demasiado a una tasa demasiado rápida.

El Ancho de Banda 4-000 puede ser medido en megabits por segundo (Mbps) y la Granularidad 4-002 puede ser la unidad de tiempo relativa a un segundo. Para reflejar de manera precisa BDP, los Bytes 4-020 son divididos por el número de Bits 4-022 de un sistema. La Latencia 4-050 es una medición del tiempo de ida y vuelta (RTT) en milisegundos (ms) entre los dos puntos.

Así por ejemplo, BDP del siguiente camino de red con estos atributos – Ancho de Banda 4-000 de 10 GigE que usa Granularidad 4-022 de un segundo, en un sistema de ocho bits sobre un camino con Latencia 4-050 de 220 ms – puede calcularse como sigue:

$$\frac{10{,}000{,}000{,}000}{1} * \frac{1}{8} * 0.220 = 275{,}000{,}000\ bits\ \ O\ \ \ 33{,}569.3\ MB$$

Por lo tanto en una línea de 10 GigE, el dispositivo emisor podría teóricamente enviar 33.569,3 megabytes de información (MB) en los 220 ms antes de que un mensaje pueda ser recibido de vuelta desde el dispositivo de cliente receptor.

Este cálculo puede también ser la base de otros algoritmos tales como uno para gobernar el tamaño de una memoria intermedia RAM, o uno para gobernar el tiempo y la cantidad de datos que son almacenados en una memoria intermedia antes de que se de cuenta de un problema tal como un vector de ataque. El estrangulamiento por el servidor de equipo podría llevar a tuberías infrautilizadas pero la aceptación de demasiados datos puede también llevar a otros problemas. El cálculo de BDP y enfoque de gestión proactiva a problemas lleva a un uso eficiente de recursos hardware y de red.

La FIG. 5 ilustra el camino de flujo del tráfico dentro de un dispositivo de punto extremo (EPD). El tráfico fluye entre la LAN 5-000 y el dispositivo de punto extremo (EPD) 5-100 sobre la conexión 5-CP00. El dispositivo de punto extremo (EPD) 5-100 fluye al punto de presencia (POP) 5-010 sobre la conexión 5-CP06. El punto de presencia (POP) 5-010 está conectado a Internet 5-020 a través de la conexión 5-CP08.

La FIG. 6 ilustra un túnel encima de todo (OTT) creado encima de una conexión de internet ordinaria. La FIG. 6 es similar a la FIG. 5 y de manera adicional muestra un servidor de punto de acceso (SRV_AP) 6-300. El servidor de punto de acceso (SRV_AP) 6-300 incluye un oyente de túnel TNL0 6-380. El dispositivo de punto extremo (EPD) 5-100 incluye un gestor de túneles TMN0 6-180. Un túnel TUN0 6-CP80 es construido que conecta el gestor de túneles TMN0 6-180 y el oyente de túneles TNL0 6-380. El túnel es construido encima de todo (OTT) de la conexión de internet ordinaria 6-CP06 y 6-CP08.

La FIG. 7 ilustra una interfaz virtual para túneles encima de todo (OTT) creados encima de una conexión de internet ordinaria. La FIG. 7 es similar a la FIG. 6 y de manera adicional incluye una interfaz virtual (VIF) como un punto de enganche en cada dispositivo EPD 7-100 y SRV_AP 7-300 para múltiples túneles a ser construidos entre dos. Esta figura también muestra múltiples túneles 7-CP80, 7-CP82, y 7-CP84 entre EPD 7-100 y SRV_AP 7-300. Una ventaja principal de la interfaz virtual VIF0 7-170 y VIF0 7-370 en cada dispositivo respectivamente es que este enfoque permite atributos de estructura limpios y un camino lógico para construcciones más complejas de túneles y subsecuente complejidad de enrutamiento.

Ciertas otras ventajas con respecto a la temporización y control de flujo serán descritas en figuras subsecuentes a continuación.

La FIG. 8 es un diagrama de flujo que describe cómo determinar el mejor punto de ingreso egreso (EIP) para que el tráfico fluya a través de una red virtual global (GVN) a internet. Algunas rutas de ejemplo desde un origen (SRC) a un destino (DST) a través de la GVN se muestran en la Tabla 1.

Tabla #1 – Rutas de ejemplo a través de una GVN

RT_ID	Camino desde Origen a Destino	Clasificación
1	Fuente ↔EPD EIP ↔POP↔Internet↔Destino	0.15
2	Fuente ↔EPD↔TUN1↔SRV_AP1 EIP ↔POP↔Internet↔ Destino	0.36
3	Fuente ↔EPD↔TUN2↔SRV_AP2 EIP ↔POP↔Internet↔ Destino	0.58
4	Fuente ↔EPD↔TUN2↔SRV_AP2↔SRV_AP3 EIP ↔POP↔ Internet↔ Destino	0.96
5	Fuente ↔EPD↔TUN3↔SRV_AP2↔WAN↔SRV_AP4 EIP ↔POP↔ Internet↔ Destino	0.85

EPD EIP y SRV_AP2 EIP denotan Puntos de Ingreso / Egreso (EIP) desde un dispositivo hacia/desde internet. El símbolo de flecha ←→ de dos lados indica el camino enrutado entre dos dispositivos. Esto puede ser bien directamente a través de internet, como un segmento de red OTT de internet como un túnel u otro mecanismo (posiblemente como parte de una GVN) o a través de otro camino de red entre dispositivos. El punto de origen está en la izquierda y el destino implica la ubicación final donde el tráfico ha de ser enrutado hacia/desde. Los caminos a través de la GVN podrían ser estructurados como una matriz multi dimensional u otro patrón de datos para denotar el camino extremo a extremo que toma el tráfico dentro de la GVN.

La clasificación es un valor calculado para una ruta basada en varios factores. Una clasificación de 0,00 implica una ruta imposible. Una clasificación de 1,00 implica la ruta más perfecta con el ancho de banda más grande en latencia de velocidad de línea cableada. RT_ID es el número de ID de la ruta para diferenciar una ruta de otra tanto para propósito de utilidad, pruebas y registro. Esto es usado para determinar la calidad de varias rutas a través de la GVN. RT_ID es una identificación para una ruta específica de una lista de rutas. La calidad de servicio (QoS) para cada ruta puede incluir evaluar seguridad, latencia, pérdida de paquetes, fluctuación, ancho de banda, y otros factores.

La evaluación de varias medidas debería tener en cuenta el camino total:

Camino Total = GVN a Egreso + Egreso a destino

Mientras se evalúa el camino total, el peso de prioridad en favor de la GVN sobre internet abierto tiene en cuenta la seguridad y optimización de la GVN para sustituir ciertas medidas.

La FIG. 9 ilustra el esfuerzo colaborativo entre varios módulos, mecanismos, tecnologías y otros componentes de la GVN.

Hay tres capas de la GVN – la capa uno es la capa de red física tal como internet en el cual la GVN es construida encima de todo (OTT). La capa tres es la capa de red de la GVN que el dispositivo de cliente ve como un camino parcial o completo al destino. La capa dos es la capa lógica entre las dos.

Hay componentes que interactúan con las condiciones 9-00 físicas. Módulos de construcción dinámica en 9-20 se esfuerzan por mantener la conectividad de la GVN. La sección de esfuerzo conjunto descrita en este documento enlaza los módulos relevantes de la GVN a elementos físicos 9-00 y dinámicos 9-20. Por ejemplo, para que el módulo G106 de enrutamiento inteligente avanzado (ASR) funcione adecuadamente, debe haber múltiples servidores (SRV_AP) GP106 de punto de acceso emplazados en varias ubicaciones, con enrutamiento adecuado y pares GR106. Para que un EPD sea capaz de seleccionar el SRV_AP más apropiado con el que establecer una conexión, necesita

información sobre qué SRV_AP son mejores. El módulo SA106 de disponibilidad de servidor ASR clasifica servidores para ese EPD específico en base a la información proporcionada por el gestor TM106 de pruebas de ASR y cuando un EPD solicita que se establezca un nuevo túnel, usa la lista SA106 de disponibilidad de servidores para construir un nuevo túnel. Las pruebas son ejecutadas entonces en ese túnel a través de TM106.

Como otro ejemplo, para operar el NAPIM G102 necesita oyentes de API y gestores HL102 en un servidor de equipo. Tanto en el cliente de equipo como en el servidor de equipo en el NAPIM, un gestor OM102 de operaciones se ejecuta para manejar la preparación, entonces enviar, manejar, procesador solicitudes y respuestas de API. La construcción dinámica del NAPIM supone un gestor PM102 par, gestor de acciones AM102 del NAPIM relacionadas, las transacciones en física TP102 y dinámica TM102.

La FIG. 10 ilustra las operaciones de capa 1, capa 2, y capa 3 de una red virtual global (GVN) y compara la red en el nivel base a través de los caminos P01 hasta P13 a la red a través de la GVN T01 hasta T03.

Mediciones significativas en el nivel CTN140 de internet base son LAN hasta GVN a través de EPD 10-100 hasta SRV_AP 10-300 para la cual las métricas de conectividad para el ancho de banda BW, latencia Δt = A ms, Pérdida de Paquetes, y otros factores son evaluados. En el otro extremo de la conexión, mediciones similares BW, Δt = C ms, Pérdida de Paquetes y otros factores en CTN142 miden la subida de tráfico en la GVN desde EPD 10-102. A través de la GVN entre SRV_AP 10-300 y SRV_AP 10-302 para GVN trans-regional OTT varios segmentos CTN340 de internet miden BW, Δt = B ms, Pérdida de Paquetes, y otros factores son evaluados. La latencia del camino total a través de la Capa Tres GVN10-3 del GVN puede ser calculada como la suma de las latencias de A + B + C para el total en milisegundos.

En la Capa Tres GVN10-3 de la GVN, ASR y otras características gobiernan cómo y dónde el tráfico fluye a través de la GVN. Esto supone determinar el mejor túnel por el que enviar el tráfico en base a la región objetivo y tipo de tráfico, QoS de los segmentos a través de la GVN y otros factores.

En la Capa Uno GVN10-1 de la GVN, las condiciones físicas de la conectividad de red base son monitorizadas y probadas para determinar las mejores opciones de ruta encima de las cuales construir túneles de GVN y caminos a través de ellos. Los caminos de GVN pueden transitar a través de túneles unidos que pasan a través del SRV_AP, SRV_BBX y otros dispositivos de hardware de la GVN. Esto también puede determinar qué túneles hacer, continuar usando y cuales rechazar.

Los mecanismos, módulos y partes de componentes en la Capa Dos GVN10-2 de la GVN ayudan a establecer, probar, gestionar y de otro modo operar la fontanería entre la Capa Tres GVN10-3 y la Capa Uno GVN10-1 de la GVN. La prueba del túnel se puede hacer en la Capa Tres en el EPD 10-100 y en el SRV_AP 10-300 a través de su probador 10-312 de túneles.

La FIG. 11 es un diagrama de flujo de Enrutamiento Inteligente Avanzado (ASR) dentro de una red virtual global (GVN). Desde el punto inicial de un dispositivo de cliente 101 de equipo en una red de área local (LAN) 102 conectada a un dispositivo de punto extremo (EPD) 103, la GVN ofrece al EPD una multitud de caminos de conexión a múltiples puntos de terminación potenciales. Este diagrama de flujo es una vista de alto nivel de la lógica de enrutamiento que un paquete podría tomar al transitar una GVN que usa ASR para rendimiento óptimo. Desde la perspectiva del cliente 101 de equipo, su tráfico fluirá a través de una red de protocolo de internet (IP) con tan pocos saltos y mejor latencia posible en la tercera capa de la GVN. La primera capa de la GVN es la internet base con configuración automática de una construcción de interfaces virtuales, túneles, enrutamiento y otras políticas de red. La segunda capa de la GVN es donde los algoritmos, software y lógica gobiernan la operación entre la capa tres y la capa uno.

La primera decisión principal de enrutamiento es una puerta 104 lógica dentro del EPOD donde el tráfico bien egresa a Internet 107 local donde el EPD está ubicado a través del camino P104 o si es para ir a través de un túnel ofuscado y envuelto seguro a través de P107 al servidor de punto de acceso (SRV_AP) 110 que ofrece la mejor conectividad a la región donde SRV_AP 110 está ubicado. Antes de que el tráfico egrese SRV_AP 110, pasa a través de una puerta 111 lógica de enrutamiento. El tráfico por egresar localmente a internet 113 irá a través del camino P111 bien a un cliente 115 de equipo o un servidor 116 de equipo allí. Si el tráfico no es local sino que será reenviado a otra región, irá a través del camino P116 a través de un túnel 118 al siguiente SRV_AP 119.

En SRV_AP 119, tres de muchas posibles opciones de enrutamiento son ilustradas por los caminos que puede tomar el tráfico. Hay una puerta 126 lógica para determinar si el tráfico debería permanecer y egresar a internet 129 local o si debería ir a través de un túnel a través de P126 a un SRV_AP en otra región 127. Otra posibilidad es ilustrada a través del camino P119 que demuestra un túnel desde SRV_AP 119 a otro EPD 121 en una región distante. Esto es un EPD 103 a EPD 121 puenteado a través de múltiples túneles de puente. Otra posibilidad es que el tráfico alcance los dispositivos 125 126 de cliente en la LAN 122 donde el EPD 121 está ubicado a través de la conexión P121 del EPD.

La FIG. 12 es un diagrama de flujo de las varias rutas disponibles a través de una GVN desde un origen C 12-002 a un destino S12-502. Pueden haber muchas más combinaciones posibles que no son mostradas o discutidas.

El camino 12-CP00 desde el Origen A Cliente C 12-002 al EPD 12-108 puede ser usado para medir el rendimiento desde el cliente a través de la LAN al EPD. La correspondencia de las mejores rutas es lograda después de pruebas y evaluaciones de datos en tiempo real de caminos disponibles. La GVN ingresa desde el EPD a través de un primer salto 12-CP00 para acceder un servidor de punto de acceso (SRV_AP) 12-102, 12-104, 12-106, 12-202, 12-204.

Los caminos desde el EPD al primer SRV_AP pueden definirse como el punto de ingreso desde el EPD en la GVN y medidos en consecuencia. Los saltos internos desde SRV_AP a SRV_AP siguen rutas internas que siempre tratan de mantener la mejor conectividad de camino. Estos podrían ser OTT internet, sobre red troncal, sobre fibra oscura, u otros enrutamientos relacionados.

También se hace seguimiento de los mejores puntos de egreso fuera de la GVN de manera local, en esa región remota y también holísticamente para el segmento de red completo desde el origen al destino.

Las pruebas se pueden ejecutar en cada segmento, combinaciones de segmentos, y el camino de red total de inicio a fin teniendo en cuenta varios factores a evaluar. El tipo de tráfico y determinación del camino pueden ser dependientes de atributos de datos y requisitos de la QoS del perfil. La elección del camino principal siempre se basa en los mejores factores para el tráfico sobre el camino. Una función de este mecanismo es hacer coincidir caminos entre destino y origen para fluir por la mejor ruta bidireccional posible. El tráfico para el destino objetivo fluye a través del punto de ingreso egreso (EIP) más ideal para ese destino específico.

Varias tablas de bases de datos pueden ser mantenidas para soportar y gobernar gestión de rutas en el mecanismo de enrutamiento inteligente avanzado:

· Una tabla “Direcciones IP en esta región” es un registro de direcciones IP para mantener locales y de egreso a internet 12-122 local a través del EIP local 12-120.

· Una tabla “Objetivos Geo-D y varios EIP” traza un camino a través de la GVN al EIP 12-320 12-322 12-324 12-326 12-328 más apropiado en una región remota para alcanzar destinos 12-512 12-522 12-532 a través de internet en regiones 12-510 12-520 12-530 remotas.

· Una tabla “Bloques IP de País para enrutamiento regional” puede ser usada para enrutar en base a las direcciones IP en varias regiones y/o países u otra granularidad de ubicación.

· Una “Lista de Disponibilidad_Servidor” puede ser compilada para cada dispositivo a través de análisis algorítmico de varios factores que incluyen mejores servidores para que ese dispositivo use así como en el estado actual y condición de los varios servidores potenciales que podría usar. Los factores de carga relacionados con la capacidad, enrutamiento, condiciones del segmento de red, y otros problemas que podrían impactar las operaciones son tomados en cuenta cuando se asignan servidores y se listan en una lista de disponibilidad de servidores creada para un dispositivo específico.

· Una tabla “Registro de Túneles” puede ser usada para hacer seguimiento de los múltiples túneles entre pares.

· “Rutas de la GVN” puede ser usada para listar el enrutamiento para extremo a extremo disponible o caminos parciales para tráfico para llevar a través de la GVN desde un punto a otro punto.

La información anterior es descrita como almacenada en tablas de bases de datos como un ejemplo de almacenamiento para asistir en esta descripción. Se podría almacenar también como listas en archivos planos, en memoria o en disco, o en varios otros formatos. Alguna o toda la información de enrutamiento puede ser usada para determinar la mejor ruta que tome el tráfico mediante la coincidencia del destino al EIP a través del mejor camino.

La FIG. 13 ilustra la unión de varios segmentos de red diferentes en un camino extremo a extremo. Por ejemplo desde el Cliente 13-000 al Servidor 13-300, el tráfico transita a través de una red de área local (LAN) 13-010 a un dispositivo de punto extremo (EPD) 13-100 a una red de proveedor de servicio de internet (ISP) 13-200 a una red troncal 13-220 a internet 13-250 en una región remota a un centro de datos de internet (IDC) punto de presencia (POP) 13-320 en la red interna del IDC 13-310 y entonces al servidor 13-200.

Como se muestra en este ejemplo, es importante comprender las características de cada segmento y cómo ese segmento impacta el flujo de tráfico con respecto al camino extremo a extremo completo. Una red interna o LAN 13-N100 normalmente tendrá una razonable cantidad de ancho de banda (BW) para uso interno tal como BW 13-B100 que es 10 GigE en tamaño. El ancho de banda para una red 13-N202 de un ISP también normalmente será razonablemente grande como se ejemplifica por el BW 13-B202 de 40 GigE. Entra estas dos redes, una conexión 13-N200 de última milla entre la ubicación del cliente y el ISP es un BW 13-B200 relativamente pequeño de 100 Mbps. Hay numerosos impulsores detrás de esto pero el principal es el coste. Un ISP llevará una tubería a un vecindario de un ancho de banda de un cierto tamaño y entonces normalmente compartirá esta cantidad con muchos usuarios diferentes a cada una de sus conexiones de última milla. Estos caminos hacia arriba son los segmentos iniciales hacia internet general más amplio y ancho.

Una red troncal 13-N220 conecta los ISP entre sí, regiones con regiones, y más y las redes troncales ofrecen conectividad de ancho de banda alta y muy profunda tal como 13-B220 de 100 GigE. Esto podría representar la capacidad de portadora de una hebra de fibra entre dos puntos, y/o el tamaño de la clasificación de capacidad de conmutación u otros factores.

Internet 13-N250 en esta figura es representado por tuberías duales de BW 13-B250 y 13-B252 cada una de 40GigE. Este es un ejemplo de una conectividad múltiple en una internet. Pueden haber muchas otras tuberías grandes en el núcleo de una internet conectadas juntas.

El pareado 13-N320 del ISP entre internet 13-N250 y una red 13-N310 IDC es representado de nuevo como conectividad múltiple BW de 10 GigE cada para 13-B320, 13-B322, y 13-B328. Esto representa la última milla dedicada para ese centro de datos. Pueden haber muchos más enlaces de comunicación para un IDC.

La red 13-N310 IDC interna normalmente tendrá un BW 13-B310 muy grande distribuido entre varias redes internas que cada una está clasificada a una cierta velocidad como 100 GigE. La notación 2 * 100 GigE representa que esta es una red dos veces 100 GigE BW.

La FIG. 14 ilustra un salto entre dos segmentos de red. El salto 14-H020 a través del Dispositivo B 14-020 es una conexión entre dos segmentos 14-1020 y 14-2030 de red que son caminos hacia el Dispositivo A 14-010 y Dispositivo C 14-030 respectivamente.

Hay varios factores que influyen el flujo del tráfico a través de un salto que incluye el ancho de banda de dos segmentos de red, la capacidad física para portar tráfico a través del Dispositivo B 14-020, el nivel actual de tráfico que fluye a través de él y la congestión correspondiente, y otros factores.

La FIG. 15 ilustra problemas potenciales que pueden ocurrir dentro de un dispositivo 15-020 en un salto entre dos segmentos P1020 y P2030 de red. Un problema 15-Problema 400 tal como problemas 15-PR400 de enrutamiento puede añadir demasiados saltos a un camino, y/o aumentar la latencia debido a caminos tortuosos. Hay otros problemas 15-Problema406 de enrutamiento tal como un extremo muerto en un salto 15-PR406 posterior que puede influir por qué segmento ese tráfico debería fluir si hay una opción tras un salto.

Otro problema 15-Problema 402 tal como filtrado 15-PR402 en el Dispositivo 15-020 podría ralentizar de manera significativa el tráfico que transita a través del salto 15-H020. Algunos tipos de filtrado pueden bloquear un tipo de tráfico completamente u operaciones de cortafuegos tal como una inspección de paquetes profunda (DPI) requieren tiempo y recursos que se añaden a la latencia a través de un salto.

Problemas 15-Problema404 relacionados 15-PR404 con la congestión tienen que ver con el volumen de tráfico como medido por el ancho de banda o podrían también estar relacionados con el problema de demasiadas conexiones concurrentes establecidas por varios flujos de datos a través del salto 15-H020, una combinación de ambas, y/o otros factores.

Otro problema 15-Problema408 tal como mal función 15-PR408 del dispositivo puede causar ralentizaciones impredecibles y perjudiciales en el tráfico a través del salto 15-H020.

Problemas 15-Problema410 tal como problemas 15-PR410 relacionados con BDP ocurren cuando un segmento es más grande que otro segmento. Si el tráfico de entrada desde el segmento más grande entra en el Dispositivo 15-020 el segmento más corto no puede aceptar la totalidad del volumen. El dispositivo puede tratar de almacenar en la memoria intermedia el exceso de tráfico en RAM para ser enviado cuando el flujo de datos disminuya. Si la RAM u otra memoria intermedia se llena completamente, el resultado será pérdida de paquetes.

Pueden haber también otros problemas 15-Problema412 que tienen un impacto directo en la eficiencia del flujo de tráfico a través de un salto, sin embargo esos pueden ser problemas 15-PR412 desconocidos y como tal el único remedio viable puede ser enrutar el tráfico alrededor de ese salto.

Otros problemas pueden ser posibles y ocurrir a través de un salto. El punto clave es que el resultado de los problemas a través de un salto son alta latencia, pérdida de paquetes, ancho de banda restringido y otros efectos que afectan de manera adversa el flujo de tráfico. Una consecuencia de la pérdida de paquetes a través de un salto es el resultado perverso de los dispositivos emisores reenviando paquetes tirados que puede causar un efecto cascada debido a aun más paquetes intentando pasar a través de un salto ya sobresaturado.

La FIG. 16 ilustra el ciclo de vida de un túnel entre un dispositivo de cliente iniciador y un dispositivo servidor oyente para construir un túnel entre los dos. Los términos cliente y servidor son usados con propósitos descriptivos y pueden reflejar los roles de los dispositivos descritos o los dispositivos pueden existir dentro de una relación par a par (p2p) con un par que se comporta como un cliente y el otro par que se comporta como un servidor.

Los pasos del proceso 16-000 de establecimiento del túnel desde el Estado de túnel: Abajo 16-200 hasta el Estado de Túnel: Arriba 16-202. Se comienza con el primer paso Iniciar Construcción Túnel 16-100. Preparar Info Túnel 16-102 comienza con el dispositivo de cliente recogiendo información sobre el servidor hacia el cual desea construir un túnel.

Si existe una relación de pares, y si la información es actual, entonces el dispositivo de cliente usará esa información. Si no existe una relación de pares, o si no hay información del túnel que podría ser usada por los dispositivos para construir un túnel entre ellos, o si la info de relación de par o info de túnel están pasadas, entonces una llamada de una API a un SRV_CNTRL (por ejemplo SRV_CNTRL 17-200 en la FIG. 17) puede ser usada por cada dispositivo para recoger información de par y túnel relevante.

El siguiente paso, Apretón de manos seguro C con S 16-104, es iniciado por el cliente con llamada al servidor. La comprobación del servidor inicial puede validar una huella dactilar e identificadores del cliente pueden verificar que está autorizado a interactuar con el servidor. Un apretón de manos TLS puede ser usado para que cada dispositivo diga al otro quien es e intercambiar claves para usar para crear una conexión encriptada entre ellos de forma que puedan hablar entre sí. Durante el establecimiento de un túnel ordinario, existe el riesgo de que el túnel pueda ser olisqueado e interferido mediante la inyección deliberada de un paquete de restablecimiento de TCP_RST enviado para romper el flujo de tráfico entre los dos pares del túnel.

El siguiente paso, Intercambio de Info C←→S 16-106, incluye información específica a la construcción del túnel, que incluye credenciales, claves, parámetros de red, ajustes de configuración, y otra información. Los ajustes entre ambos lados deben coincidir o pueden haber problemas con la construcción del túnel.

El siguiente paso, Construye túnel + encripta 16-108, usará la información sobre el túnel para construir el túnel encriptado y para prepararlo para enviar tráfico. El tráfico empieza a fluir aquí.

El siguiente paso, Aplica enrutamiento + gancho 16-110, es donde las rutas son aplicadas al túnel que determina qué tráfico debería ir a través del tráfico y qué tráfico debería quedarse dentro del dispositivo de cliente para ser manejado por la siguiente interfaz interna allí.

El siguiente paso, Aplica – Acciones Arriba 16-112, puede incluir desencadenante para ejecutar guiones, subrutinas, u otras acciones para registrar eventos del túnel en una base de datos, para comprobar rutas, o hacer otras tareas de mantenimiento tal como pruebas, aplicación de rutas, y si el reenvío IP es requerido establecerlo de manera automática, o realizar otras acciones.

En un cierto punto después de que el túnel sea construido en el paso Construye túnel + encripta 16-108, el túnel está listo y dispuesto para llevar tráfico.

Dependiendo del tamaño y complejidad de la tabla de enrutamiento aplicada en el paso Aplica enrutamiento + gancho 16-110, una cantidad relativamente significativa de tiempo puede pasar entre el inicio y el final de la construcción de la ruta.

Dado que el tráfico puede ya estar fluyendo a través del túnel durante la construcción de la ruta, un comportamiento impredecible, sistémico que afecte al flujo de tráfico puede ocurrir. Algún tráfico puede ir a través del túnel mientras que otro tráfico puede no ir a través. La fuga es por lo tanto una consecuencia no deseada de este periodo de tiempo durante la construcción de la ruta que lleva a problemas de seguridad potenciales, potencial para paquetes perdidos en un flujo, así como otros problemas. Por ejemplo el dispositivo de equipo recíproco en un flujo puede confundirse en donde enviar el tráfico de vuelta dado que el inicio del flujo estaba fluyendo desde una dirección IP de borde en el primer dispositivo que de repente cambió a la dirección IP del borde del dispositivo servidor una vez que el túnel se levantó.

Cuando un túnel se cae, de repente deja de enviar todo el tráfico fuera del túnel y el tráfico de entrada al túnel no puede encontrar el punto extremo del túnel que ya no existe y un nuevo proceso de construcción del túnel tiene que esperar a la limpieza de rutas y que el proceso 16-040 de destrucción de túnel del primer túnel se complete. Además, el resultado final es un problema de brechas en las protecciones ofrecidas por el túnel así como enrutamiento inestable que lleva a conexiones rotas. El nuevo túnel necesita tiempo para construirse antes de que pueda estar listo para llevar tráfico de manera confiable.

El Proceso de Destrucción de Túnel 16-040 describe los pasos en orden desde Estado de Túnel: Arriba 16-202 de vuelta a Estado de Túnel: Abajo 16-200. Las causas para que un túnel se rompa puede ser una orden de parada intencionada o una parada no limpia no intencionada debida a una conexión subyacente rota, una conexión pobre con latencia demasiado alta o demasiada pérdida de paquetes, o si no hay suficientes recursos del sistema para mantener el túnel, u otra razón o razones.

El paso Aplica – Acciones abajo 16-142 ejecuta guiones tales como captura de archivos de registros temporales y guarda sus datos en tablas de bases de datos, en archivos de registro, u otros formatos o almacenamiento permanente. Una entrada en un registro de base de datos puede notar el evento de túnel caído. Este paso puede también comunicarse a través de API con gestores ASR y gestores de túneles para notificar el cambio de estado del túnel. Cada dispositivo puede tomar acciones de manera independiente o en colaboración con otros dispositivos según la necesidad.

El siguiente paso, Aplica cambios de enrutamiento 16-144, elimina rutas del túnel así como elimina entradas de ruta de la entrada del túnel y de la salida. Hasta que las rutas son limpiadas, entonces el tráfico puede ser efectivamente

bloqueado como si el túnel ya no estuviera arriba pero el tráfico se enrutara hacia él, entonces el tráfico no tiene a donde ir. Una vez que las rutas son eliminadas, el tráfico puede fluir alrededor del viejo túnel.

Los pasos de caía 16-146 ordenada y liberación de recursos 16-148 completan la eliminación del túnel.

La FIG. 17 ilustra la relación e interacciones entre un dispositivo de punto extremo (EPD) 17-100, un servidor de control central (SRV_CNTRL) 17-200, y un servidor de punto de acceso (SRV_AP) 17-300 cuando se construye un túnel TUN0 17-CP80 entre el EPD 17-100 y el SRV_AP 17-300.

Los pasos para construir TUN0 17-CP80 incluyen 17-S1 Apretón de Manos, 17-S2 Intercambio de Info, y Construcción de Túnel 17-S3. Para que el Gestor (Constructor) 17-D110 de Túneles en EPD 17-100 construya el TUN0 17-CP80, necesita cierta información sobre el SRV_AP 17-300 que puede conectar para la construcción del túnel, información sobre el túnel, y más. Para que el Gestor (Oyente) 17-D310 de Túneles en SRV_AP 17-300 acepte el apretón de manos 17-S1 desde el Gestor (Constructor) 17-D110 de Túneles de EPD 17-100, para negociar el intercambio 17-S2 de información, y entonces para construir el túnel 17-S3, también requiere información similar. Por ejemplo, la asignación de puerto y dirección IP en SRV_AP 17-300 debería ser única para evitar conflictos. Además, los certificados, credenciales tales como una contraseña, e información de soporte para características del túnel avanzadas tal como envolver y/o tapar también necesitan ser conocidas por ambos pares cuando se construye el túnel.

Para información cambiante de manera dinámica y no estable usada para la construcción del túnel, un dispositivo de cliente tal como un dispositivo (EPD) 17-100 de punto extremo necesitará compartir info con un servidor tal como un servidor (SRV_AP) 17-300 de punto de acceso antes de que el Gestor (Constructor) 17-D110 de Túneles sea capaz de interactuar con el Gestor (Oyente) 17-D310 de Túneles en un SRV_AP 17-300.

La seguridad del túnel implica no solo los aspectos y atributos del túnel actual mientras que esté arriba sino que también cubre varias etapas durante un ciclo de vida del túnel. Existe una necesidad de compartir y proteger claves, credenciales, configuración, y otros ajustes. Mediante la colaboración de cada dispositivo con un SRV_CNTRL 17-200 para compartir información pertinente con los otros, esto puede proteger el envío, generación, publicación, actualización, y más manejo de la información. El apretón de manos e intercambio de claves puede protegerse a través de la encriptación y también a través de conexiones tapadas. Mientras esté arriba, el túnel puede ser protegido por la encriptación y también ofuscación a través de una tapa.

La FIG. 18 ilustra la organización lógica de interfaces e interfaces virtuales dentro de un dispositivo de punto extremo (EPD) 18-100 para soportar múltiples túneles. Las interfaces ETH0 18-102, ETH1 18-016, y ETH2 18-108 están directamente unidas a las tarjetas de interfaces de red (NIC) físicas del EPD 18-100. En este ejemplo, ETH0 18-102 está conectado a una conexión de enlace ascendente de última milla a internet 18-010 local a través de los caminos 18-P400 a los POP 18-400 y 18-P010 del ISP a internet.

La FIG. 19 es un diagrama de flujo que describe la lógica de algoritmos que potencian el enrutamiento inteligente avanzado (ASR) dentro de una red virtual global (GVN). El primer proceso es Identifica la región objetivo 19-100 con sus correspondientes subprocesos de identifica región 19-110 e identifica EIP potenciales para usar 19-120. Esto establece los procesos subsecuentes para centrarse en un punto de ingreso egreso (EIP) objetivo para usar.

El siguiente proceso, Dibuja opciones de ruta (ASR) 19-200, usa subprocesos de lista 19-210 de disponibilidad de servidores y lista de rutas clasificadas 19-220 para determinar el servidor o servidores óptimos con los cuales construir túneles si no existen.

El siguiente proceso, Examina segmentos de red 19-300, usa subprocesos de medida de segmentos 19-310 y estadísticas de red por camino 19-320 para evaluar la viabilidad de un camino a ser usado para enviar el tipo de tráfico requerido. Por ejemplo para datos de tamaño muy pequeño que requieren el camino más rápido, entonces la distancia más corta y menor latencia es lo más importante y bajo ancho de banda puede ser tolerado. Por el contrario para datos de tamaño enorme que no son sensibles al tiempo en términos de entrega del primer bit, el camino que ofrece el ancho de banda más alto es optimo porque aunque el primer bit entregado sea más lento que por el otro camino, la llegada del último bit se espera que ocurra más pronto debido al mayor ancho de banda.

El siguiente proceso, Comprueba estado de ruta 19-600, usa subprocesos Compara rutas 19-610 y Prueba: está completo el camino total 19-620 para asegurar la capacidad de entrega de los datos siguiendo ese camino.

El último proceso, Dibuja mejor ruta para tráfico 19-700, usa los subprocesos sub-algo: ¿cuál es el mejor camino? 19-710 y ¿Es este camino el mejor para el tipo de tráfico? 19-720 para determinar y establecer la mejor ruta extremo a extremo.

Cada proceso y subproceso son usados para asegurar que cada tipo de tráfico es llevado de la manera más optima por el túnel más adecuado para ese tipo de tráfico.

La FIG. 20 ilustra la funcionalidad de una interfaz virtual VIF1 20-110 con un camino de tráfico y las ventajas que ofrece. Donde la FIG. 18 ilustraba la virtud lógica de VIF como puntos de enganche para múltiples túneles a varias

regiones, esta figura describe además un enfoque práctico para organizar no solo las interfaces sino también los varios túneles activos y agrupaciones de túneles mediante los tipos de evento de ciclo de vida del túnel. Los principales tipos de eventos de ciclo de vida de túnel son: Obsoleto, Activo, En construcción, En Espera.

Los túneles obsoletos a ser destruidos 20-340 ordenadamente es donde los túneles que han sido construidos y bien usados o no usados y ya no serán usados más, son destruidos.

Los túneles activos con tráfico 20-300 enrutado es donde los túneles están arriba y conectados, capaces de empujar tráfico a uno o más servidores de punto de acceso (SRV_AP). Una ventaja clave de tener múltiples túneles activos conectados a una VIF es que una conmutación instantánea de tráfico desde un túnel a otro túnel puede hacerse sin ninguna pérdida o fuga de datos.

Los túneles en construcción 20-310 es donde nuevos túneles están siendo construidos entre el EPD 20-100 y un SRV_AP.

Los túneles en espera listos para el uso 20-320 es donde túneles construidos están arriba y funcionales entre EPD 20-100 y un SRV_AP, pero no están en un estado de producción de manejo activo de tráfico. En los túneles en modo de espera se ejecutan pruebas periódicas para evaluar su viabilidad y su estado operacional. También se mantienen viables mediante pings o envío regular de tráfico de mantener vivo.

El ciclo de vida de túneles unidos a la VIF es que nuevos túneles son construidos según necesidad, estos nuevos túneles son puestos en espera y probados. Cuando un túnel activo experimenta un problema y necesita ser rechazado y destruido, un túnel en espera puede ser activado para reemplazarlo. Túneles obsoletos son destruidos en una forma ordenada que libera recursos para usen nuevos túneles futuros.

La FIG. 21 es un diagrama de flujo que describe el algoritmo que gobierna cuando el flujo de tráfico debería ser conmutado desde un túnel a otro túnel. Esto asume que en algún punto, el túnel fue viable. El paso túnel arriba y empuje de datos 21-100 es seguido por un punto de unión 21-102 a Pruebas de Túnel 21-220. La Monitorización del Túnel 21-200 es seguida por una comprobación ¿es TUN óptimo? 21-300. Si es óptimo, el camino Sí 21-CP302 lleva de vuelta al punto de unión 21-102.

Si el tráfico no es óptimo, el flujo lógico a través del camino No CP304 para comprobar ¿algún otro túnel disponible? 21-310 para comprobar si hay otro túnel disponible. Si otro túnel no existe, el camino lógico No CP320 lleva al Constructor de Túneles: Crea nuevo túnel 21-320 y una vez arriba, el proceso construye rutas para TUN 21-330 es ejecutado. De manera alternativa, si un túnel no existe, entonces el camino lógico Sí 21-CP352 lleva o el camino para túnel creado de nuevo desde 21-320 son enviados al paso banco de pruebas de túnel para evaluar túnel o túneles alternativos 21-350. El proceso evalúa TUN conmutación 21-360 copara la calidad de servicio (QoS) para ambos túneles.

La puerta de decisión ¿Conmuta a otro TUN? 21-400 evalúa dónde o dónde no merece la pena conmutar el flujo de tráfico a través Hace conmutación TUN 21-510 o para mantener el trafico fluyendo a través del TUN actual a través del camino No CP308.

Los parámetros que gobiernan la lógica de conmutación incluyen tolerancia del túnel que puede ser establecida por la preferencia del usuario, o análisis algorítmico de condiciones actuales, u otros factores. Los registros de condiciones del túnel pueden ser usados para la comparación de métricas actuales e históricas y pueden ayudar a tomar las decisiones de conmutación contextuales más eficientes. Las métricas del estado del túnel pueden también ser usadas para la comparación de conjuntos de túneles relacionados entre ellos.

El tipo y naturaleza del tráfico actual que fluye a través del túnel tal como el volumen de tráfico, la probabilidad de que un conmutador rompa el flujo del tráfico, y otros factores son también considerados cuando se decide si conmutar o no a otro túnel.

La FIG. 22 ilustra la estructura lógica de dos interfaces virtuales VIF conectadas secuencialmente a lo largo de un camino, cada una con rutas aplicadas para enviar tráfico por túneles para una región específica. En este ejemplo, el tráfico VIF0 para el tráfico de la Región A 22-110 y VIF2 para el tráfico de la Región B 22-150.

Cada interfaz virtual tiene túneles en varias etapas del ciclo de vida de TUN como se describe en la FIG. 20 anteriormente. El uso de interfaces virtuales puede ofrecer ganancias de eficiencia significativas y hay otras ventajas para construir túneles unidos a una región en un VIF específica y túneles para otra región y otra VIF. Por ejemplo, los procesos que consumen tiempo tal como construcción de rutas pueden hacerse en la VIF, por delante del TUN de forma que cuando nuevos túneles son construidos y/o los existentes están ya disponibles, entonces el tráfico para la región objetivo puede ser conmutado instantáneamente desde un túnel al otro. Esto también simplifica las tablas de enrutamiento y gestión de recursos aplicándolos en un lugar, o la VIF mejor que tener que aplicarlas en todos y cada uno de los túneles individuales.

La FIG. 23 ilustra el tiempo requerido para procesar varios túneles (TUN) e interfaces virtuales (VIF). La estructura lógica describe un camino donde el tráfico entra en Tráfico en 23-100 al punto de unión 23-102. Dos VIF activas son

conectadas a través de los campos 23-P110 y 23-P120. La VIF00 de la Región A 23-110 enlaza a túneles destinados para la región A y la VIF02 de la Región B 23-120 enlaza con túneles destinados para la región B.

Dos VIF en espera y los túneles correspondientes son VIF06 Alt. Región A 23-116 y VIF08 Alt. Región B 23-126. La diferencia entre VIF00 y VIF06 es que la VIF06 en espera alternativa solo tiene túneles en construcción 23-316 y en espera En Espera 23-318.

Por ejemplo, los procedimientos 23-540 y 23-520 que consumen tiempo, poco comunes y lentos de construcción de interfaces virtuales, adición de rutas, y procesos relacionados toman mucho tiempo pero no ocurren muy a menudo.

Y dado que el enrutamiento del túnel ha sido desplazado hacia arriba a la VIF, las operaciones del túnel son los procedimientos 23-530 y 23-500 relativa y extremadamente rápidos y frecuentes.

Cuando una interfaz virtual como VIF00 de la Región A 23-110 se vuelve no viable, entonces el flujo lógico de tráfico 23-P110 puede ser desplazado al camino 23-P116 a una VIF En Espera VIF06 Alt. de la Región A 23-116 en operación con túneles a esa región objetivo de la VIF arriba y lista. El desplazamiento desde una VIF a otra es un procedimiento 23-510 extremadamente rápido y poco común.

La FIG. 24 ilustra la estructura lógica de múltiples VIF dispuestas secuencialmente dentro de un camino de tráfico entre el tráfico entrante 24-100 y otro tráfico 24-140. El tráfico de la región A es enviado a través de Túneles Activos 24-300 a la VIF 00 de la Región A 24-110 cuando la dirección IP del dispositivo de equipo destino objetivo hace coincidir una dirección en una lista de Lista de Direcciones IP para la Región A 24-610. La lista de direcciones IP puede incluir direcciones IP únicas, rangos de direcciones IP, descripción de notación de un rango tal como CIDR, u otra forma de definir direcciones de ubicación de un equipo. La lista 24_610 actúa como un embudo que envía todas las coincidencias a través de los túneles, y el tráfico que no coincide restante a la siguiente pata en la secuencia lógica a través de un punto de enlace entre la VIF tal como 24-112 al camino 24-P120 a la VIF02 de la Región B 24-120.

El tráfico en la VIF02 de la Región B 24-120 es entonces comprobado contra una Lista de Direcciones IP para la Región B 24-620. Si hay una coincidencia, entonces el tráfico es enviado a través de un túnel Activo 24-302. Si no hay coincidencia, entonces el tráfico continúa a lo largo del camino secuencial a través de 24-122 a la siguiente VIF etcétera.

Si no hay coincidencia para el tráfico de la Región A, Región B, o Región C, entonces continúa a lo largo del camino secuencial a Otro tráfico 24-140 donde puede bien egresar a internet abierto, ser capturado en una memoria intermedia, descartado, o por el contrario enrutado.

La FIG. 25 ilustra la estructura lógica de tres interfaces virtuales y sus varios túneles a tres regiones VIF00 de la Región A 25-110, VIF02 de la Región B 25-120, y VIF04 de la Región C 25-130 diferentes. Además esta figura muestra interfaces virtuales alternativos, en espera, y túneles VIF06 de la Alt. Región A 25-116, VIF08 de la Alt. Región B 25-126, y VIF10 de la Alt. Región C 25-136 en espera. Además, esta figura también muestra el flujo de tráfico pasadas las VIF en Otro tráfico 25-140 si no hay coincidencia de direcciones IP para ninguna de las regiones objetivo.

La FIG. 26 ilustra líneas de tiempo para operaciones relacionadas con varios túneles (TUN) e interfaces virtuales (VIF).

Tiempo Total: Túnel Ordinario – a ser construido o reconstruido 26-180 perfila el tiempo y pasos requeridos para construir y levantar un túnel TUN0 26-100.

Tiempo Total: VIF a ser construida o reconstruida y al menos un TUN a ser añadido 26-280 perfila el tiempo y pasos requeridos para construir y levantar una interfaz VIF0 26-200 virtual y adjuntar un primer túnel listo para empujar tráfico.

Tiempo Total: Túnel en VIF - a ser construido o reconstruido 26-380 perfila el tiempo y pasos requeridos para construir un túnel TUN2 26-300 subsecuente en una VIF.

Tiempo Total: Túnel en VIF – tráfico de conmutación hacia 26-880 perfila el tiempo y un paso requerido para tráfico de conmutación desde un túnel a otro túnel TUN8 26-800 anexado a una VIF.

Tiempo Total: Túnel en VIF – a ser destruido 26-380 perfila el tiempo y paso requerido para rechazar un túnel TUN4 26-400.

Esta figura no está a escala pero muestra lo relativa las ventajas de tiempo de construir túneles en interfaces virtuales con enrutamiento aplicado a la VIF hacia arriba desde los TUN.

La FIG. 27 es un diagrama de flujo que describe el algoritmo que gobierna el proceso de toma de decisiones o si hay que conmutar o no desde una interfaz virtual a otra interfaz virtual. Específicamente el algoritmo puede comprobar si la VIF actual es óptima, si hay un camino al EIP objetivo, y si TUN son óptimos para decidir si es mejor usar la VIF actual o conmutar a una alternativa.

La FIG. 28 ilustra la estructura lógica de tres interfaces virtuales y sus varios túneles a tres regiones diferentes. La FIG. 28 es similar a la FIG. 25 e ilustra la conmutación desde VIF02 Vieja Región B 28-120 a su VIF08 de la Región B 28-126 en espera.

Para que la VIF08 sea activada, el flujo de tráfico tiene que ser enrutado a través de 28-P120 hacia él. Y desde la VIF08 de la Región B 28-126 a la VIF04 de la Región C 28-130 a través del camino 28-P130.

Como se observó en la FIG. 23 anterior, la conmutación entre VIF es un procedimiento 23-510 extremadamente rápido y poco común. Una vez que la decisión de desplazar tráfico se toma a través de un algoritmo como se describe en la FIG. 27, entonces el desplazamiento de tráfico es sin obstáculos y rápido.

La FIG. 29 es un diagrama de flujo que describe el algoritmo que gobierna la destrucción ordenada de una interfaz virtual (VIF). En el inicio de este proceso, antes de que se tome cualquier acción, otros factores son comprobados en el paso 29-008 para asegurar que el problema es con la VIF y no con algún otro factor. Por ejemplo, si la conectividad de internet base se cae y no puede empujar tráfico, no tiene mucho sentido destruir una interfaz virtual y reconstruir la VIF porque sin una conexión de internet base, la VIF no será capaz de enviar o recibir tráfico.

También asegura que una VIF alternativa está disponible 29-116 y que esta VIF alternativa está disponible 29-210, conectada 29-250 y si es así a través el camino 29-CP260, entonces el proceso de destruir la VIF comienza en 29-260. Una comprobación final se hace para asegurar que la VIF ha sido realmente eliminada 29-278.

Si una VIF alternativa no está disponible 29-210, la lógica fluye a través el camino 29-CP220 a un proceso para construir 29-220 y para probar la nueva VIF 29-230.

La FIG. 30 ilustra cómo un túnel encriptado protege datos. TUN0 en GWD0 30-000 hacia GWD2 30-002 encripta paquetes en GWD0 30-000 y los desencripta en GWD2 30-002. Y para el tráfico en la otra dirección, los paquetes son encriptados en GWD2 30-002 y desencriptados en GWD0 30-000. Si los paquetes son interceptados en medio, la encriptación presenta la carga del paquete del túnel como no legible como se ilustra por 30-ATTK00 y 30-ATTK02. Sin embargo, si los paquetes son interceptados y su encriptación se rompe, entonces existe el riesgo de que Datos Robados 30-444 sean legibles y capaces de ser robados.

La FIG. 31 ilustra la seguridad ofrecida por un túnel TUN0 envuelto en otro túnel TUN2. El factor diferencial entre esta figura y la FIG. 30 es que los tres intentos en la intercepción 31-ATTK00, 31-ATTK02, y 31-ATTK04 de paquetes de datos resultan en fallos. Aunque el intento 31-ATTK04 en esta figura es una ruptura exitosa del túnel exterior, la carga que roba todavía está encriptada 31-444.

La FIG. 32 ilustra un túnel envuelto y tapado. En el camino de red lógico, el CAP está más cerca a la NIC. El CAP codifica y descodifica cargas a nivel de bit por byte.

En este ejemplo, 32-ATTK02 resulta en la interceptación de Datos Codificados 32-444. El codificador para el CAP se puede basar en la desunión exclusiva mediante el uso de claves rotativas y otra lógica para codificar las cargas de datos.

La FIG. 33 ilustra un codificador de byte de 8 bits en dos dispositivos GWD0 y GWD2 de puerta de enlace. Muestra cómo los bits de la carga de tráfico son codificados y decodificados por byte. El codificado es dinámico y aleatorio que protege el Byte de Tránsito Codificado 33-004

La FIG. 34 ilustra tres fases de codificación diferentes para bytes codificados de bit de un CAP. Mientras que hay solo 256 combinaciones potenciales de bits codificados para un sistema de 8 bits, una clave rotatoria basada en tiempo o tics u otros factores ofrecen más protección.

La FIG. 35 ilustra un túnel interno a través de una serie de envolturas y entonces un CAP. El flujo local desde GWD0 35-000 entra en el primer túnel TUN1 35-100, entonces en TUN2 35-200, y en TUN3 35-300, y entonces codificado por CAP 35-600. Cuando el tráfico entra GWD2 35-002 fluye en CAP 35-602 para ser decodificado, entonces desde TUN3 35-302 hacia TUN2 35-202 hacia TUN1 35-102 y entonces a 35-002.

Esta figura también describe el hinchado de paquete debido a las capas extras de seguridad que tienen el efecto de reducir el tamaño de carga útil.

La FIG. 36 ilustra tráfico de túnel de cortafuegos a cortafuegos durante un fallo de túnel. El tráfico de túnel de cortafuegos a cortafuegos a través del dispositivo de punto extremo (EPD) 36-100 puede fluir a través de un túnel 36-CP202 a un servidor de punto de acceso (SRV_AP) 36-202 o desde el EPD al SRV_AP 36-200 a través del túnel 36-CP200 al dispositivo FWD2 36-002. El túnel activo era 36-CP200 pero se cayó mientras empujaba tráfico con desplazamiento de fallo del tráfico al TUN 36-CP202. El tráfico desde el SRV_AP 36-200 egresó a través del punto de ingreso egreso EIP 36-210 al camino 36-CP210. El tráfico desde el SRV_AP 36-202 sale a través del EIP 36-212 al FWD2 36-002 a través del camino 36-CP002. Sin embargo, aunque el EPD conoce cómo enrutar tráfico al nuevo SRV_AP y el FWD2 36-002 recibe tráfico puede todavía intentar enviarlo al camino 36-CP210. Esto puede causar que el túnel interno desde FWD0 a FWD2 se rompa.

La FIG. 37 ilustra tráfico de túnel de cortafuegos a cortafuegos durante un fallo de túnel. La FIG. 37 es similar a la FIG. 36, con la adición de una estructura para mantener el enrutamiento entre dispositivos intacto aun después de desplazamientos de túneles internos a diferentes caminos de red. El EPD 37-100 permite conmutación dinámica desde un TUN 37-CP200 a otro 37-CP202. Cuando el tráfico egresa a través del EIP 37-218, el FWD2 37-002 puede encontrar el EPD independientemente de qué camino de túnel interno es usado.

La FIG. 38 ilustra tráfico de túnel de cortafuegos a cortafuegos durante un fallo de túnel. La FIG. 38 ilustra el tráfico ininterrumpido que fluye después del desplazamiento desde el viejo TUN 38-CP200 (no mostrado) a 38-CP202. Esto es atribuible al hecho de que el FWD2 38-002 es capaz de encontrar el camino de retorno de vuelta ya que la dirección IP que conoce para el EIP 38-218 en el SRV_AP 38-208 permanece la misma independientemente de un desplazamiento de enrutamiento de tráfico interno.

La FIG. 39 ilustra el enlace de dos o más redes de área local (LAN) LAN 000 LAN 002 en una red de área extensa (WAN). Subredes únicas son requeridas para evitar conflictos. Automatización y comunicación dispositivo a dispositivo permiten redes correspondidas de manera dinámica y puede evitar conflictos de IP debido al solapamiento de rangos de subredes.

Este mecanismo puede ser usado tanto para calcular direcciones IP, asignaciones de rangos de dirección IP y otros factores que pueden ser usados bien por sistemas automáticos, o pueden ser la base de la mensajería de administradores de red para hacer configuraciones manuales o para tomar otras acciones.

La FIG. 40 ilustra la importancia de una lista de disponibilidad de servidores y cómo las direcciones IP y rangos son asignados para varios dispositivos. Aunque IPv6 ofrece un enorme rango de direcciones IP posibles, el estándar IPv4 tiene una cantidad finita de tanto direcciones IP públicas como privadas. Esto tiene una influencia en qué EPD pueden conectarse con qué SRV_AP.

En esta figura, EPD 40-100 construye túneles con SRV_AP 40-300, 40-302 y 40-306. EPD 40-102 construye túneles con SRV_AP 40-300, 40-304, y 40-308.

Este ejemplo demuestra cómo el rango de IP interno 10.10.191.0 hasta 10.10.191.255 puede ser usado en dos SRV_AP 40-302 y 40-304, y el rango IP 10.10.192.0 hasta 10.10.192.255 puede ser usado en ambos SRV_AP 40-306 y 40-308.

Por lo tanto por ejemplo, 10.10.191.18 puede ser usado por EPD 40-100 para construir un túnel a SVR_AP 40-302 y al mismo tiempo 10.10.191.18 puede ser usado también por EPD 40-102 para conectar con SRV_AP 40-304.

EPD 40-100 y EPD 40-102 no tienen que interactuar directamente entre sí para evitar conflictos porque la lista de disponibilidad de servidores publicada para cada EPD en coordinación con el gestor de TUN asignará combinaciones de direcciones IP (interna y externa) para que los EPD se conecten con SRV_AP sin ningún conflicto.

La FIG. 41 ilustra múltiples flujos únicos paralelos entre dispositivos. Este ejemplo muestra múltiples flujos únicos paralelos a través de cuatro túneles usados para enviar datos de manera concurrente entre un EPD 41-100 y un SRV_AP 41-300. Los flujos A, B, C, y D son enviados por separado y recombinados en el otro extremo. Este multi flujo es efectivo y eficiente asumiendo que la conectividad base es de buena calidad. A, B, C, y D son presentados como un ejemplo. El número real de flujos paralelos puede ser dinámico en base a la capacidad de carga de la línea. Esto tiene una dependencia en una línea limpia.

La FIG. 42 ilustra múltiples flujos no únicos paralelos entre dispositivos. Este ejemplo muestra dos flujos duplicados separados de forma que dos A y dos B son transmitidos de manera concurrente. Si uno o el otro paquete A se pierde y no llega, el otro todavía se recibe. Esto es una característica clave del modo tiempo tormentoso para mantener datos fluyendo durante tiempos de pérdida de paquetes.

Enviar flujos paralelos consume más tráfico y ancho de banda. Sin embargo, durante periodos de conectividad de red inestable, el tráfico todavía llega debido a la redundancia. Así en el caso de que un usuario tenga una conexión de última milla de 20 Mbps, si hay una gran cantidad de pérdida de paquetes en un único flujo la experiencia de usuario (UX) puede ser menor que la ideal debido a los tiempos acabados, flujos de video rotos, y otros efectos no deseables.

Si un flujo es duplicado, el tamaño efectivo de la tubería de la última milla es reducida a 10 Mbps o menos, sin embargo los datos llegarán mejorando la UX. Como una extensión de esto, como por ejemplo si la duplicación de un flujo es cuadruplicada, la reducción del ancho de banda es disminuida por cuatro. Así una condición de 20 Mbps podría reducirse a 5 Mbps o menos, sin embargo, el enlace continuará funcionando.

La FIG. 43 ilustra el marco lógico y la estructura algorítmica para el modo de tiempo tormentoso (SWM). El paso de búsqueda de parámetros 43-010 establece el análisis basado en los atributos de la conexión base y otros factores. Cuando trata con pérdida de paquetes 43-310, los flujos duplicados pueden ser usados para evitar pérdida y la necesidad de retransmisiones subsecuentes.

Si durante periodos de micro cortes 43-P330, el SWM puede reconocer la situación, y mantener las VIF y TUN arriba. El tráfico puede ser almacenado internamente, la conectividad mantenida viva, y cuando el corte se acaba, una puesta al día ordenada con el flujo mediante la liberación suave del contenido de la memoria intermedia.

La clave para el modo de tiempo tormentoso para tomar medidas es comprender correctamente las condiciones y tomar las acciones de remedio apropiadas.

La FIG. 44 ilustra múltiples túneles entre dispositivos dentro de una red virtual global (GVN) sobre múltiples regiones. El EPD está en una ubicación 44-M0. SRV_AP en la región 44-M2 incluye SRV_AP 44-300, SRV_AP 44-302, y SRV_AP 44-304. SRV_AP en la región 44-M3 SRV_AP 44-310, SRV_AP 44-312, y SRV_AP 44-314. El enrutamiento inteligente avanzado (ASR) es usado para gestionar el enrutamiento sobre los múltiples túneles y caminos entre el EPD y los varios dispositivos SRV_AP. ASR puede mitigar el riesgo de bucles, enrutamiento por destino geográfico erróneo, retroceso de redireccionamiento remoto ASR, enlaces rotos entre SRV_AP, regiones, y otros problemas.

La FIG. 45 ilustra problemas potenciales con cuellos de botella a través de un salto entre dos segmentos de red. Durante el servicio de un archivo desde un servidor a un cliente, ciertos algoritmos gobiernan el ancho de banda de la transferencia en base a la capacidad de carga de la línea extremo a extremo. Si la ráfaga de tráfico es demasiado alta, el servidor estrangula el ancho de banda para habilitar de la manera más eficiente la mitigación de la pérdida debido a la congestión. Esto puede resultar en el servidor siendo un ciudadano bueno y responsable con respecto al uso de la tubería pero también puede resultar en un gobierno demasiado agresivo del ancho de banda ralentizando de manera significativa la transferencia bien por debajo de la capacidad de carga de la línea extremo a extremo real.

Cuando un servidor empieza a servir un flujo de datos o un archivo, lanzará muchos paquetes por segundo en base a lo que asume que es el ancho de banda alto de un segmento 45-100 de red. El servidor está conectado a este gran segmento de red de tubería.

Si el flujo de datos es restringido en 45-300, fuerza al servidor a estrangular de manera agresiva el flujo ralentizando la transferencia, y debido a la necesidad de retransmitir los paquetes perdidos, el servidor puede reducir la tasa de transferencia de manera demasiado agresiva ralentizando el proceso total.

La FIG. 46 ilustra la organización y reporte de información en el SRV_CNTRL. Esta información incluye un análisis de puertos por dirección IP a cada SRV_AP, la calidad de servicio (QoS) y clasifica cada puerto en el tiempo. Esta información puede ser usada para comparar grupos de puertos entre sí y para identificar patrones en el tiempo y en series/conjuntos que intersectan.

La FIG. 47 es un diagrama de flujo que describe la lógica usada para pruebas de túneles. Hay pruebas hechas en el túnel 47-110 actual, pruebas hechas en la conexión base fuera del túnel 47-120, pruebas fuera del túnel a un SRV_AP 47-120 alternativo, y pruebas ejecutadas en TUN hacia SRV_AP alternativos en la misma región 47-140. Mediante la comparación de las pruebas entre sí, las comparaciones de la QoS entre conexión base y túnel, túnel alternativo, y más pueden ser comprobadas.

La FIG.48 ilustra la ejecución de pruebas de túneles paralelas para medir latencia 48-100, ancho de banda 48-110, pérdida de paquetes 48-120 y otros factores 48-150.

Después de probar, otros procesos son ejecutados posteriormente a la ejecución de las pruebas para limpiar, y liberar recursos 48-300. Al final de las pruebas, resultados 48-320 de pruebas de registro guardan información pertinente.

La FIG. 49 ilustra la ejecución de pruebas de conectividad sin interferir con el uso del túnel de usuario actual. Antes de que cualquier ciclo de pruebas comience, analiza el uso 49-1100 actual examina el uso actual de la conectividad por usuarios, por tipo de tráfico así como qué tráfico se queda local y qué tráfico transita a través de un túnel.

El siguiente paso asigna y usa capacidad libre para ejecutar pruebas 49-1200 de forma que las pruebas no roban ancho de banda de los usuarios que podrían tener un efecto perjudicial en su UX.

En analiza conectividad 49-1300, tanto las pruebas de conectividad como el uso de usuario real son tenidas en cuenta en modo agregado e individualmente para analizar la conectividad.

Las pruebas ejecutadas durante las horas laborables cuando una red en “producción” está ocupada serán ejecutadas de forma que no afecte el flujo de trabajo. Las pruebas ejecutadas durante las horas fuera del horario laboral pueden no proporcionar información precisa de una red más amplia bajo carga porque no pueden detectar problemas de congestión individual que ocurren cuando múltiples grupos están también usando los recursos de red.

Las pruebas ejecutadas en una red ocupada pueden interrumpir el flujo de trabajo y mientras sea necesario diagnosticar problemas, si se ejecutan demasiado a menudo y le da el derecho a monopolizar demasiados recursos, entonces la prueba actual podría volverse un factor que contribuya al problema.

El uso de la red total puede ser medido mediante el análisis del tráfico por el camino 49-CP306.

El tráfico solo local puede ser comprobado haciendo el total de todo el tráfico del túnel y restando esa suma del tráfico a través de 49-CP306 con lo restante siendo el tráfico total.

La FIG. 50 ilustra la interacción entre tres dispositivos que colaboran en el proceso de la construcción de túneles. Los tres dispositivos son un dispositivo de punto extremo (EPD) 50-100, un servidor de punto de acceso (SRV_AP) 50-300 y un servidor de control central (SRV_CNTRL) 50-200. Esta figura muestra la estructura lógica de los dispositivos, los componentes clave que se ejecutan en cada dispositivo, así como el marco de trabajo de la API para las comunicaciones entre ellos.

Para que el túnel TUN 50-100300 sea construido, cierta información sobre el túnel, sobre los pares en el par, y otra información puede ser compartida por la API.

Información sobre con qué SRV_AP 50-300 un EPD 50-100 debería conectar está disponible a través de una lista de disponibilidad de servidores que es generada en el SRV_CNTRL 50-200.

El túnel es iniciado en el EPD 50-100 por el Constructor de Túneles 50-112. Es gobernado por el Gestor de Túneles que a su vez recoge información de Info Túnel 50-116 para configuraciones, Índice de túneles 50-118, y guarda información 50-122 del túnel.

El oyente 50-312 de túneles opera en el SRV_AP 50-300 y es gobernado por el gestor de túneles 50-310. Información en cada dispositivo puede ser almacenada en RAM, en una base de datos 50-B100, 50-B300, y 50-B200, o en un disco 50-H100 o 50-H300, u otras formas de almacenamiento (no mostradas).

La FIG. 51 ilustra las relaciones entre varias tablas de bases de datos usadas para almacenar información de conectividad. La información de conectividad es usada para hacer túneles 51-210, información de túnel 51-220, y Disponibilidad de Servidor 51-280. Más tablas pueden ser usadas, y los campos y relaciones indicadas son solo de ejemplo y pueden diferir dependiendo del uso dentro de varios sistemas.

La FIG. 52 ilustra los requisitos para información única por túnel para evitar colisiones. Esta información puede incluir el nombre del túnel, ID del túnel, nombre de la interfaz del túnel, el número de puerto escuchado en una dirección IP específica, y debería ser única para cada túnel.

Esta figura ilustra la conexión desde los dispositivos al SRV_AP 52-300, tal como EPD 52-100 al puerto 26158 a través de 52-P100, EPD 52-102 al puerto 9836 a través de 52-P102, desde PEPD 52-110 al puerto 45373 a través de 52-P110, EPD 104 al puerto 33172 a través de 52-P104, PEPD 52-112 al puerto 15942, y EPD 52-106 al puerto 51625 a través de 52-P106.

El oyente de túneles 52-312 solo abrirá esos puertos con los cuales espera que se construyan túneles y cerrará el resto. Además, solo conexiones desde pares conocidos serán aceptadas. Los puertos asignados a TUN a través del mecanismo de disponibilidad de servidores son únicos y aleatorios. El tipo de túnel no puede ser identificado por el puerto usado. Subredes únicas que no entran en conflicto serán también asignadas a través del oyente de túneles gobernado por el listado de disponibilidad de servidores y gestor de túneles 52-310.

La FIG. 53 es un diagrama de flujo que ilustra el flujo lógico usado para asignar un puerto a una dirección IP usada para construir un túnel. El flujo tiene en cuenta varios factores cuando selecciona el puerto y dirección IP a usar.

El primer paso es recoger parámetros 53-010 para el puerto para la asignación de dirección IP mediante la comprobación para ver si el puerto deseado y Dirección_IP han sido especificados para ser usados por un dispositivo específico por su Dispositivo_ID, y otros factores. Los parámetros también delinean un valor de suelo y un valor de techo para el número de puerto, y más configuraciones de gobierno.

El paso de puerta lógica ¿IP + puerto especificado? 53-020 comprueba para ver si hay una solicitud para un puerto específico anexado a una dirección IP específica para un dispositivo servidor por Dispositivo_IP.

Si el puerto y dirección IP han sido especificados, entonces la disponibilidad para su uso es aceptada y la lógica sigue el camino Sí 53-P022. Si un puerto e IP preferentes no son especificados entonces la lógica sigue el camino No 53-P030 al generador de números aleatorios para que se genere un puerto aleatorio dentro del rango 53-030.

Una búsqueda se hace en el paso 53-050 para comprobar contra el uso actual e histórico (a través del camino 53-B102 a Db Registro 53-B100) para esa correspondencia de puerto a dirección IP para ver si el puerto está libre o si está actualmente en uso. Una segunda comprobación se hace al mirar el uso histórico para ser si indica que esa combinación de puerto e IP ha sido usada en el pasado por ese dispositivo u otros dispositivos, y si es así, si ese uso probó ser relativamente problemático. Algunos puertos inestables o de no confianza debido al filtrado o congestión a través de dispositivos u otras razones pueden ser marcados como problemáticos. Si hay también una tendencia a bloquear puertos problemáticos para otros dispositivos, entonces la combinación de puerto a dirección IP puede ser marcada como no disponible.

Si el puerto no está disponible en el paso 53-060, el proceso de generación de una correspondencia de puerto a dirección IP es reiniciado a través del punto de unión 53-012.

Si el puerto está disponible, entonces el puerto a dirección IP será asignado para usar en el paso 53-100. Esta asignación será guardada en el Db registro 53-B100 a través del camino 53-B112. A continuación, la asignación Puerto a Dirección IP es publicada a través de una llamada 53-120 API para que dispositivos relevantes sepan sobre el estado de disponibilidad del puerto. El último paso es registrar la asignación 53-130 de puerto a dirección IP que incluye la lógica usada y otros factores que podrían ayudar en la mejora de la eficiencia de futuras asignaciones de puertos.

La FIG. 54 es un diagrama de flujo que describe una estructura para una serie de pruebas de varios puertos de una dirección IP. La estructura incluye un bucle mientras que continuará mientras el contador VAR sea menor que el número prescrito de pruebas a ejecutar. Los resultados por prueba son guardados en una matriz multidimensional o guardados en la base de datos o archivo de registro.

En los resultados del proceso, añade a la matriz de resultados, prepara para el paso de registro 54-090, análisis estadístico en curso puede ser ejecutado en la prueba actual comparado con las otras pruebas ejecutadas en la serie.

La FIG. 55 es un diagrama de flujo que muestra la lógica al respecto de la gestión de relaciones de pares entre dispositivos. El algoritmo comprueba para ver si hay una relación en lugar 55-020, si está actualizada 55-030, y también comprueba para ver si tiene los derechos adecuados para crear 55-130 y o actualizar 55-100 la relación. Si una nueva relación es creada o una existente es actualizada, una llamada a API 55-220 a través del SRV_CNTRL comparte la información con el otro par en la pareja.

La FIG. 56 ilustra los pasos usados en el establecimiento y posterior ejecución de pruebas de túneles. Esto es una alternativa a la operación como se describe en la FIG. 54.

La FIG. 57 ilustra un punto extremo virtual (VEP) extendido en la nube. El VEP es alcanzable bien por dirección IP dedicada a través del camino 57-CP000 a 57-CP010 o una combinación de dirección IP + puerto a través de los caminos 57-CP002 a 57-CP-012.

El punto de ingreso egreso (EIP) 57-212 en un servidor de punto de acceso (SRV_AP) 57-202 llevará tráfico recibido en el puerto específico en la dirección IP a través del camino 57-CP010 a través del túnel TUN 57-202 al EPD 57-100 a través de la LAN 57-102 al Dispositivo LAN 57-108.

Si no se especifica puerto, el tráfico a través de 57-CP012 dirección IP Dedicada puede ser enviado al EPD 57-100 y puede ser manejado a través de 57-118.

La FIG. 58 ilustra la unión de un nombre de dominio a un VEP dinámico en un SRV_AP 58-202. Esto permite al tráfico “encontrar” el EIP 58-212 después de que el nombre de dominio sea buscado por un servidor de nombre de dominio (SRV_DNS) 58-022. Una granularidad más fina de enrutamiento ocurre en un servidor nombredeservidor (SRV_NS) 58-028. Este mecanismo permite que un NombreDominio.gTLD se haga corresponder a este EPD 58-118.

La FIG. 59 ilustra el enrutamiento de tráfico para un dominio.gTLD para entrar en una red virtual global (GVN) a través del punto de ingreso egreso (EIP) óptimo. El punto de ingreso egreso (EIP) optimo puede ser punto de ingreso egreso 59-312 en el servidor de punto de acceso (SRV_AP) 59-310 o EIP 59-322 en SRV_AP 59-320. El tráfico desde bien SRV__AP 59-310 o SRV_AP 59-320 enrutará al EPD 59-100 a través del camino optimo a través de la GVN. Por el contrario el tráfico de vuelta es enrutado inteligente de vuelta.

La FIG. 60 ilustra un registro de dispositivos de punto extremo (EPD) y dispositivos de punto extremo personales (PEPD) que pueden ser ubicados y alcanzados a través de un dominio.gTLD.

gTLD significa dominio de nivel superior global. El registro además almacena información para dispositivos individuales ubicados en la red de área local (LAN) detrás de un EPD o una red de área personal (PAN) detrás de un PEPD. Por ejemplo PC.dominio100.gTLD encontrará PC 60-128 a través del camino 60-P128 que está en la red interna detrás de EPD 60-100. La configuración de seguridad puede también gobernar si los dispositivos dentro de una LAN son alcanzables o no desde internet abierto, o solo desde direcciones IP origen conocidas, o solo desde la GVN, o desde EPD conocidos, o través de otras reglas.

La FIG. 61 ilustra dispositivos que pueden ser alcanzados a través de un subdominio de un dominio de nivel superior global. Este ejemplo muestra dispositivos alcanzables por subdominio.nombredominio.gTLD tal como Servidor 61-126 a través de Servidor.Dominio100.gTLD detrás de EPD 61-100. Sin embargo, Dispositivo LAN 61-108 no es asignado un subdominio y por lo tanto no es alcanzable desde fuera a través de un punto extremo virtual (VEP).

La FIG. 62 ilustra un método para usar una interfaz de usuario gráfica (GUI) que se ejecuta en un buscador en un Dispositivo de Cliente para gestionar información de punto extremo virtual. La interfaz de usuario (GUI) 62-028 se ejecuta en un buscador en un Dispositivo de Cliente 62_118. El cliente en la GUI puede conectarse a través de Equipo 62-102 en el EPD 62-100 o Equipo 62-222 alojado en SRV_CNTRL (publico) 62-220.

La lista de dominios.gTLD y subdominios asociados es gestionada y tras “guardar” o “comprometer”, los cambios son compartidos con el Repositorio 62-200 de SRV_CNTRL (Interno) a través de su API 62-222 para ser guardada en la base de datos allí 62-B300. El Gestor de VEP 62-380 publica esta información en el servidor de registro de dominios

(SRV_DREG) 62-026, el servidor (SRV_DNS) 62-022 del servidor de nombre de dominio (DNS), y en el servidor de nombreservidor (SRV_NS) 62-028.

La FIG. 63 ilustra cómo el enrutamiento de subdominios.dominios.gTLD puede aprovecharse del enrutamiento inteligente avanzado (ASR) en una red virtual global (GVN). Esto puede ser usado tanto para encontrar el punto de ingreso egreso (EIP) optimo desde internet abierto 63-010 o 63-050 así como usar ASR para usar la ruta interna optima a través de la GVN. ASR puede usar una combinación de tanto caminos externos como caminos internos a través de túneles para seleccionar el camino extremo a extremo más ideal.

La FIG. 64 muestra un diagrama de bloques de tecnología usada por y habilitada por una red virtual global ("GVN") que incluye los elementos del núcleo de la GVN G0, módulos de GVN G100, y tecnología habilitada G200 por la red virtual global GVN. El núcleo de la GVN incluye una vista general del mecanismo G1 y sus partes componentes constituyentes de las capas de Topología G2, Construcción G3, Lógica G4, y Control G5. El núcleo de la GVN G0 también incorpora las relaciones para y con los Elementos G6 de la GVN.

La GVN puede incluir módulos G100 de la GVN de enchufar y/o autónomos que incluyen no pero no se limitan a: Mecanismo API Neutral ("NAPIM") G102, descrito en el documento PCT/US16/12178; Geodestino ("Geo-D") G104, descrito en el documento PCT/US15/64242, Enrutamiento Inteligente Avanzado ("ASR") G106, Conexión G108, y otros módulos G110 descritos en el documento de Solicitud Provisional de Estados Unidos US62/151.174.

La GVN también proporciona una plataforma que puede habilitar otras tecnologías que incluye pero no se limita a: Tapiz de Red G202; MPFWM G204; Tirachinas de Red G206; Baliza de Red G208, Granularidad de un tic G210, y otras tecnologías G212. Estos son descritos en un documento de Solicitud Provisional de Estados unidos 62/174.394, Solicitud Provisional de Estados Unidos 62/266.060.

Los módulos (G100) de la GVN y la Tecnología (G200) habilitados por la GVN pueden operar encima de una GVN existente, como una parte componente de una GVN, o puede ser independiente y usar todas o algunas de las partes aisladas de una GVN para soportar sus propias operaciones autónomas.

La FIG. 65 ilustra algunos módulos de sistema y componentes para un dispositivo de punto extremo EPD 100, servidor de control central SRV_CNTRL 200, y un servidor de punto de acceso SRV_AP 300. Esta figura también ilustra una base de datos 5100 en el EPD 100, base de datos 5200 en el SRV_CNTRL 200, base de datos repositorio 5202 en el SRV_CNTRL 200, y base de datos 5300 en el SRV_AP. La figura es jerárquica, con los dispositivos de hardware de nivel más bajo en la parte inferior, y los sistemas subsecuentes, componentes, módulos y gestores construidos en la parte superior de las padas inferiores. Los archivos y datos son almacenados en los dispositivos de almacenamiento anexos 65-H100 del Sistema de Archivos Jerárquico (HFS) en EPD 100, 65-H200 en SRV_CNTRL 200, y 65-H300 en SRV_AP 200. Los componentes ilustrados en estos diagramas de sistemas todos operan de manera independiente pero pueden también depender de información sobre otros dispositivos con los que interactúan.

RAM significa memoria de acceso aleatorio, CPU unidad de procesamiento central (que también puede incluir sub-procesadores), NIC tarjeta de interfaz de red, Db software de base de datos, DNS sistema de nombre de dominio, HOST software de equipo, API interfaz de programación de aplicación, ASR enrutamiento inteligente avanzado, GeoD geodestino, GVN red virtual global, CDA agente de entrega de contenido, CPA agente de extracción de contenido, y RF BOT robot buscador remoto. Pueden haber módulos, gestores, sistemas o componentes de software adicionales.

La FIG. 66 ilustra algunos módulos de sistema y componentes para un dispositivo de punto extremo EPD 100, servidor de control central SRV_CNTRL 200, y un servidor de punto de acceso SRV_AP 300. Esta figura además identifica subsistemas para cada dispositivo tal como EPD sub-sis 1000 para EPD 100, SRV_CNTRL Sub-sis 2000 para CNTRL 200, y SRV_AP sub-sis 3000 para SRV_AP 300. Los subsistemas han sido identificados mediante función y son indicados con prefijos que incluyen FW para subsistemas relacionados con cortafuegos, TUN con subsistemas relacionados con túneles, VIF para subsistemas relacionados con interfaces virtuales, SRV_Avail para la lista de disponibilidad de servidores y subsistemas relacionados, BUFF Mgr para el gestor de memoria intermedia y subsistemas relacionados, LOG para el módulo de registro y subsistemas relacionados, y CONECTIVIDAD para operaciones de conectividad general.

La FIG. 67 ilustra algunos módulos de sistema y componentes para un dispositivo de punto extremo EPD 100, servidor de control central SRV_CNTRL 200, y un servidor de punto de acceso SRV_AP 300. Los subsistemas han sido identificados por función y son indicados con prefijos que incluyen Conectividad para operaciones de conectividad general, ASR para enrutamiento inteligente avanzado, API para interfaz e programación de aplicación, LOG para el módulo de registro y subsistemas relacionados, GeoD para el módulo de geodestino y subsistemas relacionados, SRV_Avail para la lista de disponibilidad de servidores y subsistemas relacionados, Buffer para gestor de memoria intermedia y subsistemas relacionados.

REIVINDICACIONES

1. Un sistema de red para conectar dispositivos a través de una red virtual global, que comprende:

un dispositivo de punto extremo que comprende al menos un gestor de túneles, donde cada gestor de túneles está configurado para construir nuevos túneles, una primera interfaz virtual y otra interfaz virtual;

una pluralidad de servidores de punto de acceso cada uno que comprende al menos un oyente de túneles y una segunda interfaz virtual, donde cada oyente de túneles está configurado para abrir puertos sobre los que construir túneles;

una pluralidad de caminos de comunicación cada uno que comprende uno o más túneles, donde cada túnel conecta un gestor de túneles y un oyente de túneles;

donde la primera interfaz virtual proporciona al dispositivo de punto extremo un punto lógico de acceso a la pluralidad de caminos de comunicación, y donde la primera interfaz virtual tiene una lista asociada de direcciones IP correspondientes a una primera región;

donde la segunda interfaz virtual proporciona el servidor de punto de acceso respectivo un punto lógico de acceso a la pluralidad de caminos de comunicación; y

un módulo de enrutamiento configurado para gestionar el enrutamiento sobre la pluralidad de caminos de comunicación entre el dispositivo de punto extremo y la pluralidad de servidores de punto de acceso;

donde la primera interfaz virtual está configurada para enrutar tráfico que tiene una dirección IP que coincide en la lista de direcciones IP a través de un túnel activo de uno de la pluralidad de caminos de comunicación y para enrutar tráfico que tiene una dirección IP que no coincide en la lista de direcciones IP a la otra interfaz virtual.

2. El sistema de red según la reivindicación 1, donde la primera interfaz virtual y la segunda interfaz virtual son adaptadas para mantener el estado de los túneles que han establecido.

3. El sistema de red según la reivindicación 1, donde al menos uno de los caminos de comunicación incluye uno o más túneles que son envueltos en otro túnel.

4. El sistema de red según la reivindicación 1 o reivindicación 3, donde al menos uno de los caminos de comunicación incluye un túnel tapado que comprende una tapa que incluye un codificador que está configurado para codificar una carga de datos del túnel tapado.

5. El sistema de red según la reivindicación 1, donde el dispositivo de punto extremo y al menos uno de los servidores de punto de acceso están configurados para mantener flujos no únicos paralelos entre ellos.

6. El sistema de red según la reivindicación 1, donde al menos uno de la pluralidad de caminos de comunicación comprende dos o más túneles;

donde al menos un túnel de los dos o más túneles está en un estado activo; y

donde al menos otro túnel de los dos o más túneles está en un estado en construcción, en espera, u obsoleto.

7. El sistema de red según la reivindicación 6, donde el al menos otro túnel está en el estado en espera y el sistema de red está adaptado para comprobar periódicamente el al menos otro túnel para evaluar su viabilidad y capacidad operacional.

8. El sistema de red según la reivindicación 6, donde el sistema de red está adaptado para comprobar periódicamente que el al menos un túnel de los dos o más túneles está en estado activo para evaluar su viabilidad y capacidad operacional.

9. El sistema de red según la reivindicación 6, donde el al menos otro túnel está en estado en espera y el sistema de red está adaptado para mantener el al menos otro túnel vivo con al menos uno entre ping o tráfico de mantener vivo.

10. El sistema de red según la reivindicación 6, donde el sistema de red está adaptado para:

convertir el al menos un túnel de los dos o más túneles que está en el estado activo al estado obsoleto; y

convertir el al menos otro túnel que está en el estado en espera al estado activo.

11. El sistema de red según la reivindicación 6, donde el sistema de red está adaptado para:

comprobar periódicamente el al menos un túnel de los dos o más túneles que está en el estado activo para evaluar su viabilidad y capacidad operacional;

comprobar periódicamente el al menos otro túnel para evaluar su viabilidad y capacidad operacional; y

cuando la calidad de servicio (QoS) indica que el al menos otro túnel en el estado en espera es el túnel optimo entonces:

convertir el al menos un túnel de los dos o más túneles que está en el estado activo al estado obsoleto y entonces convertir el al menos otro túnel que está en el estado en espera al estado activo.

12. El sistema de red según la reivindicación 1, donde al menos dos túneles están en el estado activo;

donde el sistema de red está adaptado para:

enviar de manera concurrente flujos únicos de datos sobre los al menos dos túneles en el estado activo y entre el dispositivo de punto extremo y el servidor de punto de acceso durante periodos de baja pérdida de paquetes; y

enviar de manera concurrente flujos duplicados de datos sobre los al menos dos túneles en el estado activo y entre el dispositivo de punto extremo y el servidor de punto de acceso durante periodos de alta pérdida de paquetes.

13. El sistema de red según la reivindicación 1, que además comprende:

una pluralidad de otras interfaces virtuales, dicha pluralidad que incluye la otra interfaz virtual; y

al menos una interfaz física.

14. El sistema de red según la reivindicación 13, donde la primera interfaz virtual está además configurada para enrutar tráfico que tiene una dirección IP en un registro de direcciones IP a través de la al menos una interfaz física a una red local.

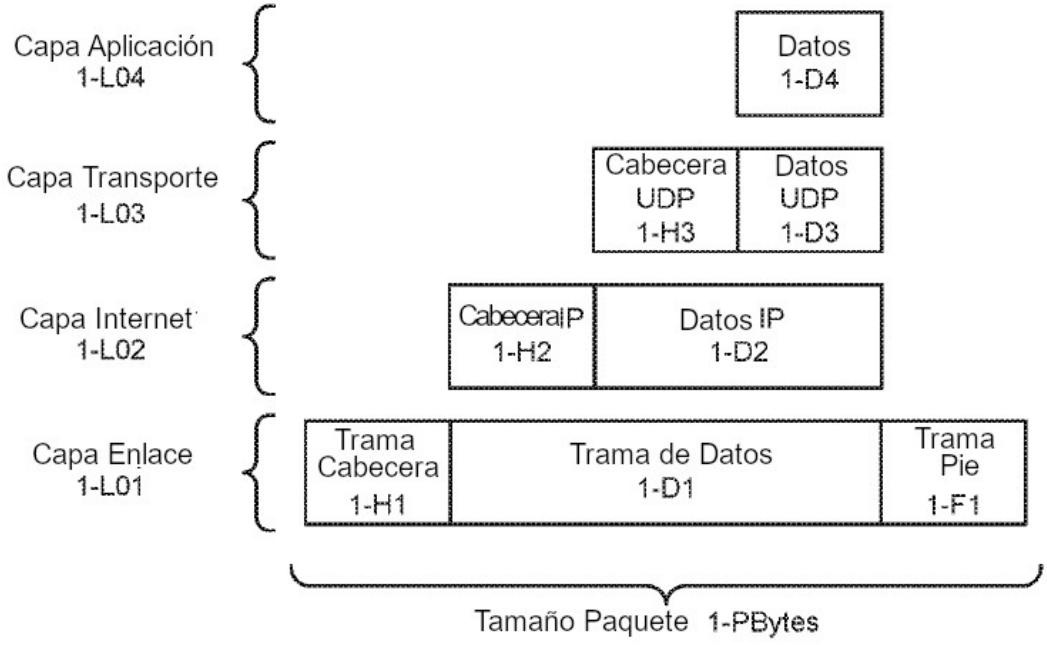
Capa Aplicación
1-L04
Datos
1-D4
Capa Transporte
1-L03
Cabecera
UDP
1-H3
Datos
UDP
1-D3
Capa Internet
1-L02
Cabecera IP
1-H2
Datos IP
1-D2
Capa Enlace
1-L01
Trama
Cabecera
1-H1
Trama de Datos
1-D1
Trama
Pie
1-F1
Tamaño Paquete 1-PBytes

FIG. 1

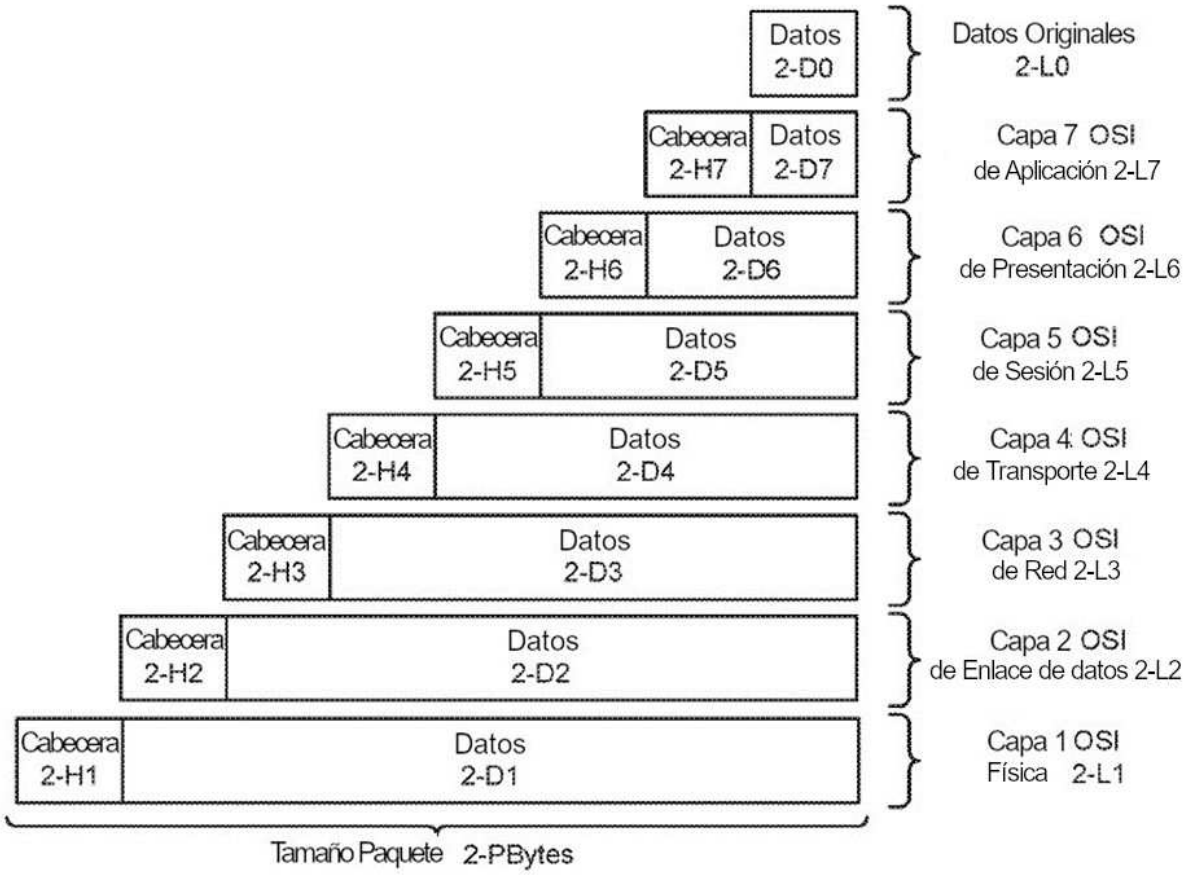
Datos
2-D0
Datos Originales
2-L0
Cabecera
2-H7
Datos
2-D7
Capa 7 OSI
de Aplicación 2-L7
Cabecera
2-H6
Datos
2-D6
Capa 6 OSI
de Presentación 2-L6
Cabecera
2-H5
Datos
2-D5
Capa 5 OSI
de Sesión 2-L5
Cabecera
2-H4
Datos
2-D4
Capa 4 OSI
de Transporte 2-L4
Cabecera
2-H3
Datos
2-D3
Capa 3 OSI
de Red 2-L3
Cabecera
2-H2
Datos
2-D2
Capa 2 OSI
de Enlace de datos 2-L2
Cabecera
2-H1
Datos
2-D1
Capa 1 OSI
Física 2-L1
Tamaño Paquete 2-PBytes

FIG. 2

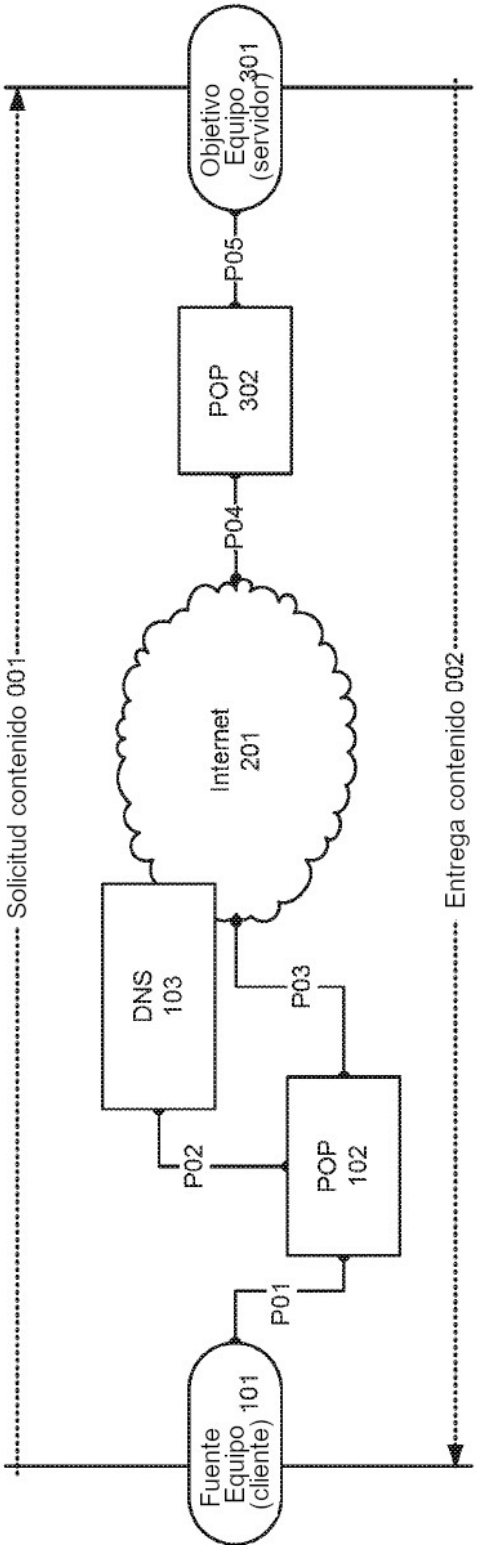
Objetivo
Equipo
(servidor) 301
P05
POP
302
P04
Internet
201
DNS
103
P03
P02
POP
102
P01
Fuente
Equipo
(cliente) 101
Solicitud contenido 001
Entrega contenido 002

FIG. 3


Ancho de banda
4-000
Granularidad
4-002
*
Bytes
4-020
Bits
4-022
*
Latencia
4-050
=
BDP
4-080

FIG. 4

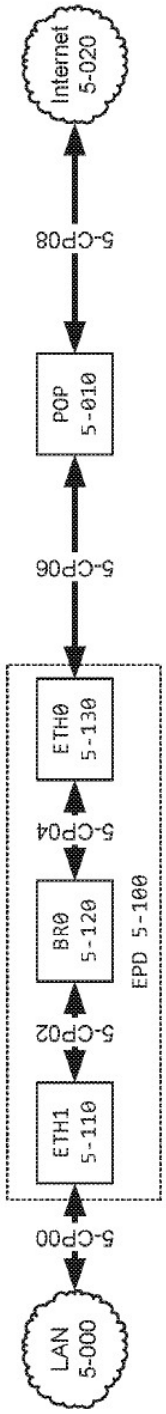
Internet
5-020
5-CP08
POP
5-010
5-CP06
ETH0
5-130
5-CP04
BR0
5-120
EPD 5-100
5-CP02
ETH1
5-110
5-CP00
LAN
5-000

FIG. 5

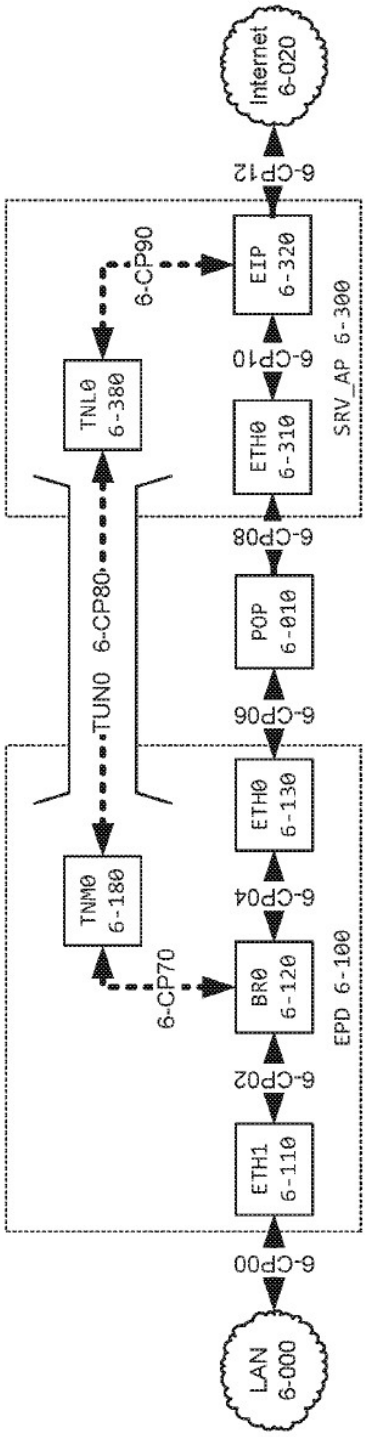
Internet
6-020
6-CP12
EIP
6-320
6-CP90
6-CP10
TNL0
6-380
ETH0
6-310
SRV_AP 6-300
6-CP08
TUN0 6-CP80
POP
6-010
6-CP06
ETH0
6-130
TNM0
6-180
6-CP04
6-CP70
BR0
6-120
EPD 6-100
6-CP02
ETH1
6-110
6-CP00
LAN
6-000

FIG. 6

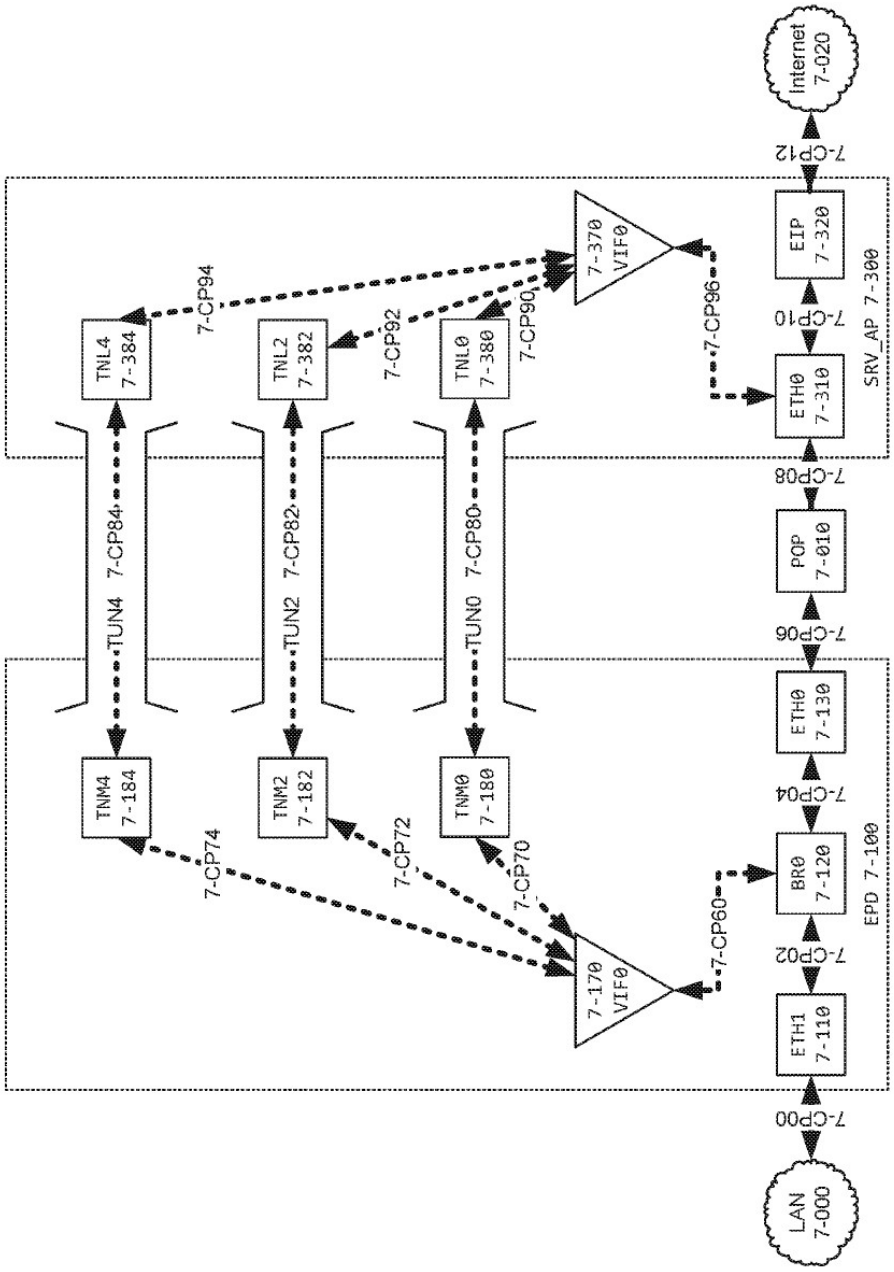
LAN
7-000
7-CP00
ETH1
7-110
7-CP02
BR0
7-120
7-CP04
ETH0
7-130
7-CP06
POP
7-010
7-CP08
ETH0
7-310
7-CP10
EIP
7-320
7-CP12
Internet
7-020
EPD 7-100
SRV_AP 7-300
7-170
VIF0
7-370
VIF0
7-CP60
7-CP70
7-CP72
7-CP74
7-CP90
7-CP92
7-CP94
7-CP96
TNM0
7-180
TNM2
7-182
TNM4
7-184
TNL0
7-380
TNL2
7-382
TNL4
7-384
TUN0
7-CP80
TUN2
7-CP82
TUN4
7-CP84

FIG. 7

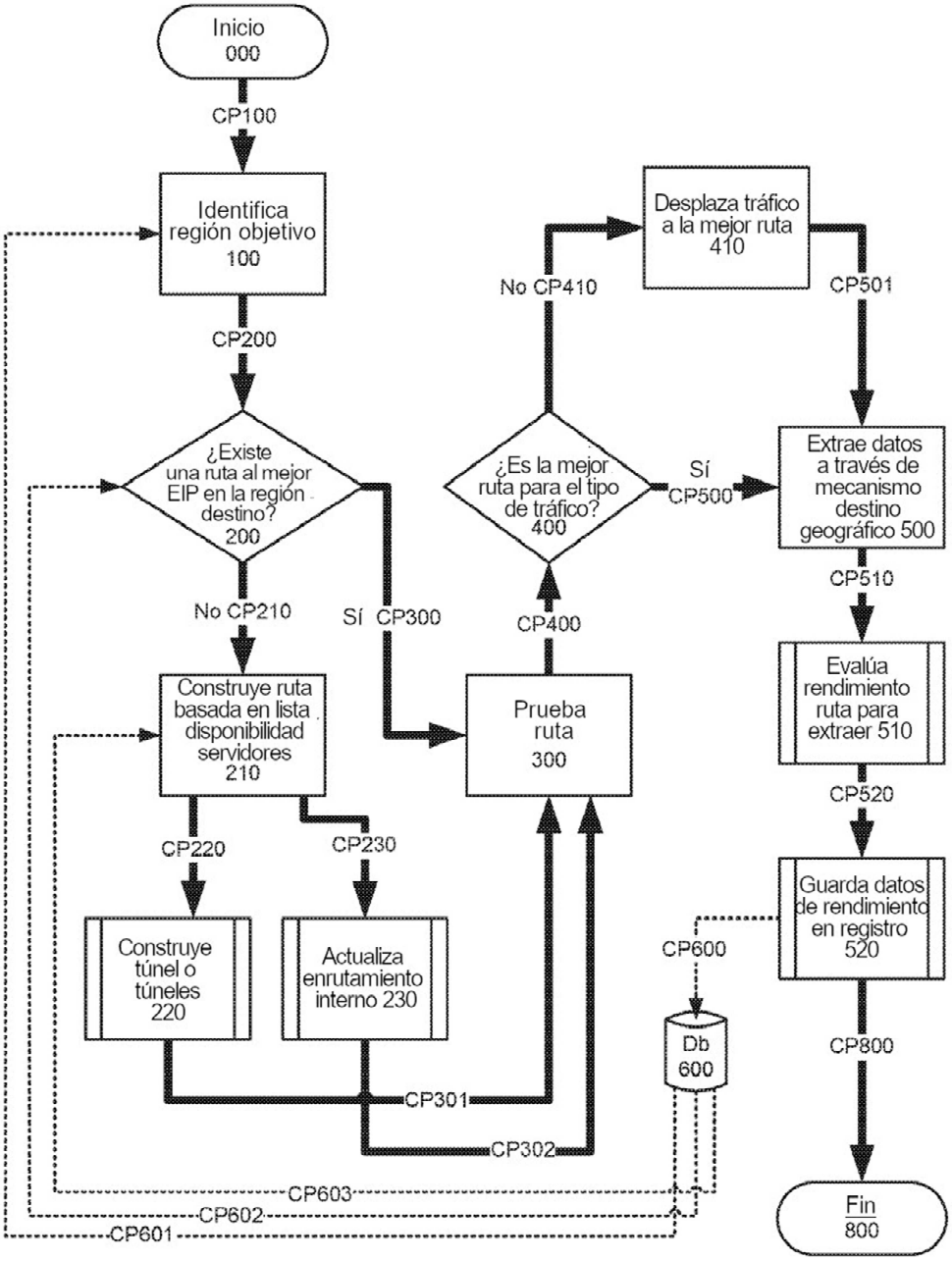
Inicio
000
CP100
Identifica
región objetivo
100
CP200
¿Existe
una ruta al mejor
EIP en la región
destino?
200
No CP210
Sí CP300
Construye ruta
basada en lista
disponibilidad
servidores
210
CP220
CP230
Construye
túnel o
túneles
220
Actualiza
enrutamiento
interno 230
Prueba
ruta
300
CP301
CP302
CP400
¿Es la mejor
ruta para el tipo
de tráfico?
400
No CP410
Desplaza tráfico
a la mejor ruta
410
Sí
CP500
CP501
Extrae datos
a través de
mecanismo
destino
geográfico 500
CP510
Evalúa
rendimiento
ruta para
extraer 510
CP520
Guarda datos
de rendimiento
en registro
520
CP600
Db
600
CP800
Fin
800
CP603
CP602
CP601

FIG. 8

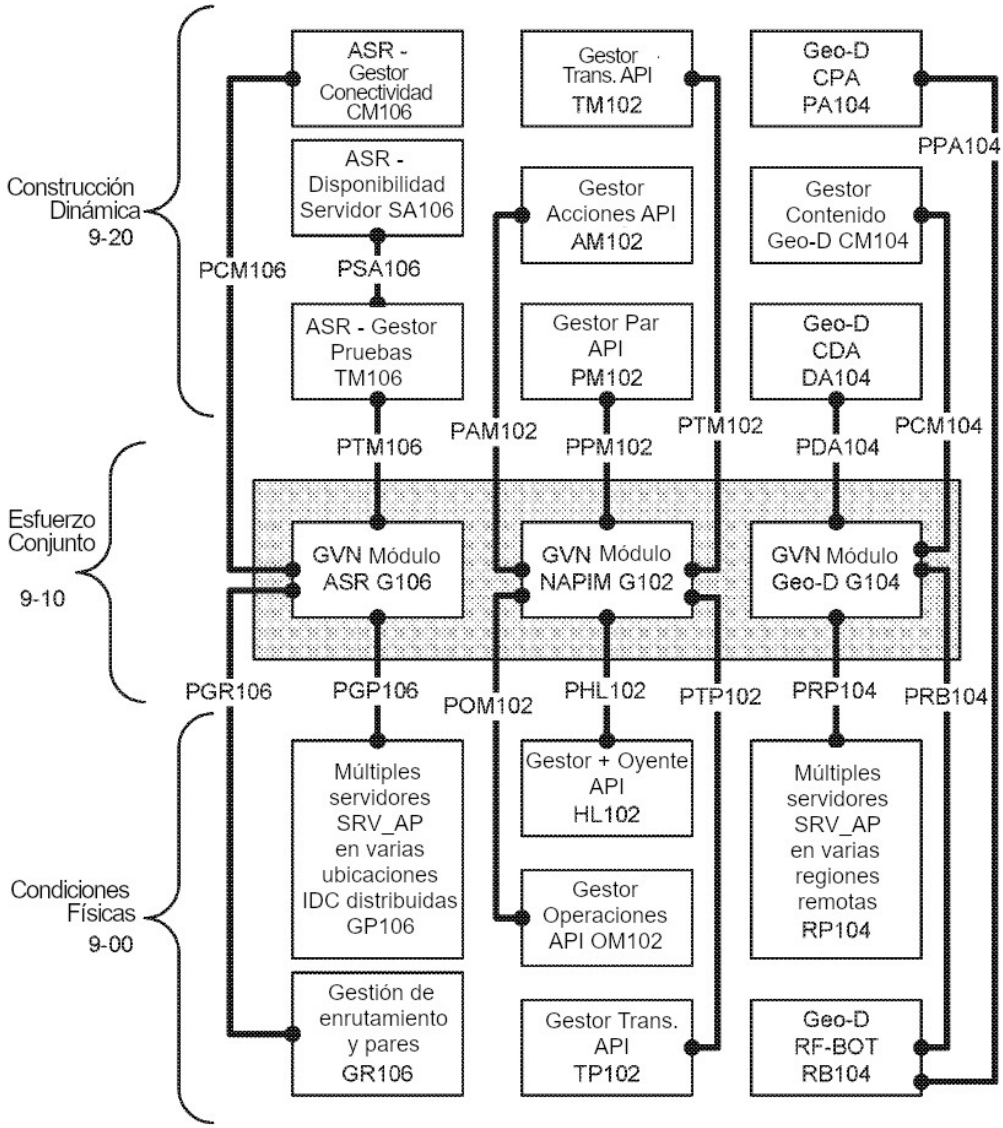
Construcción Dinámica 9-20
Esfuerzo Conjunto 9-10
Condiciones Físicas 9-00
ASR - Gestor Conectividad CM106
Gestor Trans. API TM102
Geo-D CPA PA104
ASR - Disponibilidad Servidor SA106
Gestor Acciones API AM102
Gestor Contenido Geo-D CM104
ASR - Gestor Pruebas TM106
Gestor Par API PM102
Geo-D CDA DA104
GVN Módulo ASR G106
GVN Módulo NAPIM G102
GVN Módulo Geo-D G104
Múltiples servidores SRV_AP en varias ubicaciones IDC distribuidas GP106
Gestor + Oyente API HL102
Múltiples servidores SRV_AP en varias regiones remotas RP104
Gestor Operaciones API OM102
Gestión de enrutamiento y pares GR106
Gestor Trans. API TP102
Geo-D RF-BOT RB104
PCM106
PSA106
PTM106
PAM102
PPM102
PTM102
PDA104
PCM104
PPA104
PGR106
PGP106
POM102
PHL102
PTP102
PRP104
PRB104

FIG. 9

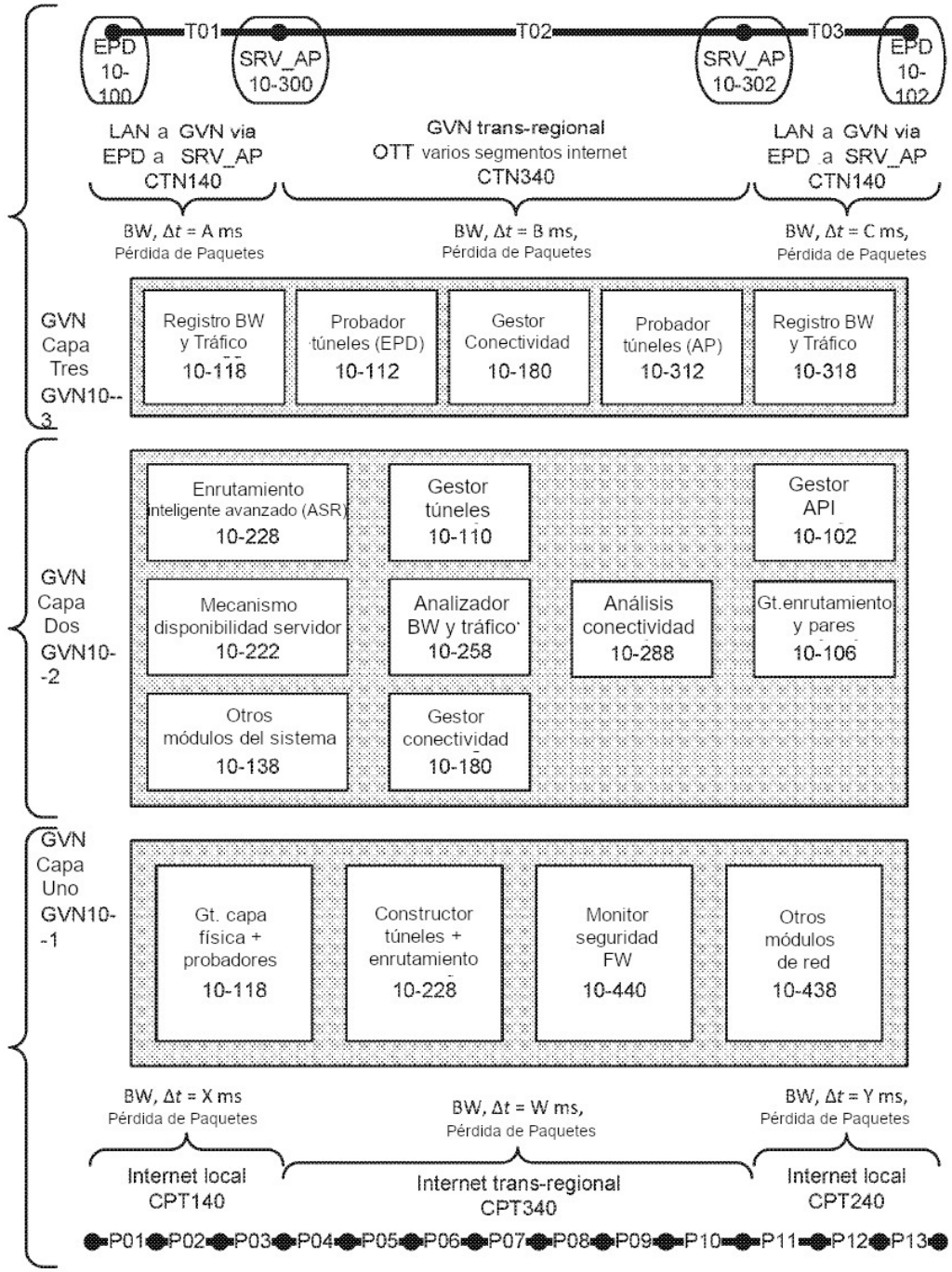
EPD 10-100
T01
SRV_AP 10-300
T02
SRV_AP 10-302
T03
EPD 10-102
LAN a GVN via EPD a SRV_AP CTN140
GVN trans-regional OTT varios segmentos internet CTN340
LAN a GVN via EPD a SRV_AP CTN140
BW, Δt = A ms Pérdida de Paquetes
BW, Δt = B ms, Pérdida de Paquetes
BW, Δt = C ms, Pérdida de Paquetes
GVN Capa Tres GVN10--3
Registro BW y Tráfico 10-118
Probador túneles (EPD) 10-112
Gestor Conectividad 10-180
Probador túneles (AP) 10-312
Registro BW y Tráfico 10-318
GVN Capa Dos GVN10--2
Enrutamiento inteligente avanzado (ASR) 10-228
Gestor túneles 10-110
Gestor API 10-102
Mecanismo disponibilidad servidor 10-222
Analizador BW y tráfico 10-258
Análisis conectividad 10-288
Gt.enrutamiento y pares 10-106
Otros módulos del sistema 10-138
Gestor conectividad 10-180
GVN Capa Uno GVN10--1
Gt. capa física + probadores 10-118
Constructor túneles + enrutamiento 10-228
Monitor seguridad FW 10-440
Otros módulos de red 10-438
BW, Δt = X ms Pérdida de Paquetes
BW, Δt = W ms, Pérdida de Paquetes
BW, Δt = Y ms, Pérdida de Paquetes
Internet local CPT140
Internet trans-regional CPT340
Internet local CPT240
P01 P02 P03 P04 P05 P06 P07 P08 P09 P10 P11 P12 P13

FIG. 10

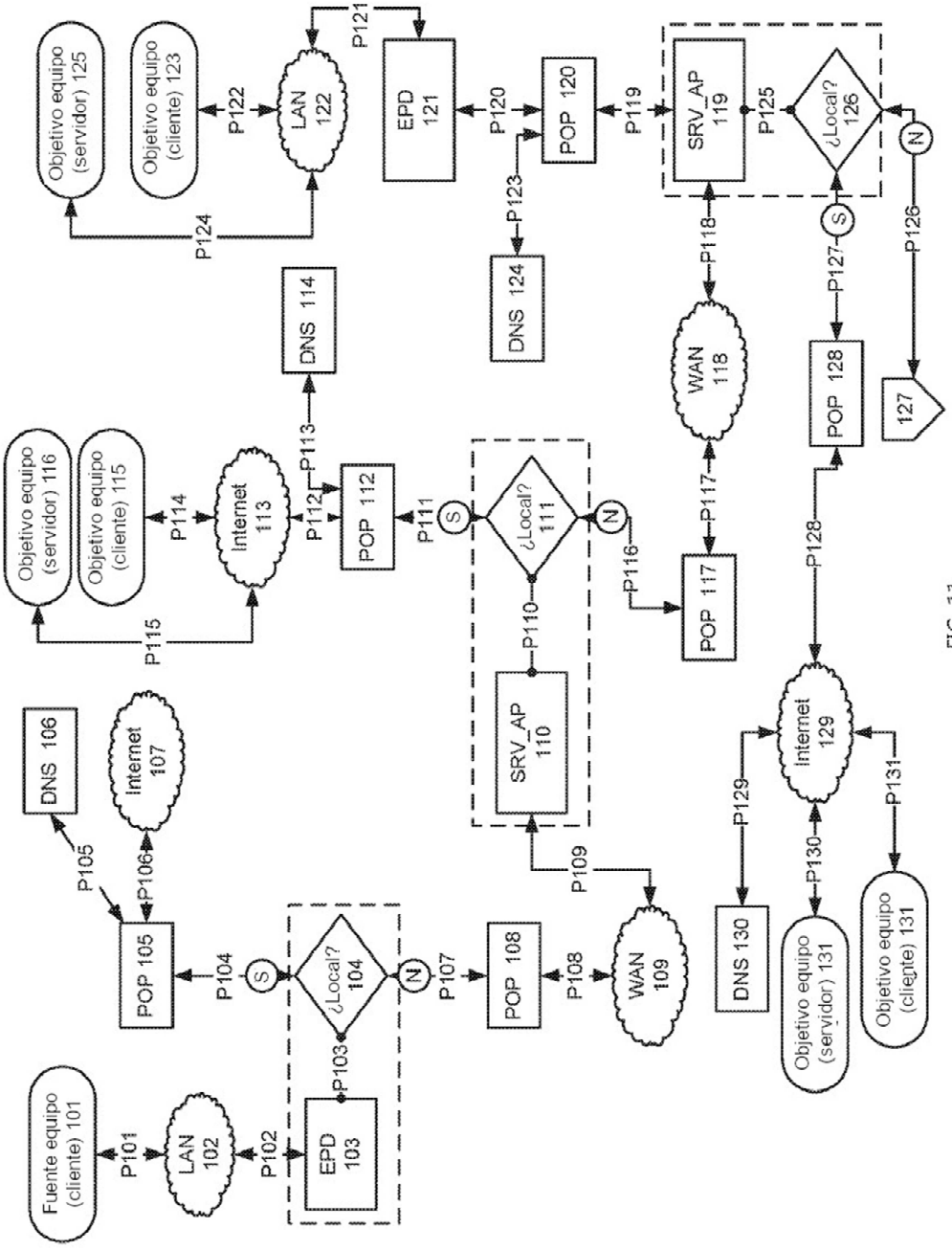
Fuente equipo (cliente) 101
P101
LAN 102
P102
EPD 103
P103
¿Local? 104
P104
S
N
POP 105
P105
DNS 106
P106
Internet 107
P107
POP 108
P108
WAN 109
P109
SRV_AP 110
P110
¿Local? 111
P111
S
N
POP 112
P112
P113
DNS 114
P114
Internet 113
P115
Objetivo equipo (servidor) 116
Objetivo equipo (cliente) 115
P116
POP 117
P117
WAN 118
P118
SRV_AP 119
P119
POP 120
P120
P123
DNS 124
EPD 121
P121
LAN 122
P122
P124
Objetivo equipo (servidor) 125
Objetivo equipo (cliente) 123
P125
¿Local? 126
S
N
P127
POP 128
P128
Internet 129
P129
DNS 130
P130
Objetivo equipo (servidor) 131
P131
Objetivo equipo (cliente) 131
P126
127

FIG. 11

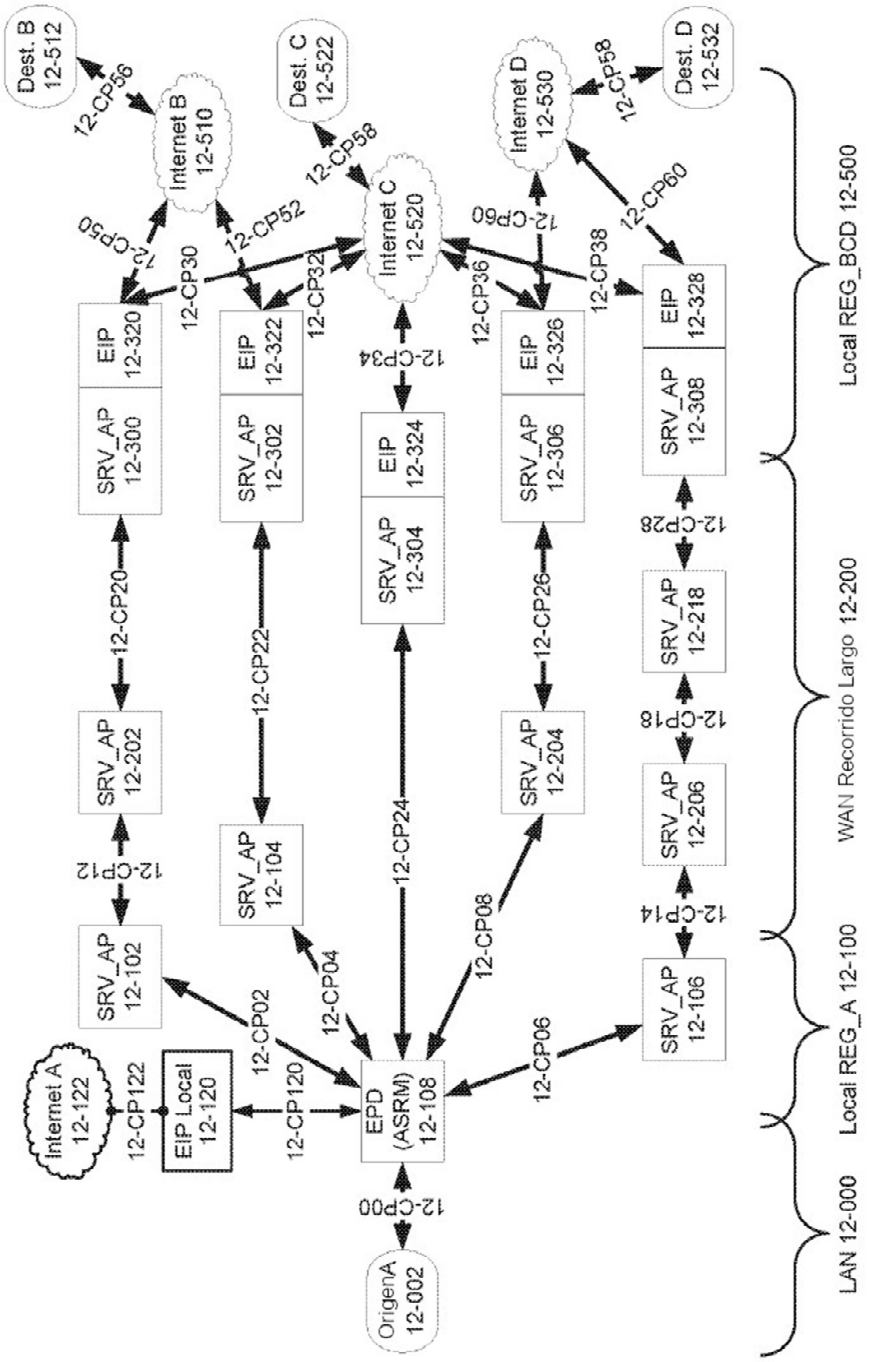
Dest. B 12-512
Dest. C 12-522
Dest. D 12-532
Internet A 12-122
Internet B 12-510
Internet C 12-520
Internet D 12-530
EIP Local 12-120
EPD (ASRM) 12-108
OrigenA 12-002
SRV_AP 12-102
SRV_AP 12-104
SRV_AP 12-106
SRV_AP 12-202
SRV_AP 12-204
SRV_AP 12-206
SRV_AP 12-218
SRV_AP 12-300
SRV_AP 12-302
SRV_AP 12-304
SRV_AP 12-306
SRV_AP 12-308
EIP 12-320
EIP 12-322
EIP 12-324
EIP 12-326
EIP 12-328
12-CP00
12-CP02
12-CP04
12-CP06
12-CP08
12-CP12
12-CP14
12-CP18
12-CP20
12-CP22
12-CP24
12-CP26
12-CP28
12-CP30
12-CP32
12-CP34
12-CP36
12-CP38
12-CP50
12-CP52
12-CP56
12-CP58
12-CP60
12-CP120
12-CP122
LAN 12-000
Local REG_A 12-100
WAN Recorrido Largo 12-200
Local REG_BCD 12-500

FIG. 12

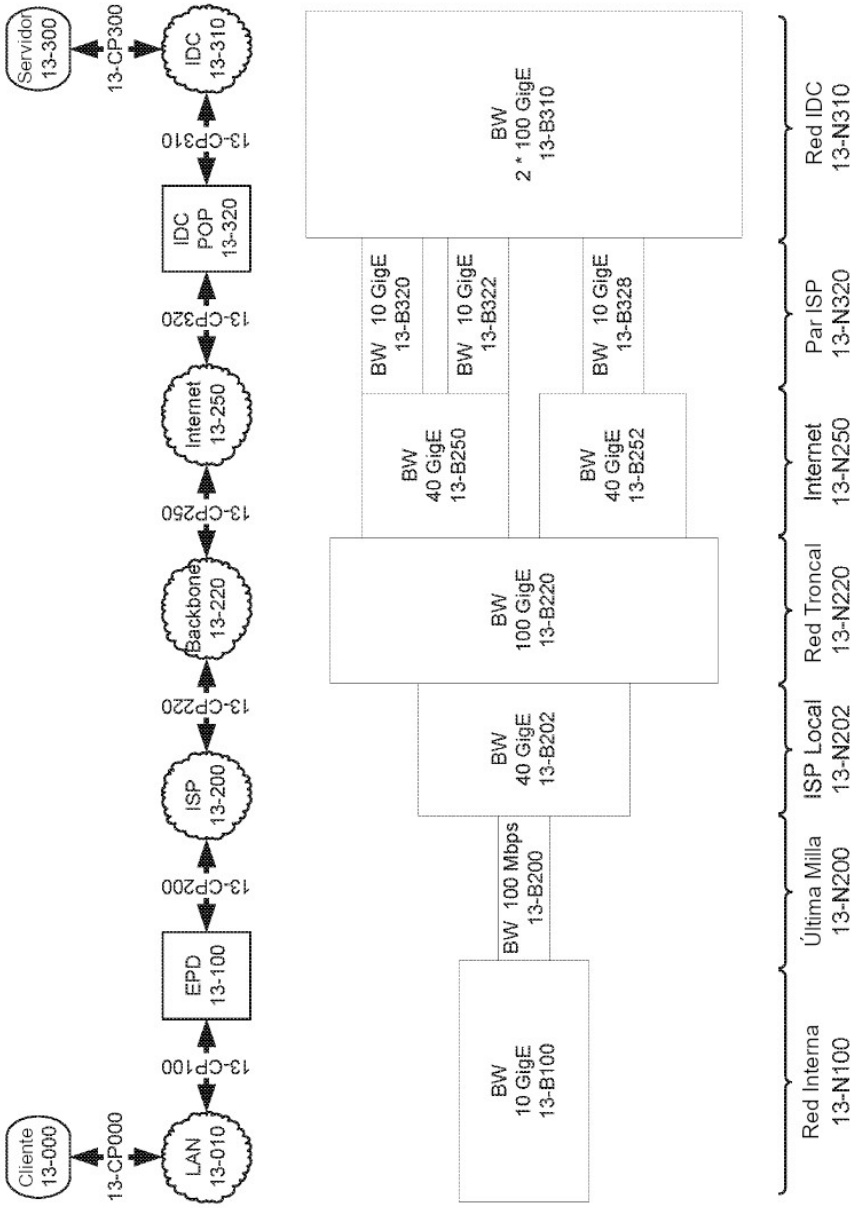
Cliente 13-000
13-CP000
LAN 13-010
13-CP100
EPD 13-100
13-CP200
ISP 13-200
13-CP220
Backbone 13-220
13-CP250
Internet 13-250
13-CP320
IDC POP 13-320
13-CP310
IDC 13-310
13-CP300
Servidor 13-300
BW 10 GigE 13-B100
BW 100 Mbps 13-B200
BW 40 GigE 13-B202
BW 100 GigE 13-B220
BW 40 GigE 13-B250
BW 40 GigE 13-B252
BW 10 GigE 13-B320
BW 10 GigE 13-B322
BW 10 GigE 13-B328
BW 2 * 100 GigE 13-B310
Red Interna 13-N100
Última Milla 13-N200
ISP Local 13-N202
Red Troncal 13-N220
Internet 13-N250
Par ISP 13-N320
Red IDC 13-N310

FIG. 13

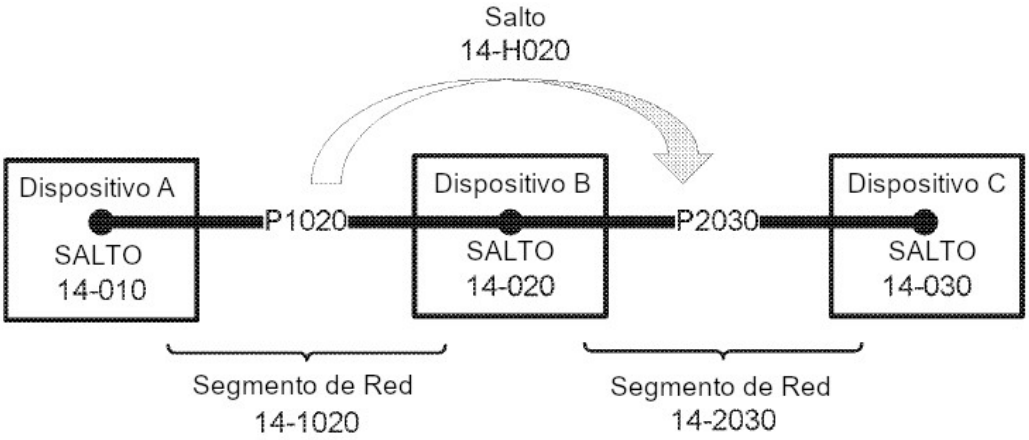
Salto
14-H020
Dispositivo A
SALTO
14-010
P1020
Dispositivo B
SALTO
14-020
P2030
Dispositivo C
SALTO
14-030
Segmento de Red
14-1020
Segmento de Red
14-2030

FIG. 14

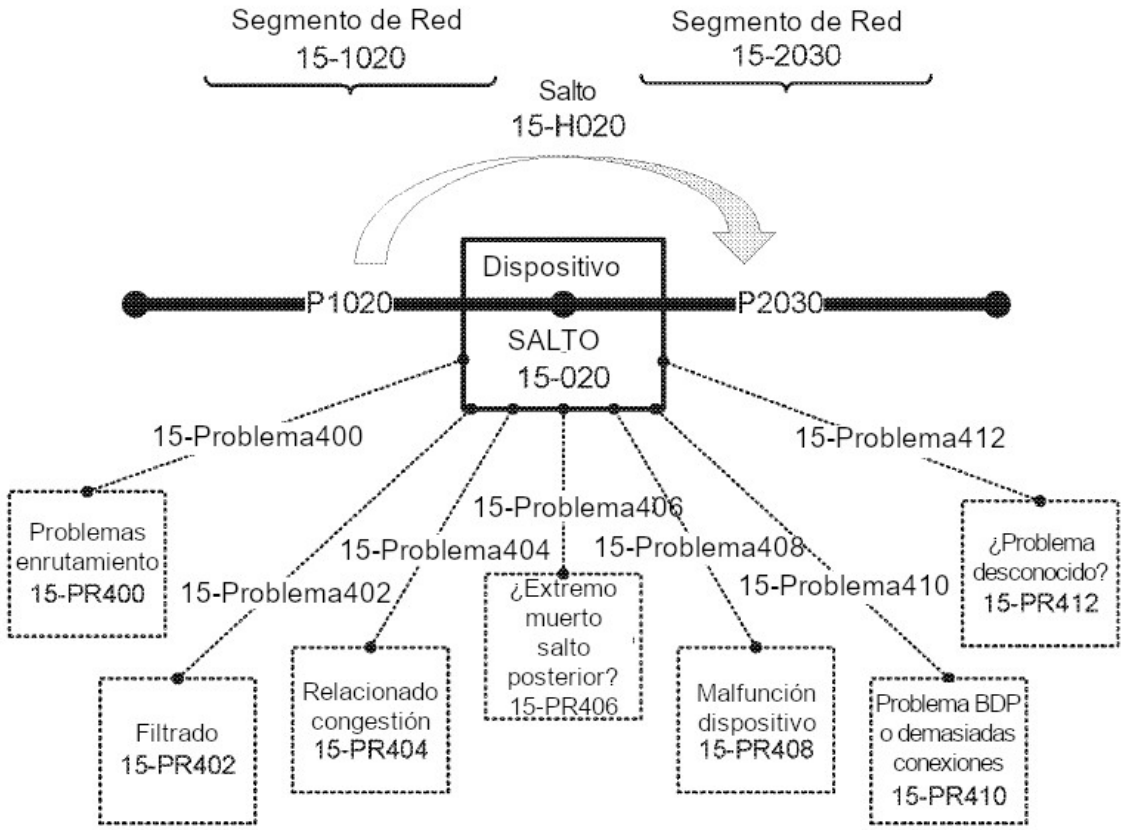
Segmento de Red
15-1020
Segmento de Red
15-2030
Salto
15-H020
Dispositivo
P1020
P2030
SALTO
15-020
15-Problema400
15-Problema412
15-Problema406
15-Problema404
15-Problema408
15-Problema402
15-Problema410
Problemas enrutamiento
15-PR400
¿Problema desconocido?
15-PR412
¿Extremo muerto salto posterior?
15-PR406
Filtrado
15-PR402
Relacionado congestión
15-PR404
Malfunción dispositivo
15-PR408
Problema BDP o demasiadas conexiones
15-PR410

FIG. 15

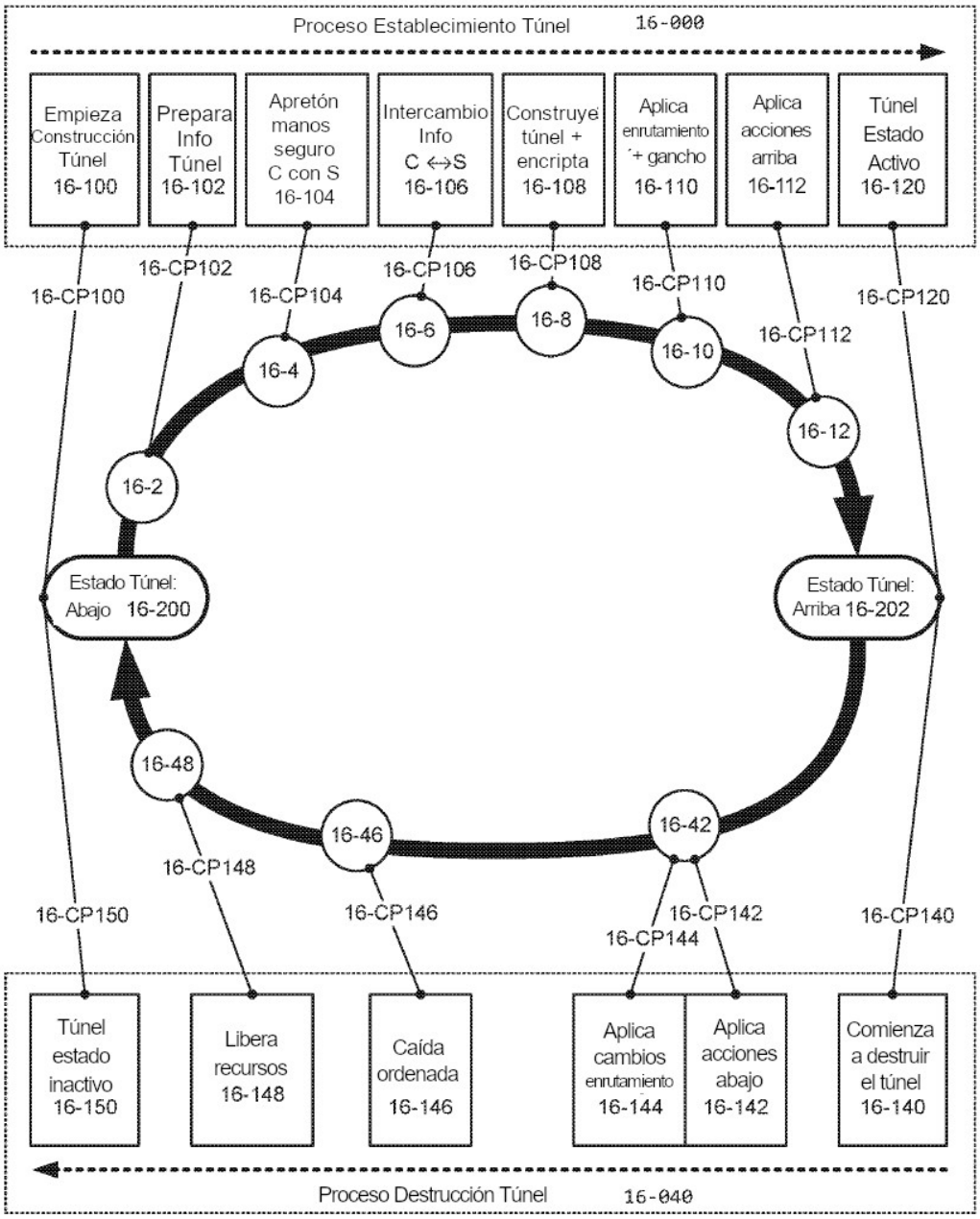
Proceso Establecimiento Túnel 16-000
Empieza Construcción Túnel 16-100
Prepara Info Túnel 16-102
Apretón manos seguro C con S 16-104
Intercambio Info C ↔S 16-106
Construye túnel + encripta 16-108
Aplica enrutamiento + gancho 16-110
Aplica acciones arriba 16-112
Túnel Estado Activo 16-120
16-CP100
16-CP102
16-CP104
16-CP106
16-CP108
16-CP110
16-CP112
16-CP120
16-2
16-4
16-6
16-8
16-10
16-12
Estado Túnel: Abajo 16-200
Estado Túnel: Arriba 16-202
16-48
16-46
16-42
16-CP148
16-CP150
16-CP146
16-CP144
16-CP142
16-CP140
Túnel estado inactivo 16-150
Libera recursos 16-148
Caída ordenada 16-146
Aplica cambios enrutamiento 16-144
Aplica acciones abajo 16-142
Comienza a destruir el túnel 16-140
Proceso Destrucción Túnel 16-040

FIG. 16

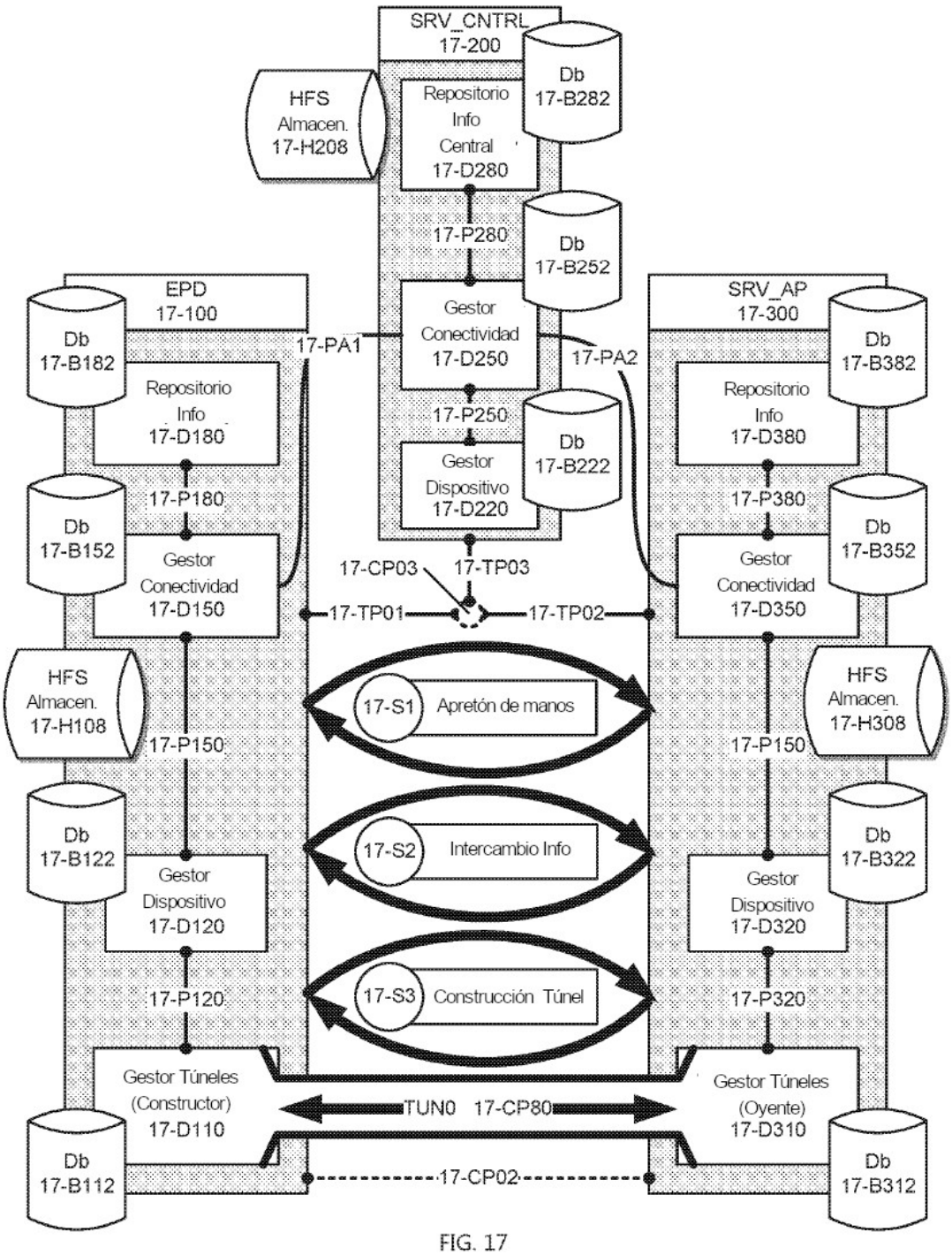
SRV_CNTRL
17-200
Db
17-B282
HFS
Almacen.
17-H208
Repositorio
Info
Central
17-D280
17-P280
Db
17-B252
Gestor
Conectividad
17-D250
17-PA1
17-PA2
17-P250
Db
17-B222
Gestor
Dispositivo
17-D220
EPD
17-100
Db
17-B182
Repositorio
Info
17-D180
17-P180
Db
17-B152
Gestor
Conectividad
17-D150
17-CP03
17-TP03
17-TP01
17-TP02
HFS
Almacen.
17-H108
17-P150
Db
17-B122
Gestor
Dispositivo
17-D120
17-P120
Gestor Túneles
(Constructor)
17-D110
Db
17-B112
SRV_AP
17-300
Db
17-B382
Repositorio
Info
17-D380
17-P380
Db
17-B352
Gestor
Conectividad
17-D350
HFS
Almacen.
17-H308
17-P150
Db
17-B322
Gestor
Dispositivo
17-D320
17-P320
Gestor Túneles
(Oyente)
17-D310
Db
17-B312
17-S1
Apretón de manos
17-S2
Intercambio Info
17-S3
Construcción Túnel
TUN0
17-CP80
17-CP02

FIG. 17

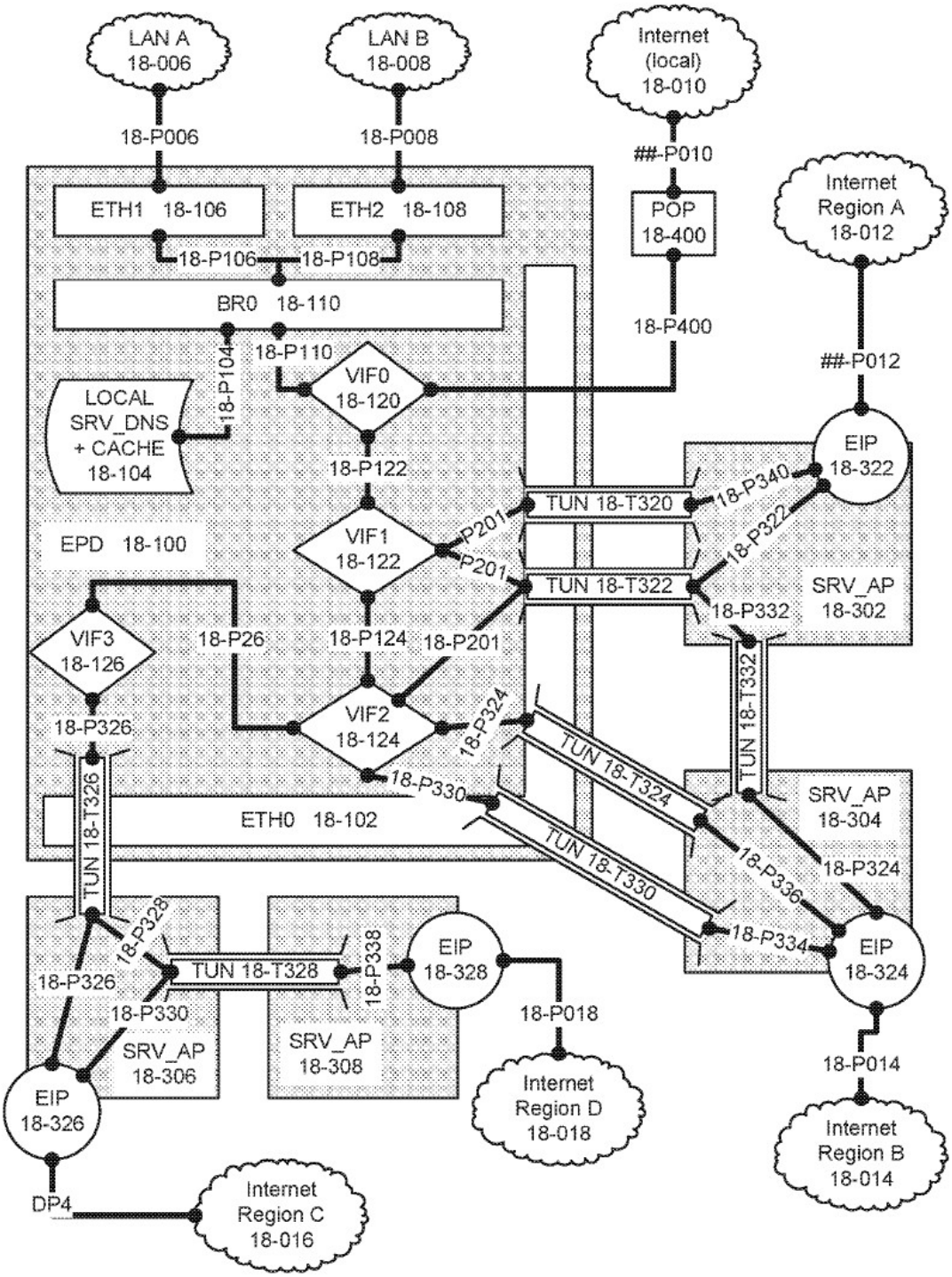
LAN A
18-006
LAN B
18-008
Internet
(local)
18-010
18-P006
18-P008
##-P010
ETH1 18-106
ETH2 18-108
POP
18-400
Internet
Region A
18-012
18-P106
18-P108
BR0 18-110
18-P400
18-P104
18-P110
VIF0
18-120
##-P012
LOCAL
SRV_DNS
+ CACHE
18-104
EIP
18-322
18-P122
18-P340
TUN 18-T320
EPD 18-100
VIF1
18-122
P201
18-P322
P201
TUN 18-T322
SRV_AP
18-302
VIF3
18-126
18-P26
18-P124
18-P201
18-P332
TUN 18-T332
18-P326
VIF2
18-124
18-P324
TUN 18-T324
18-P330
SRV_AP
18-304
ETH0 18-102
TUN 18-T330
TUN 18-T326
18-P336
18-P324
18-P328
18-P334
EIP
18-324
EIP
18-328
18-P338
18-P326
TUN 18-T328
18-P018
18-P330
SRV_AP
18-308
18-P014
SRV_AP
18-306
Internet
Region D
18-018
EIP
18-326
Internet
Region B
18-014
DP4
Internet
Region C
18-016

FIG. 18

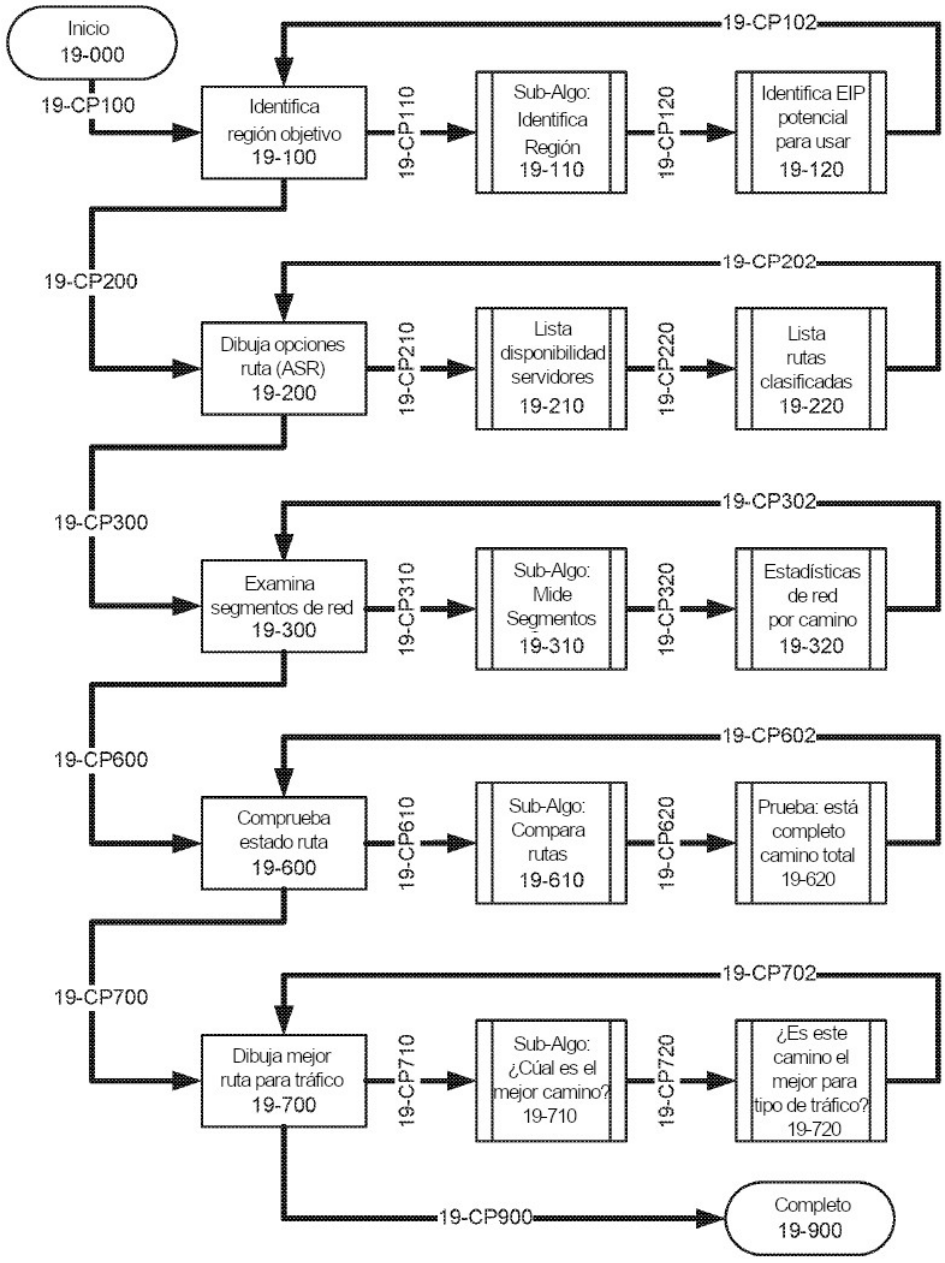
Inicio
19-000
19-CP100
Identifica
región objetivo
19-100
19-CP110
Sub-Algo:
Identifica
Región
19-110
19-CP120
Identifica EIP
potencial
para usar
19-120
19-CP102
19-CP200
Dibuja opciones
ruta (ASR)
19-200
19-CP210
Lista
disponibilidad
servidores
19-210
19-CP220
Lista
rutas
clasificadas
19-220
19-CP202
19-CP300
Examina
segmentos de red
19-300
19-CP310
Sub-Algo:
Mide
Segmentos
19-310
19-CP320
Estadísticas
de red
por camino
19-320
19-CP302
19-CP600
Comprueba
estado ruta
19-600
19-CP610
Sub-Algo:
Compara
rutas
19-610
19-CP620
Prueba: está
completo
camino total
19-620
19-CP602
19-CP700
Dibuja mejor
ruta para tráfico
19-700
19-CP710
Sub-Algo:
¿Cúal es el
mejor camino?
19-710
19-CP720
¿Es este
camino el
mejor para
tipo de tráfico?
19-720
19-CP702
19-CP900
Completo
19-900

FIG. 19

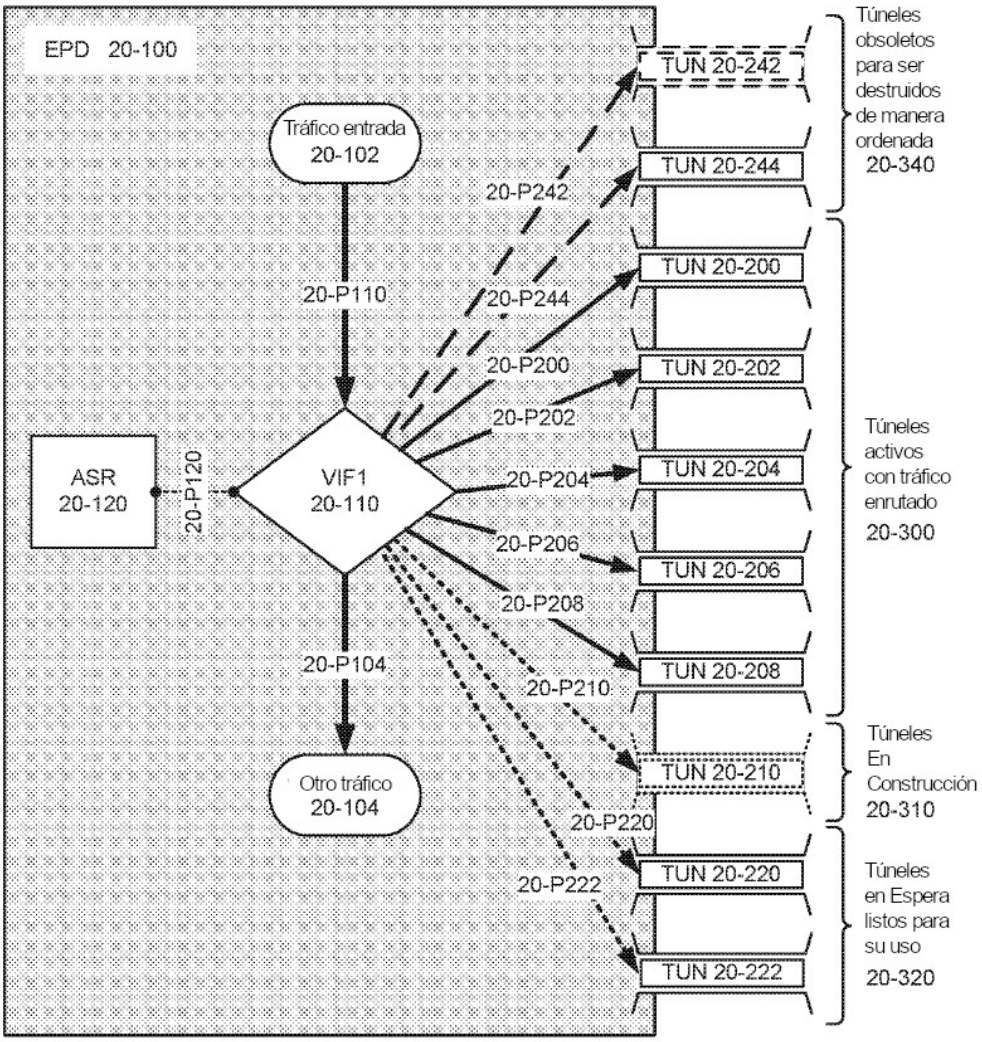
EPD 20-100
Tráfico entrada
20-102
20-P110
ASR
20-120
20-P120
VIF1
20-110
20-P104
Otro tráfico
20-104
20-P242
20-P244
20-P200
20-P202
20-P204
20-P206
20-P208
20-P210
20-P220
20-P222
TUN 20-242
TUN 20-244
TUN 20-200
TUN 20-202
TUN 20-204
TUN 20-206
TUN 20-208
TUN 20-210
TUN 20-220
TUN 20-222
Túneles obsoletos para ser destruidos de manera ordenada
20-340
Túneles activos con tráfico enrutado
20-300
Túneles En Construcción
20-310
Túneles en Espera listos para su uso
20-320

FIG. 20

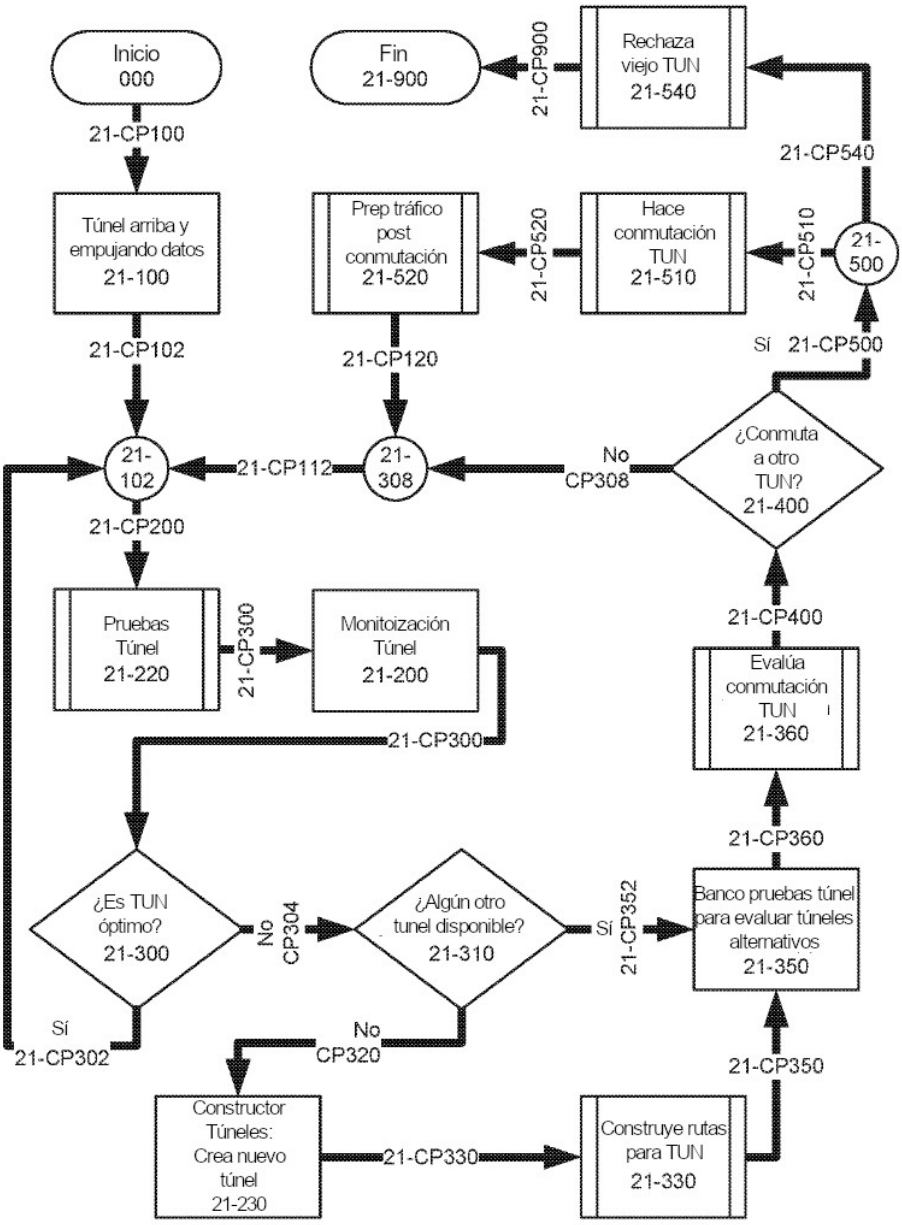
Inicio
000
21-CP100
Túnel arriba y empujando datos
21-100
21-CP102
21-102
21-CP200
Pruebas Túnel
21-220
21-CP300
Monitoización Túnel
21-200
21-CP300
¿Es TUN óptimo?
21-300
No
CP304
¿Algún otro tunel disponible?
21-310
Sí
21-CP352
Banco pruebas túnel para evaluar túneles alternativos
21-350
21-CP350
Construye rutas para TUN
21-330
21-CP330
Constructor Túneles: Crea nuevo túnel
21-230
No
CP320
Sí
21-CP302
21-CP112
21-308
21-CP120
Prep tráfico post conmutación
21-520
21-CP520
Hace conmutación TUN
21-510
21-CP510
21-500
21-CP540
Rechaza viejo TUN
21-540
21-CP900
Fin
21-900
Sí 21-CP500
¿Conmuta a otro TUN?
21-400
No
CP308
21-CP400
Evalúa conmutación TUN
21-360
21-CP360

FIG. 21

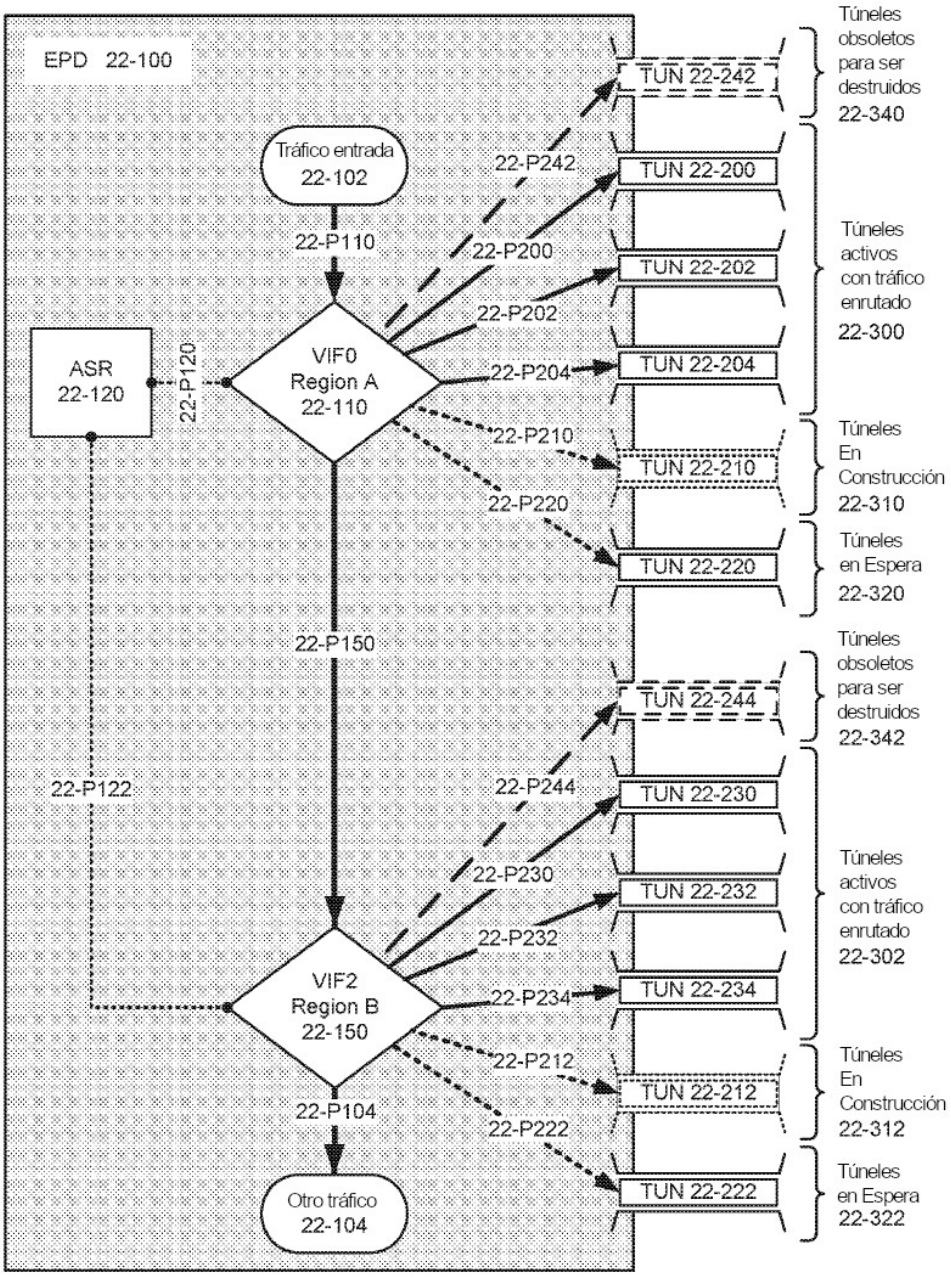
EPD 22-100
Tráfico entrada
22-102
22-P110
ASR
22-120
22-P120
VIF0
Region A
22-110
22-P150
22-P122
VIF2
Region B
22-150
22-P104
Otro tráfico
22-104
22-P242
22-P200
22-P202
22-P204
22-P210
22-P220
22-P244
22-P230
22-P232
22-P234
22-P212
22-P222
TUN 22-242
TUN 22-200
TUN 22-202
TUN 22-204
TUN 22-210
TUN 22-220
TUN 22-244
TUN 22-230
TUN 22-232
TUN 22-234
TUN 22-212
TUN 22-222
Túneles obsoletos para ser destruidos 22-340
Túneles activos con tráfico enrutado 22-300
Túneles En Construcción 22-310
Túneles en Espera 22-320
Túneles obsoletos para ser destruidos 22-342
Túneles activos con tráfico enrutado 22-302
Túneles En Construcción 22-312
Túneles en Espera 22-322

FIG. 22

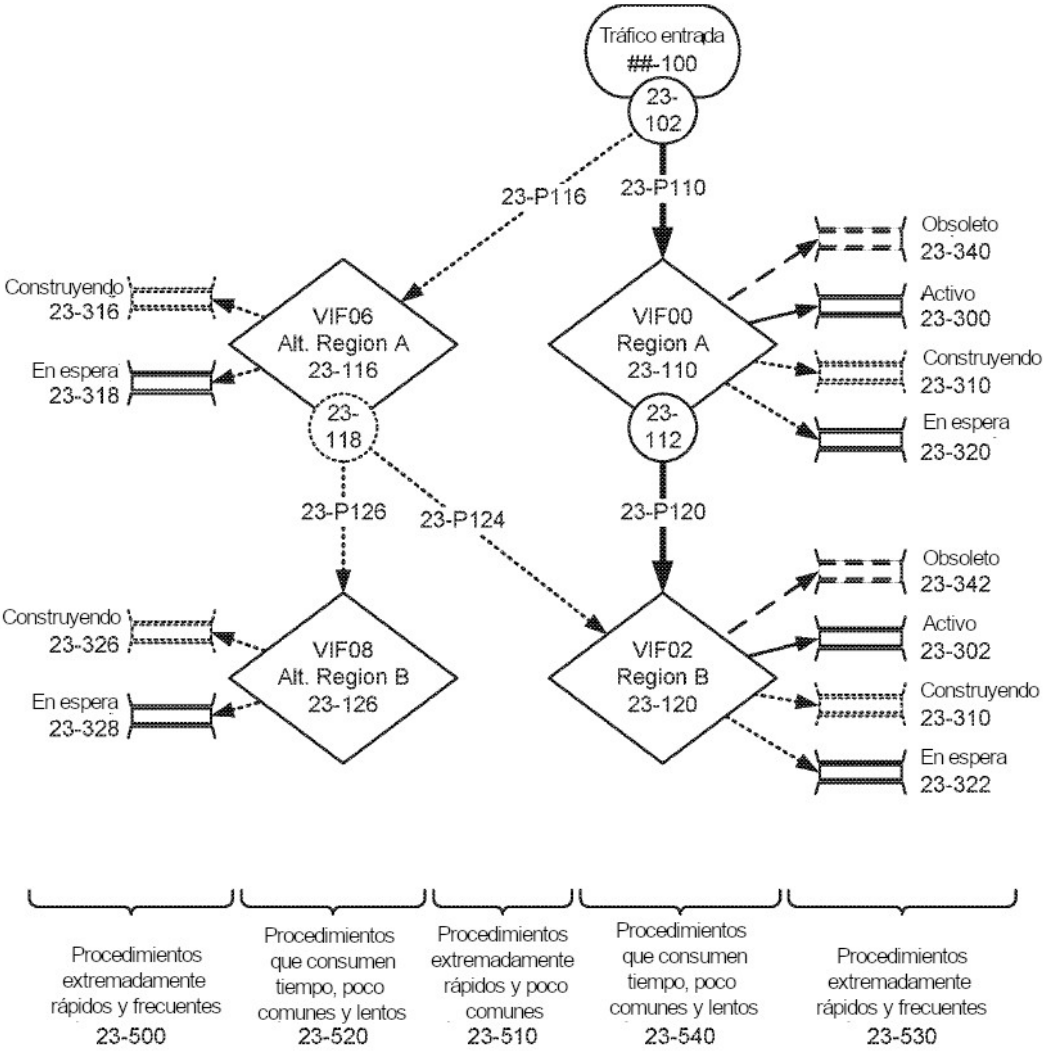
Tráfico entrada
##-100
23-102
23-P116
23-P110
Construyendo
23-316
En espera
23-318
VIF06
Alt. Region A
23-116
23-118
VIF00
Region A
23-110
23-112
Obsoleto
23-340
Activo
23-300
Construyendo
23-310
En espera
23-320
23-P126
23-P124
23-P120
Construyendo
23-326
En espera
23-328
VIF08
Alt. Region B
23-126
VIF02
Region B
23-120
Obsoleto
23-342
Activo
23-302
Construyendo
23-310
En espera
23-322
Procedimientos extremadamente rápidos y frecuentes
23-500
Procedimientos que consumen tiempo, poco comunes y lentos
23-520
Procedimientos extremadamente rápidos y poco comunes
23-510
Procedimientos que consumen tiempo, poco comunes y lentos
23-540
Procedimientos extremadamente rápidos y frecuentes
23-530

FIG. 23

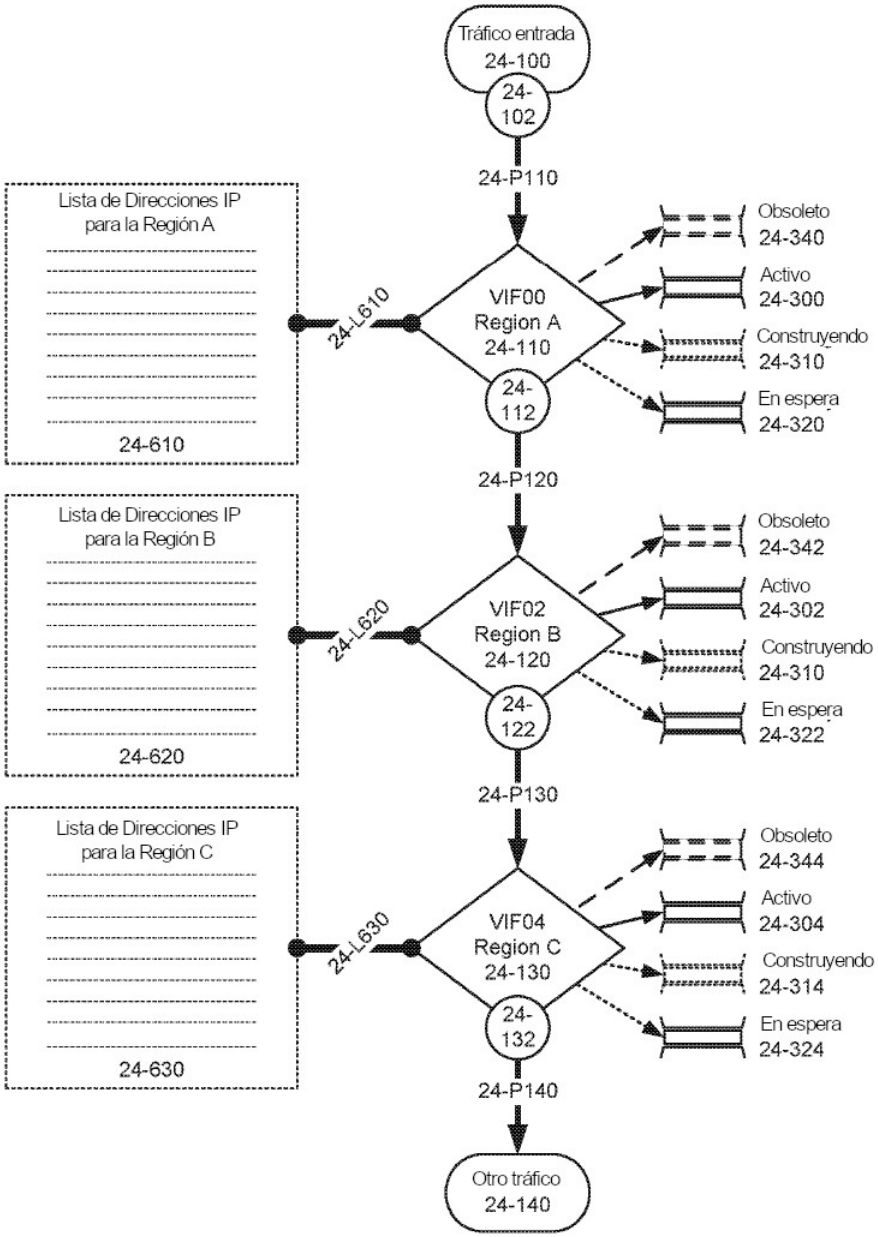
Tráfico entrada
24-100
24-102
24-P110
Lista de Direcciones IP para la Región A
24-610
24-L610
VIF00 Region A 24-110
24-112
Obsoleto 24-340
Activo 24-300
Construyendo 24-310
En espera 24-320
24-P120
Lista de Direcciones IP para la Región B
24-620
24-L620
VIF02 Region B 24-120
24-122
Obsoleto 24-342
Activo 24-302
Construyendo 24-310
En espera 24-322
24-P130
Lista de Direcciones IP para la Región C
24-630
24-L630
VIF04 Region C 24-130
24-132
Obsoleto 24-344
Activo 24-304
Construyendo 24-314
En espera 24-324
24-P140
Otro tráfico
24-140

FIG. 24

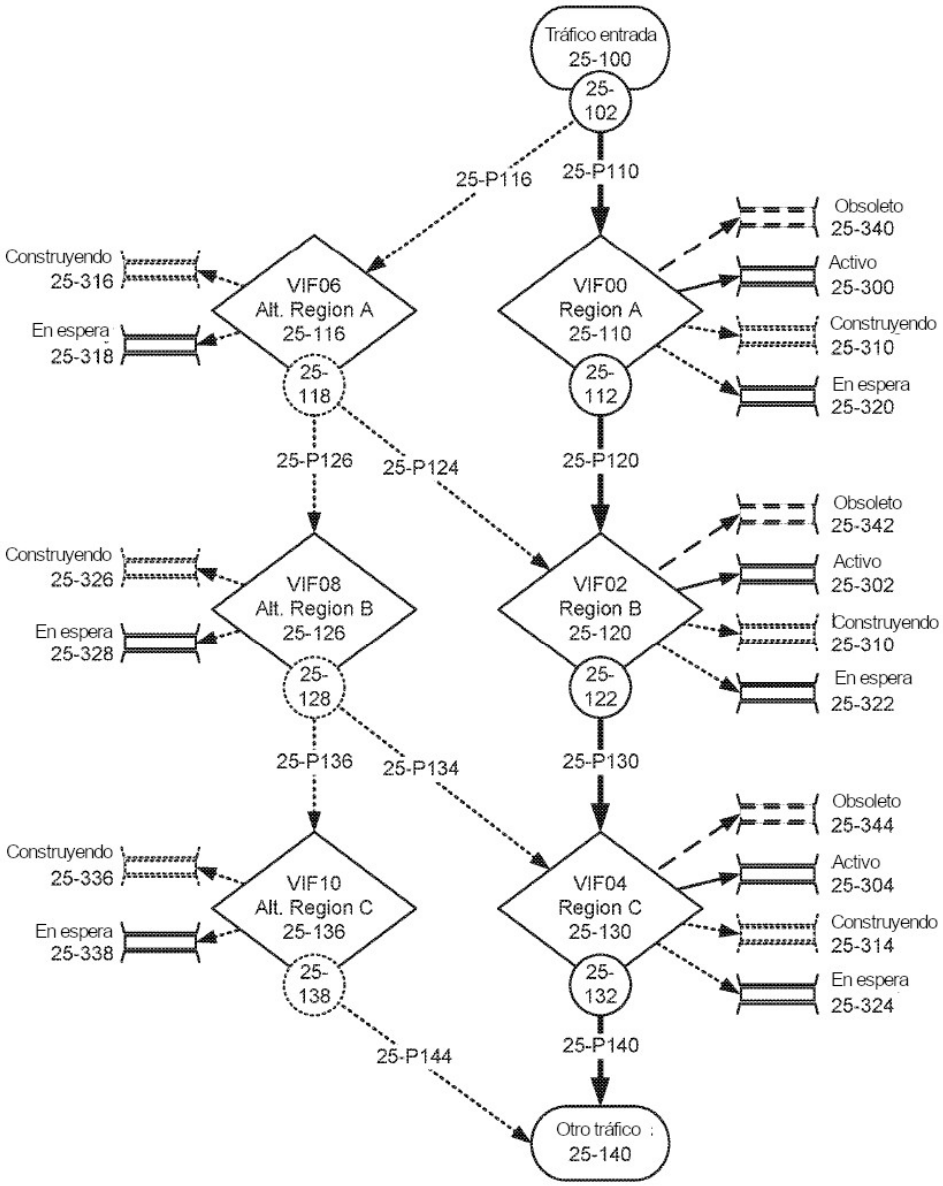
Tráfico entrada
25-100
25-102
25-P116
25-P110
Construyendo
25-316
En espera
25-318
VIF06
Alt. Region A
25-116
25-118
VIF00
Region A
25-110
25-112
Obsoleto
25-340
Activo
25-300
Construyendo
25-310
En espera
25-320
25-P126
25-P124
25-P120
Construyendo
25-326
En espera
25-328
VIF08
Alt. Region B
25-126
25-128
VIF02
Region B
25-120
25-122
Obsoleto
25-342
Activo
25-302
Construyendo
25-310
En espera
25-322
25-P136
25-P134
25-P130
Construyendo
25-336
En espera
25-338
VIF10
Alt. Region C
25-136
25-138
VIF04
Region C
25-130
25-132
Obsoleto
25-344
Activo
25-304
Construyendo
25-314
En espera
25-324
25-P144
25-P140
Otro tráfico
25-140

FIG. 25

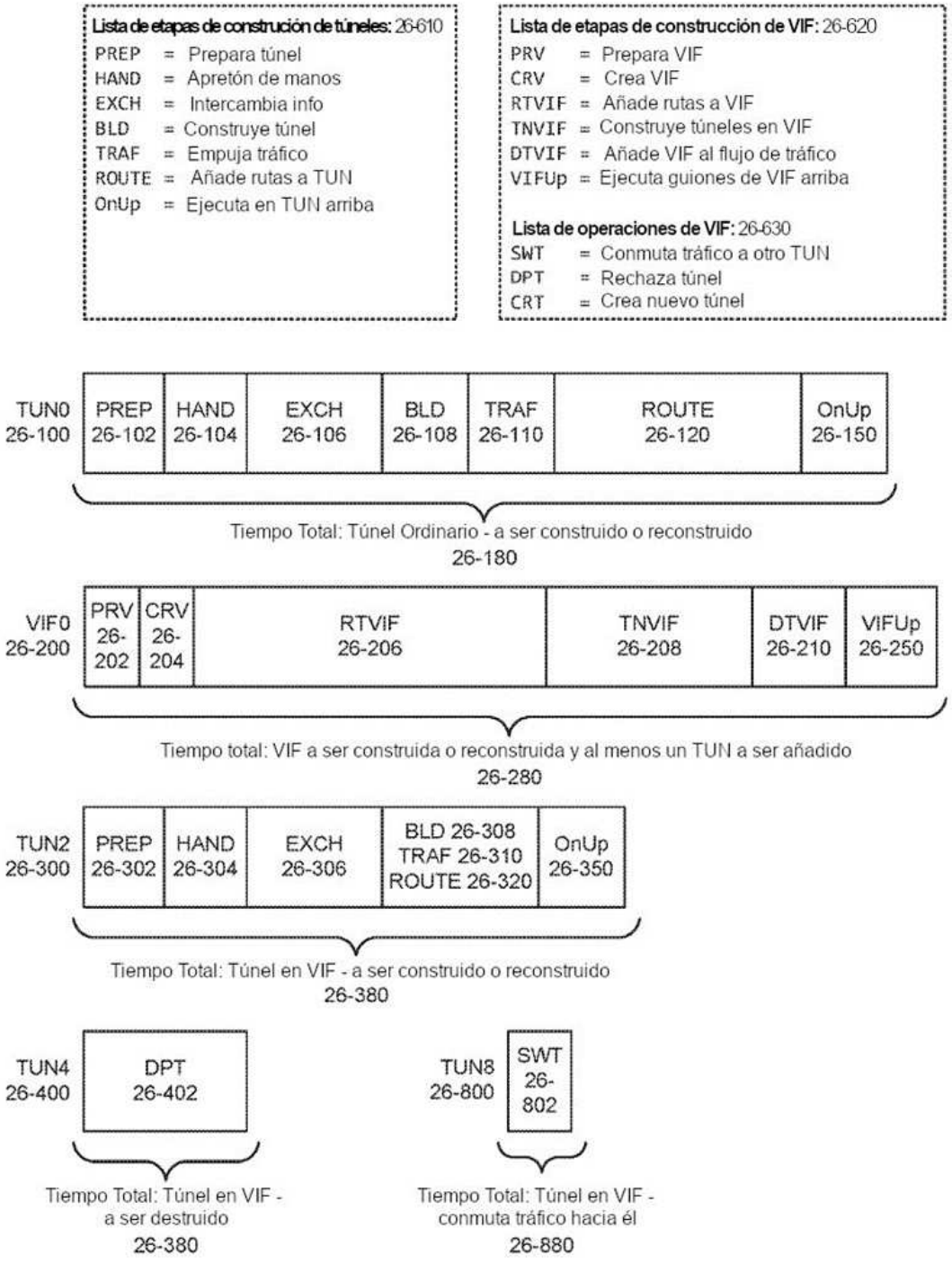
Lista de etapas de construción de túneles: 26-610
PREP = Prepara túnel
HAND = Apretón de manos
EXCH = Intercambia info
BLD = Construye túnel
TRAF = Empuja tráfico
ROUTE = Añade rutas a TUN
OnUp = Ejecuta en TUN arriba
Lista de etapas de construcción de VIF: 26-620
PRV = Prepara VIF
CRV = Crea VIF
RTVIF = Añade rutas a VIF
TNVIF = Construye túneles en VIF
DTVIF = Añade VIF al flujo de tráfico
VIFUp = Ejecuta guiones de VIF arriba
Lista de operaciones de VIF: 26-630
SWT = Conmuta tráfico a otro TUN
DPT = Rechaza túnel
CRT = Crea nuevo túnel
TUN0 26-100
PREP 26-102
HAND 26-104
EXCH 26-106
BLD 26-108
TRAF 26-110
ROUTE 26-120
OnUp 26-150
Tiempo Total: Túnel Ordinario - a ser construido o reconstruido 26-180
VIF0 26-200
PRV 26-202
CRV 26-204
RTVIF 26-206
TNVIF 26-208
DTVIF 26-210
VIFUp 26-250
Tiempo total: VIF a ser construida o reconstruida y al menos un TUN a ser añadido 26-280
TUN2 26-300
PREP 26-302
HAND 26-304
EXCH 26-306
BLD 26-308
TRAF 26-310
ROUTE 26-320
OnUp 26-350
Tiempo Total: Túnel en VIF - a ser construido o reconstruido 26-380
TUN4 26-400
DPT 26-402
Tiempo Total: Túnel en VIF - a ser destruido 26-380
TUN8 26-800
SWT 26-802
Tiempo Total: Túnel en VIF - conmuta tráfico hacia él 26-880

FIG. 26

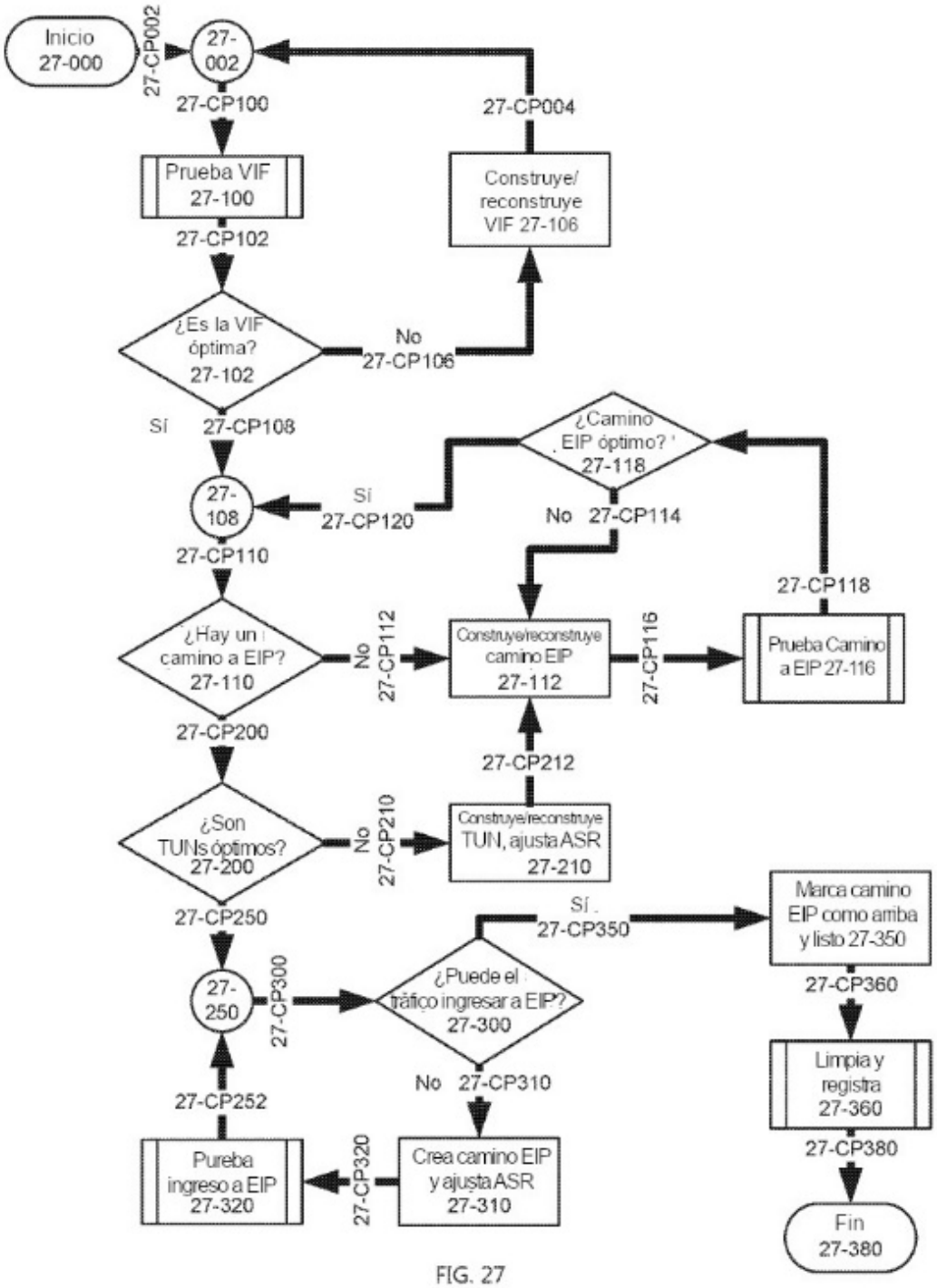
Inicio 27-000
27-CP002
27-002
27-CP100
Prueba VIF 27-100
27-CP102
¿Es la VIF óptima? 27-102
No
27-CP106
27-CP004
Construye/ reconstruye VIF 27-106
Sí
27-CP108
27-108
27-CP110
¿Hay un camino a EIP? 27-110
No
27-CP112
Construye/reconstruye camino EIP 27-112
27-CP116
Prueba Camino a EIP 27-116
27-CP118
¿Camino EIP óptimo? 27-118
Sí
27-CP120
No 27-CP114
27-CP200
¿Son TUNs óptimos? 27-200
No
27-CP210
Construye/reconstruye TUN, ajusta ASR 27-210
27-CP212
27-CP250
27-250
27-CP300
¿Puede el tráfico ingresar a EIP? 27-300
Sí
27-CP350
Marca camino EIP como arriba y listo 27-350
27-CP360
Limpia y registra 27-360
27-CP380
Fin 27-380
No 27-CP310
27-CP252
Pureba ingreso a EIP 27-320
27-CP320
Crea camino EIP y ajusta ASR 27-310

FIG. 27

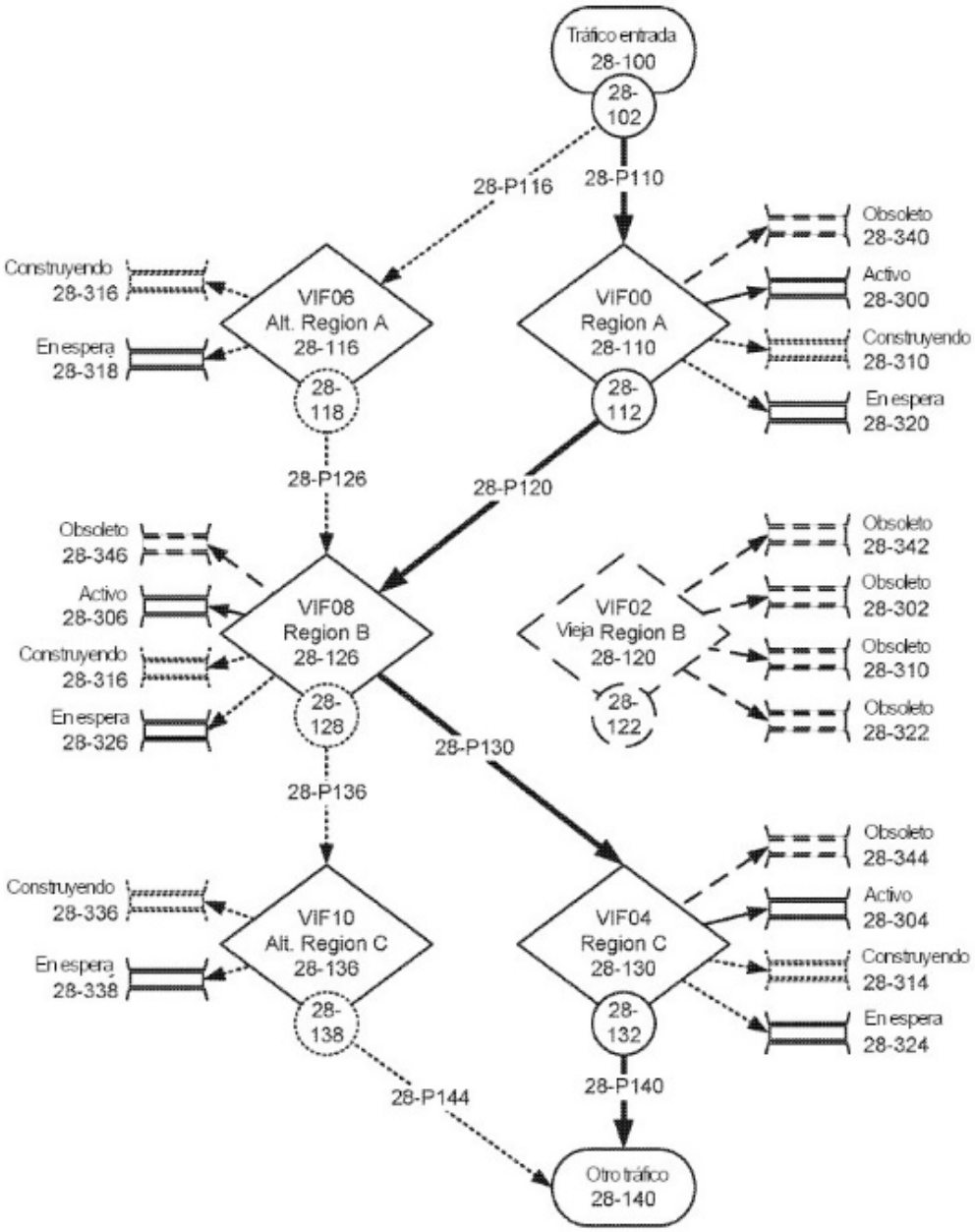
Tráfico entrada
28-100
28-102
28-P116
28-P110
Construyendo
28-316
En espera
28-318
VIF06
Alt. Region A
28-116
28-118
VIF00
Region A
28-110
28-112
Obsoleto
28-340
Activo
28-300
Construyendo
28-310
En espera
28-320
28-P126
28-P120
Obsoleto
28-346
Activo
28-306
Construyendo
28-316
En espera
28-326
VIF08
Region B
28-126
28-128
VIF02
Vieja Region B
28-120
28-122
Obsoleto
28-342
Obsoleto
28-302
Obsoleto
28-310
Obsoleto
28-322
28-P130
28-P136
Construyendo
28-336
En espera
28-338
VIF10
Alt. Region C
28-136
28-138
VIF04
Region C
28-130
28-132
Obsoleto
28-344
Activo
28-304
Construyendo
28-314
En espera
28-324
28-P140
28-P144
Otro tráfico
28-140

FIG. 28

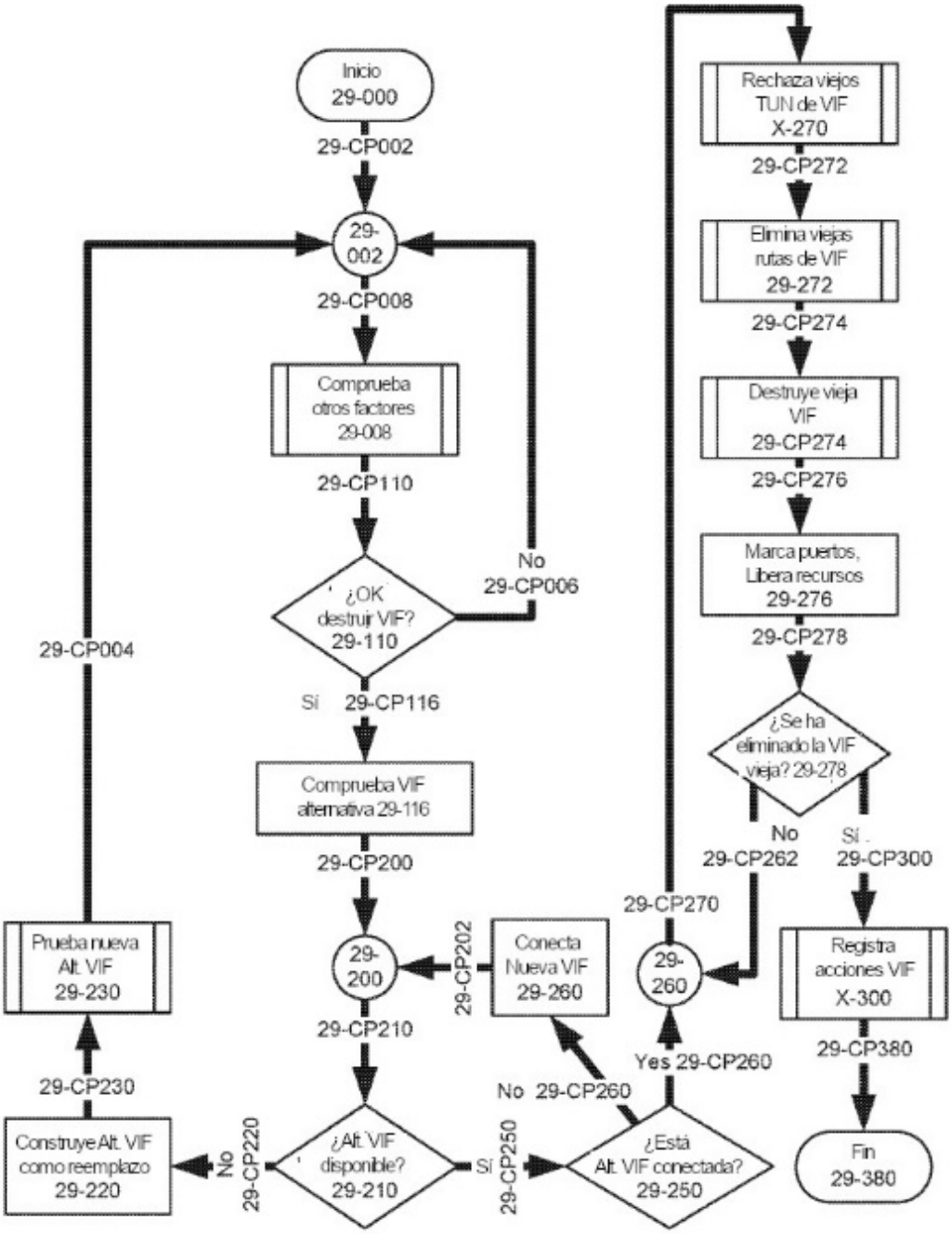
Inicio
29-000
29-CP002
29-002
29-CP008
Comprueba otros factores 29-008
29-CP110
¿OK destruir VIF? 29-110
No
29-CP006
29-CP004
Sí
29-CP116
Comprueba VIF alternativa 29-116
29-CP200
29-200
29-CP202
Conecta Nueva VIF 29-260
29-CP210
Prueba nueva Alt. VIF 29-230
29-CP230
Construye Alt. VIF como reemplazo 29-220
No
29-CP220
¿Alt. VIF disponible? 29-210
Sí
29-CP250
¿Está Alt. VIF conectada? 29-250
No 29-CP260
Yes 29-CP260
29-260
29-CP270
Rechaza viejos TUN de VIF X-270
29-CP272
Elimina viejas rutas de VIF 29-272
29-CP274
Destruye vieja VIF 29-274
29-CP276
Marca puertos, Libera recursos 29-276
29-CP278
¿Se ha eliminado la VIF vieja? 29-278
No
29-CP262
Sí
29-CP300
Registra acciones VIF X-300
29-CP380
Fin
29-380

FIG. 29

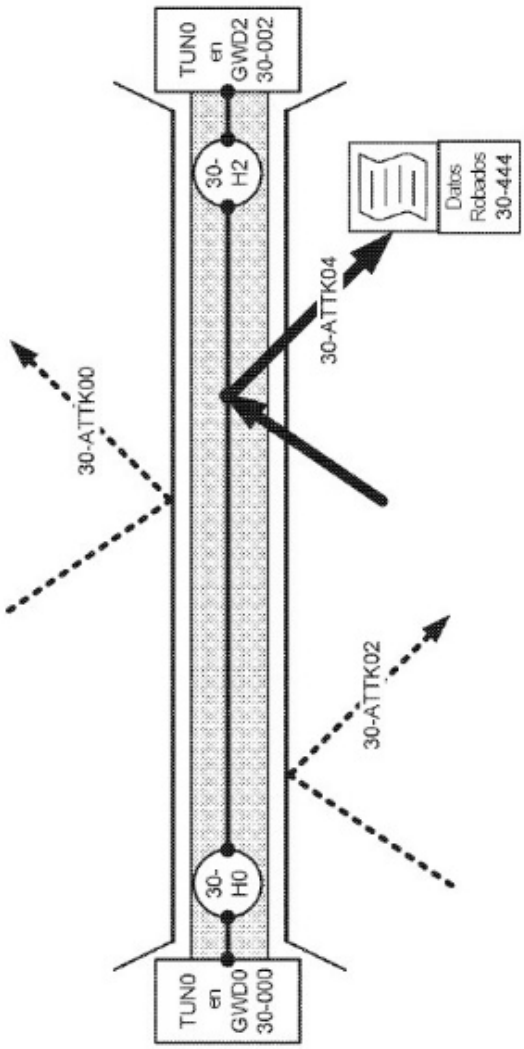
TUN0
en
GWD2
30-002
30-
H2
Datos
Robados
30-444
30-ATTK04
30-ATTK00
30-ATTK02
30-
H0
TUN0
en
GWD0
30-000

FIG. 30

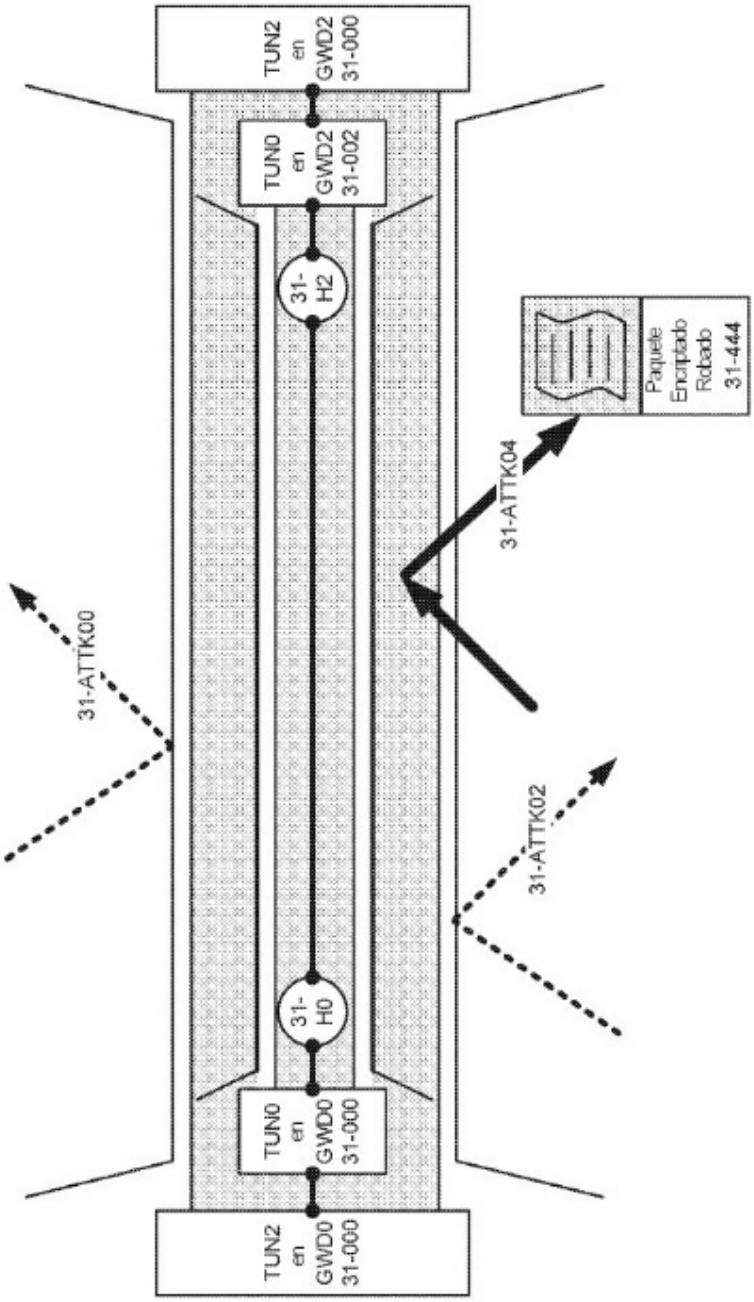
TUN2 en GWD2 31-000
TUN0 en GWD2 31-002
31-H2
Paquete Encriptado Robado 31-444
31-ATTK04
31-ATTK00
31-ATTK02
31-H0
TUN0 en GWD0 31-000
TUN2 en GWD0 31-000

FIG. 31

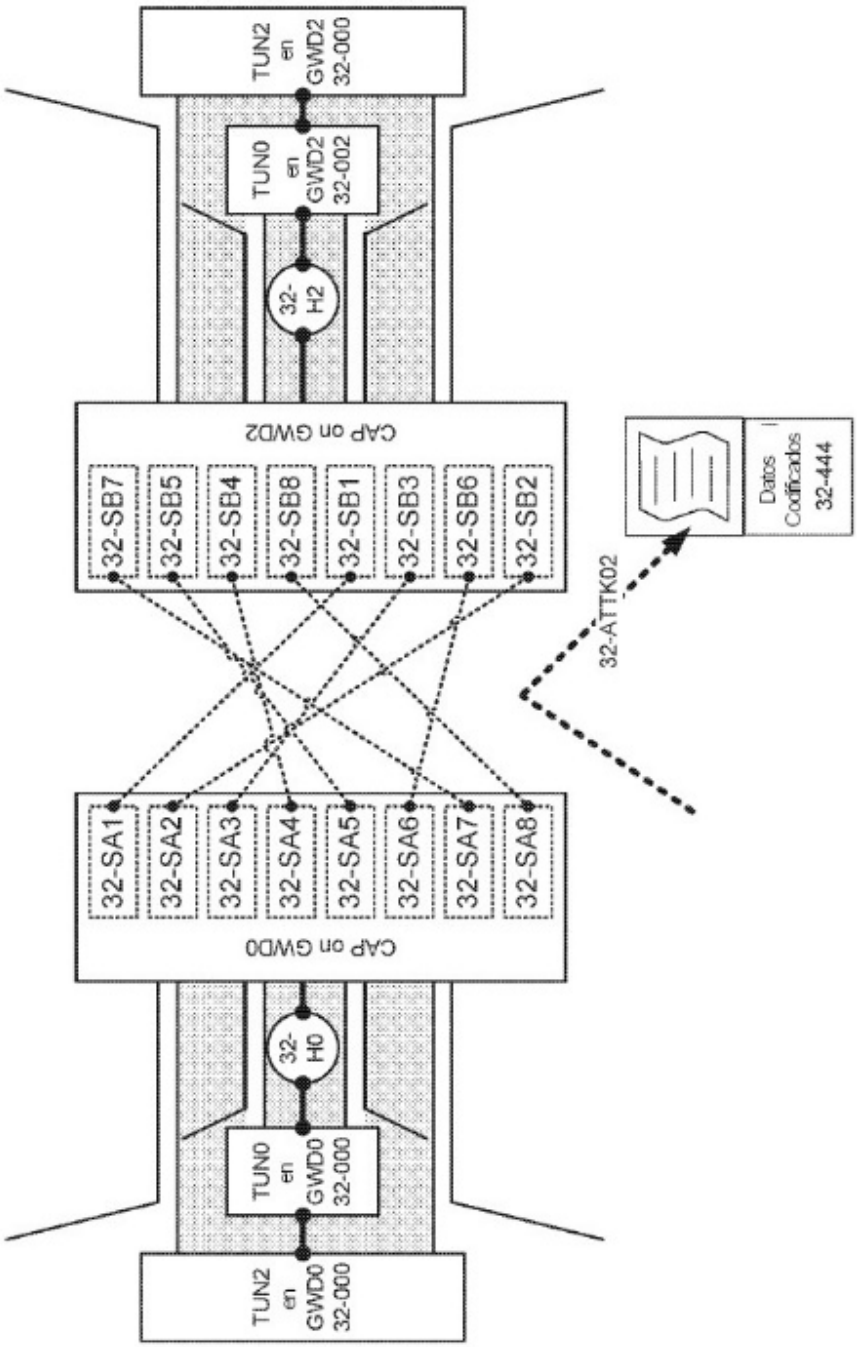
TUN2 en GWD2 32-000
TUN0 en GWD2 32-002
32-H2
CAP on GWD2
32-SB7
32-SB5
32-SB4
32-SB8
32-SB1
32-SB3
32-SB6
32-SB2
32-ATTK02
Datos Codificados 32-444
32-SA1
32-SA2
32-SA3
32-SA4
32-SA5
32-SA6
32-SA7
32-SA8
CAP on GWD0
32-H0
TUN0 en GWD0 32-000
TUN2 en GWD0 32-000

FIG. 32

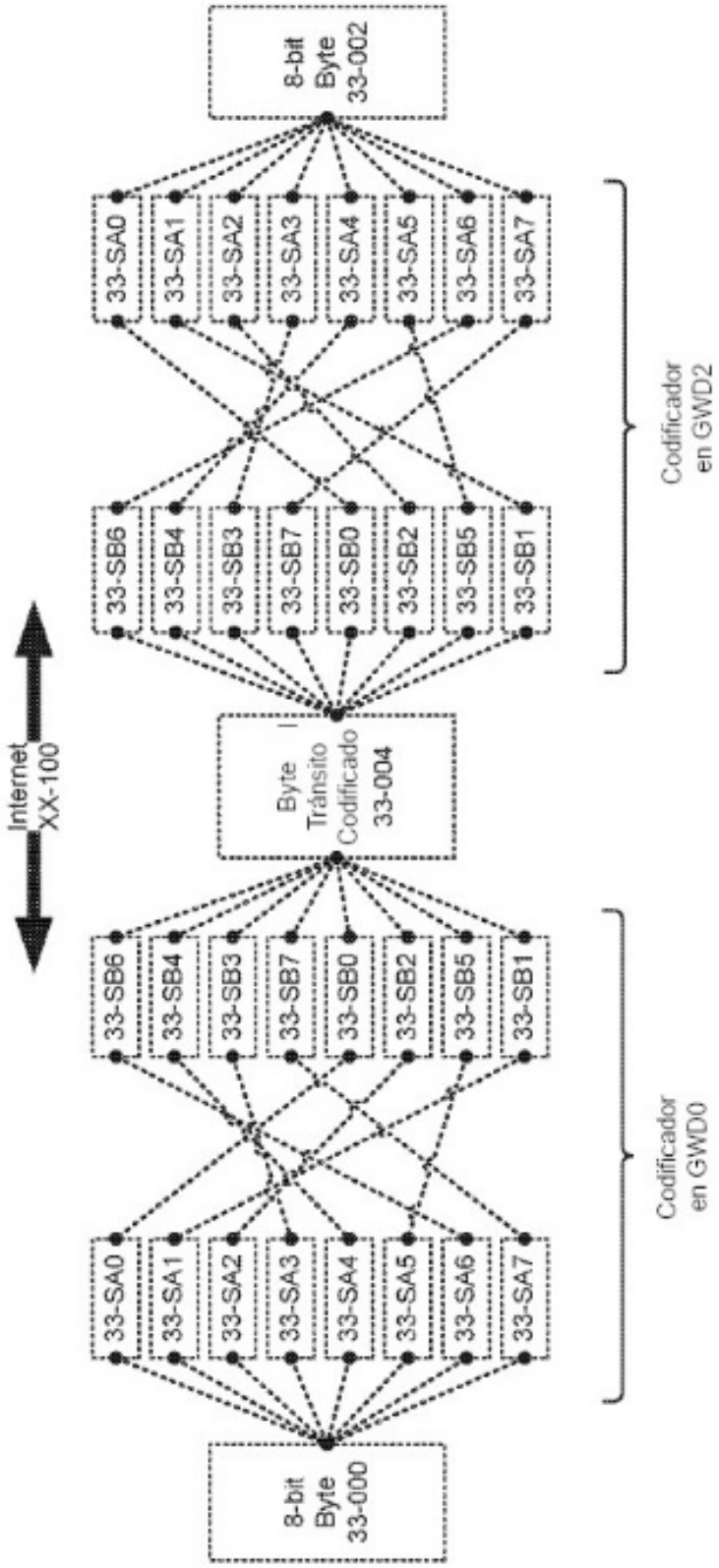
8-bit Byte 33-000
33-SA0
33-SA1
33-SA2
33-SA3
33-SA4
33-SA5
33-SA6
33-SA7
33-SB6
33-SB4
33-SB3
33-SB7
33-SB0
33-SB2
33-SB5
33-SB1
Codificador en GWD0
Byte Tránsito Codificado 33-004
Internet XX-100
33-SB6
33-SB4
33-SB3
33-SB7
33-SB0
33-SB2
33-SB5
33-SB1
33-SA0
33-SA1
33-SA2
33-SA3
33-SA4
33-SA5
33-SA6
33-SA7
Codificador en GWD2
8-bit Byte 33-002

FIG. 33

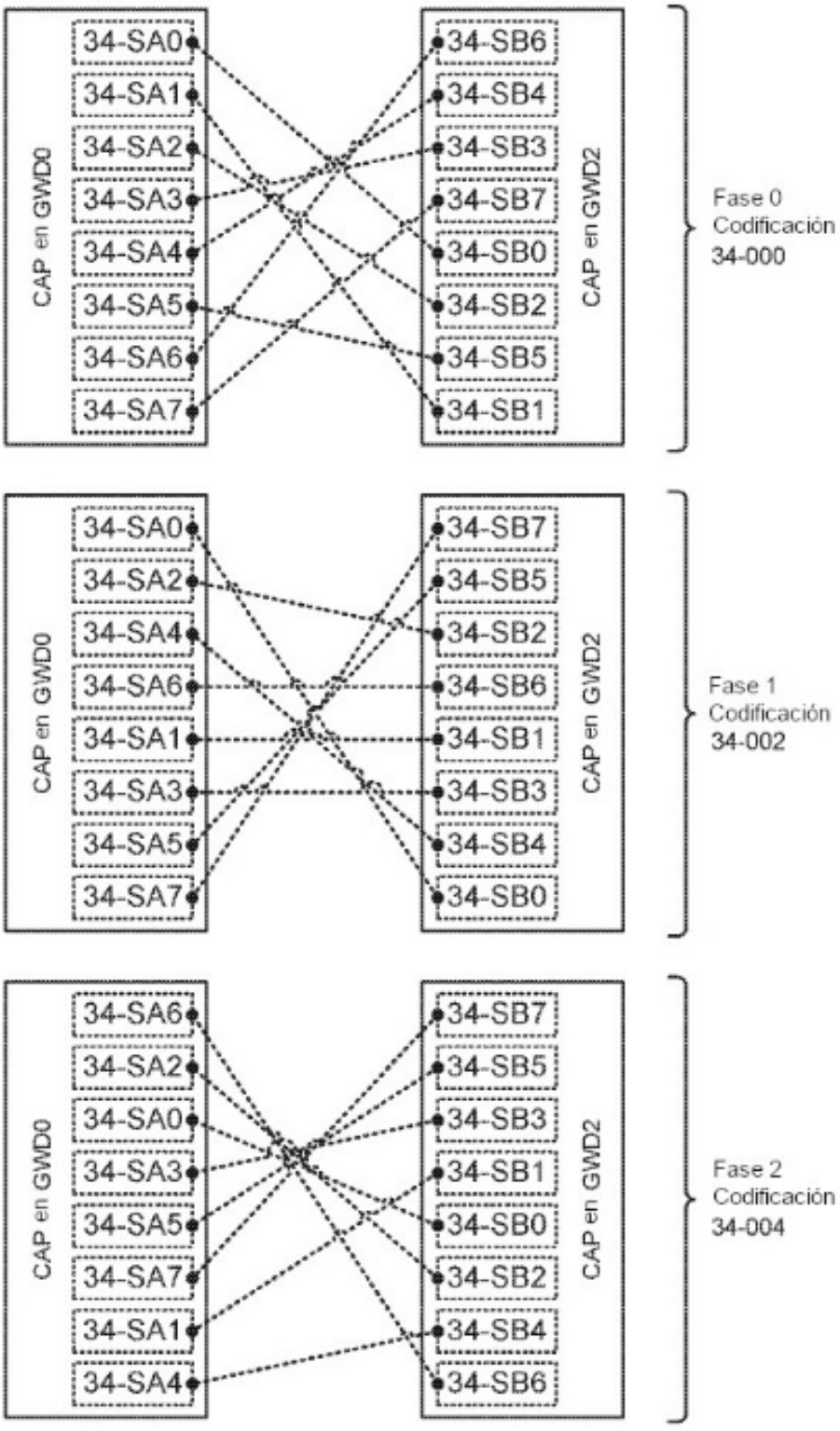
CAP en GWD0
34-SA0
34-SA1
34-SA2
34-SA3
34-SA4
34-SA5
34-SA6
34-SA7
CAP en GWD2
34-SB6
34-SB4
34-SB3
34-SB7
34-SB0
34-SB2
34-SB5
34-SB1
Fase 0
Codificación
34-000
CAP en GWD0
34-SA0
34-SA2
34-SA4
34-SA6
34-SA1
34-SA3
34-SA5
34-SA7
CAP en GWD2
34-SB7
34-SB5
34-SB2
34-SB6
34-SB1
34-SB3
34-SB4
34-SB0
Fase 1
Codificación
34-002
CAP en GWD0
34-SA6
34-SA2
34-SA0
34-SA3
34-SA5
34-SA7
34-SA1
34-SA4
CAP en GWD2
34-SB7
34-SB5
34-SB3
34-SB1
34-SB0
34-SB2
34-SB4
34-SB6
Fase 2
Codificación
34-004

FIG. 34

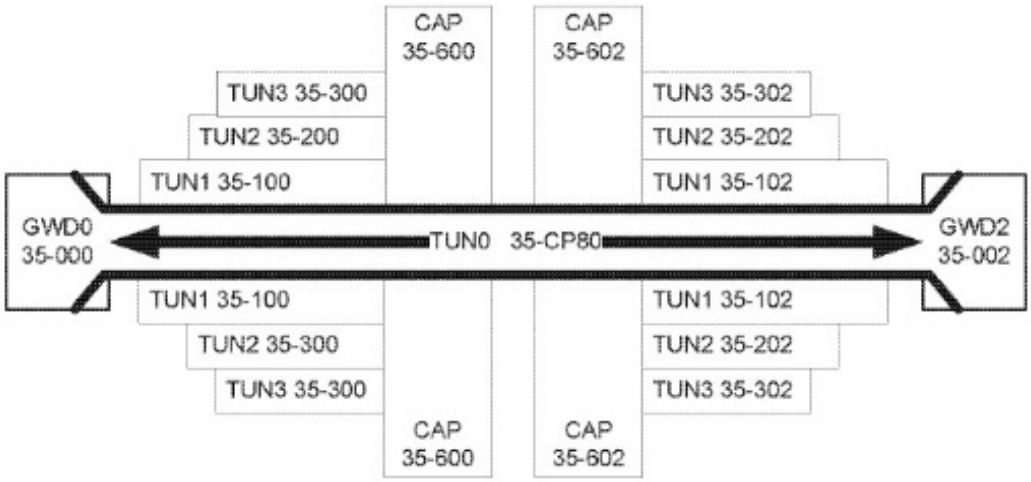
CAP
35-600
CAP
35-602
TUN3 35-300
TUN3 35-302
TUN2 35-200
TUN2 35-202
TUN1 35-100
TUN1 35-102
GWD0
35-000
TUN0 35-CP80
GWD2
35-002
TUN1 35-100
TUN1 35-102
TUN2 35-300
TUN2 35-202
TUN3 35-300
TUN3 35-302
CAP
35-600
CAP
35-602

FIG. 35

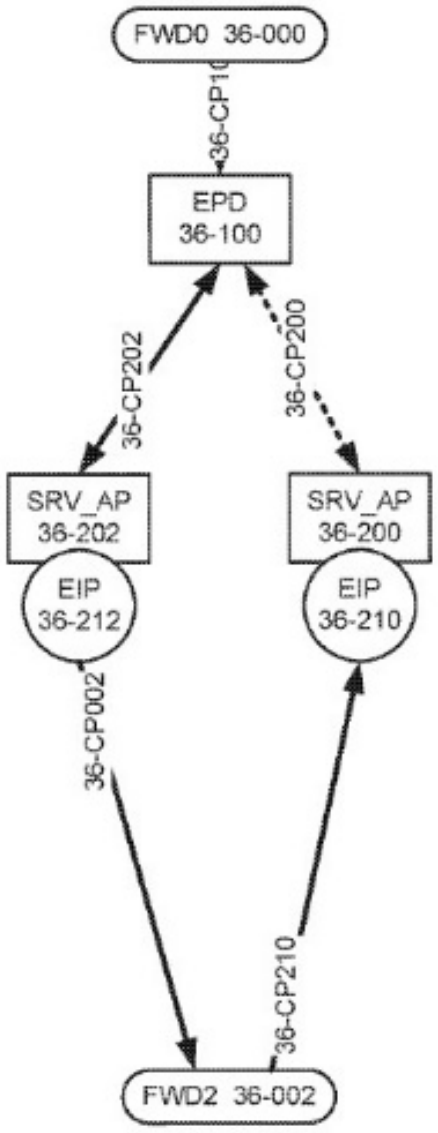
FWD0 36-000
36-CP10
EPD
36-100
36-CP202
36-CP200
SRV_AP
36-202
SRV_AP
36-200
EIP
36-212
EIP
36-210
36-CP002
36-CP210
FWD2 36-002

FIG. 36

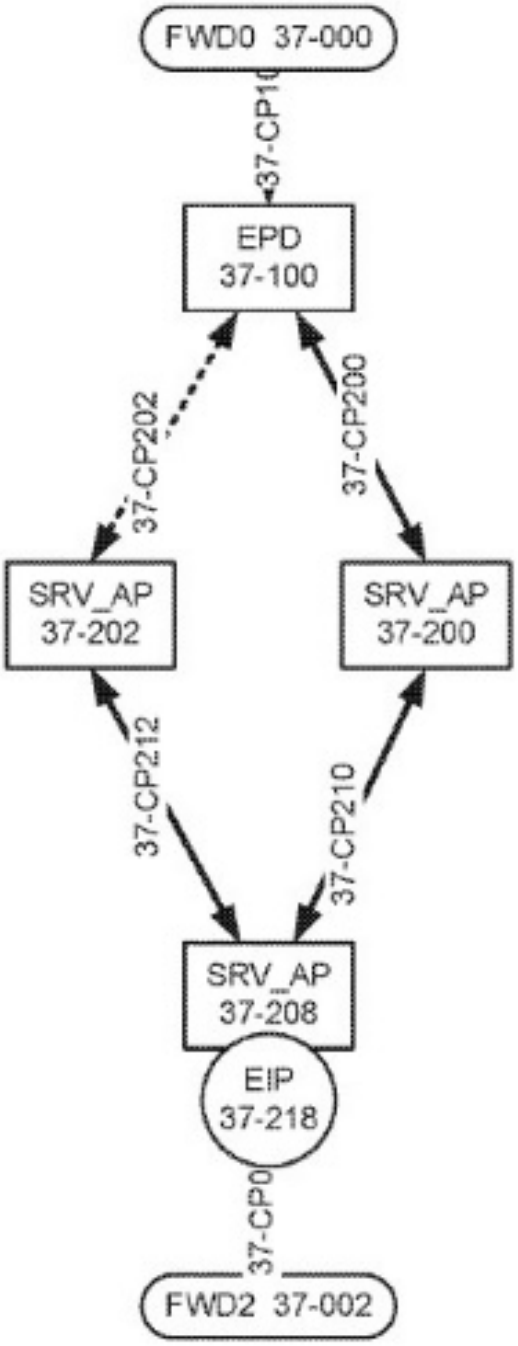
FWD0 37-000
37-CP10
EPD
37-100
37-CP202
37-CP200
SRV_AP
37-202
SRV_AP
37-200
37-CP212
37-CP210
SRV_AP
37-208
EIP
37-218
37-CP0
FWD2 37-002

FIG. 37

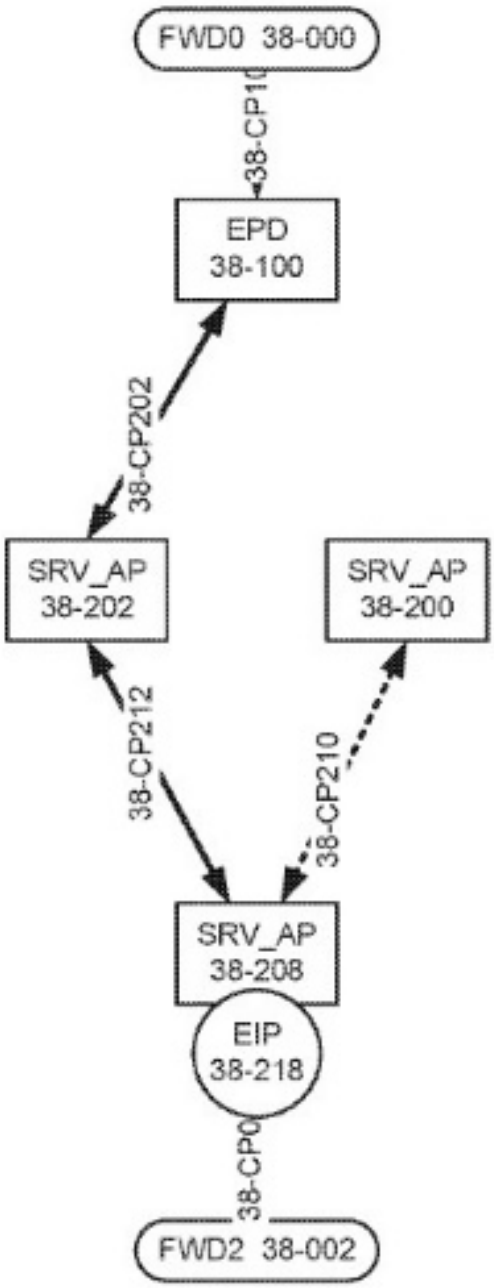
FWD0 38-000
38-CP10
EPD
38-100
38-CP202
SRV_AP
38-202
SRV_AP
38-200
38-CP212
38-CP210
SRV_AP
38-208
EIP
38-218
38-CP0
FWD2 38-002

FIG. 38

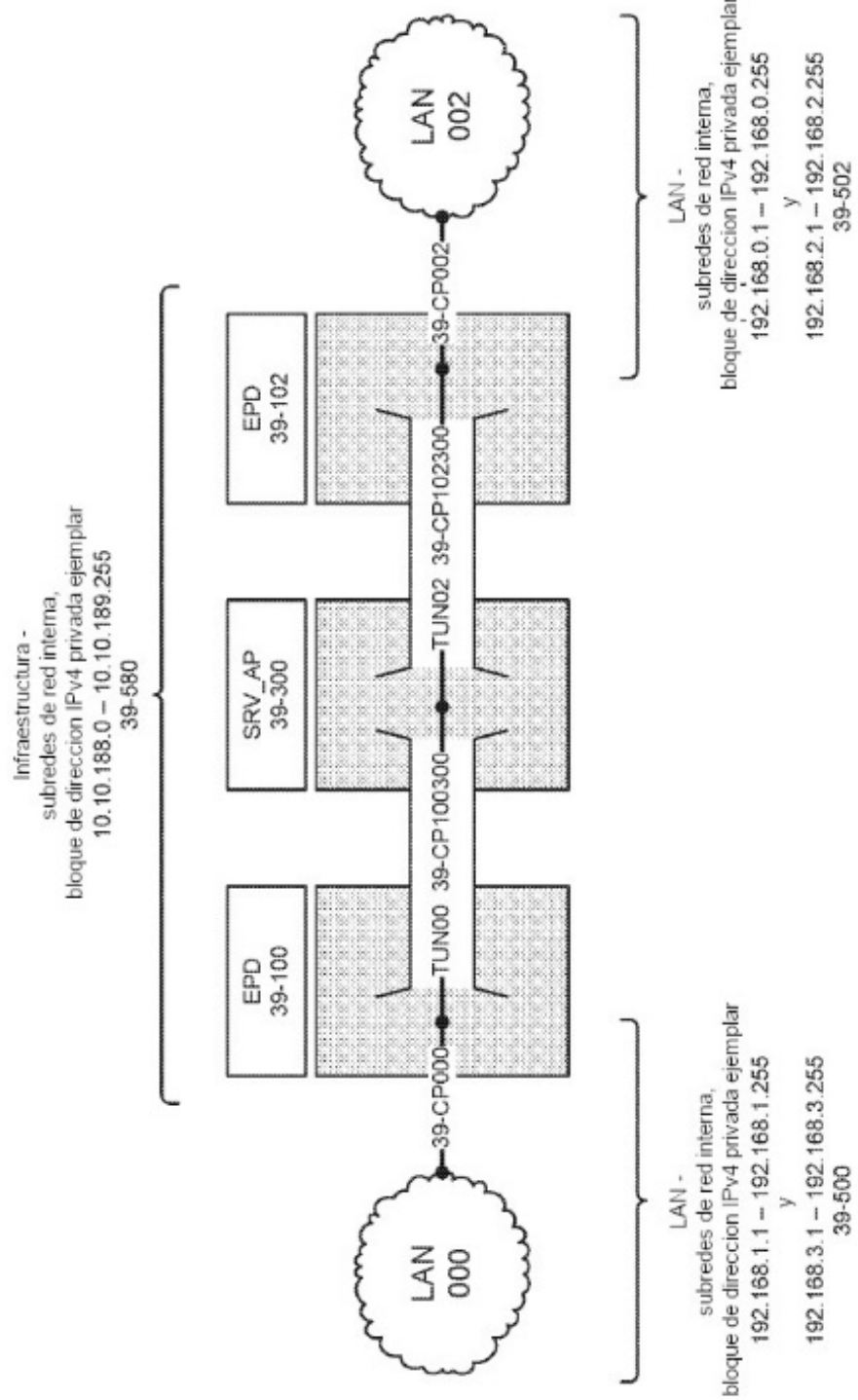
Infraestructura -
subredes de red interna,
bloque de direccion IPv4 privada ejemplar
10.10.188.0 – 10.10.189.255
39-580
EPD
39-100
SRV_AP
39-300
EPD
39-102
LAN
000
LAN
002
39-CP000
TUN00
39-CP100300
TUN02
39-CP102300
39-CP002
LAN -
subredes de red interna,
bloque de direccion IPv4 privada ejemplar
192.168.1.1 – 192.168.1.255
y
192.168.3.1 – 192.168.3.255
39-500
LAN -
subredes de red interna,
bloque de direccion IPv4 privada ejemplar
192.168.0.1 – 192.168.0.255
y
192.168.2.1 – 192.168.2.255
39-502

FIG. 39

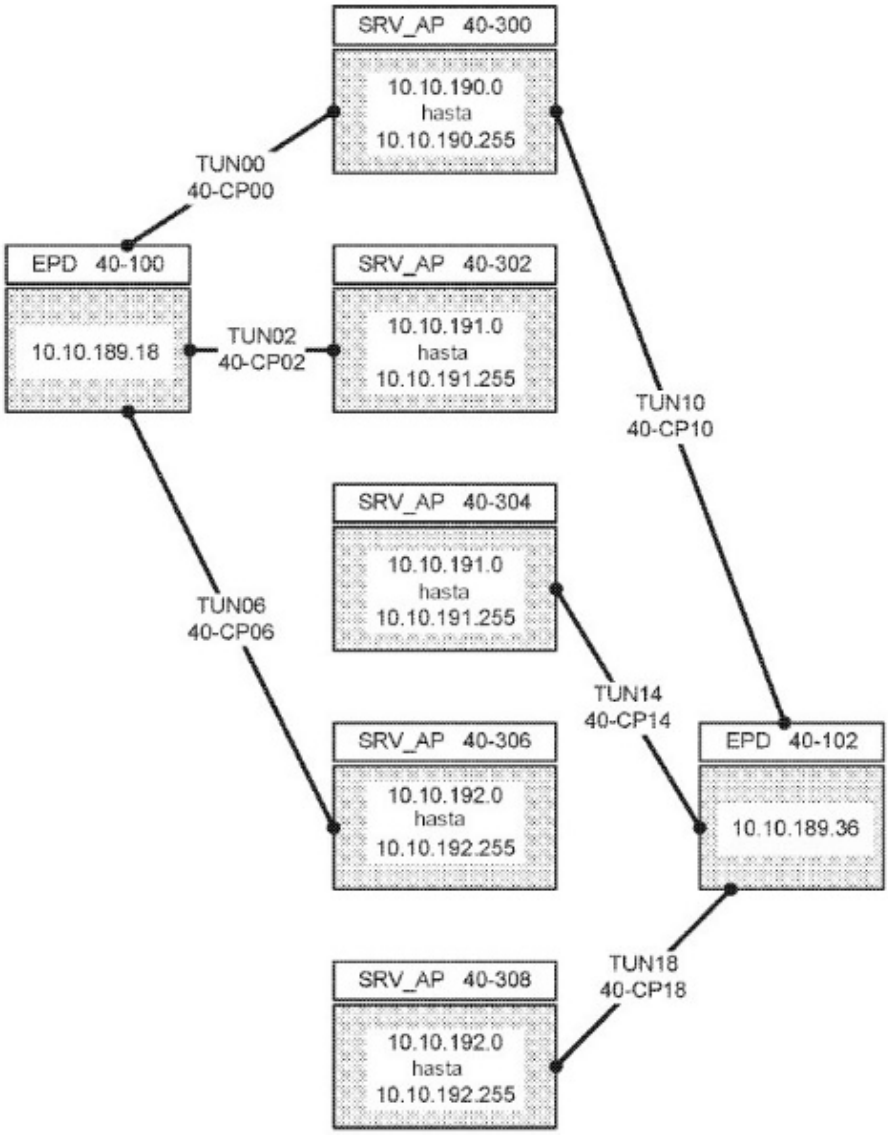
SRV_AP 40-300
10.10.190.0
hasta
10.10.190.255
TUN00
40-CP00
EPD 40-100
10.10.189.18
TUN02
40-CP02
SRV_AP 40-302
10.10.191.0
hasta
10.10.191.255
TUN10
40-CP10
SRV_AP 40-304
10.10.191.0
hasta
10.10.191.255
TUN06
40-CP06
TUN14
40-CP14
SRV_AP 40-306
10.10.192.0
hasta
10.10.192.255
EPD 40-102
10.10.189.36
TUN18
40-CP18
SRV_AP 40-308
10.10.192.0
hasta
10.10.192.255

FIG. 40

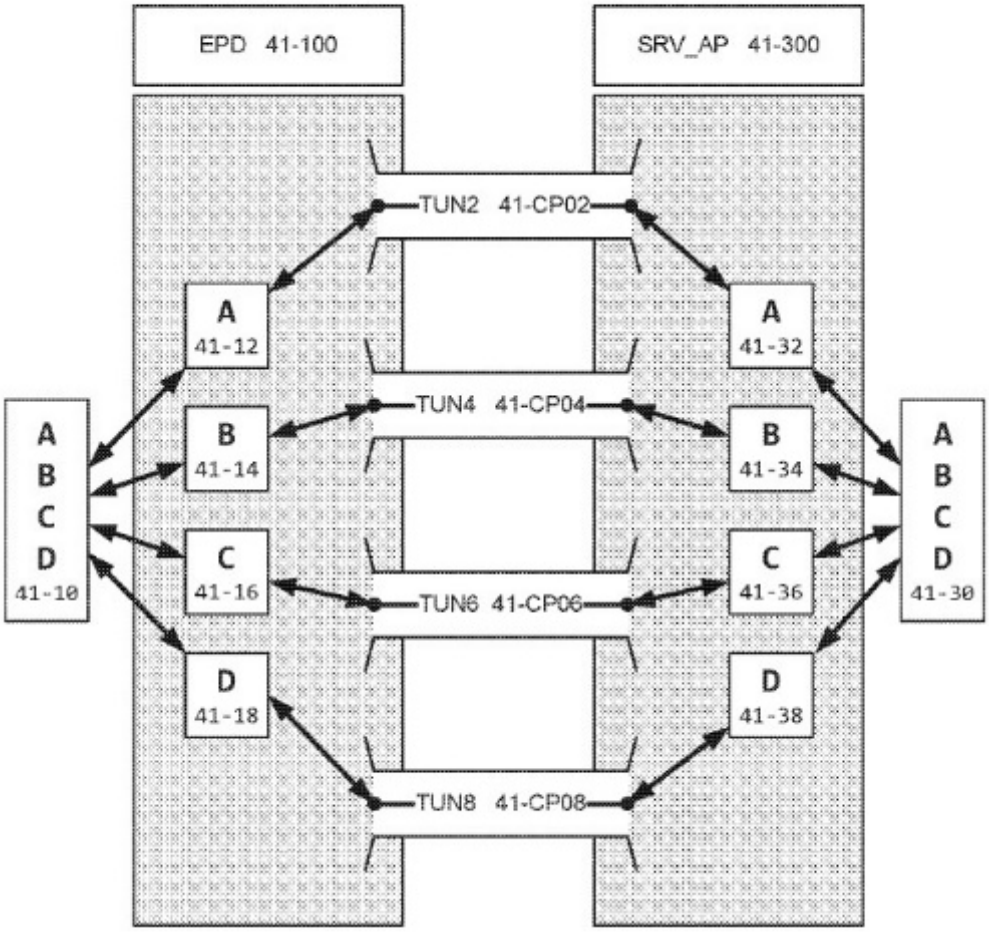
EPD 41-100
SRV_AP 41-300
TUN2 41-CP02
TUN4 41-CP04
TUN6 41-CP06
TUN8 41-CP08
A
B
C
D
41-10
A
41-12
B
41-14
C
41-16
D
41-18
A
41-32
B
41-34
C
41-36
D
41-38
A
B
C
D
41-30

FIG. 41

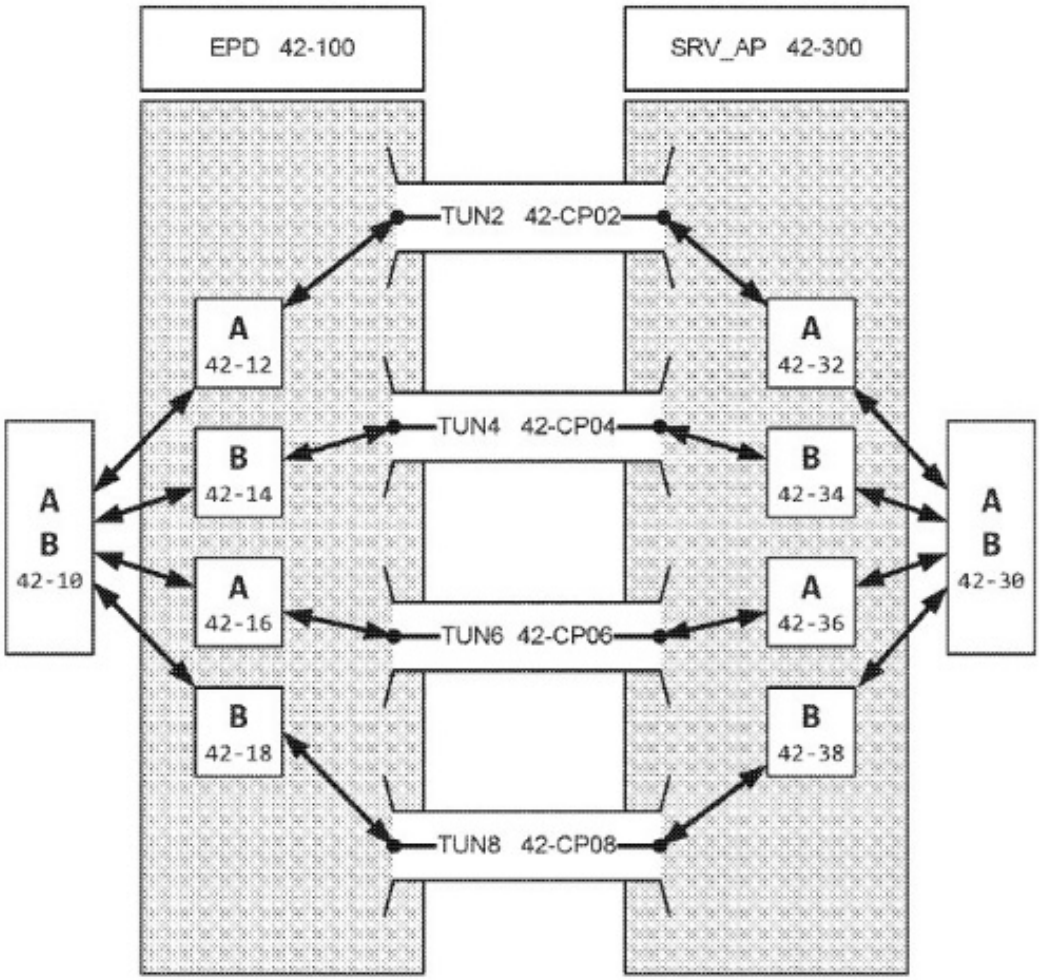
EPD 42-100
SRV_AP 42-300
TUN2 42-CP02
TUN4 42-CP04
TUN6 42-CP06
TUN8 42-CP08
A
B
42-10
A
42-12
B
42-14
A
42-16
B
42-18
A
42-32
B
42-34
A
42-36
B
42-38
A
B
42-30

FIG. 42

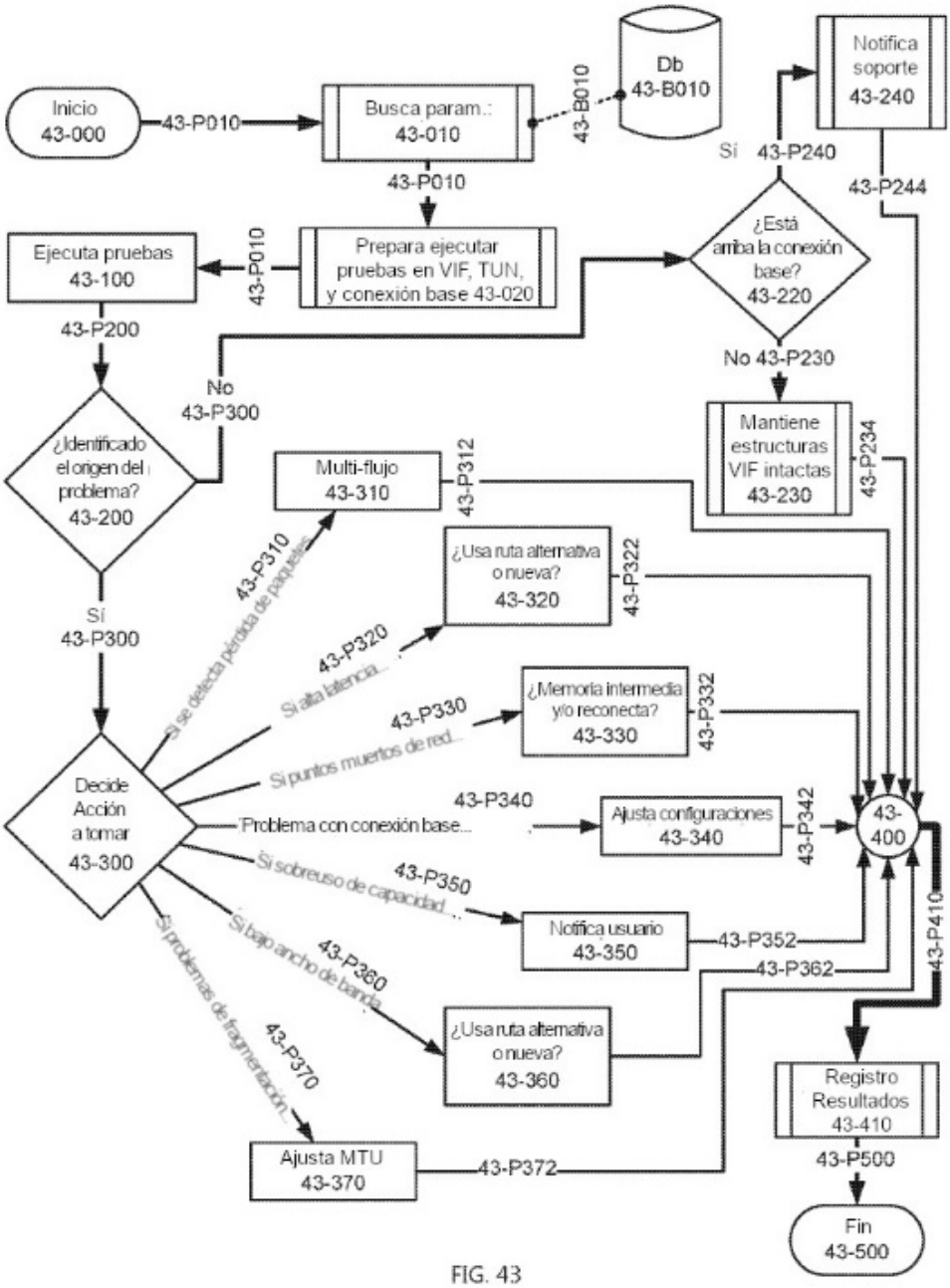
Inicio
43-000
43-P010
Busca param.:
43-010
43-B010
Db
43-B010
Notifica
soporte
43-240
Sí
43-P240
43-P244
43-P010
Ejecuta pruebas
43-100
43-P010
Prepara ejecutar
pruebas en VIF, TUN,
y conexión base 43-020
¿Está
arriba la conexión
base?
43-220
43-P200
No
43-P300
No 43-P230
¿Identificado
el origen del
problema?
43-200
Multi-flujo
43-310
43-P312
Mantiene
estructuras
VIF intactas
43-230
43-P234
43-P310
Si se detecta pérdida de paquetes...
¿Usa ruta alternativa
o nueva?
43-320
43-P322
Sí
43-P300
43-P320
Si alta latencia...
¿Memoria intermedia
y/o reconecta?
43-330
43-P332
43-P330
Si puntos muertos de red...
Decide
Acción
a tomar
43-300
43-P340
Problema con conexión base...
Ajusta configuraciones
43-340
43-P342
43-
400
Si sobreuso de capacidad...
43-P350
Notifica usuario
43-350
43-P352
43-P410
Si bajo ancho de banda...
43-P360
43-P362
¿Usa ruta alternativa
o nueva?
43-360
Si problemas de fragmentación...
43-P370
Registro
Resultados
43-410
Ajusta MTU
43-370
43-P372
43-P500
Fin
43-500

FIG. 43

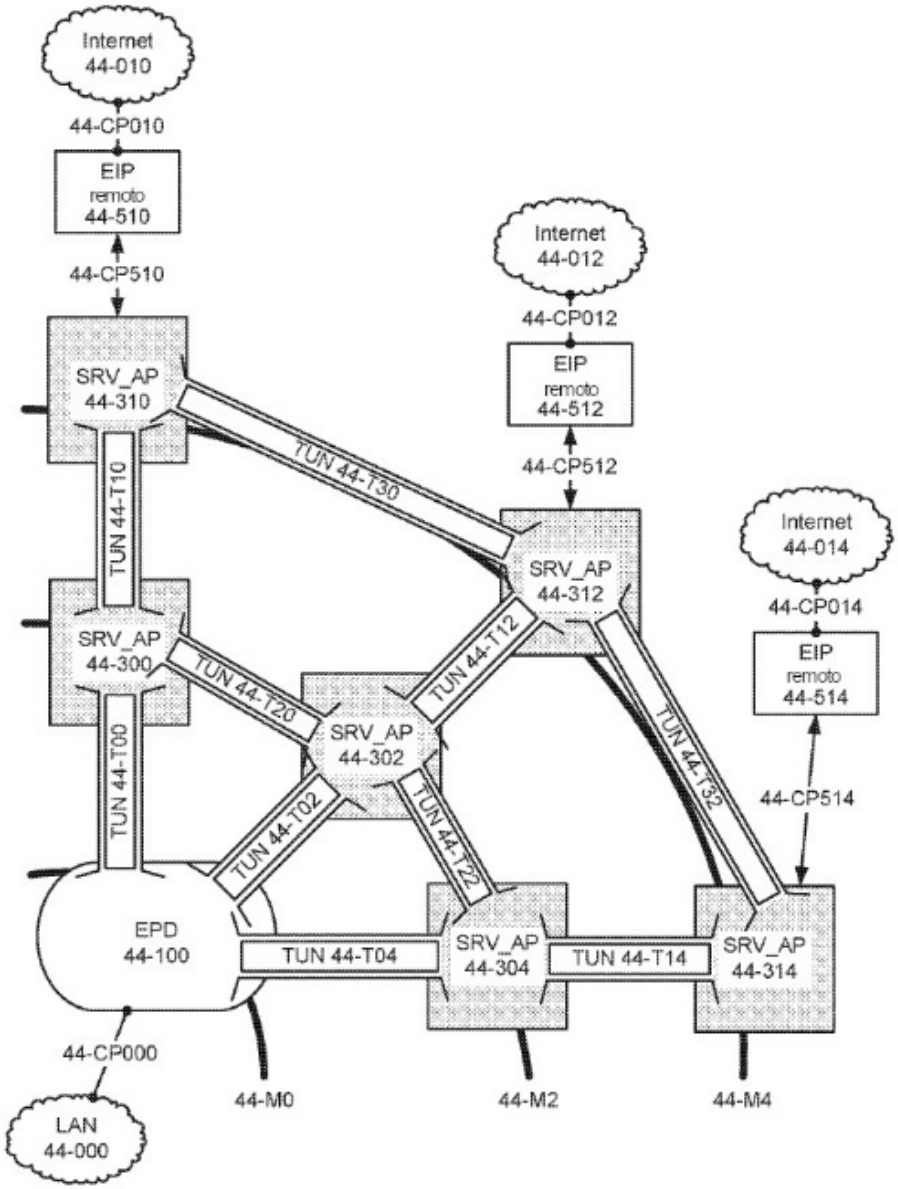
Internet
44-010
44-CP010
EIP
remoto
44-510
44-CP510
Internet
44-012
44-CP012
EIP
remoto
44-512
44-CP512
Internet
44-014
44-CP014
EIP
remoto
44-514
44-CP514
SRV_AP
44-310
SRV_AP
44-312
SRV_AP
44-300
SRV_AP
44-302
SRV_AP
44-304
SRV_AP
44-314
TUN 44-T10
TUN 44-T30
TUN 44-T12
TUN 44-T20
TUN 44-T00
TUN 44-T02
TUN 44-T22
TUN 44-T32
TUN 44-T04
TUN 44-T14
EPD
44-100
44-CP000
LAN
44-000
44-M0
44-M2
44-M4

FIG. 44

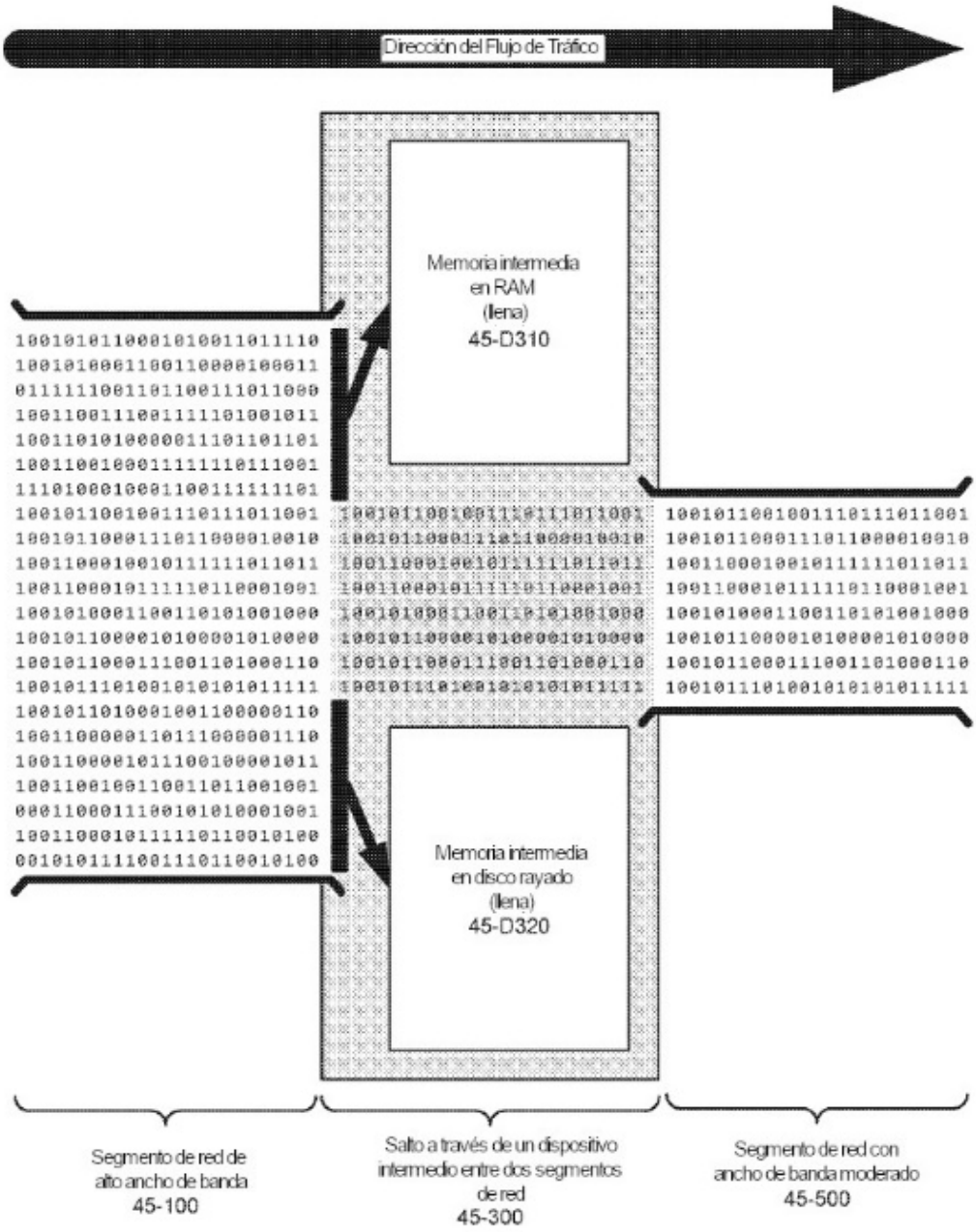
Dirección del Flujo de Tráfico
Memoria intermedia en RAM (llena) 45-D310
Memoria intermedia en disco rayado (llena) 45-D320
Segmento de red de alto ancho de banda 45-100
Salto a través de un dispositivo intermedio entre dos segmentos de red 45-300
Segmento de red con ancho de banda moderado 45-500

FIG. 45

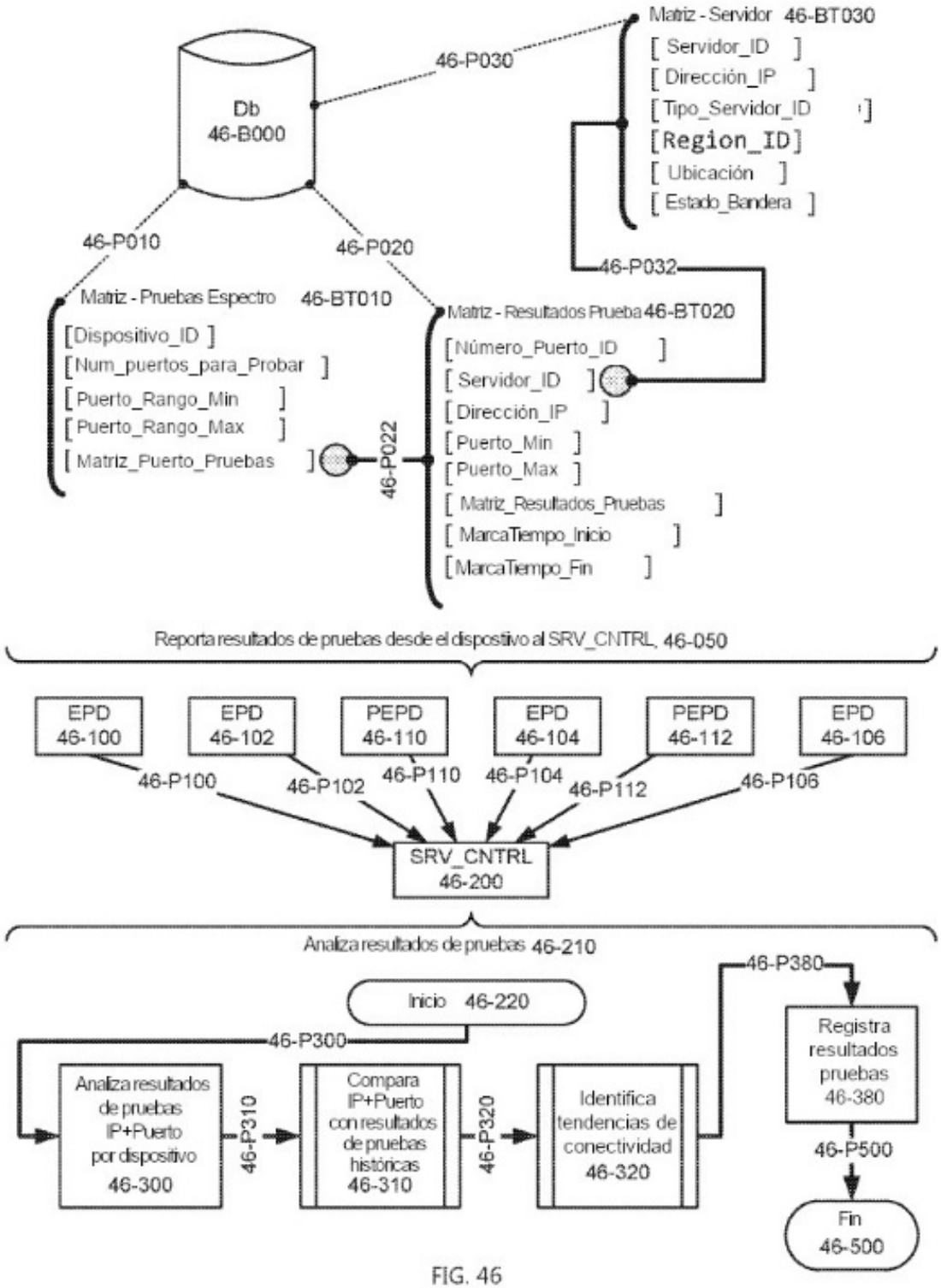
Matriz - Servidor 46-BT030
[Servidor_ID]
[Dirección_IP]
[Tipo_Servidor_ID]
[Region_ID]
[Ubicación]
[Estado_Bandera]
46-P030
Db
46-B000
46-P010
46-P020
46-P032
Matriz - Pruebas Espectro 46-BT010
[Dispositivo_ID]
[Num_puertos_para_Probar]
[Puerto_Rango_Min]
[Puerto_Rango_Max]
[Matriz_Puerto_Pruebas]
46-P022
Matriz - Resultados Prueba 46-BT020
[Número_Puerto_ID]
[Servidor_ID]
[Dirección_IP]
[Puerto_Min]
[Puerto_Max]
[Matriz_Resultados_Pruebas]
[MarcaTiempo_Inicio]
[MarcaTiempo_Fin]
Reporta resultados de pruebas desde el dispositivo al SRV_CNTRL, 46-050
EPD 46-100
EPD 46-102
PEPD 46-110
EPD 46-104
PEPD 46-112
EPD 46-106
46-P100
46-P102
46-P110
46-P104
46-P112
46-P106
SRV_CNTRL 46-200
Analiza resultados de pruebas 46-210
Inicio 46-220
46-P300
Analiza resultados de pruebas IP+Puerto por dispositivo 46-300
46-P310
Compara IP+Puerto con resultados de pruebas históricas 46-310
46-P320
Identifica tendencias de conectividad 46-320
46-P380
Registra resultados pruebas 46-380
46-P500
Fin 46-500

FIG. 46

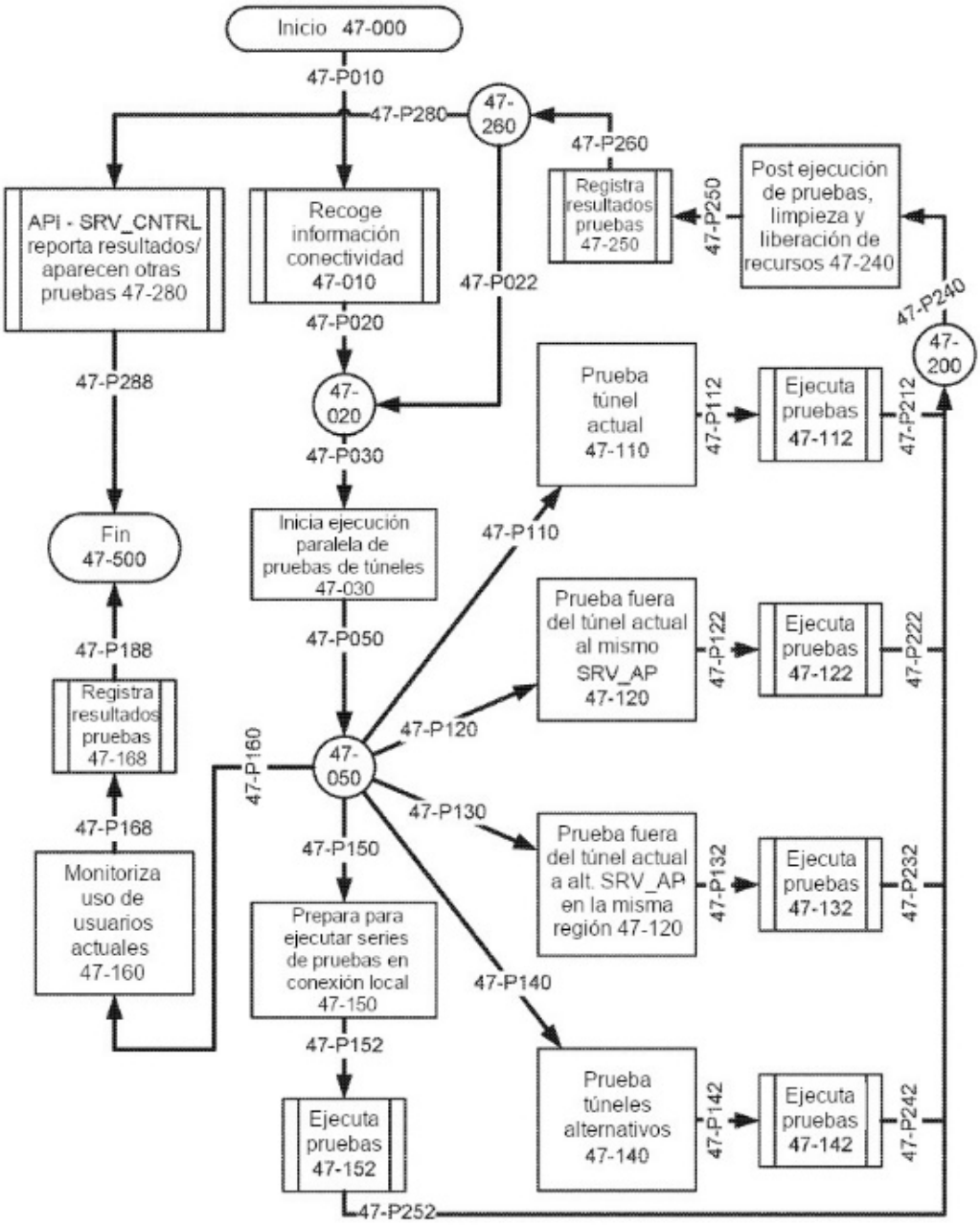
Inicio 47-000
47-P010
47-P280
47-260
47-P260
Registra resultados pruebas 47-250
47-P250
Post ejecución de pruebas, limpieza y liberación de recursos 47-240
47-P240
47-200
API - SRV_CNTRL reporta resultados/ aparecen otras pruebas 47-280
Recoge información conectividad 47-010
47-P022
47-P020
47-P288
47-020
47-P030
Prueba túnel actual 47-110
47-P112
Ejecuta pruebas 47-112
47-P212
Fin 47-500
Inicia ejecución paralela de pruebas de túneles 47-030
47-P110
47-P050
Prueba fuera del túnel actual al mismo SRV_AP 47-120
47-P122
Ejecuta pruebas 47-122
47-P222
47-P188
Registra resultados pruebas 47-168
47-P120
47-P160
47-050
47-P130
47-P168
47-P150
Prueba fuera del túnel actual a alt. SRV_AP en la misma región 47-120
47-P132
Ejecuta pruebas 47-132
47-P232
Monitoriza uso de usuarios actuales 47-160
Prepara para ejecutar series de pruebas en conexión local 47-150
47-P140
47-P152
Prueba túneles alternativos 47-140
47-P142
Ejecuta pruebas 47-142
47-P242
Ejecuta pruebas 47-152
47-P252

FIG. 47

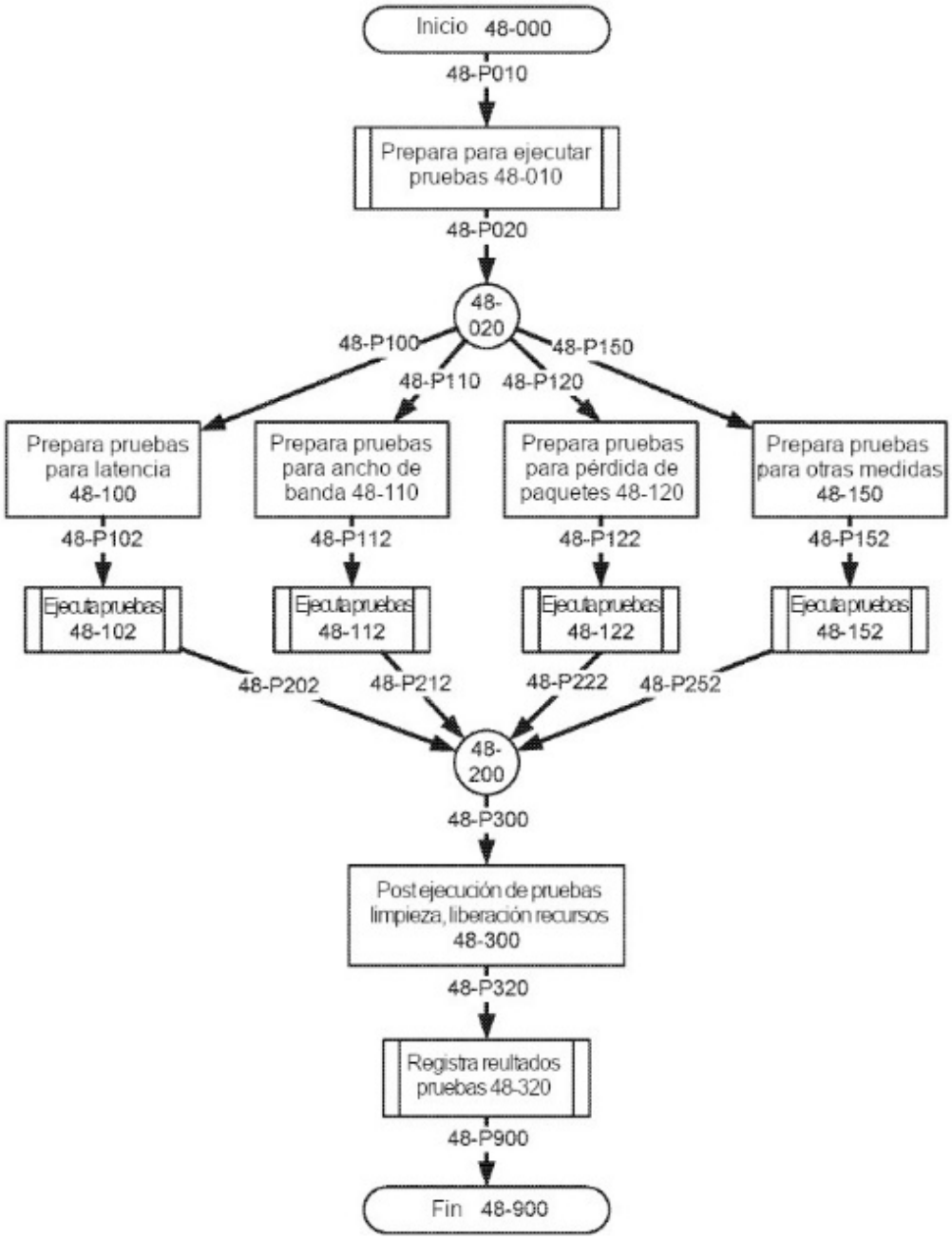
Inicio 48-000
48-P010
Prepara para ejecutar pruebas 48-010
48-P020
48-020
48-P100
48-P110
48-P120
48-P150
Prepara pruebas para latencia 48-100
Prepara pruebas para ancho de banda 48-110
Prepara pruebas para pérdida de paquetes 48-120
Prepara pruebas para otras medidas 48-150
48-P102
48-P112
48-P122
48-P152
Ejecuta pruebas 48-102
Ejecuta pruebas 48-112
Ejecuta pruebas 48-122
Ejecuta pruebas 48-152
48-P202
48-P212
48-P222
48-P252
48-200
48-P300
Post ejecución de pruebas limpieza, liberación recursos 48-300
48-P320
Registra reultados pruebas 48-320
48-P900
Fin 48-900

FIG. 48

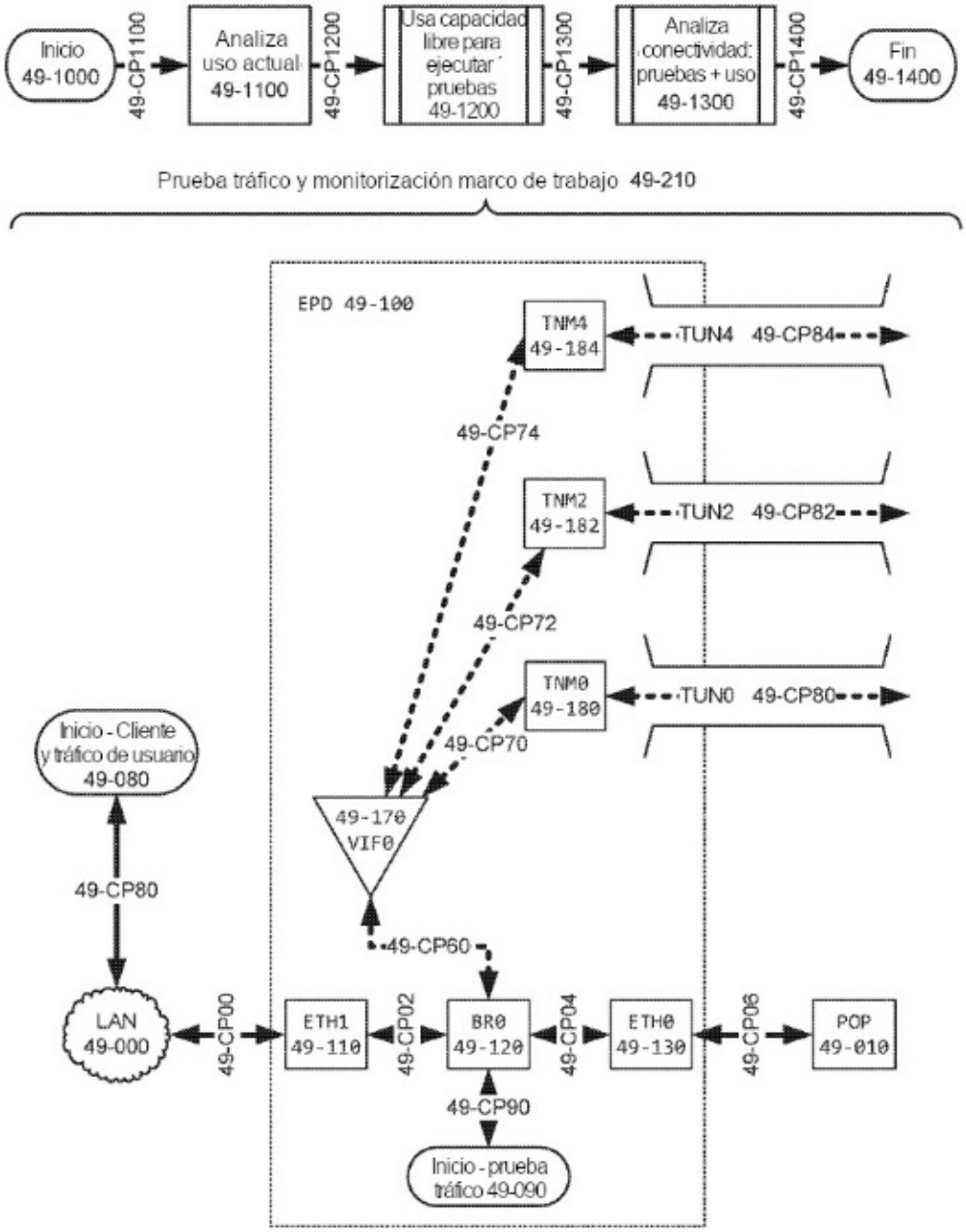
Inicio
49-1000
49-CP1100
Analiza
uso actual
49-1100
49-CP1200
Usa capacidad
libre para
ejecutar
pruebas
49-1200
49-CP1300
Analiza
conectividad:
pruebas + uso
49-1300
49-CP1400
Fin
49-1400
Prueba tráfico y monitorización marco de trabajo 49-210
EPD 49-100
TNM4
49-184
TUN4 49-CP84
49-CP74
TNM2
49-182
TUN2 49-CP82
49-CP72
TNM0
49-180
TUN0 49-CP80
49-CP70
49-170
VIF0
Inicio - Cliente
y tráfico de usuario
49-080
49-CP80
49-CP60
LAN
49-000
49-CP00
ETH1
49-110
49-CP02
BR0
49-120
49-CP04
ETH0
49-130
49-CP06
POP
49-010
49-CP90
Inicio - prueba
tráfico 49-090

FIG. 49

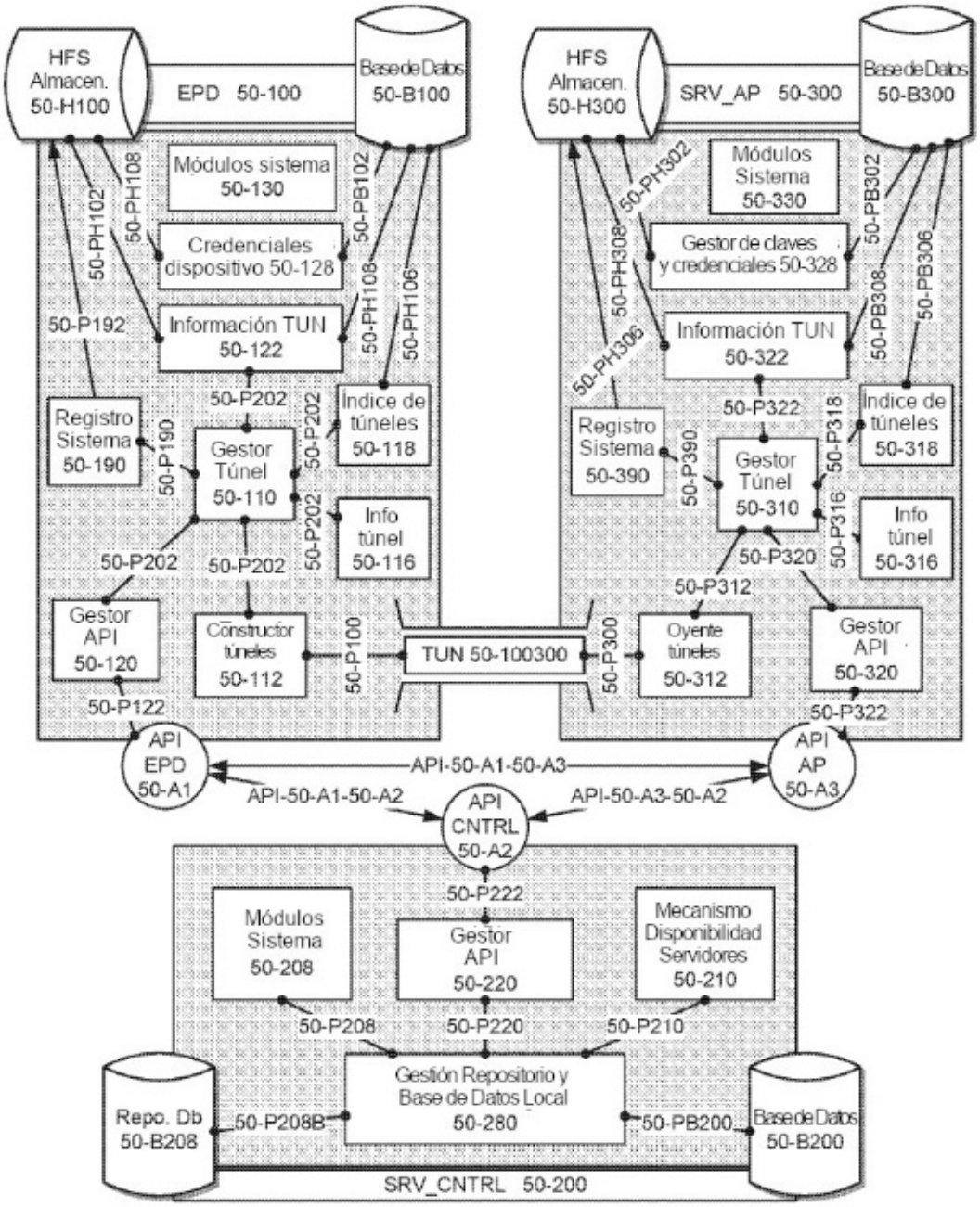
HFS Almacen. 50-H100
EPD 50-100
Base de Datos 50-B100
HFS Almacen. 50-H300
SRV_AP 50-300
Base de Datos 50-B300
Módulos sistema 50-130
Credenciales dispositivo 50-128
Información TUN 50-122
Registro Sistema 50-190
Gestor Túnel 50-110
Índice de túneles 50-118
Info túnel 50-116
Gestor API 50-120
Constructor túneles 50-112
TUN 50-100300
Módulos Sistema 50-330
Gestor de claves y credenciales 50-328
Información TUN 50-322
Registro Sistema 50-390
Gestor Túnel 50-310
Índice de túneles 50-318
Info túnel 50-316
Oyente túneles 50-312
Gestor API 50-320
API EPD 50-A1
API AP 50-A3
API-50-A1-50-A3
API-50-A1-50-A2
API-50-A3-50-A2
API CNTRL 50-A2
Módulos Sistema 50-208
Gestor API 50-220
Mecanismo Disponibilidad Servidores 50-210
Gestión Repositorio y Base de Datos Local 50-280
Repo. Db 50-B208
Base de Datos 50-B200
SRV_CNTRL 50-200
50-PH102
50-PH108
50-PB102
50-PH106
50-P192
50-P202
50-P190
50-P100
50-PH302
50-PH308
50-PH306
50-PB302
50-PB308
50-PB306
50-P322
50-P318
50-P390
50-P316
50-P320
50-P312
50-P300
50-P122
50-P222
50-P208
50-P220
50-P210
50-P208B
50-PB200

FIG. 50

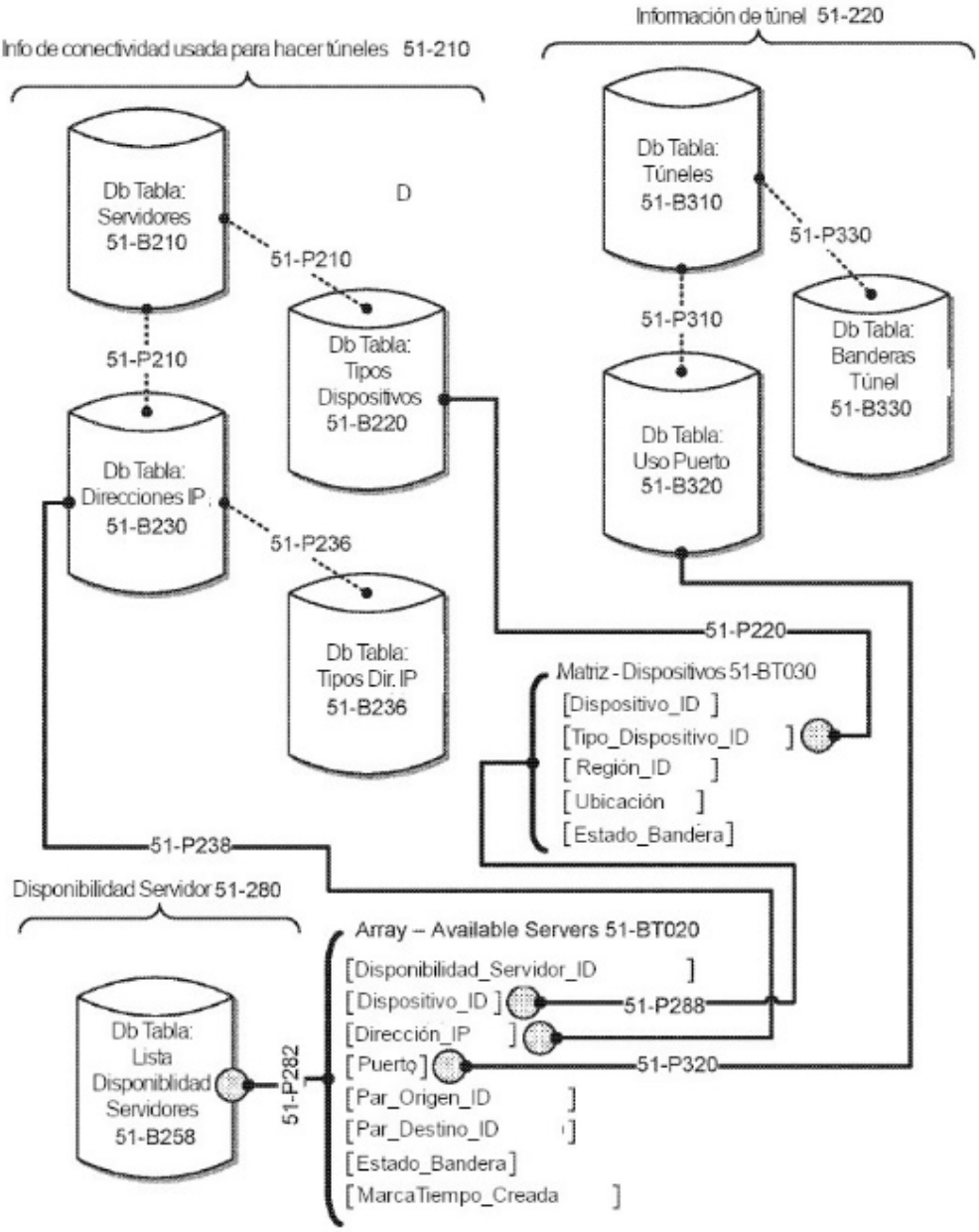
Info de conectividad usada para hacer túneles 51-210
Información de túnel 51-220
Db Tabla: Servidores 51-B210
D
51-P210
Db Tabla: Tipos Dispositivos 51-B220
51-P210
Db Tabla: Direcciones IP 51-B230
51-P236
Db Tabla: Tipos Dir. IP 51-B236
Db Tabla: Túneles 51-B310
51-P330
51-P310
Db Tabla: Banderas Túnel 51-B330
Db Tabla: Uso Puerto 51-B320
51-P220
Matriz - Dispositivos 51-BT030
[Dispositivo_ID]
[Tipo_Dispositivo_ID]
[Región_ID]
[Ubicación]
[Estado_Bandera]
51-P238
Disponibilidad Servidor 51-280
Array -- Available Servers 51-BT020
[Disponibilidad_Servidor_ID]
[Dispositivo_ID]
51-P288
[Dirección_IP]
[Puerto]
51-P320
[Par_Origen_ID]
[Par_Destino_ID]
[Estado_Bandera]
[MarcaTiempo_Creada]
Db Tabla: Lista Disponiblidad Servidores 51-B258
51-P282

FIG. 51

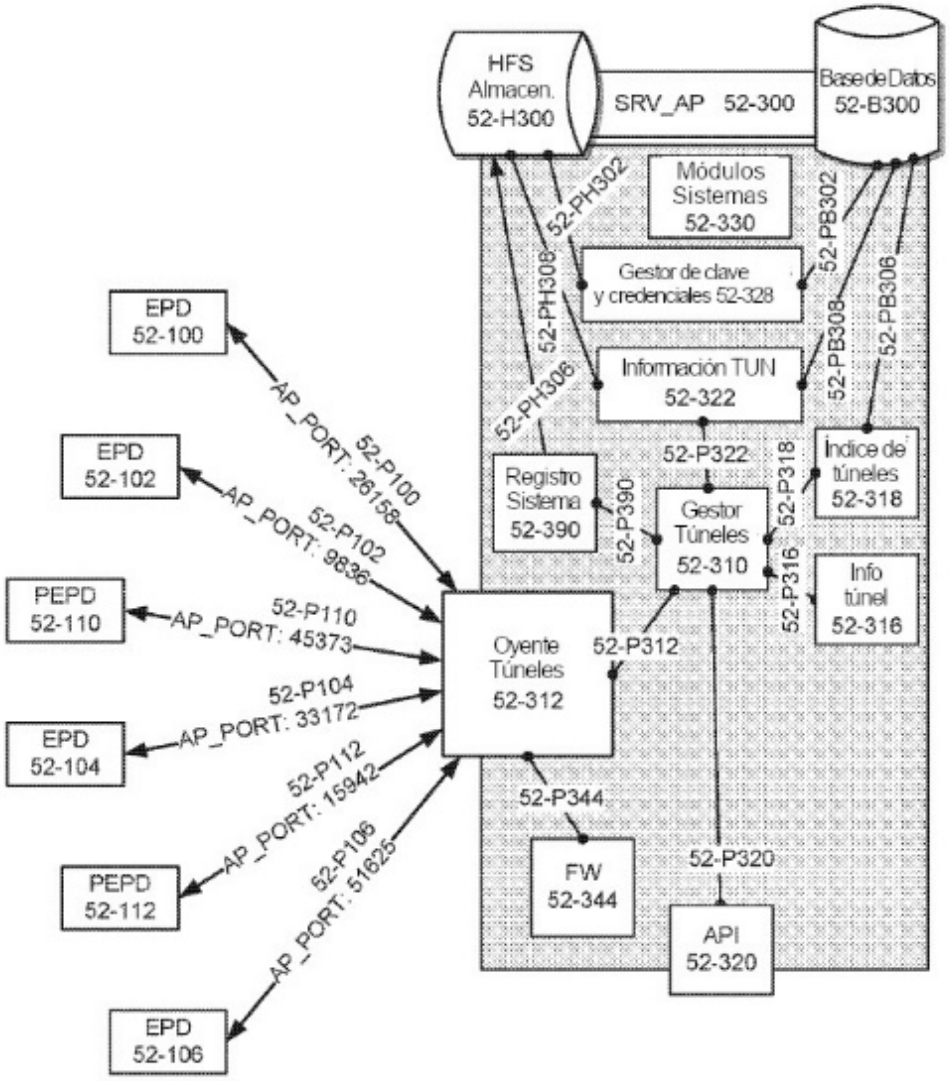
HFS
Almacen.
52-H300
SRV_AP 52-300
Base de Datos
52-B300
Módulos
Sistemas
52-330
Gestor de clave
y credenciales 52-328
Información TUN
52-322
Registro
Sistema
52-390
Gestor
Túneles
52-310
Índice de
túneles
52-318
Info
túnel
52-316
Oyente
Túneles
52-312
FW
52-344
API
52-320
52-PH302
52-PH308
52-PH306
52-PB302
52-PB308
52-PB306
52-P322
52-P390
52-P318
52-P316
52-P312
52-P344
52-P320
EPD
52-100
EPD
52-102
PEPD
52-110
EPD
52-104
PEPD
52-112
EPD
52-106
AP_PORT: 26158
52-P100
AP_PORT: 9836
52-P102
AP_PORT: 45373
52-P110
AP_PORT: 33172
52-P104
AP_PORT: 15942
52-P112
AP_PORT: 51625
52-P106

FIG. 52

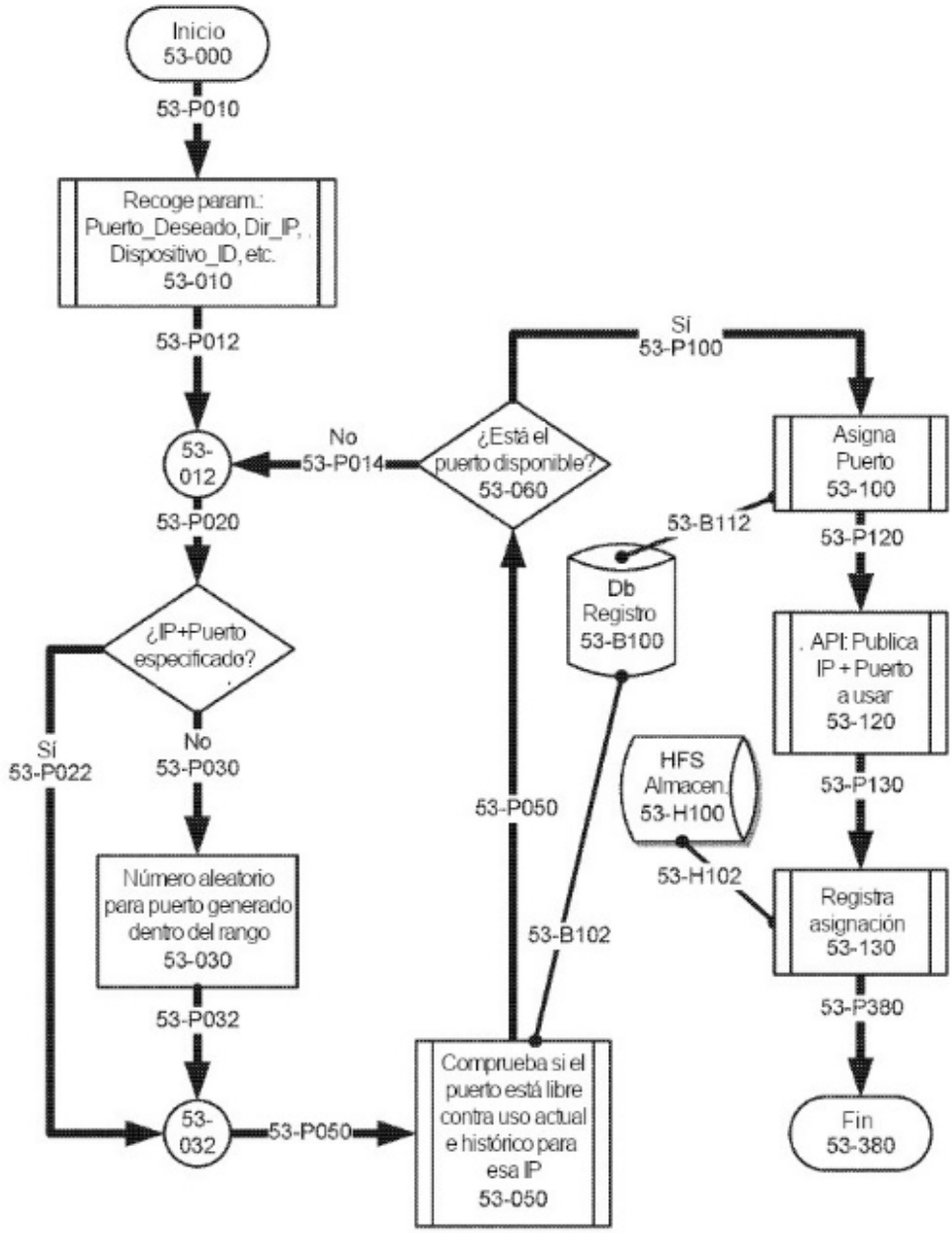
Inicio
53-000
53-P010
Recoge param.:
Puerto_Deseado, Dir_IP,
Dispositivo_ID, etc.
53-010
53-P012
53-
012
53-P020
¿IP+Puerto
especificado?
Sí
53-P022
No
53-P030
Número aleatorio
para puerto generado
dentro del rango
53-030
53-P032
53-
032
53-P050
Comprueba si el
puerto está libre
contra uso actual
e histórico para
esa IP
53-050
No
53-P014
¿Está el
puerto disponible?
53-060
Sí
53-P100
Asigna
Puerto
53-100
53-B112
53-P120
Db
Registro
53-B100
API: Publica
IP + Puerto
a usar
53-120
53-P130
HFS
Almacen
53-H100
53-H102
Registra
asignación
53-130
53-P380
Fin
53-380
53-P050
53-B102

FIG. 53

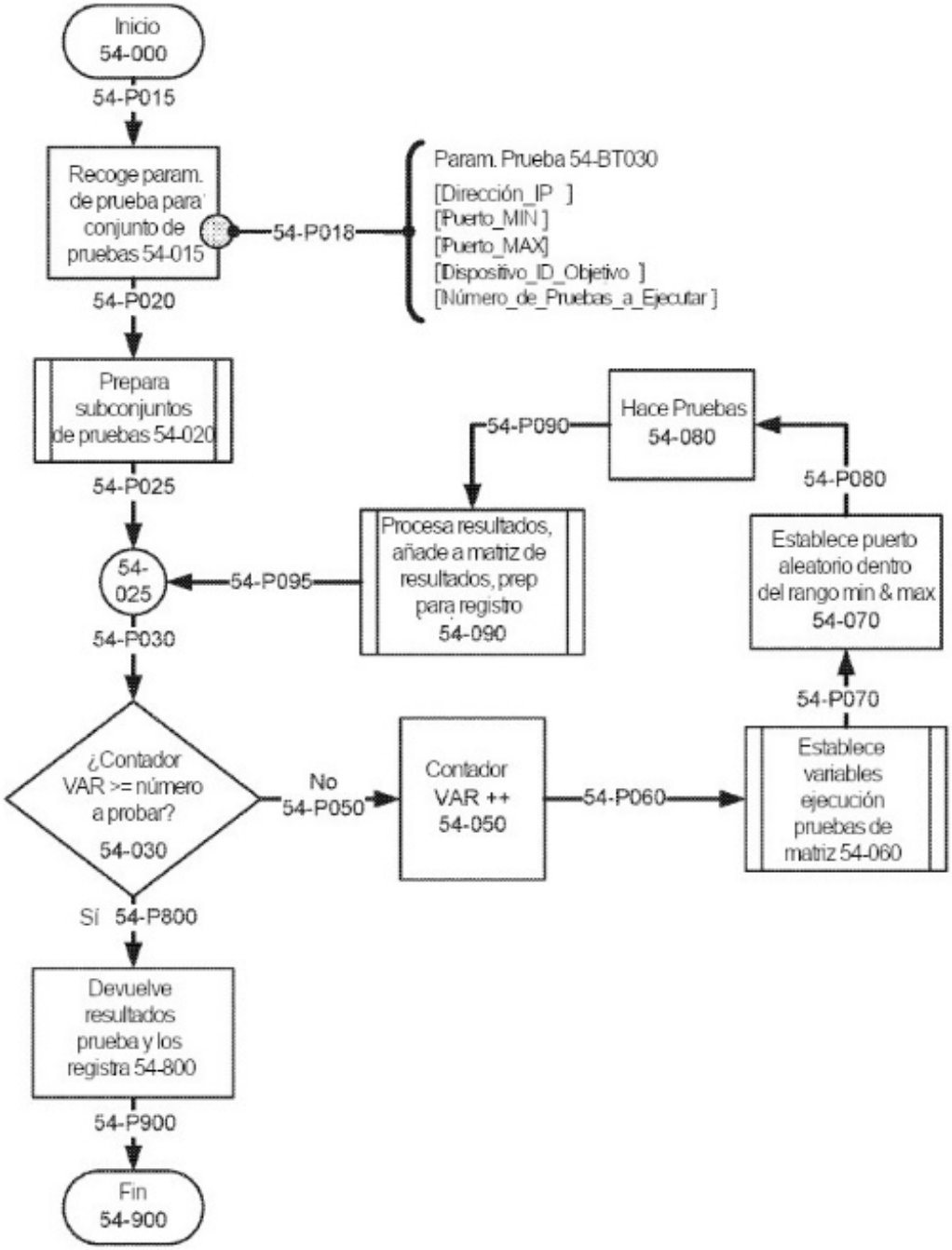
Inicio
54-000
54-P015
Recoge param. de prueba para conjunto de pruebas 54-015
54-P018
Param. Prueba 54-BT030
[Dirección_IP]
[Puerto_MIN]
[Puerto_MAX]
[Dispositivo_ID_Objetivo]
[Número_de_Pruebas_a_Ejecutar]
54-P020
Prepara subconjuntos de pruebas 54-020
54-P025
54-025
54-P095
Procesa resultados, añade a matriz de resultados, prep para registro 54-090
54-P090
Hace Pruebas 54-080
54-P080
Establece puerto aleatorio dentro del rango min & max 54-070
54-P070
Establece variables ejecución pruebas de matriz 54-060
54-P060
Contador VAR ++ 54-050
No
54-P050
54-P030
¿Contador VAR >= número a probar?
54-030
Sí 54-P800
Devuelve resultados prueba y los registra 54-800
54-P900
Fin
54-900

FIG. 54

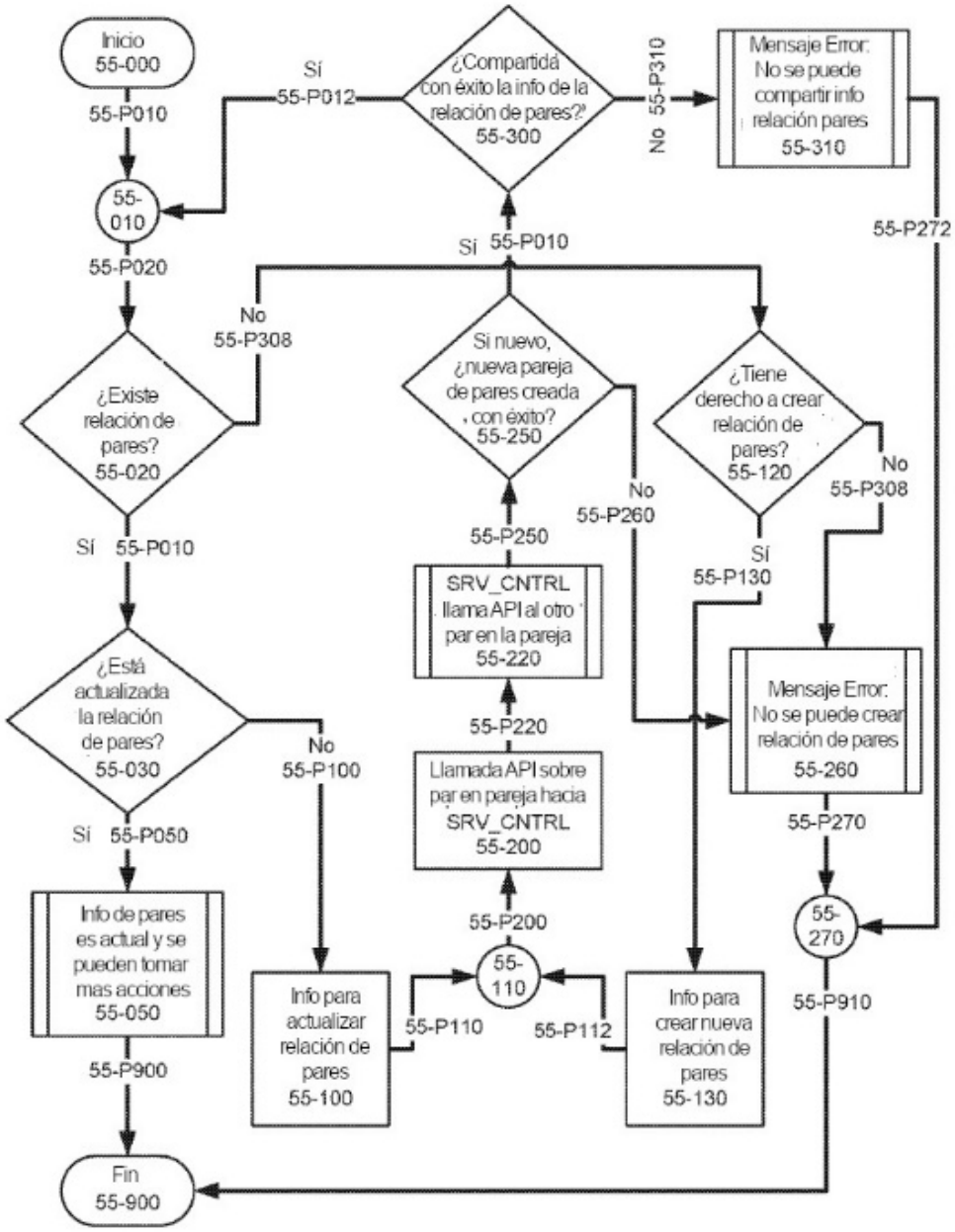
Inicio
55-000
55-P010
55-
010
55-P020
¿Existe relación de pares?
55-020
Sí 55-P010
¿Está actualizada la relación de pares?
55-030
Sí 55-P050
Info de pares es actual y se pueden tomar mas acciones
55-050
55-P900
Fin
55-900
No
55-P100
Info para actualizar relación de pares
55-100
55-P110
55-
110
55-P112
55-P200
Llamada API sobre par en pareja hacia SRV_CNTRL
55-200
55-P220
SRV_CNTRL llama API al otro par en la pareja
55-220
55-P250
Si nuevo, ¿nueva pareja de pares creada con éxito?
55-250
No
55-P260
Info para crear nueva relación de pares
55-130
Sí
55-P130
¿Tiene derecho a crear relación de pares?
55-120
No
55-P308
Mensaje Error: No se puede crear relación de pares
55-260
55-P270
55-
270
55-P910
No
55-P308
Mensaje Error: No se puede compartir info relación pares
55-310
55-P272
Sí
55-P012
¿Compartida con éxito la info de la relación de pares?
55-300
No 55-P310
Sí 55-P010

FIG. 55

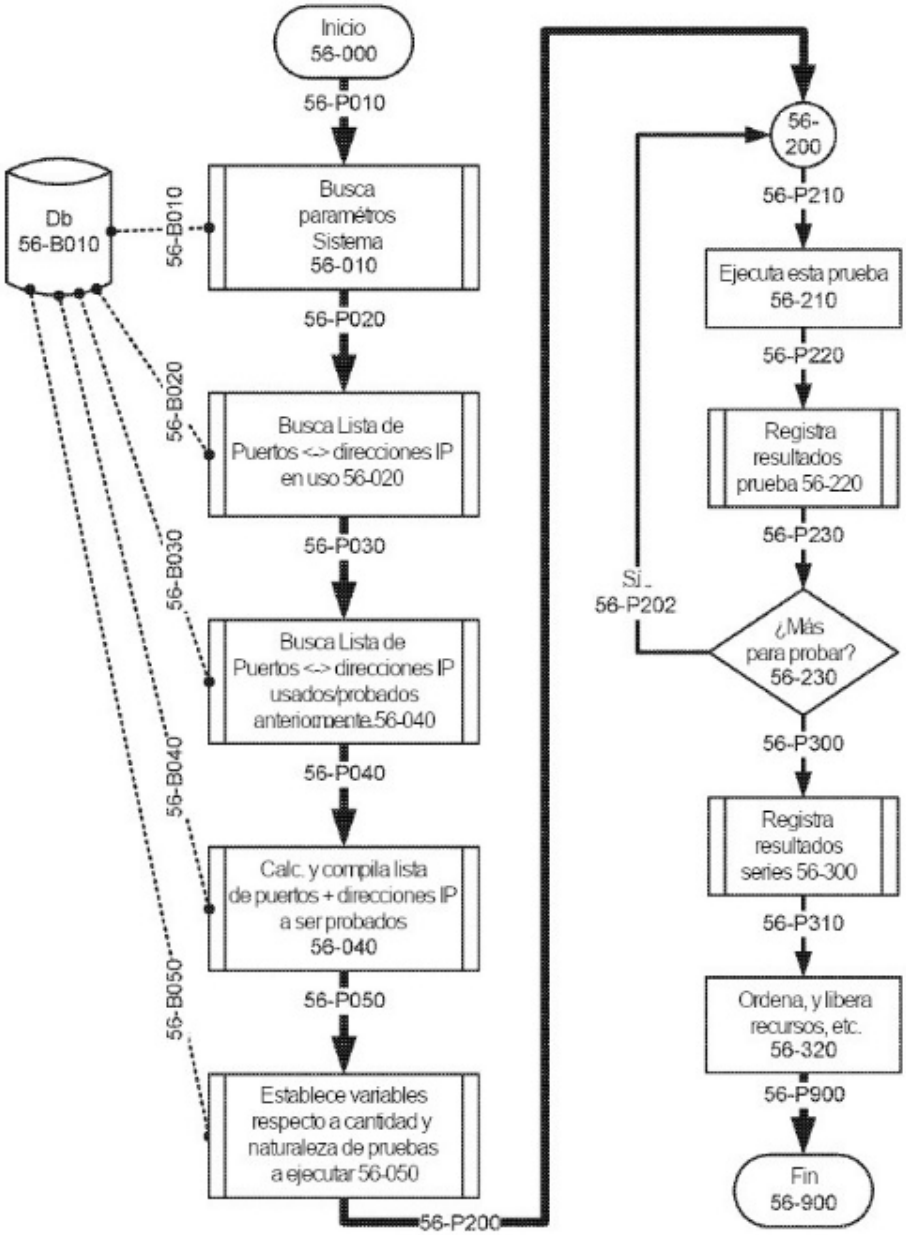
Inicio
56-000
56-P010
Db
56-B010
56-B010
Busca
paramétros
Sistema
56-010
56-P020
56-B020
Busca Lista de
Puertos <-> direcciones IP
en uso 56-020
56-P030
56-B030
Busca Lista de
Puertos <-> direcciones IP
usados/probados
anteriormente.56-040
56-P040
56-B040
Calc. y compila lista
de puertos + direcciones IP
a ser probados
56-040
56-P050
56-B050
Establece variables
respecto a cantidad y
naturaleza de pruebas
a ejecutar 56-050
56-P200
56-
200
56-P210
Ejecuta esta prueba
56-210
56-P220
Registra
resultados
prueba 56-220
56-P230
¿Más
para probar?
56-230
Si
56-P202
56-P300
Registra
resultados
series 56-300
56-P310
Ordena, y libera
recursos, etc.
56-320
56-P900
Fin
56-900

FIG. 56

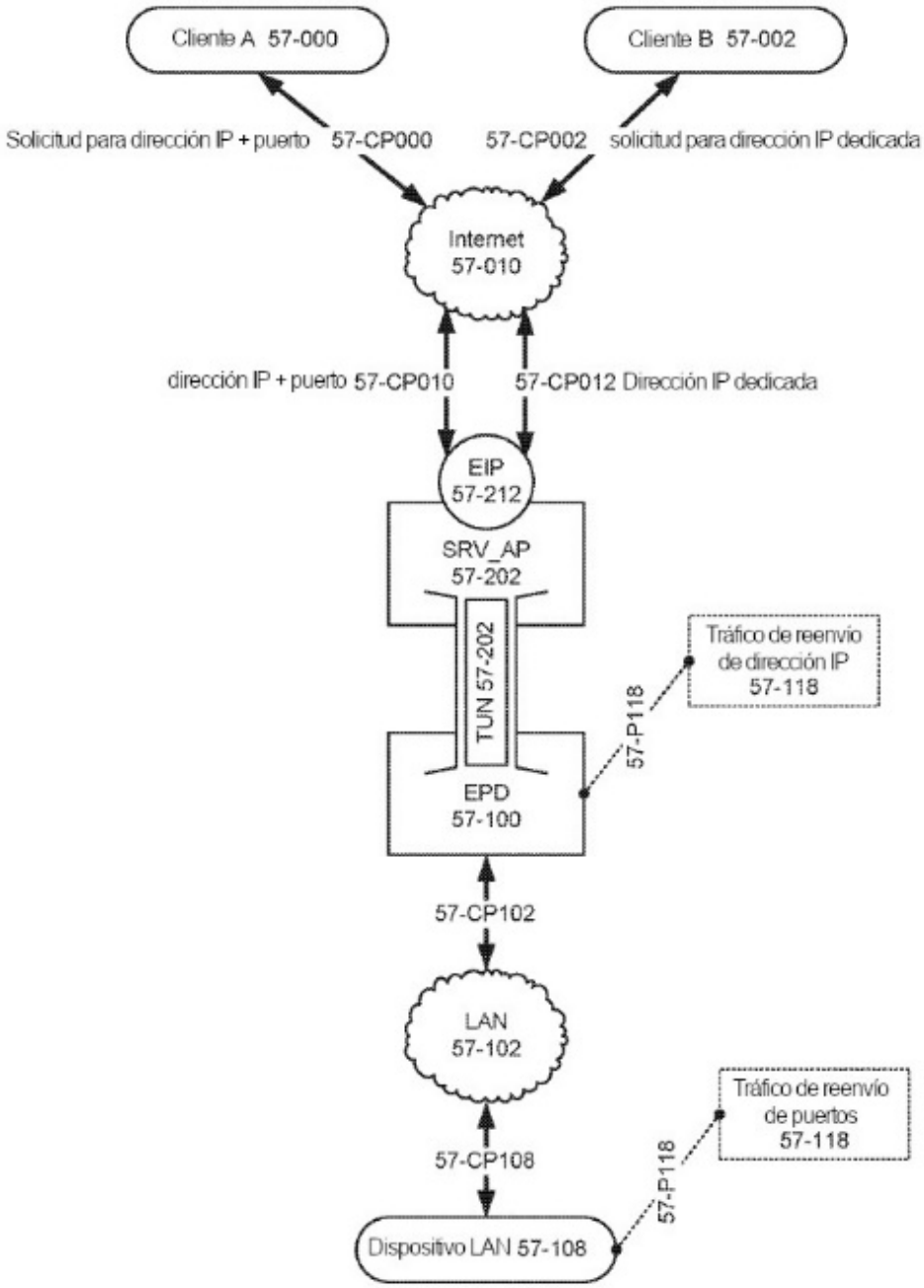
Cliente A 57-000
Cliente B 57-002
Solicitud para dirección IP + puerto
57-CP000
57-CP002
solicitud para dirección IP dedicada
Internet
57-010
dirección IP + puerto 57-CP010
57-CP012 Dirección IP dedicada
EIP
57-212
SRV_AP
57-202
TUN 57-202
Tráfico de reenvío
de dirección IP
57-118
57-P118
EPD
57-100
57-CP102
LAN
57-102
Tráfico de reenvío
de puertos
57-118
57-CP108
57-P118
Dispositivo LAN 57-108

FIG. 57

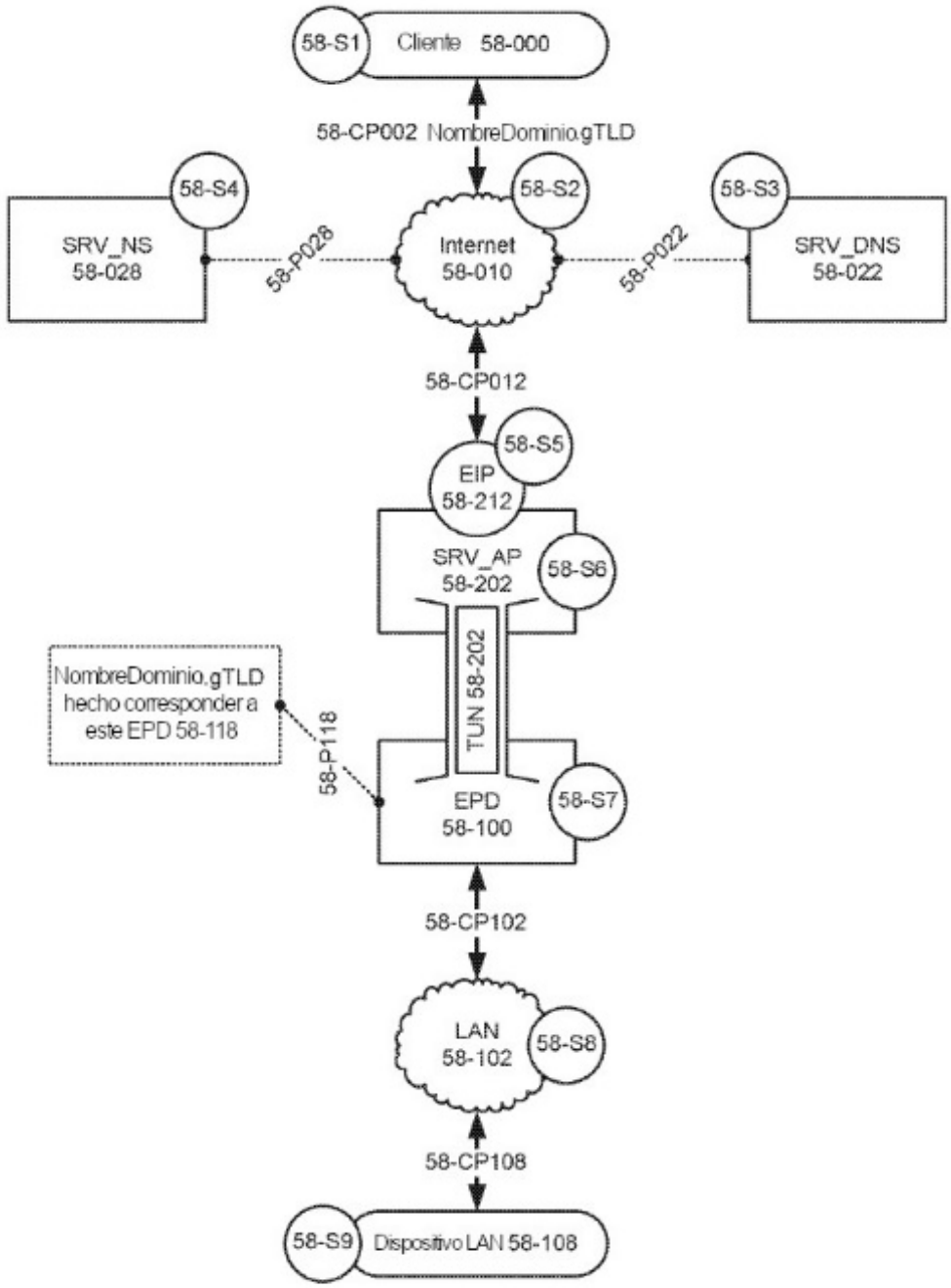
58-S1
Cliente 58-000
58-CP002 NombreDominio.gTLD
58-S4
SRV_NS
58-028
58-P028
58-S2
Internet
58-010
58-P022
58-S3
SRV_DNS
58-022
58-CP012
58-S5
EIP
58-212
SRV_AP
58-202
58-S6
TUN 58-202
NombreDominio.gTLD
hecho corresponder a
este EPD 58-118
58-P118
EPD
58-100
58-S7
58-CP102
LAN
58-102
58-S8
58-CP108
58-S9
Dispositivo LAN 58-108

FIG. 58

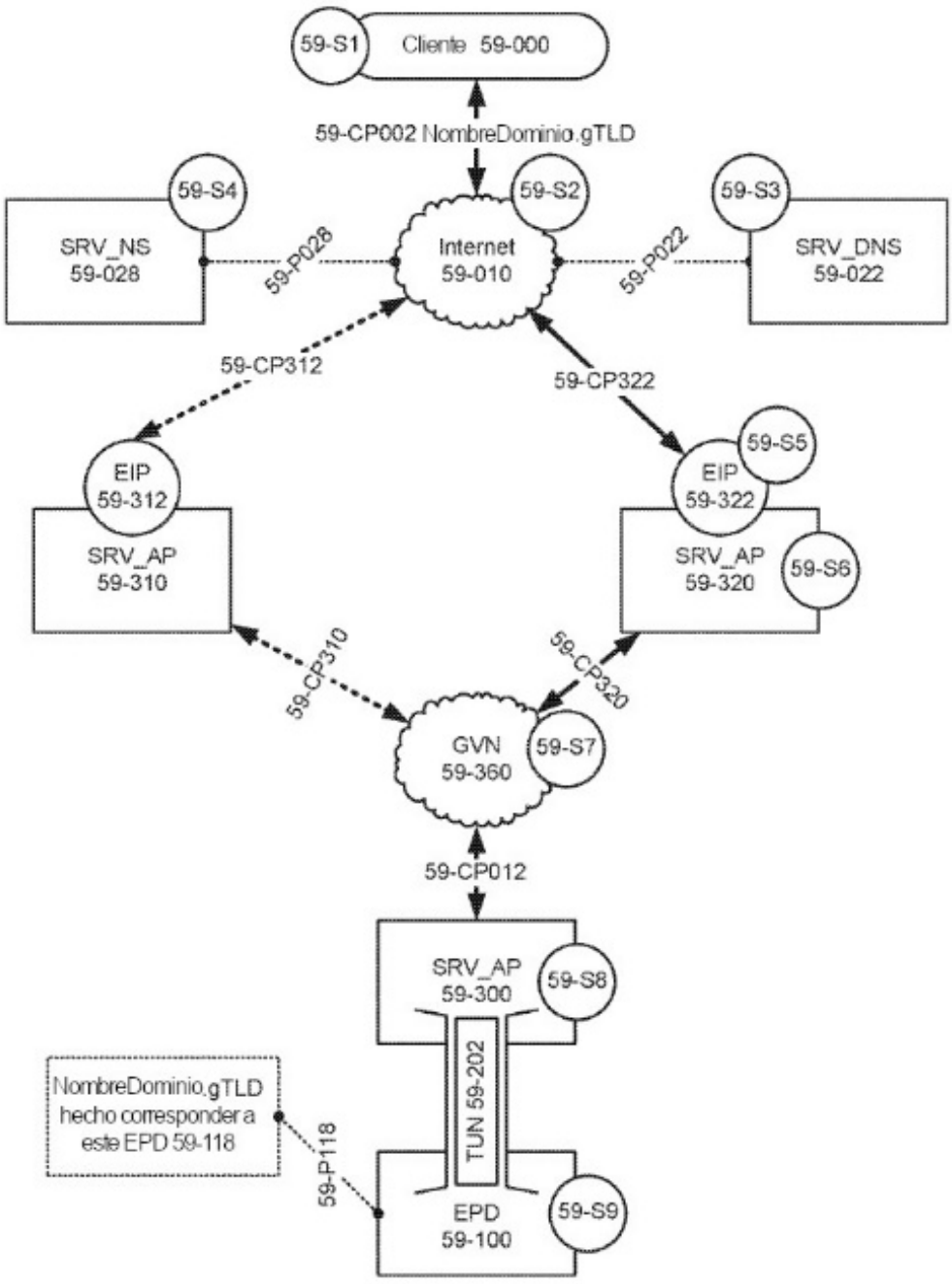
59-S1
Cliente 59-000
59-CP002 NombreDominio.gTLD
59-S4
SRV_NS
59-028
59-P028
59-S2
Internet
59-010
59-P022
59-S3
SRV_DNS
59-022
59-CP312
59-CP322
EIP
59-312
SRV_AP
59-310
59-S5
EIP
59-322
SRV_AP
59-320
59-S6
59-CP310
59-CP320
GVN
59-360
59-S7
59-CP012
SRV_AP
59-300
59-S8
TUN 59-202
NombreDominio.gTLD
hecho corresponder a
este EPD 59-118
59-P118
EPD
59-100
59-S9

FIG. 59

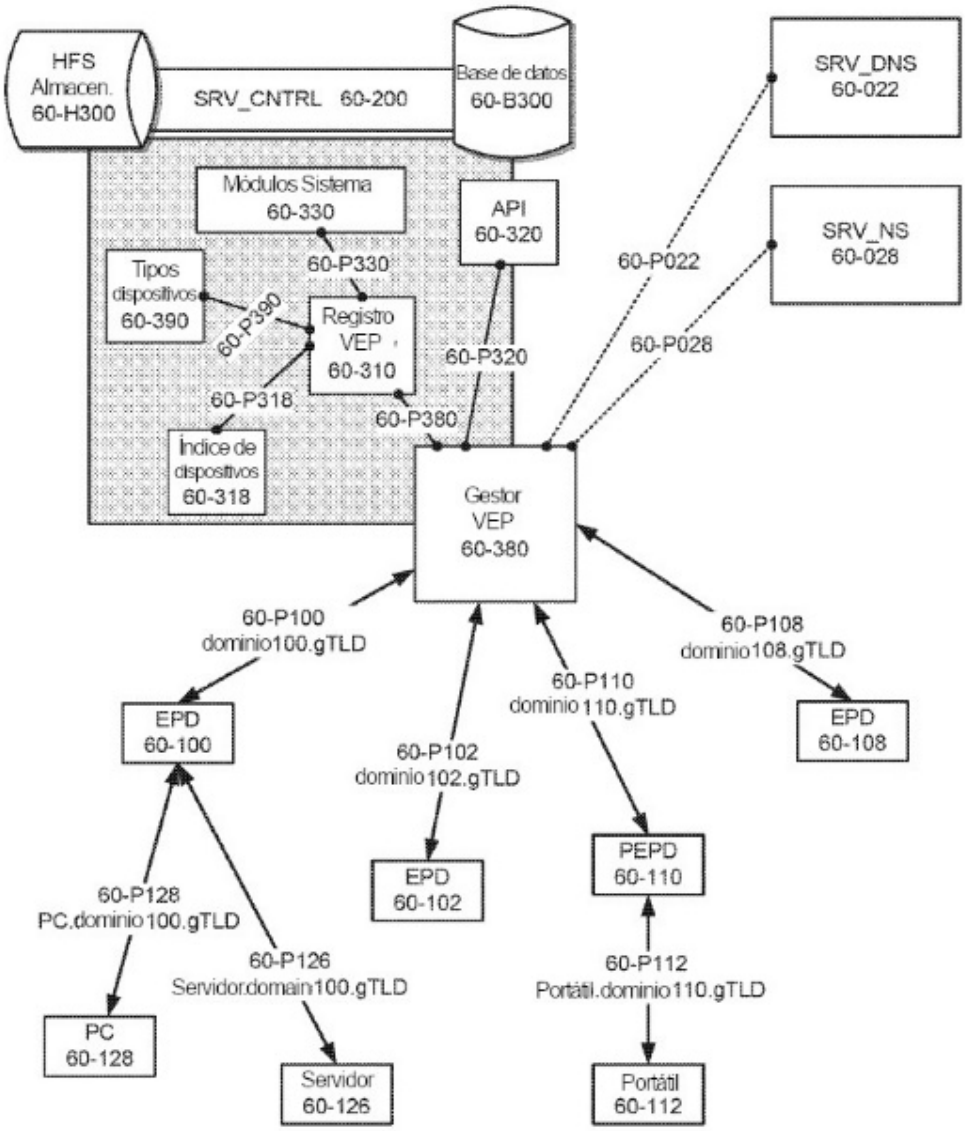
HFS
Almacen.
60-H300
SRV_CNTRL 60-200
Base de datos
60-B300
SRV_DNS
60-022
Módulos Sistema
60-330
API
60-320
SRV_NS
60-028
Tipos
dispositivos
60-390
60-P330
60-P022
60-P390
Registro
VEP
60-310
60-P320
60-P028
60-P318
60-P380
Índice de
dispositivos
60-318
Gestor
VEP
60-380
60-P100
dominio100.gTLD
60-P108
dominio108.gTLD
60-P110
dominio110.gTLD
EPD
60-100
EPD
60-108
60-P102
dominio102.gTLD
EPD
60-102
PEPD
60-110
60-P128
PC.dominio100.gTLD
60-P126
Servidor.domain100.gTLD
60-P112
Portátil.dominio110.gTLD
PC
60-128
Servidor
60-126
Portátil
60-112

FIG. 60

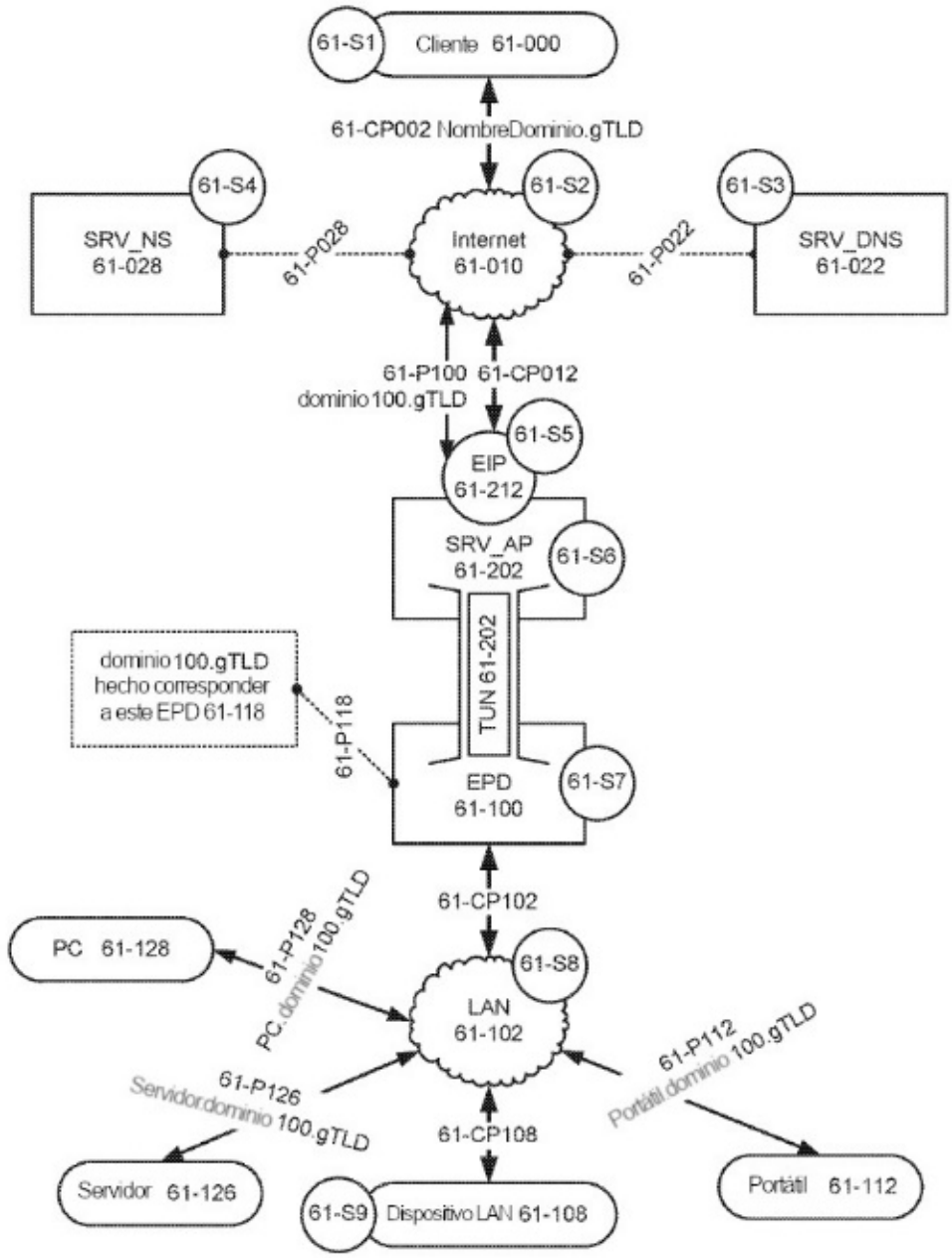
61-S1
Cliente 61-000
61-CP002 NombreDominio.gTLD
61-S4
SRV_NS
61-028
61-P028
61-S2
Internet
61-010
61-P022
61-S3
SRV_DNS
61-022
61-P100
dominio100.gTLD
61-CP012
61-S5
EIP
61-212
SRV_AP
61-202
61-S6
TUN 61-202
dominio100.gTLD
hecho corresponder
a este EPD 61-118
61-P118
EPD
61-100
61-S7
61-CP102
PC 61-128
61-P128
PC.dominio100.gTLD
61-S8
LAN
61-102
61-P126
Servidor.dominio 100.gTLD
61-P112
Portátil.dominio 100.gTLD
61-CP108
Servidor 61-126
61-S9
Dispositivo LAN 61-108
Portátil 61-112

FIG. 61

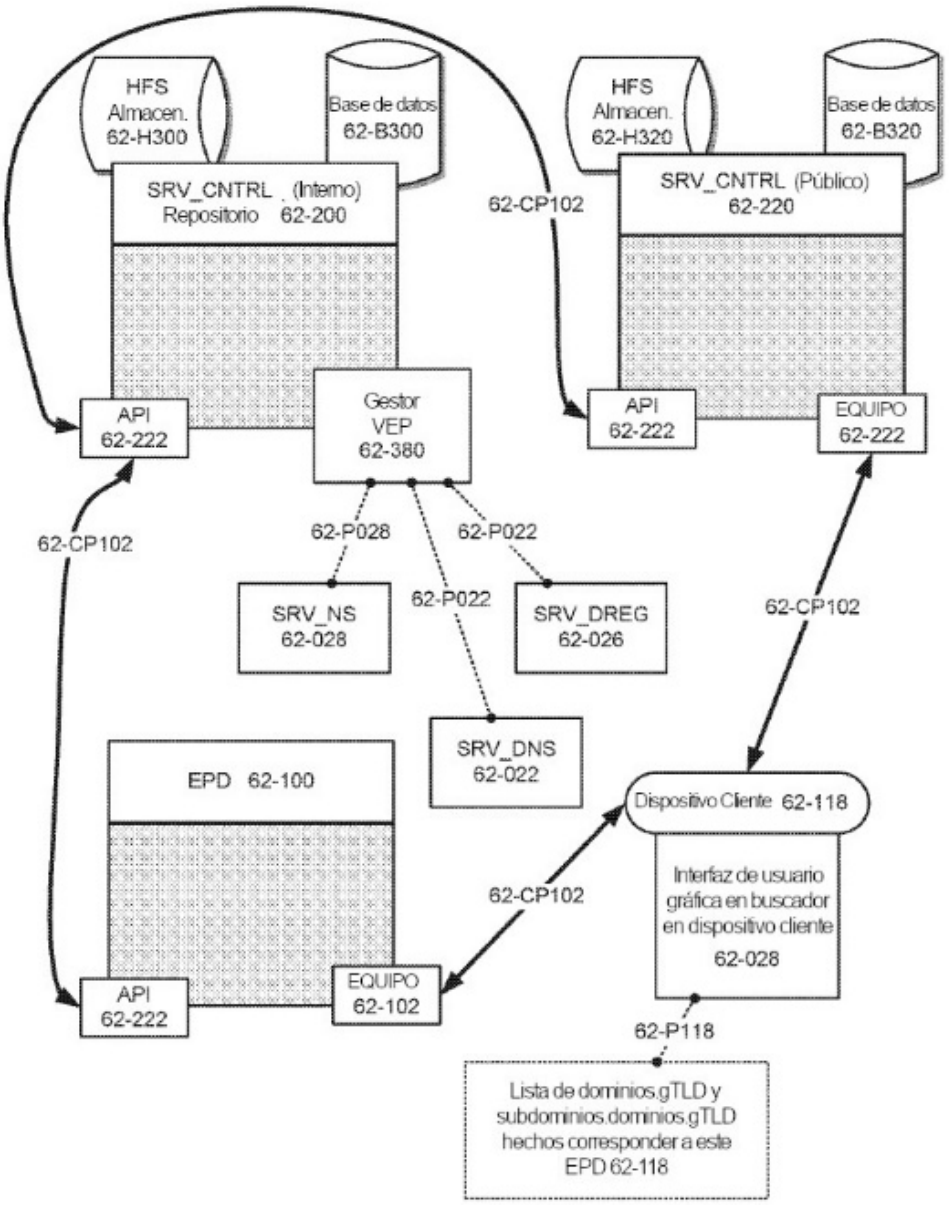
HFS
Almacen.
62-H300
Base de datos
62-B300
SRV_CNTRL (Interno)
Repositorio 62-200
API
62-222
Gestor
VEP
62-380
62-CP102
HFS
Almacen.
62-H320
Base de datos
62-B320
SRV_CNTRL (Público)
62-220
API
62-222
EQUIPO
62-222
62-CP102
62-P028
62-P022
62-P022
SRV_NS
62-028
SRV_DREG
62-026
SRV_DNS
62-022
62-CP102
EPD 62-100
Dispositivo Cliente 62-118
Interfaz de usuario
gráfica en buscador
en dispositivo cliente
62-028
62-CP102
API
62-222
EQUIPO
62-102
62-P118
Lista de dominios gTLD y
subdominios dominios gTLD
hechos corresponder a este
EPD 62-118

FIG. 62

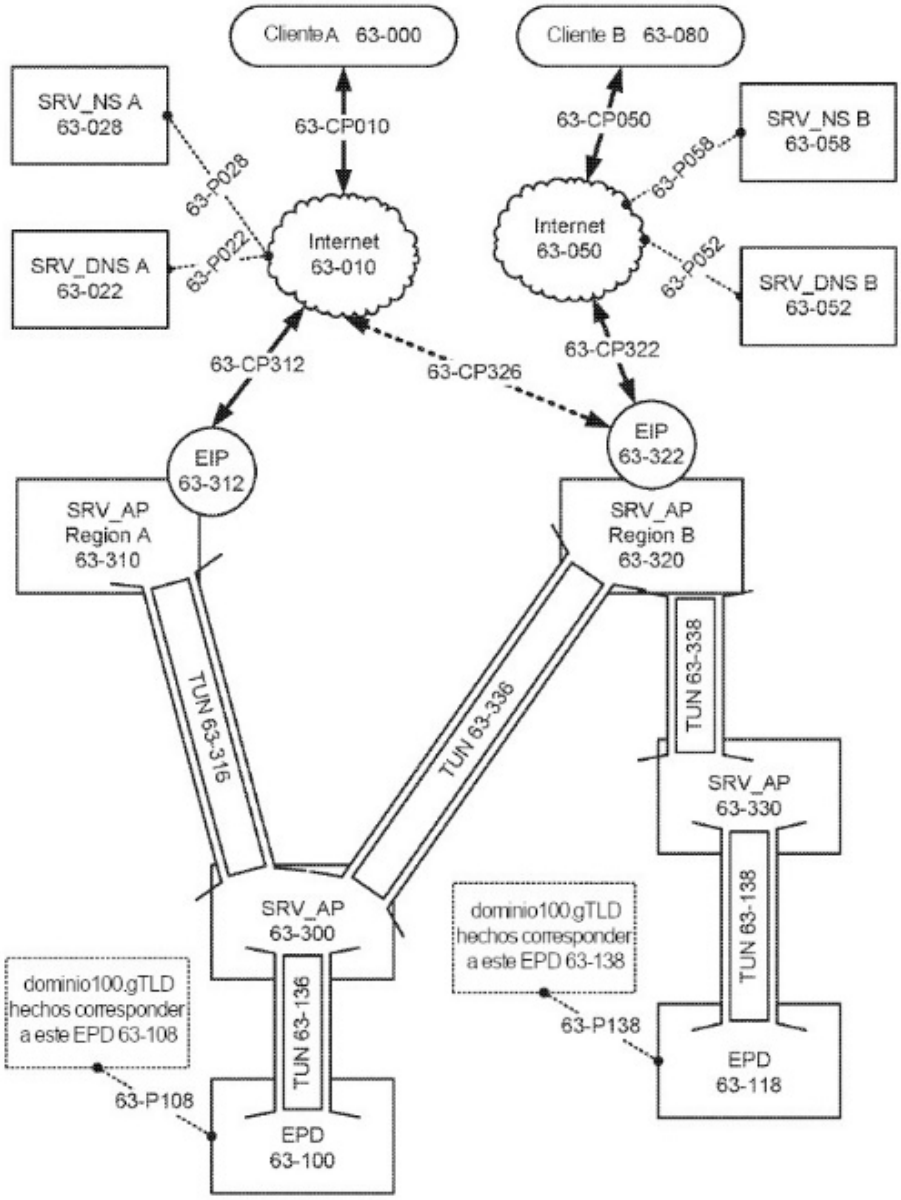
Cliente A 63-000
Cliente B 63-080
SRV_NS A 63-028
63-CP010
63-CP050
SRV_NS B 63-058
63-P028
63-P058
Internet 63-010
Internet 63-050
SRV_DNS A 63-022
63-P022
63-P052
SRV_DNS B 63-052
63-CP312
63-CP326
63-CP322
EIP 63-312
EIP 63-322
SRV_AP Region A 63-310
SRV_AP Region B 63-320
TUN 63-316
TUN 63-336
TUN 63-338
SRV_AP 63-330
SRV_AP 63-300
TUN 63-138
TUN 63-136
dominio100.gTLD hechos corresponder a este EPD 63-138
dominio100.gTLD hechos corresponder a este EPD 63-108
63-P138
63-P108
EPD 63-118
EPD 63-100

FIG. 63

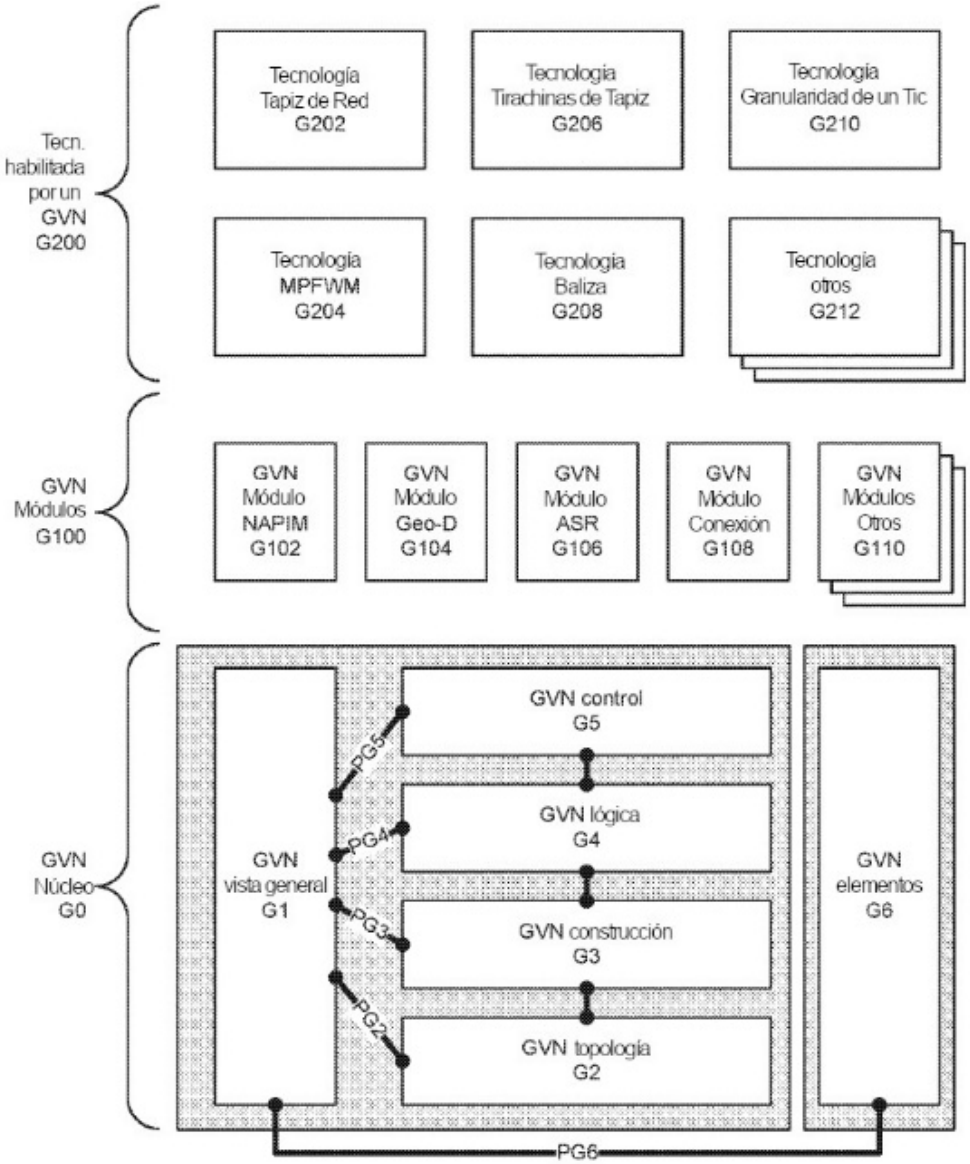
Tecn. habilitada por un GVN G200
Tecnología Tapiz de Red G202
Tecnología Tirachinas de Tapiz G206
Tecnología Granularidad de un Tic G210
Tecnología MPFWM G204
Tecnología Baliza G208
Tecnología otros G212
GVN Módulos G100
GVN Módulo NAPIM G102
GVN Módulo Geo-D G104
GVN Módulo ASR G106
GVN Módulo Conexión G108
GVN Módulos Otros G110
GVN Núcleo G0
GVN vista general G1
GVN control G5
GVN lógica G4
GVN construcción G3
GVN topología G2
GVN elementos G6
PG5
PG4
PG3
PG2
PG6

FIG. 64

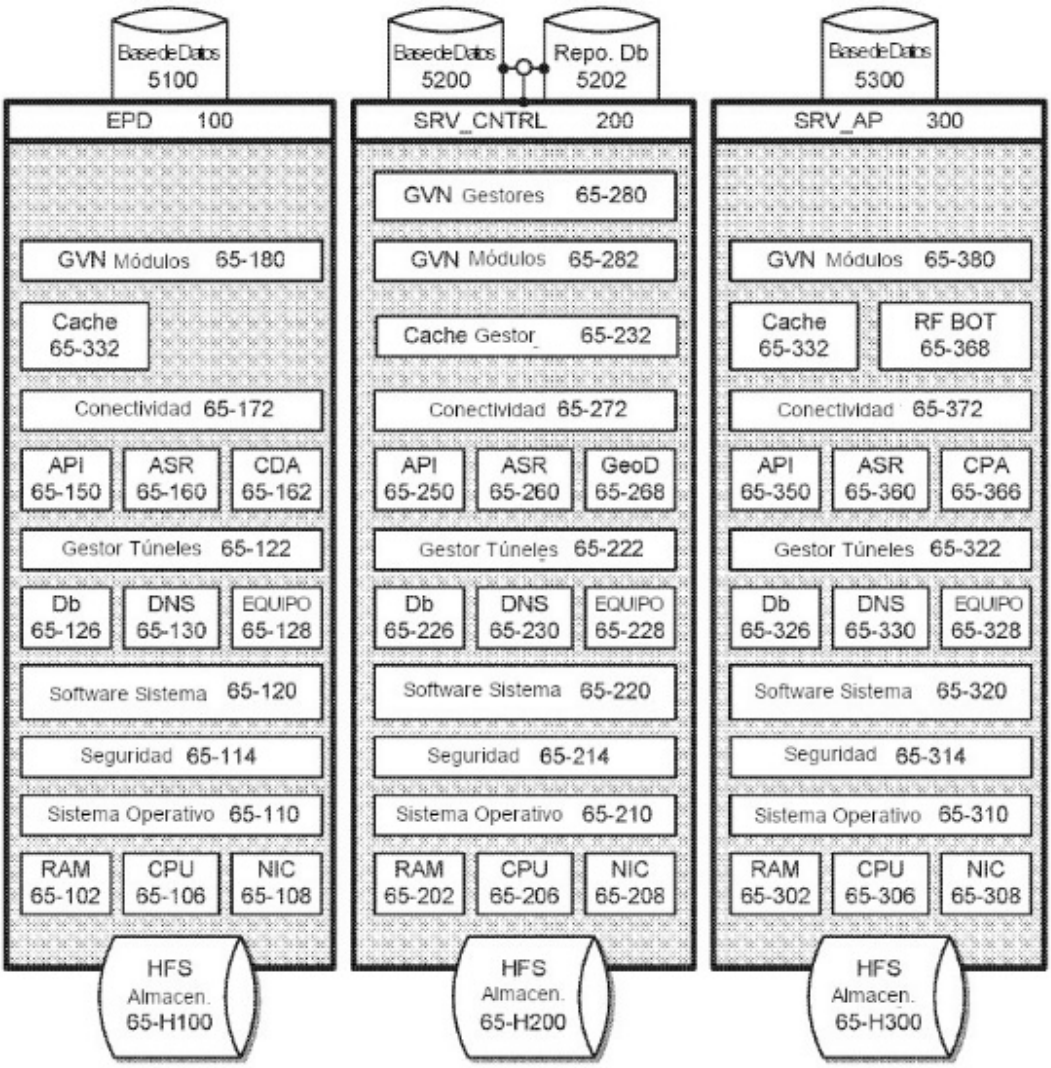
Base de Datos 5100
Base de Datos 5200
Repo. Db 5202
Base de Datos 5300
EPD 100
SRV_CNTRL 200
SRV_AP 300
GVN Gestores 65-280
GVN Módulos 65-180
GVN Módulos 65-282
GVN Módulos 65-380
Cache 65-332
Cache Gestor 65-232
Cache 65-332
RF BOT 65-368
Conectividad 65-172
Conectividad 65-272
Conectividad 65-372
API 65-150
ASR 65-160
CDA 65-162
API 65-250
ASR 65-260
GeoD 65-268
API 65-350
ASR 65-360
CPA 65-366
Gestor Túneles 65-122
Gestor Túneles 65-222
Gestor Túneles 65-322
Db 65-126
DNS 65-130
EQUIPO 65-128
Db 65-226
DNS 65-230
EQUIPO 65-228
Db 65-326
DNS 65-330
EQUIPO 65-328
Software Sistema 65-120
Software Sistema 65-220
Software Sistema 65-320
Seguridad 65-114
Seguridad 65-214
Seguridad 65-314
Sistema Operativo 65-110
Sistema Operativo 65-210
Sistema Operativo 65-310
RAM 65-102
CPU 65-106
NIC 65-108
RAM 65-202
CPU 65-206
NIC 65-208
RAM 65-302
CPU 65-306
NIC 65-308
HFS Almacen. 65-H100
HFS Almacen. 65-H200
HFS Almacen. 65-H300

FIG. 65

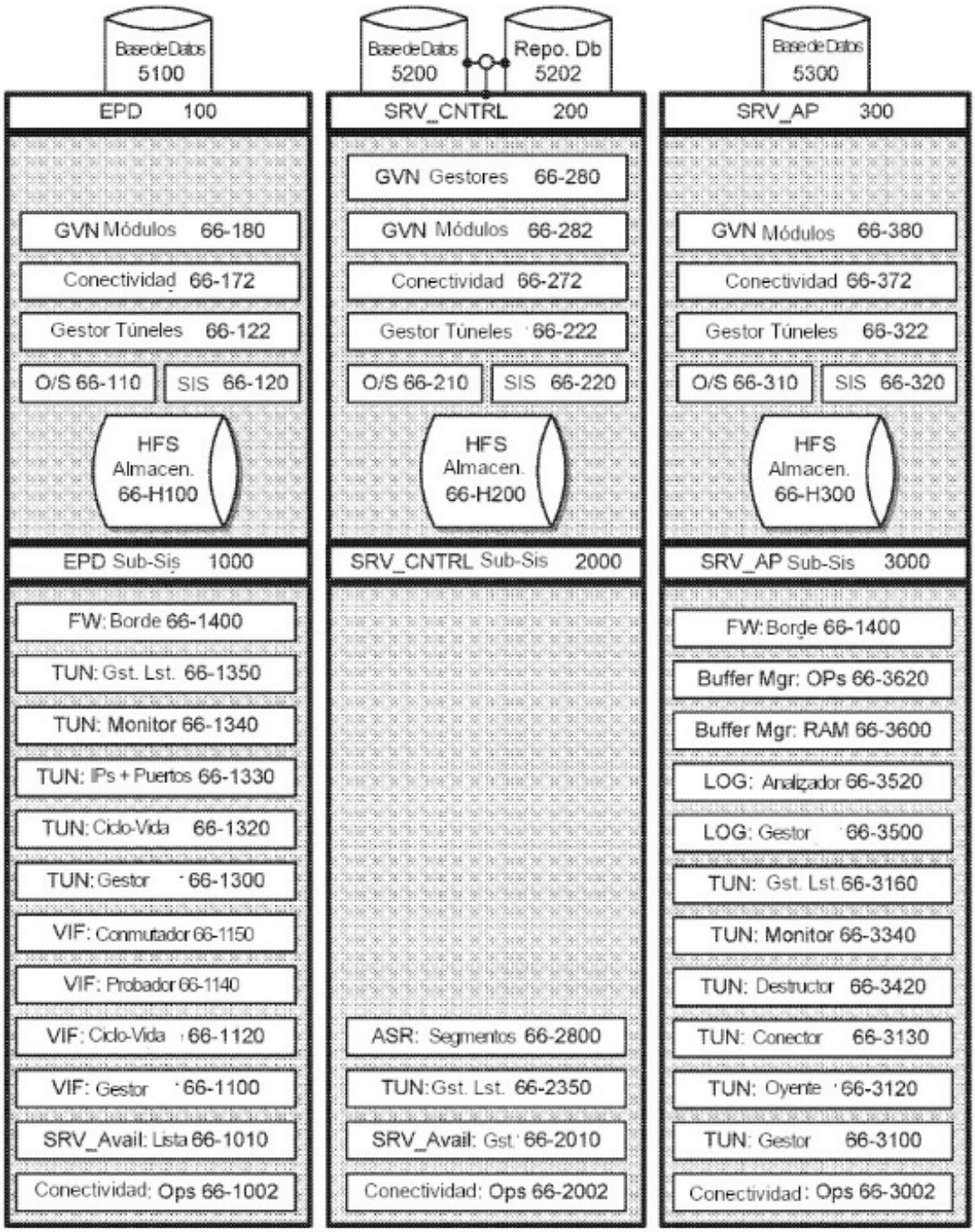
Base de Datos 5100
Base de Datos 5200
Repo. Db 5202
Base de Datos 5300
EPD 100
SRV_CNTRL 200
SRV_AP 300
GVN Módulos 66-180
Conectividad 66-172
Gestor Túneles 66-122
O/S 66-110
SIS 66-120
HFS Almacen. 66-H100
GVN Gestores 66-280
GVN Módulos 66-282
Conectividad 66-272
Gestor Túneles 66-222
O/S 66-210
SIS 66-220
HFS Almacen. 66-H200
GVN Módulos 66-380
Conectividad 66-372
Gestor Túneles 66-322
O/S 66-310
SIS 66-320
HFS Almacen. 66-H300
EPD Sub-Sis 1000
SRV_CNTRL Sub-Sis 2000
SRV_AP Sub-Sis 3000
FW: Borde 66-1400
TUN: Gst. Lst. 66-1350
TUN: Monitor 66-1340
TUN: IPs + Puertos 66-1330
TUN: Ciclo-Vida 66-1320
TUN: Gestor 66-1300
VIF: Conmutador 66-1150
VIF: Probador 66-1140
VIF: Ciclo-Vida 66-1120
VIF: Gestor 66-1100
SRV_Avail: Lista 66-1010
Conectividad: Ops 66-1002
ASR: Segmentos 66-2800
TUN: Gst. Lst. 66-2350
SRV_Avail: Gst. 66-2010
Conectividad: Ops 66-2002
FW: Borde 66-1400
Buffer Mgr: OPs 66-3620
Buffer Mgr: RAM 66-3600
LOG: Analizador 66-3520
LOG: Gestor 66-3500
TUN: Gst. Lst. 66-3160
TUN: Monitor 66-3340
TUN: Destructor 66-3420
TUN: Conector 66-3130
TUN: Oyente 66-3120
TUN: Gestor 66-3100
Conectividad: Ops 66-3002

FIG. 66

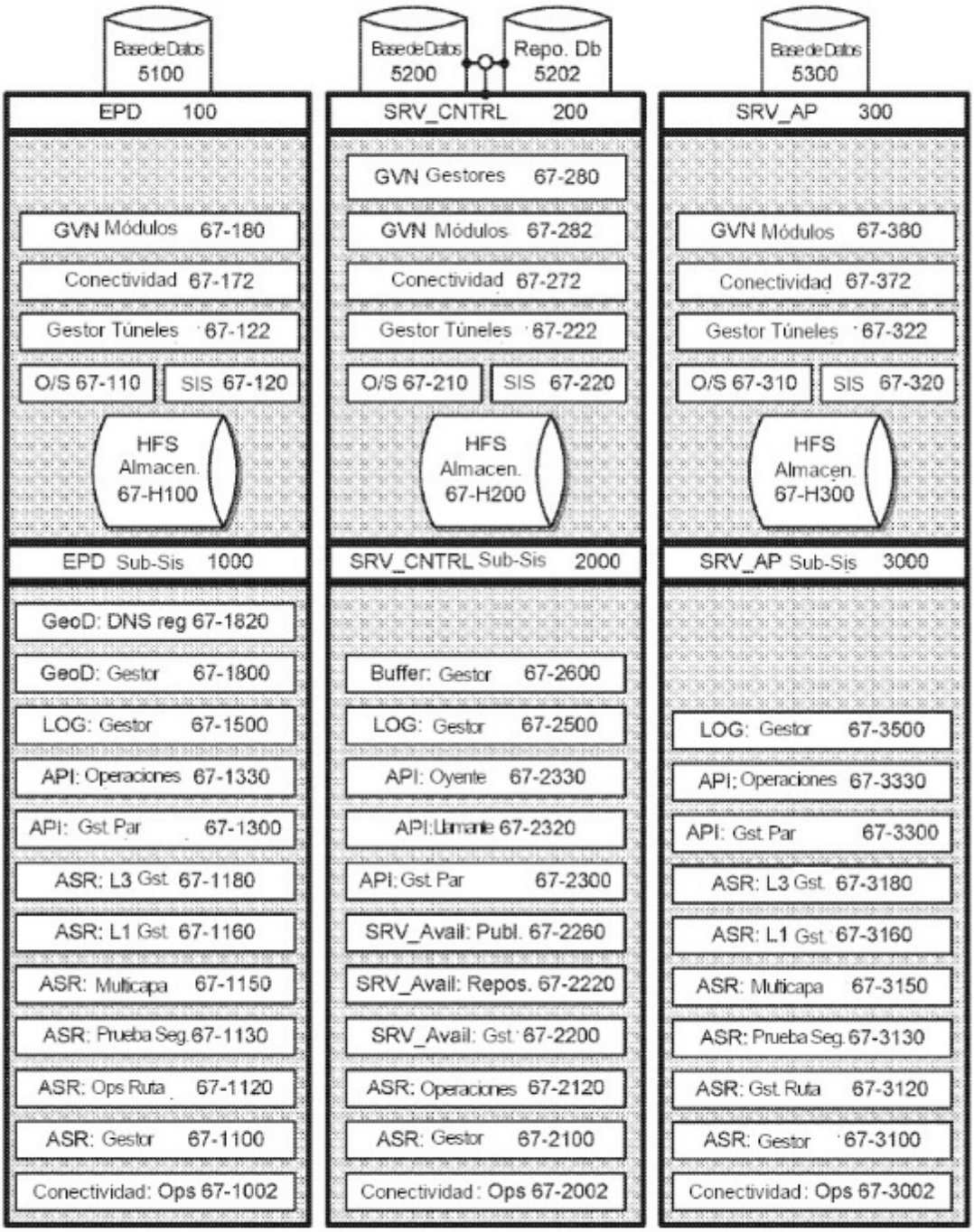
Base de Datos 5100
Base de Datos 5200
Repo. Db 5202
Base de Datos 5300
EPD 100
SRV_CNTRL 200
SRV_AP 300
GVN Módulos 67-180
Conectividad 67-172
Gestor Túneles 67-122
O/S 67-110
SIS 67-120
HFS Almacen. 67-H100
GVN Gestores 67-280
GVN Módulos 67-282
Conectividad 67-272
Gestor Túneles 67-222
O/S 67-210
SIS 67-220
HFS Almacen. 67-H200
GVN Módulos 67-380
Conectividad 67-372
Gestor Túneles 67-322
O/S 67-310
SIS 67-320
HFS Almacen. 67-H300
EPD Sub-Sis 1000
SRV_CNTRL Sub-Sis 2000
SRV_AP Sub-Sis 3000
GeoD: DNS reg 67-1820
GeoD: Gestor 67-1800
LOG: Gestor 67-1500
API: Operaciones 67-1330
API: Gst Par 67-1300
ASR: L3 Gst 67-1180
ASR: L1 Gst 67-1160
ASR: Multicapa 67-1150
ASR: Prueba Seg 67-1130
ASR: Ops Ruta 67-1120
ASR: Gestor 67-1100
Conectividad: Ops 67-1002
Buffer: Gestor 67-2600
LOG: Gestor 67-2500
API: Oyente 67-2330
API: Llamante 67-2320
API: Gst Par 67-2300
SRV_Avail: Publ. 67-2260
SRV_Avail: Repos. 67-2220
SRV_Avail: Gst 67-2200
ASR: Operaciones 67-2120
ASR: Gestor 67-2100
Conectividad: Ops 67-2002
LOG: Gestor 67-3500
API: Operaciones 67-3330
API: Gst Par 67-3300
ASR: L3 Gst 67-3180
ASR: L1 Gst 67-3160
ASR: Multicapa 67-3150
ASR: Prueba Seg 67-3130
ASR: Gst Ruta 67-3120
ASR: Gestor 67-3100
Conectividad: Ops 67-3002

FIG. 67