UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PROPUESTA DE UN SISTEMA DE CONECTIVIDAD CORPORATIVA
PARA UNA EMPRESA PETROLERA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

ALEXIS RAPHAEL GUERRERO HERRERA

PROMOCIÓN
1997-I

LIMA-PERÚ
2012

PROPUESTA DE UN SISTEMA DE CONECTIVIDAD CORPORATIVA PARA UNA EMPRESA PETROLERA

A Jesucristo, mi Señor y Salvador de mi vida, a mis padres por su esfuerzo y constante apoyo, a mi esposa, por ser mi ayuda idónea y a mis hijos, herencia de Dios.

SUMARIO

El presente trabajo desarrolla una solución que es parte de un proyecto mayor orientado a proveer mayor disponibilidad en los servicios de transmisión de datos a nivel WAN (conectividad). La solución en particular se enfoca en optimizar la transferencia de datos en dicha conectividad mediante:

- La mejora de la transferencia de datos (Uso de técnicas de compresión de datos)
- El Análisis del tráfico cursado (Uso de protocolo NetFlow).

La solución era necesaria debido a falta de disponibilidad de la conectividad, además de la lentitud en la transferencia de información y desconocimiento del tipo de tráfico cursado (uso de recursos) entre las diferentes sedes de la empresa petrolera, lo que limitaba el uso de aplicaciones de voz y video, requeridas por la empresa.

Las técnicas de compresión de datos son implementadas en dispositivos especialmente diseñados para ello. El planteamiento de la solución realiza un análisis situacional del caso de estudio y luego evalúa las alternativas para luego dimensionar el proyecto de optimización de tráfico WAN, por otra parte el análisis/administración de tráfico es realizado mediante el protocolo NetFlow (propietario de Cisco) que facilita esta labor de registro, análisis y reporte del tráfico cursado

La solución se desarrolla para todas las sedes de la corporación, por ello se presentará la metodología y aspectos funcionales y de configuración de manera general, es decir, se explica la solución técnica ofrecida para la empresa petrolera.

ÍNDICE

INTRODUCCIÓN

El proyecto de optimización de conectividad corporativa de una empresa petrolera surge por la problemática de disponibilidad y lentitud de tráfico (debida en parte a la utilización de tecnología de menor calidad), además de la necesidad de la empresa de utilizar eficientemente aplicaciones de voz y video.

Parte de la solución se basó en la migración de ADSL a Ethernet o a TDM dependiendo de la disponibilidad de esta tecnología en los nodos del proveedor, así como en el cambio de los enlaces de cobre como medio de acceso por fibra óptica (también los equipos correspondientes), y la realización de un upgrade (mejora) en el ancho de banda a los enlaces radiales y modernización de equipamiento.

Es sobre la solución descrita que se optimiza la transferencia de datos en la WAN mediante el uso de técnicas de compresión de datos implementadas sobre dispositivos de propósito especial con la finalidad de que los canales transporten mayor cantidad de información, así mismo se provee una técnica para que se pueda analizar el tráfico cursado y así optimizar el uso de los recursos.

La solución es efectuada sobre 29 sedes (LAN) que conforman la WAN, cada una con sus propias características en cuanto a cantidad de usuarios, cantidad de sesiones concurrentes por usuarios y tipo de protocolo y/o aplicaciones.

La tecnología de la solución aplicada es denominada "Wide Area Application Services" o WAAS. Cisco fue el primero en proveer este sistema de optimización de la WAN que fuera transparente a la red. Esto se cumple por cuanto se preserva los detalles de la cabecera de los paquetes IP, esto incluye las direcciones IP, y los números de puerto TCP, lo cual es considerado importante para que los dispositivos y servicios intermedios funcionen de manera apropiada.

La solución también es desarrollada con el protocolo NetFlow, el cual es imprescindible para una buena utilización de los recursos de red, ya que permite conocer el estado de la misma y sus tendencias de consumo.

El informe está dividido en cuatro capítulos principales:

- Capítulo I "Planteamiento de Ingeniería del Problema".- Se presenta la problemática, se precisa los objetivos y los alcances del informe.
- Capítulo II "Marco Teórico".- Desarrolla los siguientes tópicos: Aspectos conceptuales de la WAN, Optimización de la WAN, Protocolo de red NetFlow.

- Capítulo III "Metodología para la Solución del Problema".- Es donde se realiza el planteamiento de la solución, la descripción de la solución de optimización de tráfico de datos, y la Implementación de la solución de análisis de tráfico cursado (NetFlow).
- Capítulo IV "Análisis y Presentación de Resultados".- Se presentan los siguientes tópicos: Niveles de optimización, Presupuesto y tiempo de ejecución, Cronograma de trabajos.

CAPÍTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

En este capítulo se realiza el planteamiento de ingeniería del problema. Primeramente se describe el problema y el objetivo del trabajo. Se realiza una evaluación del problema y además se precisan los alcances del informe, finalmente se presenta una síntesis del diseño trabajado.

1.1 Descripción del problema

Falta de disponibilidad en los servicios de transmisión de datos a nivel WAN, además de la lentitud o demora en la transferencia de información y desconocimiento del tipo de tráfico cursado (uso de recursos) entre las diferentes sedes, lo que limitaba el uso de aplicaciones de voz y video requeridas por la empresa.

La empresa petrolera experimentaba los problemas mencionados, básicamente debido al uso de tecnología ADSL y TDM vía cobre (sustracción de cable por terceros y averías en la línea), además se desconocía el uso de los diferentes tipos de tráfico.

Nota:

ADSL son siglas de Asymmetric Digital Subscriber Line (Línea de abonado digital asimétrica).
TDM son siglas de Time-division multiplexing (Multiplexación por División de Tiempo)

1.2 Objetivos del trabajo

Optimizar la transferencia de datos corporativa de la empresa petrolera de mediante la aplicación de las siguientes técnicas:

- Compresión de datos.
- Análisis de tráfico cursado.

1.3 Evaluación del problema

El trabajo presentado en este informe es parte de la solución general brindada por el proveedor al cliente (Figura 1.1), la cual se pasa a explicar.

La problemática de disponibilidad y lentitud o demora en la transmisión de datos a nivel WAN era debida en parte a la utilización de tecnología ADSL. Para este caso se migró de ADSL a Ethernet o a TDM dependiendo de la disponibilidad de esta tecnología en los nodos del proveedor.

Esta problemática también se basaba en el uso de enlaces de cobre como medio de acceso para lo cual el proveedor cambió el medio por fibra óptica así como los equipos

correspondientes. En el caso de los enlaces radiales, a estos solo se les realizó un upgrade (mejora) en el ancho de banda y modernización de equipamiento.

Disponibilidad en los servicios de transmisión de datos a nivel WAN, respecto a un periodo de un mes (tiempo), se refiere al porcentaje de tiempo que el servicio ofrecido ha sido utilizado por el cliente considerando los tiempos de fallas, presentado en el servicio. La siguiente es la ecuación de disponibilidad que se consideró para este diseño.

$$\text{Disponibilidad} = \frac{(\text{Tiempo total} - \text{Tiempo total no disponible}) \times 100}{\text{Tiempo total}} \quad (1.1)$$

Tiempo total: es la cantidad total de tiempo de cada enlace usado por la empresa petrolera. Suponiendo que el 100% de disponibilidad es de 60 minutos por hora, 24 horas por día, 7 días a la semana, el servicio pudo haber estado disponible durante un periodo de un mes.

Tiempo total no disponible: es la cantidad total de tiempo no disponible de los enlaces durante un mes. No se considera dentro del tiempo de no disponibilidad las interrupciones de servicio que pudieran producirse por causas ajenas al proveedor.

La disponibilidad de los enlaces era menor a la solicitada por el cliente (99.98%), lo cual se debía a los problemas de saturación del servicio ADSL y a problemas relacionados al medio de última milla (cobre) en algunas sedes, lo que estuvo ocasionando penalidades antes de la implantación de la solución desarrollada.

Lentitud en los servicios de transmisión de datos a nivel WAN, es percibido por los usuarios cuando el ancho de banda esta saturado, ocasionado por la demanda de tráfico que generan los usuarios en las distintas sedes, esto conlleva a la presentación de averías por los usuarios a la empresa proveedora del servicio contratado.

La solución para la problemática previamente mencionada es descrita a continuación. Esta descripción agrupa a las sedes por el tipo de solución implementada (las letras entre paréntesis de la Figura 1.1 corresponden al listado mostrado). Es necesario recalcar que las sedes están interconectadas a través de la VPN (Red Privada Virtual). En la información se incluye las capacidades de los enlaces principales así como los de respaldo (lo cual proveyó mayor disponibilidad):

(a) Sede Central.- Involucra la instalación de un enlace principal y un enlace de respaldo. El enlace principal VPN vía Ethernet (ancho de banda de 20 Mbps) tiene una fibra óptica monomodo, llegando a un equipo modem óptico, para conectarse a un equipo router el cual se instala y configura en el switch core (switch principal) del cliente. El enlace de respaldo VPN vía TDM (ancho de banda de 4 Mbps) consta de dos enlaces de cobre en balanceo de carga de 2 Mbps cada uno el cual llega a un modem y se conecta a un router, el mismo que se instala y configura en el switch core del cliente.

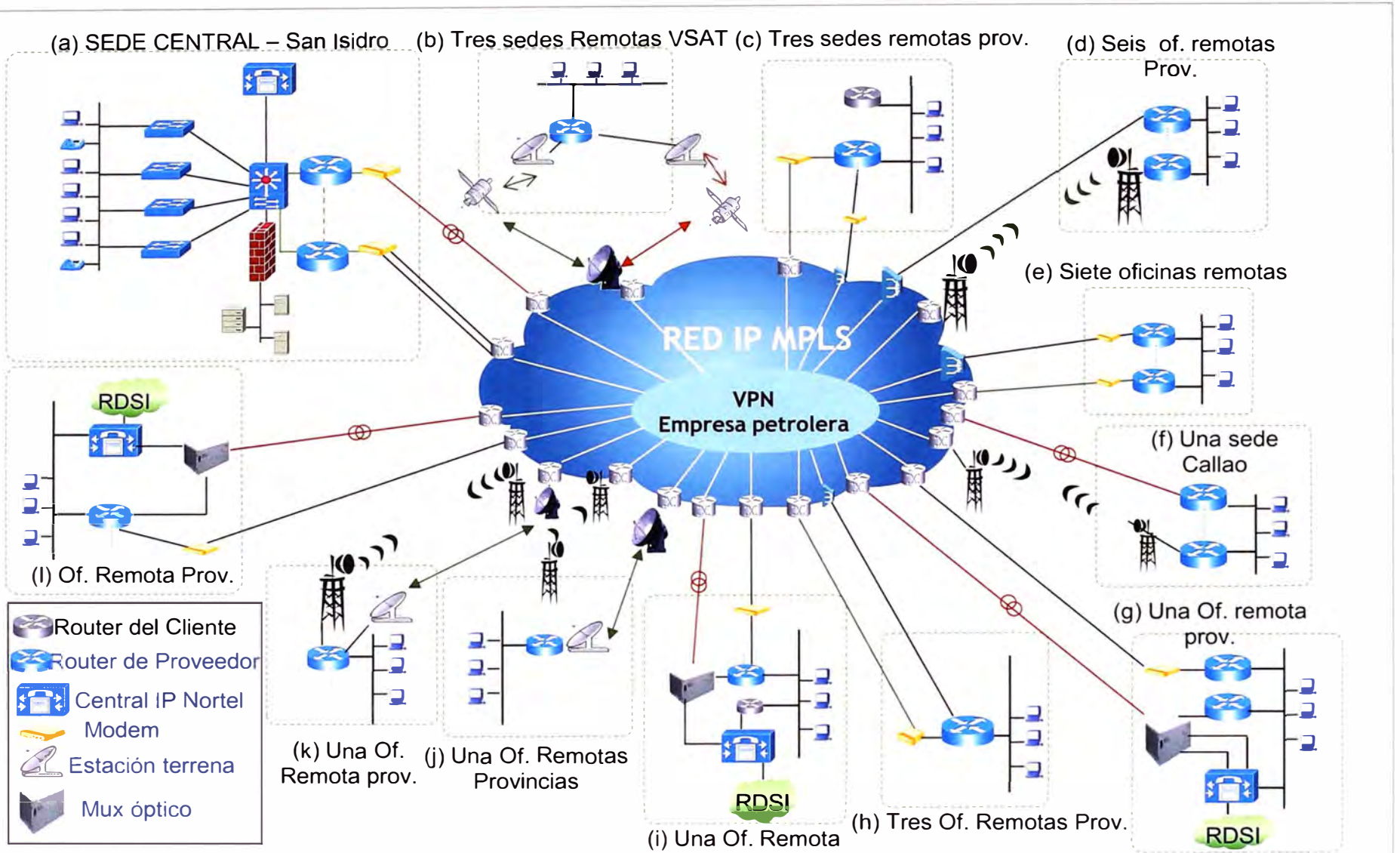

Figura 1.1 Esquema de la red de la entidad petrolera (fuente propia)

(b) Tres sedes remotas VSAT.- Involucra las sedes Pto Maldonado (ancho de banda principal 1 Mbps y de respaldo 256 Kbps), Mazuco (ancho de banda principal 1 Mbps y de respaldo 256 Kbps) y Cerro de Pasco (ancho de banda principal 512 Kbps y de respaldo 128 Kbps). Los enlaces principales son mediante el servicio Clear Channel, conectándose a un modem y luego al router local del cliente. Los enlaces de contingencia se brindan a través del servicio VSAT, instalándose la antena VSAT, un modem y un router conectado al switch de la LAN de cada sede.

(c) Tres sedes remotas provincias.- Involucra las sedes de Juliaca (ancho de banda principal 512 Kbps y de respaldo 600/256 Kbps), Yurimaguas (ancho de banda principal 256 Kbps y de respaldo 128 Kbps), Aeropuerto Cuzco (ancho de banda principal 512 Kbps y de respaldo 600/256 Kbps). Los enlaces principales son a través de VPN vía TDM, conectándose a un modem y luego a un router en cada sede. Los enlaces de contingencia se brindan a través de ADSL, instalándose un modem y conectándose al mismo router del enlace principal.

(**d) Seis oficinas remotas provincias**.- Involucra las oficinas de Pucallpa (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps), Supe (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps), Pisco (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps), Piura (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps), Tarapoto (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps) y Cusco (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps). Los enlaces principales, cuatro de ellos son a través de VPN vía TDM y dos enlaces son por radioenlace, cada uno de ellos tienen instalados un modem y un router. Los enlaces de contingencia se brindan a través de ADSL, instalándose un modem y un router. Los router de ambos enlaces, están conectados al switch de la LAN de cada sede.

(e) Siete oficinas remotas.- Involucra las sedes de Salaverry (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps), Chiclayo (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps), Chimbote (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps), Ilo (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps), Mollendo (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps), Distribuidora Arequipa (ancho de banda principal 512 Kbps y de respaldo 900/256 Kbps). Los enlaces principales son a través de VPN vía TDM, un modem y un router. Los enlaces de contingencia se brindan a través de ADSL, instalándose un modem y un router. Los router de ambos enlaces, están conectados al switch de la LAN de cada sede.

(f) Una sede Callao.- El enlace principal es VPN vía Ethernet (ancho de banda 2 Mbps) utilizando como medio de acceso fibra óptica monomodo, instalándose un media converter y un router. El enlace de respaldo se brinda utilizando la tecnología WiMax

(ancho de banda 128 Kbps), instalándose un modem y un router. Ambos routers están instalados en el switch de la LAN del cliente.

(g) Una oficina remota provincia (Talara).- El enlace principal ha sido instalado vía fibra óptica monomodo utilizando VPN vía Ethernet (ancho de banda 4 Mbps), instalando un mux y un router. El enlace de respaldo es VPN vía TDM (ancho de banda 1 Mbps), instalando un modem y un router. Ambos equipos están instalados en el switch de la LAN de esta sede.

(h) Tres oficinas remotas provincias.- Involucra Trujillo (ancho de banda principal 512 Kbps y de respaldo 600/256 Kbps), Tacna (ancho de banda principal 512 Kbps y de respaldo 600/256 Kbps) y Arequipa (ancho de banda principal 512 Kbps y de respaldo 600/256 Kbps). El enlace principal es VPN vía TDM instalando un modem y un router. El enlace de respaldo se brinda a través de ADSL instalando un modem y este se conecta al router del enlace principal. Este router está instalado al swtich de la LAN de estas sedes.

(i) Una oficina remota provincia (Iquitos).- El enlace principal es vía fibra óptica monomodo utilizando VPN vía Ethernet (ancho de banda 2 Mbps), instalando un mux y un router. El enlace de respaldo es VPN vía TDM (ancho de banda 1 Mbps), instalando un modem y un router. Ambos equipos están instalados en el switch de la LAN de esta sede.

(j) Una oficina remota (Conchán).- El enlace principal está formado por dos enlaces vía radioenlace en balanceo de carga (ancho de banda de 2 Mbps cada uno), instalando un modem y un router. El enlace de respaldo es un VSAT (ancho de banda 1 Mbps), instalando un modem conectado al router del enlace principal, este router está instalado en el switch de la LAN de esta sede.

(k) Una oficina remota (Bayovar).- El enlace principal ha sido instalado por un radioenlace (ancho de banda 2 Mbps), instalando un modem y un router. El enlace de respaldo es un VSAT (ancho de banda 512 Kbps), instalando un modem conectado al router del enlace principal, este router está instalado en el switch de la LAN de esta sede.

(l) Una oficina remota (Oleoducto).- El enlace principal es vía fibra óptica monomodo utilizando VPN vía Ethernet (ancho de banda 2 Mbps), instalando un multiplexor y un router. El enlace de respaldo es VPN vía TDM (ancho de banda 512 Kbps), instalando un modem, el cual está conectado al router del enlace principal.

Es sobre este escenario donde, para optimizar la transferencia de datos, se incorpora una solución adicional, la cual consiste en la compresión de datos a fin de que los canales transporten mayor cantidad de información, mejorando de esta manera los recursos de cada enlace.

Del mismo modo, se provee una técnica para que se pueda analizar el tráfico cursado

y así optimizar el uso de los recursos.

1.4 Alcance del trabajo

Con el escenario arriba descrito es que el informe se enfoca en:

El desarrollo de la solución de compresión de datos para todas las sedes mencionadas, por ello se presentará la metodología, aspectos funcionales y de configuración de manera general, explicando la solución técnica ofrecida.

La aplicación de un protocolo para el análisis del tráfico cursado en los servicios de transmisión de datos a nivel WAN. Esto también es realizado en cada sede mostrada.

1.5 Síntesis del trabajo

Para el desarrollo de cada solución se toma en cuenta los requerimientos, para luego evaluar las alternativas. Con la alternativa seleccionada, es que se procede a dimensionar indicando las tareas a realizar así como el equipamiento necesario.

Posteriormente se explica la metodología de la solución para cada caso (compresión de datos, y análisis de tráfico cursado), incluyendo las topologías y configuración general.

El informe se complementa con el soporte teórico que desarrolla los tópicos de:

- Aspectos conceptuales de la WAN (Accesos de última milla, Tecnología MPLS, Red privada virtual (VPN), MPLS con tecnología VPN, Optimización de la WAN (Superación de los desafíos de la WAN mediante los optimizadores,
- Proceso de optimización de tráfico, Servicios que ayudan a la optimización del tráfico, Compresión de datos universal Lempel-Ziv).
- Protocolo de red NetFlow, Descripción del NetFlow, Monitorización del rendimiento tradicional de SNMP, Reconocimiento de Redes basada en NetFlow, Flujo IP, Accediendo a los datos producidos por NetFlow.

CAPÍTULO II
MARCO TEÓRICO CONCEPTUAL

Las empresas se enfrentan a numerosos desafíos en la entrega de datos y aplicaciones críticas del negocio a oficinas remotas. A medida que el trabajo se hace más descentralizado, toma fuerza los niveles adecuados de servicios para toda la organización, lo cual se hace más difícil el desplegar equipos para cada oficina remota con la finalidad de brindar servicios como correo electrónico, video, distribución de software y servicios de impresión como ejemplos.

En base a las exigencias del mercado, la presencia en localidades distintas y lejanas se hace necesaria, por lo que se deberá buscar el utilizar y distribuir las aplicaciones mejorando la protección de los datos, la seguridad y disponibilidad de los mismos, manteniendo el mismo nivel de servicio brindado en la oficina principal. Además se deberá considerar que cada vez las aplicaciones de las empresas son más robustas y complejas, lo que conlleva a que la información a ser entregada a las oficinas remotas sea difícil y costosa.

Por tal motivo se debe buscar mecanismos que aminoren los gastos de envío de información sobre la WAN, asegurando la disponibilidad de las aplicaciones y la agilidad en la transferencia de información a través de la nube. Sin embargo, el tiempo de respuesta de las aplicaciones experimentado por los usuarios de las oficinas remotas, mayormente se responsabiliza a la WAN. Esta demora, latencia, de la conexión WAN o Internet entre la oficina principal, donde se encuentran los servidores de datos, y el usuario en la oficina remota, afecta negativamente en el rendimiento del negocio.

Una solución para el desafío del rendimiento de las aplicaciones en las oficinas remotas es lograr la optimización WAN, lo cual conlleva a un cambio en la infraestructura en la nube, logrando acelerar la respuesta de las aplicaciones, optimizando el ancho de banda y mejorando la productividad de las oficinas remotas.

En este capítulo se exponen los conceptos más relevantes para la comprensión del trabajo expuesto. Se desarrollan los siguientes temas:

- Aspectos conceptuales de la WAN.
- Optimización de la WAN.
- Protocolo de red NetFlow.

2.1 Aspectos conceptuales de la WAN

La WAN (Red de Área Amplia) permite la interconexión de las diversas LAN (Redes de Área Local) de una entidad que así lo requiera. Un ejemplo de ello se mostró en la figura 1.1 del capítulo anterior, en donde se muestra el esquema de la red de la entidad petrolera, la cual consta de muchas oficinas, cada una con su propia característica (velocidad, enlace, etc.). A continuación se precisan los conceptos más resaltantes de la WAN orientada al proyecto realizado: Accesos de última milla, Tecnología MPLS, Red privada virtual (VPN), MPLS con tecnología VPN [1] [2] [3] [4] [5].

2.1.1 Accesos de última milla

Es muy importante destacar que para brindar el servicio a las LAN estas acceden a la WAN a través de nodos que forman parte de la WAN. Para ello se usan diversos tipos de enlaces así como tecnologías para la transmisión de los datos. A continuación se desarrollan los ítems mencionados.

a. Medios de acceso en última milla (Cobre, Radioenlace, Fibra)

Básicamente se dispone de tres tipos de medios para la conectividad entre las sedes de la empresa petrolera, para los cuales existen equipos de comunicaciones especializados o tarjetas que permiten su utilización:

a.1 Acceso vía cobre

Este tipo de medio de acceso es el más usado y popular, proporcionando conectividad de redes LAN de una oficina hacia otra en diferentes lugares. Este tipo de medio de acceso, no puede soportar anchos de banda superiores a los 2Mbps, lo cual es una desventaja, sumado el alto índice de robo de cable por su material (cobre), el cual es comercializado en el mercado negro.

a.2 Acceso vía Radioenlace

Es utilizado para los casos en los cuales la empresa proveedora de servicios no puede llegar al domicilio del cliente con un medio alámbrico, recurriendo a la implementación de un sistema de radioenlace, el cual se implementa entre dos puntos fijos situados en la superficie terrestre, que proporcionan una capacidad de información, con características de calidad y disponibilidad determinada.

Los radioenlaces establecen un concepto de comunicación del tipo full dúplex, de donde se deben transmitir dos portadoras moduladas, una para la transmisión y otra para la recepción. Al par de frecuencias asignadas para la transmisión y recepción de las señales se le denomina radio canal. Los enlaces se hacen básicamente entre puntos visibles, es decir puntos altos de la topografía.

a.3 Acceso vía Fibra Óptica

La fibra óptica es muy utilizada en estos días por empresas proveedora, las cuales

dan mayor garantía y seguridad al usuario final, las mismas que tienen mayor capacidad que los medios por cobre, utilizando hilos muy finos de material transparente, vidrio o materiales plásticos por el que se envían pulsos de luz que representan los datos a transmitir. La fibra óptica es instalada como acceso de última milla desde el nodo más cercado del local del cliente hasta el mismo, siendo la solución adecuada para distancias grandes. En la mayoría de casos es subterránea y muchas de ellas tienen características de antiroedores y con material cero halógeno que contribuye a la no propagación de incendio.

b. Tecnologías relacionadas (ADSL, TDM, Ethernet)

Se desarrollan los siguientes conceptos:

b.1 ADSL

En la transmisión de datos sobre ADSL están involucrados protocolos como PPP, ATM y Ethernet. Un DSLAM es un dispositivo situado en la CO y que contiene varias tarjetas DSL o ATU-Cs. Su función es mover datos desde el abonado hasta el siguiente punto en dirección al punto final, que sería un switch ATM integrado en otro DSLAM. Cuando los datos pasan por la red ATM se transmiten usando celdas hasta llegar al punto de agregación en la salida a Internet del proveedor. La Figura 2.1 muestra una vista de dicha arquitectura.

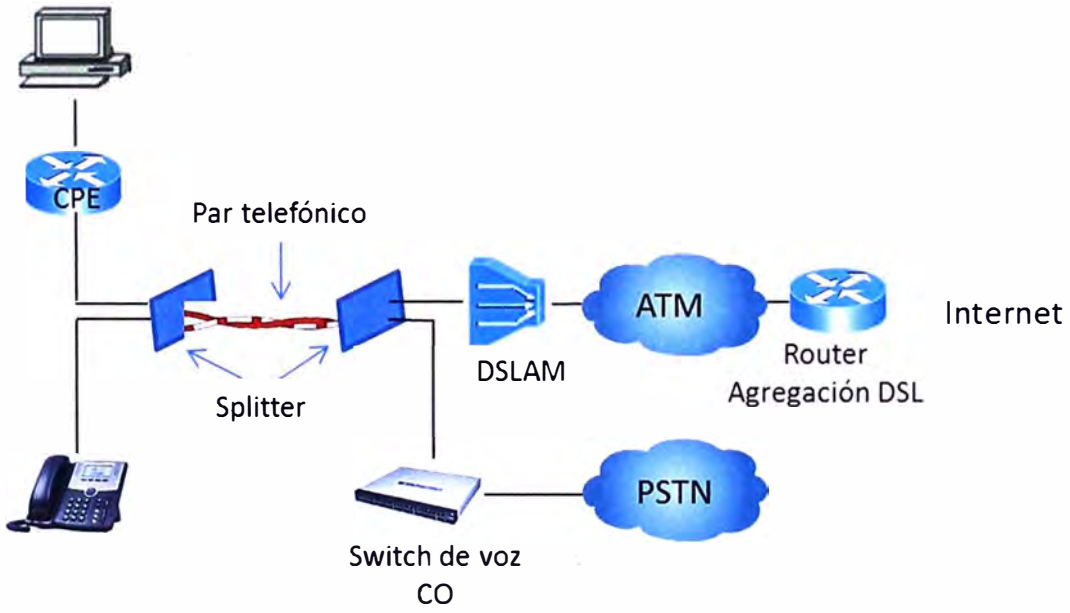

Figura 2.1 Arquitectura ADSL (Fuente [2])

Existen tres formas de encapsular y transportar datos desde el CPE al router de agregación:

- RFC 1483/2684 Bridging. Define encapsulación de datos multiprotocolo (AAL5SNAP) sobre circuitos ATM. Básicamente es bridging de las tramas Ethernet del abonado sobre la red ATM.

- PPP sobre Ethernet. Utiliza tramas Ethernet para encapsular y transportar tramas PPP,
- PPP sobre ATM. Utiliza celdas ATM para encapsular y transportar tramas PPP.

b.2 TDM (Time Division Multiple)

La Multiplexación por división de tiempo es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal de transmisión a partir de distintas fuentes, de esta manera se logra un mayor aprovechamiento del medio de transmisión. El ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo).

b.3 Ethernet

Es un estándar de redes de área local para computadores con acceso al medio por contienda CSMA/CD (Acceso múltiple por detección de portadora con detección de colisiones), la cual es una técnica usada en redes Ethernet para mejorar sus prestaciones.

Las nuevas velocidades de Ethernet lo hacen ideal como alternativa para redes de área metropolitana (MAN) e incluso áreas amplias (WAN), representando una solución sencilla y escalable. La idea de Ethernet como una tecnología ubicada en las redes de los operadores y proveedores de servicios como lo es hoy en las redes corporativas es la que está animando al grupo del IEEE conocido como "Ethernet in the First Mile" (EFM), literalmente "Ethernet en la primera milla".

Esta tecnología de banda ancha permite velocidades de conexión de hasta 40 Mbps tanto para la descarga como para la subida mediante líneas de teléfono de cobre tradicionales. Esto hace que sea ideal para servicios de Internet de alta velocidad y de red de datos.

Estas admirables velocidades se logran gracias a que EFM no sólo puede alcanzar una velocidad mucho mayor en un solo par de cables de cobre, sino también a que está tecnología permite juntar hasta 8 pares de cobre en una sola conexión. También gracias a que utiliza Ethernet (el mismo protocolo que LAN), no se desperdicia ancho de banda convirtiendo el tráfico entre protocolos. Con EFM puede elegir un ancho de banda simétrico de entre 12 y 40 Mbps a una distancia de hasta dos kilómetros de la centralita telefónica (aunque las restricciones normativas en algunos países limitan el ancho de banda máximo, por ejemplo, Italia limita el ancho de banda máximo a 12 Mbps).

2.1.2 Tecnología MPLS

MPLS (Multi-Protocol Label Switching) es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios Prívate Line, Frame Relay o ATM. Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y

multimedia. Y todo ello en una única red.

MPLS (Multiprotocol Label Switching) intenta conseguir las ventajas de ATM, pero sin sus inconvenientes. Asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (solo se mira la etiqueta, no la dirección de destino).

MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS).La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS en la SLA. Por tanto MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente. El etiquetado en capa 2 permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, FrameRelay, líneas dedicadas, LANs.

MPLS es una tecnología Wan que está definida en la RFC3031. Para poder saber cómo funciona esta nueva tecnología, así como las ventajas que introduce, es necesario saber cómo funcionaban sus antecesores. Las conexiones Wan tradicionales son conexiones de capa 2 que se pueden clasificar como punto a punto o multipunto. Estas redes no entienden de calidad de servicio de capa 3 (QoS). En algunos casos muy específicos se pueden priorizar circuitos en los dispositivos frontera.

A través de las redes Wan existen muy poco o casi nada de protección del tráfico. Las Wan tradicionalmente existen en un número limitado de arquitecturas según cada empresa y también dependen del ancho de banda de cada uno de dichos sitios.

2.1.3 Red privada virtual (VPN)

Una red privada virtual, RPV o VPN, de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Una VPN proporciona a usuarios remotos, que utilizan una infraestructura pública, la misma conectividad a la red que si estuvieran sobre una red privada. Sin embargo, antes de permitir a un usuario acceder a una red privada, es preciso tomar ciertas precauciones para asegurar la autenticidad, la integridad de los datos y la encriptación.

Los servicios VPN incluyen autenticación, integridad de datos y confidencialidad. A continuación puede ver una breve descripción de los dos tipos básicos de VPN:

VPNs sitio a sitio: Actualmente hay disponibles dos tipos de estas VPN:

- Las VPN Intranet conectan las oficinas centrales corporativas, las oficinas remotas y las oficinas troncales a través de una infraestructura pública.
- Las VPN Extranet enlazan a clientes, proveedores, socios o comunidades de interés a una intranet corporativa mediante una infraestructura pública.

VPNs de acceso remoto: Conectan de manera segura a usuarios remotos, como teletrabajadores, a la empresa.

Las VPN sitio a sitio (Figura 2.2) pueden emplearse para conectar sitios corporativos. En el pasado, esta operación se realizaba mediante una línea alquilada o una conexión Frame Relay. En la actualidad, la mayor parte de las empresas disponen de acceso a Internet. Con él, las costosas líneas alquiladas y Frame Relay pueden ser sustituidas con VPNs sitio a sitio, las cuales pueden emplearse para ofrecer conexión a la red.

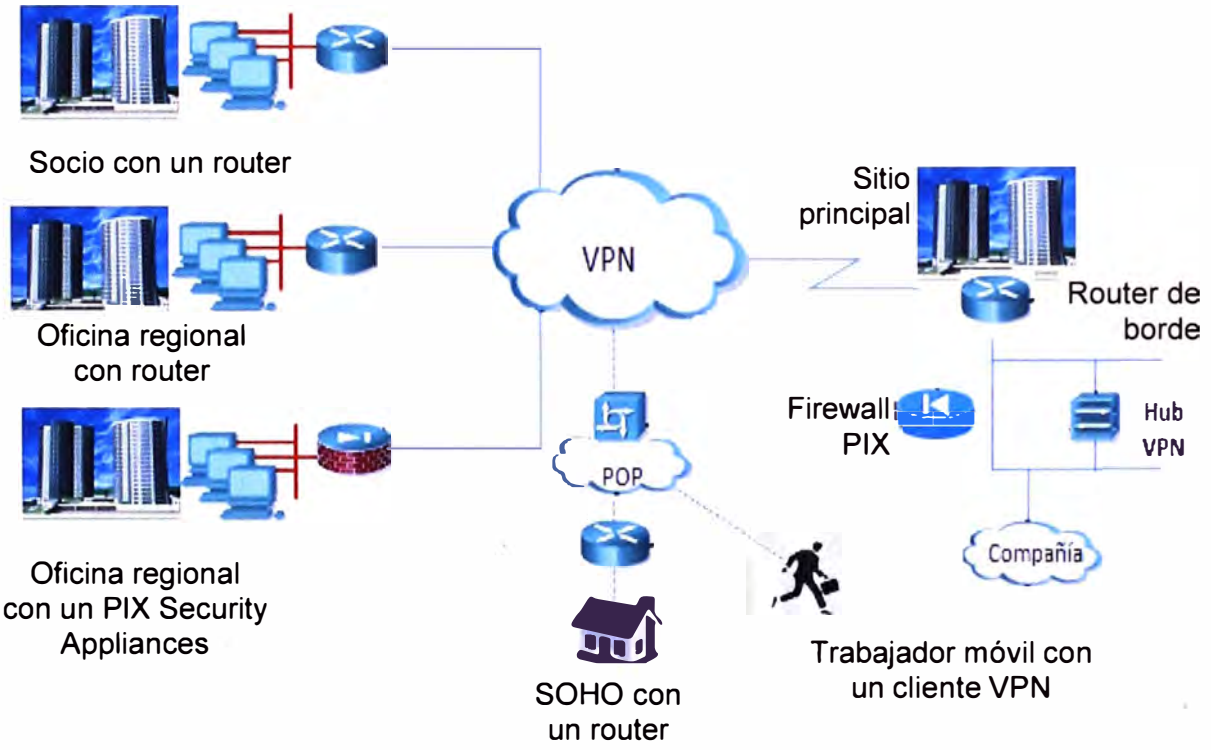

Figura 2.2 VPN Sitio a Sitio (Fuente [1])

Las VPN pueden soportar las intranets de la compañía y las extranets de los socios. Una VPN sitio a sitio es una extensión de una WAN clásica que tiene las mismas políticas y el mismo rendimiento, y que puede construirse usando routers, firewalls y hubs VPN.

La Figura 2.3, muestra los métodos de protección implementados en distintas capas. Con la implementación de la encriptación en una de ellas, dicha capa y todas las que están por encima de ella están protegidas automáticamente. La protección en la capa de red ofrece una de las soluciones más flexible porque es independiente del medio además de serlo de la aplicación.

En el pasado, lo más habitual era proporcionar privacidad y otros servicios criptográficos en la capa de aplicación (Capa 7). En algunas situaciones, esto aún sigue usándose. Sin embargo, este tipo de seguridad es específica de la aplicación, lo que significa que los métodos de protección necesarios deben implementarse en cada una de ellas.

Algunos protocolos como el SSL (Secure Socket Layer, Capa de socket seguro) han

ofrecido un cierto grado de estandarización en la capa de transporte (Capa 4) del modelo de referencia OSI para ofrecer privacidad, autenticidad e integridad a aplicaciones basadas en TCP. El uso de SSL está muy extendido en los sitios de comercio electrónico (e-commerce) modernos; sin embargo, falla en temas tan importantes como la flexibilidad, la facilidad de implementación y la independencia de la aplicación. Una de las últimas tecnologías que han llegado al mercado, TLS (Transport Layer Security, Seguridad en la capa de transporte), resuelve muchas de las limitaciones de SSL.

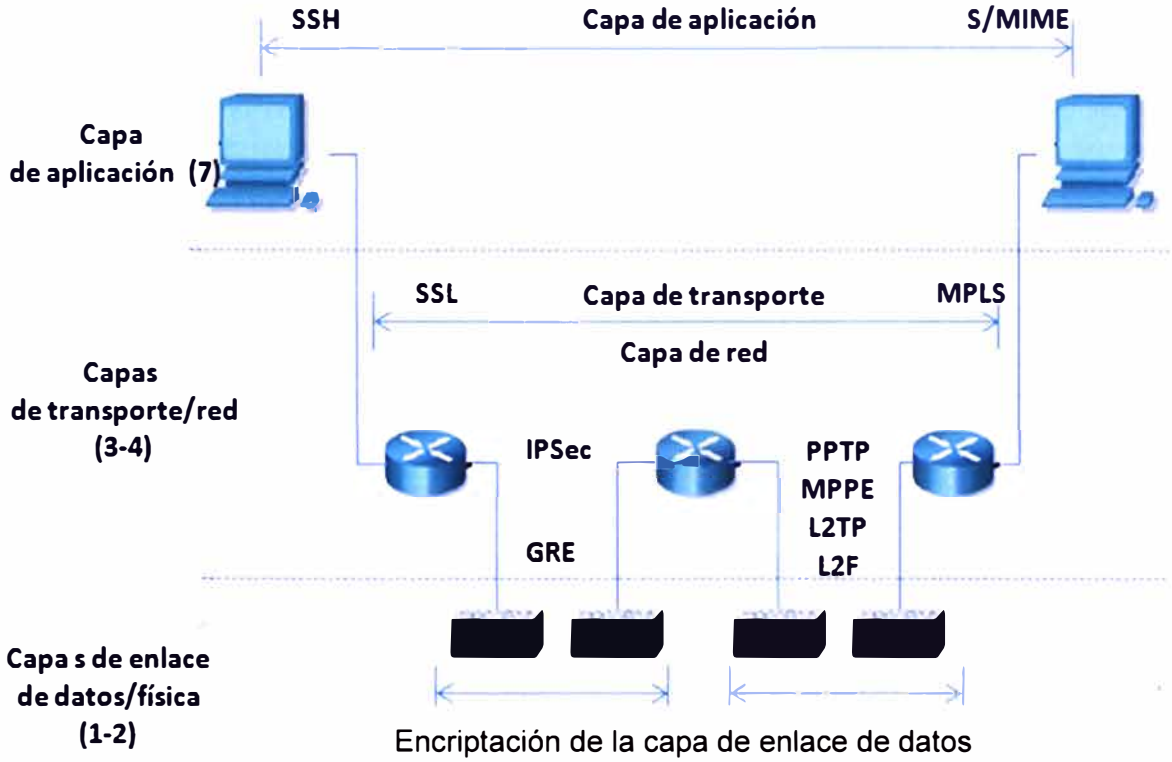

Figura 2.3 Métodos de protección implementados en distintas capas (Fuente [1])

Los sistemas de comunicación del pasado usaban protección en los niveles inferiores de la pila OSI, especialmente en la capa de enlace de datos (Capa 2).

Esto proporcionaba un sistema de protección independiente del protocolo a enlaces no-fiables específicos. Sin embargo, la protección a este nivel es cara de implementarse a una escala mayor porque se debe proteger cada enlace de forma independiente. Por lo general, provee de protección contra ataques del tipo "hombre en el medio" en estaciones intermedias, o routers, y suele ser propietaria.

Debido a todas estas limitaciones, la capa de red (Capa 3) se ha convertido en la más popular para aplicar protección criptográfica al tráfico de la red.

2.1.4 MPLS con tecnología VPN

Para comprender debidamente la tecnología que ofrece las VPN sobre MPLS es necesario comprender anticipadamente los posibles problemas que pueden surgir. Las VPN en MPLS son una solución WAN de capa 3 que soluciona el problema de las WAN

de capa 2, proporcionando conectividad de muchos a muchos entre sitios de una manera económica y efectiva. En el pasado cada vez que era necesario extender la topología suponía un desembolso importante de dinero lo que siempre hacia difícil dicha extensión. Una topología de malla extendida puede ser muy robusta pero extremadamente costosa, mientras que otras menos caras no ofrecen la solución adecuada.

MPLS significó la respuesta y la solución a este problema. Con esta tecnología es posible tener una topología de malla completa pero con la capacidad de hacerlo a nivel de capa 3. La posibilidad de arquitectura que proporciona esta solución es la creación de redes WAN entre los circuitos existentes a nivel de capa 2.

La idea de las VPN siempre se asocia con los conceptos de privacidad y seguridad. El término VPN abarca conceptos muy amplios, la Figura 2.4 ilustra algunos de éstos:

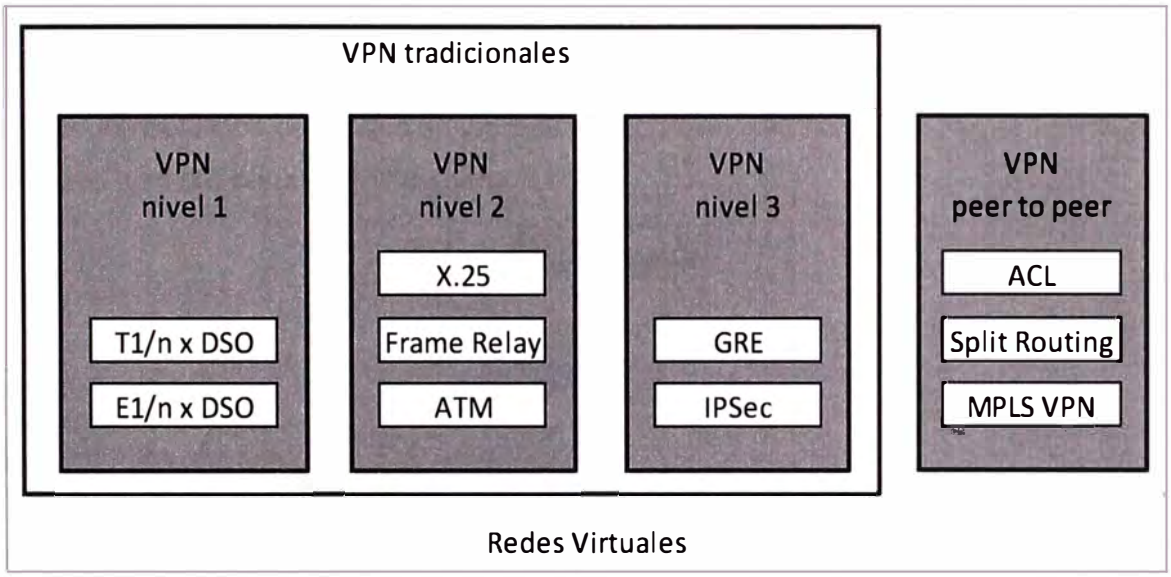

Figura 2.4 Esquema de redes virtuales y VPN tradicionales (Fuente [2])

Esta figura muestra la evolución de la VPN y cómo éstas abarcan un conjunto diferente de tecnologías dependiendo de cómo sean desarrolladas o desplegadas.

Las VPN permiten el uso de infraestructura compartida ofrecida por un ISP (Proveedor de Servicios de Internet) para implementar redes privadas. El uso de seguridad está sujeto a negociación, los ISP ofrecen servicios adicionales tales como firewall para filtrar tráfico indeseado.

Desde un punto de vista de implementación de VPN existen dos tipos de modelos:

1. Overlay VPN, o tradicionales, incluye tecnologías como X.25, Frame Relay, ATM para VPN de capa 2 y túneles GRE e IPsec para VPN de nivel 3.
2. Peer to peer VPN, son implementadas con ISP compartidos y las infraestructuras son realizadas con ACL para separar a los destinos clientes.

a. VPN tradicionales

Las VPN tradicionales han sido utilizadas durante mucho tiempo y se basan en el

modelo de capa 2 en el que el ISP ofrece una cantidad de circuitos virtuales. Como muchas otras tecnologías de red las conexiones VPN van evolucionando desde la capa 1 hasta las capas superiores. El concepto de VPN comenzó años atrás cuando se utilizaban circuitos TDM (Time Division Multiplex – Multiplexación por División de Tiempo), la evolución fue constante hasta alcanzar la capa 2 y la capa 3.

Las implementaciones de VPN de capa 1 fueron ofrecidas por algunos ISP como simples circuitos de capa 1. Esto incluye tecnologías como RDSI y también los servicios DS como T1 de 1544 Mbps o E1 de 2048 Mbps. Otras tecnologías como SONET o SDH también fueron implementadas posteriormente con el objeto de ofrecer mayor velocidad.

El ISP implementaba la capa 1 y el cliente era el responsable de aplicar las características necesarias de capa 2.

Las VPN de capa 2 tienen relación con tecnologías como X.25, Frame Relay, ATM, HDLC, SDLC, SMDS y otras. En este punto el ISP ofrece servicios de capa 1 y capa 2 dejando los servicios de niveles superiores a discreción del cliente. La Figura 2.5 muestra el clásico ejemplo de una VPN de capa 2.

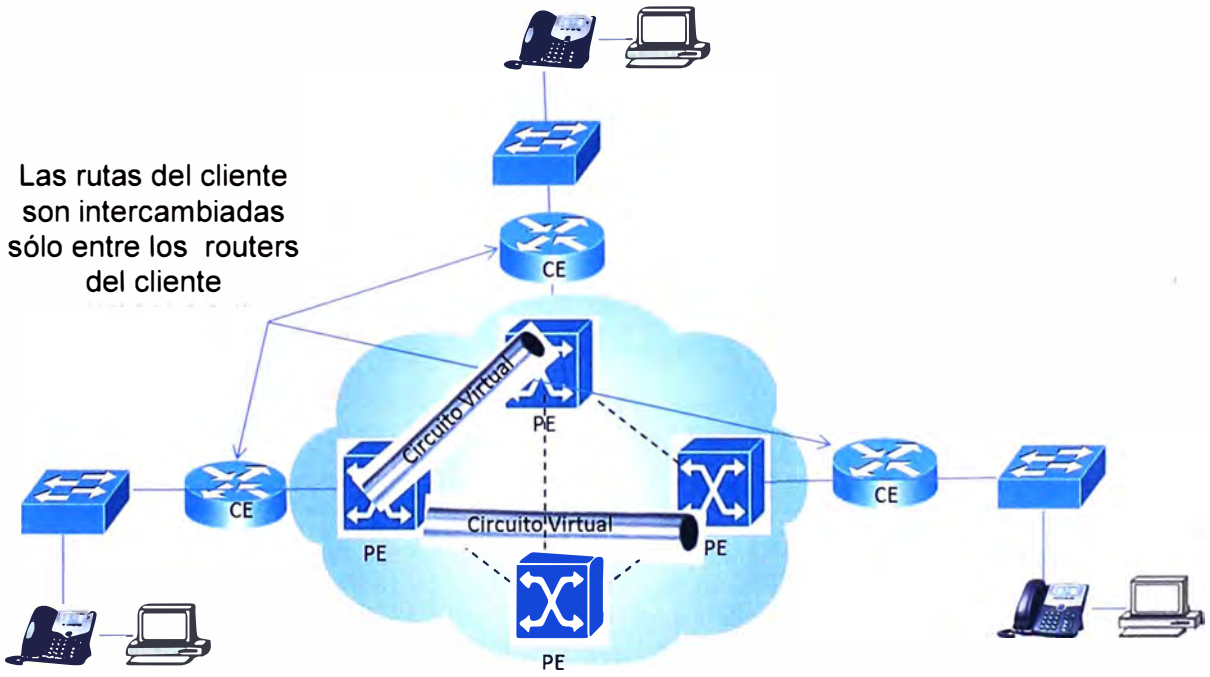

Figura 2.5 Ejemplo de una VPN de capa 2 (Fuente Cisco)

La conectividad tradicional WAN conlleva parámetros de configuración manual de capa 3 para opciones de enrutamiento a través de los circuitos WAN. Un ejemplo son las opciones de broadcast en las configuraciones Frame Relay para permitir que las actualizaciones de enrutamiento se transmitan sin problemas.

b. VPN peer to peer

Las VPN peer to peer hacen que el ISP tenga un papel más activo en las operaciones de enrutamiento de cada cliente. El ISP mantendrá información de instancias de

enrutamiento separadas dentro de su red. El router CE (Customer Edge) comparte información sólo con el router PE (Provider Edge) a través del circuito del ISP. Esta conexión e intercambio de información con el ISP facilita el concepto de VPN peer to peer. Esta evolución hace que la VPN no sólo transporte tráfico de capa 3 sino que además sepa de qué tipo de tráfico se trata y sepa para que utilizarlo. La Figura 2.6 ilustra este concepto:

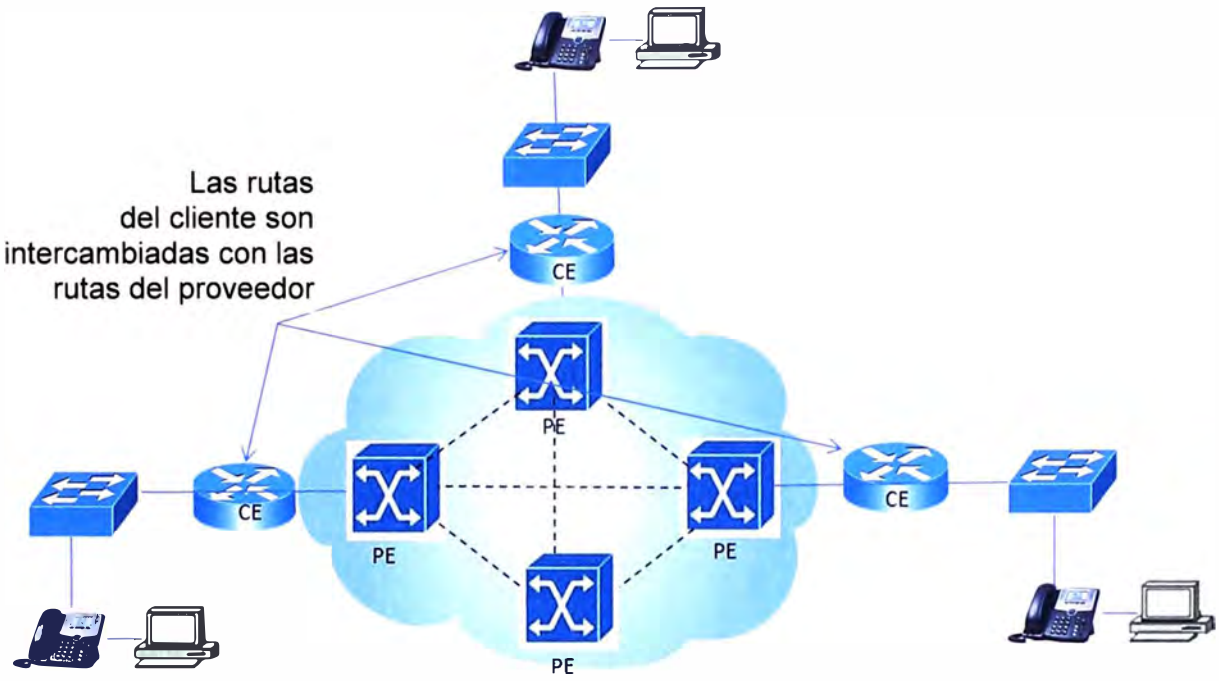

Figura 2.6 Transporte capa 3 en VPN (Fuente Cisco)

Incluso cuando el bucle local permanece igual, el sentido y escénica de la red ha cambiado. El proveedor de servicios toma parte activa en la infraestructura de enrutamiento. Una topología de malla extendida se pone en funcionamiento con un solo enlace hacia la red del proveedor. La red es ahora mucho más robusta porque es una extensión de la red del ISP.

c. MPLS VPN

MPLS VPN contiene lo mejor de las VPN tradicionales y de las VPN peer to peer al mismo tiempo pero en un solo producto. MPLS VPN son precisamente implementaciones de VPN peer to peer.

La información de enrutamiento de cada cliente es guardada de manera segura y separada del resto de la información de los otros clientes mediante los RD (Router Distinguisher), que hacen que cada cliente sea único.

El uso de los RD permite al ISP (Proveedor de servicios de internet) darle a cada cliente una separación lógica del resto aunque no estén físicamente separados. La información específica es actualizada por los propios protocolos de enrutamiento en instancias separadas en el mismo RD.

La tabla creada por el protocolo de enrutamiento en el RD se llama VRF (Virtual Routing and Forwarding). Básicamente se puede decir que es una instancia de la tabla de enrutamiento. A continuación se mencionan las siguientes terminologías:

- C network: red interna del cliente.
- CE: router del cliente que se conecta al PE.
- Label-Switched Path (LSP): es la ruta establecida para el uso de etiquetas en los paquetes a través de la red P en el tránsito hacia un destino en particular.
- P network: red del proveedor del servicio.
- P router: es el router MPLS en el core o backbone de la red y nunca está de cara al cliente. No lleva rutas VPN.
- PE router: es el router MPLS del ISP, contiene rutas VPN y es el dispositivo que se conecta al router CE.
- Penultimate Hop Pop (PHP): es el router P anterior al router P de destino y que se encarga de quitar la etiqueta y entregar el paquete al router PE.
- PoP: punto de presencia del ISP.
- Router Distinguisher (RD): es un identificador de 64 bits que se antepone delante de la dirección IPv4 haciendo que ésta sea globalmente única.
- Router Target (RT): es un atributo que se asocia a las rutas VPNv4 BGP.
- Virtual Routing and Forwarding (VRF): es una instancia de enrutamiento específica para un cliente.

2.2 Optimización de la WAN

Un sistema de optimización de la WAN consta de un conjunto de dispositivos llamados motores de aplicaciones de área amplia (wide area application engines WAEs) que funcionan juntos para optimizar el tráfico TCP (Transmission Control Protocol, Protocolo para el control de la transmisión) a través de su red. Cuando las aplicaciones de cliente servidor intenten comunicarse entre sí, la red intercepta y redirecciona este tráfico a los WAEs de modo que pueda actuar en nombre de la aplicación cliente servidor.

Los WAEs examinan el tráfico y uso de las políticas de integración para determinar si se puede optimizar el tráfico o se debe dejar pasar sin optimizar [6] [7].

Un sistema de optimización de la WAN ayuda a las empresas a cumplir con los siguientes objetivos:

- Proporcionar a los empleados de las oficinas remotas con una LAN, el acceso de la información y aplicaciones a través de la red distribuida geográficamente.
- Mitigación de aplicaciones y servidores de archivos de las oficinas remotas en centro de datos gestionados y centralizados.
- Minimizar el consumo innecesario de ancho de banda WAN mediante el uso de

algoritmo de compresión avanzada.

- Impresión virtualizada y otros servicios locales a los usuarios de las oficinas remotas. Se recomienda que se configure un WAE con Windows en una hoja virtual, de modo que no se necesite implementar un sistema dedicado a la prestación de servicios locales, tales como servicios de impresión, directorio activo (Active Directory), DNS, DHCP.
- Mejorar el rendimiento de las aplicaciones sobre la WAN, abordando los siguientes problemas comunes:

- Ancho de banda limitado.
- Latencia alta de la red.
- Pérdida de paquetes (baja confiabilidad).

Se han desarrollado diversas metodologías para optimizar y superar los problemas en la WAN, es decir para que se transmita mayor información por unidad de tiempo. A continuación se desarrollan los siguientes conceptos:

- Superación de los desafíos de la WAN mediante los optimizadores.
- Proceso de Optimización de tráfico
- Servicios que ayudan a la optimización del tráfico
- Compresión de datos universal Lempel-Ziv (LZ)

2.2.1 Superación de los desafíos de la WAN mediante los optimizadores

Los optimizadores, a veces también llamados aceleradores de tráfico, utilizan una combinación de técnicas de optimización TCP y características de aceleración de aplicaciones para superar los desafíos más comunes asociados con el transporte de tráfico a través de una WAN.

Las aplicaciones generalmente trabajan bien en las redes LAN ya que tienen pocas limitantes para la performance, es decir, gran ancho de banda, poca latencia, y alta confiabilidad, en ese sentido las respuestas son rápidas. Lo contrario ocurre cuando se pasa a un ambiente WAN, donde las oficinas remotas necesitan de las aplicaciones ubicadas en los centros de datos de la oficina principal, encontrando congestión en la red WAN, poco ancho de banda, latencia y pérdidas de paquetes, lo que ocasiona que las respuestas sean lentas (observar Figura 2.7). En la tabla 2.1 se describe esta solución.

Tabla 2.1 Solución de optimización de la WAN (Fuente [6])

Problemas de la WAN	**Solución de optimización**
Latencia alta en la red	Inteligentes adaptadores de protocolo reducen el número y tiempo de respuestas comunes de ida y vuelta (roundtrip time, RTT, tiempo de ida y vuelta) con protocolo de aplicación de habla.
Ancho de banda restringida	Almacenamiento de datos proporcionado con las características de los archivos de servicios y compresión de datos, reduce la cantidad de datos enviados a través de la

	WAN, aumentando la transferencia de datos. Estas soluciones mejoran el tiempo de respuesta en los enlaces congestionados mediante la reducción de la cantidad de datos enviados a través de la WAN.
Mala utilización de los enlaces	Características de optimización TCP mejoran el rendimiento de la red mediante la reducción del número de errores TCP enviados a través de la WAN y la maximización del tamaño de la ventana TCP que determina la cantidad de datos que un cliente puede recibir al mismo tiempo.
Pérdida de Paquetes	TCP optimizado configurado en el optimizador de la WAN supera los problemas asociados con la alta pérdida de paquetes y protege la comunicación en todos los puntos de la red WAN.

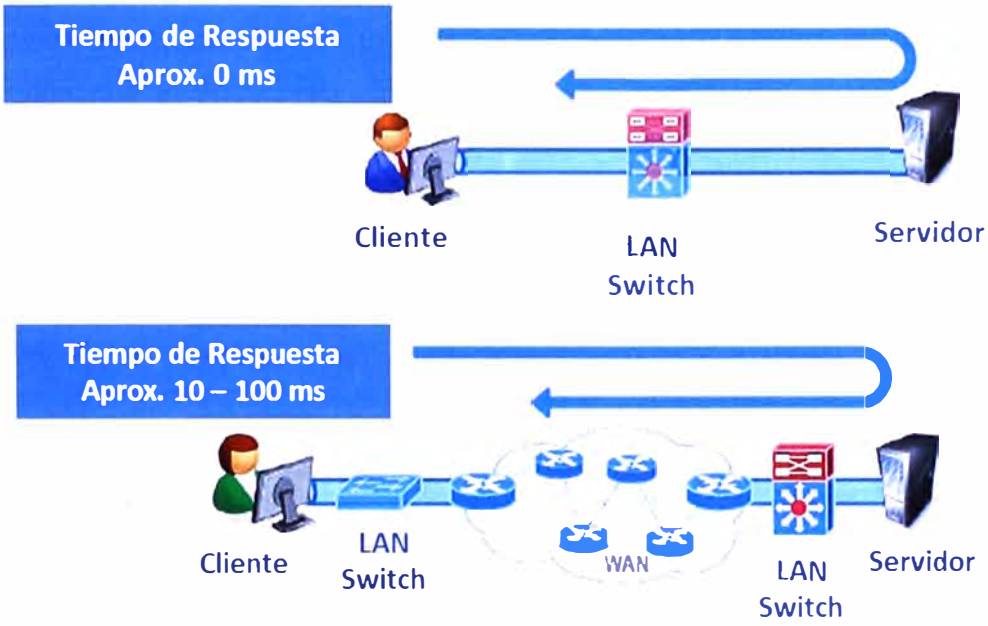

Figura 2.7 Tiempo de respuesta en una LAN y en una WAN (Fuente Cisco)

2.2.2 Proceso de optimización de tráfico

En la Figura 2.8 se muestra el proceso que sigue un optimizador para optimizar el tráfico de las aplicaciones.

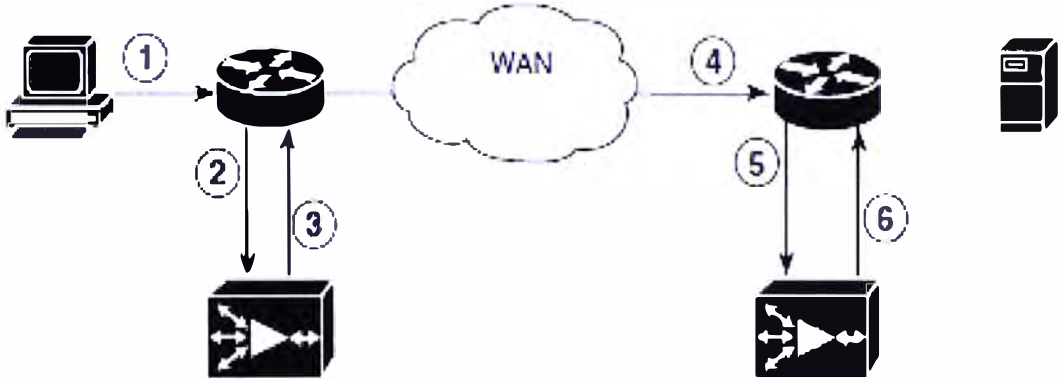

Figura 2.8 Proceso de optimización de tráfico (Fuente Cisco)

A continuación se describen los pasos de cómo se optimiza una red en una conexión de una oficina principal (donde están ubicados sus servidores) con una oficina remota:

1. Un usuario cliente de la oficina remota se intenta conectar a un servidor de su oficina principal.

2. El optimizador utiliza un protocolo de comunicación de almacenamiento web (Web Cache Communication Protocol – WCCP) o un enrutamiento basado en políticas (Policy-Based Routing – PBR) para interceptar la solicitud del cliente. También se puede configurar el equipo optimizador en modo línea, es decir, entre el router y el equipo terminal. La topología adjunta en la Figura 2.8 se llama en modo fuera de línea.

3. El equipo optimizador realiza las siguientes acciones:

- Examina los parámetros en la cabecera del tráfico TCP y a continuación revisa las políticas de aplicación determinando si el tráfico interceptado debe ser optimizado. La información en la cabecera TCP, tales como la dirección IP (origen y destino), y el puerto IP, permiten que el WAE coincida el tráfico a una política de aplicación (los equipos optimizadores traen políticas predefinidas).
- Si el equipo optimizador determina que el tráfico debe ser optimizado, añade información a la cabecera de la TCP que informa al WAE siguiente en la ruta de red para optimizar el tráfico.

4. El WAE recibe la solicitud del cliente a través de la red siendo su destino final el servidor.

5. El centro de datos del WAE realiza las siguientes acciones:

- Intercepta el tráfico que tiene como destino el servidor.
- Establece una conexión optimizada con el equipo WAE. Si el centro de datos del WAE tiene la optimización deshabilitada, entonces no se establecerá una conexión optimizada y el tráfico pasará sobre la red sin optimizar.

6. Por esta conexión, el equipo optimiza el tráfico recibido en el numeral 4 y gestionado en el centro de datos del WAE.

El equipo optimizador no optimiza el tráfico en las siguientes situaciones:

- El WAE no intercepta el tráfico TCP (por ejemplo UDP o ICMP)
- El WAE está sobrecargado y no tiene los recursos para optimizar el tráfico.
- El tráfico interceptado coincide con una política de aplicación que especifica que se debe pasar el tráfico sin optimizar.

2.2.3 Servicios que ayudan a la optimización del tráfico

El equipo optimizador cuenta con servicios que ayudarán a la optimización del tráfico en la red WAN:

- Optimización TFO
- Compresión
- Aceleración de aplicaciones específicas

a.1 Ampliación de ventana

La ampliación de ventana permite que el receptor de un paquete TCP pueda anunciar que su ventana puede superar los 64Kbps. El tamaño de la ventana de recepción determina la cantidad de espacio que el receptor tiene a su disposición para los datos sin acuse de recibo. De forma predeterminada, las cabeceras TCP limitan el tamaño de la ventana de recepción a 64Kbps, pero la ampliación de ventana permite que la cabecera TCP pueda especificar una ventana receptora hasta de 1 Gbps.

La ampliación de ventana permite a los extremos TCP aprovechar el ancho de banda disponible en la red y no se limita al tamaño de la ventana por defecto especificado en la cabecera TCP.

En la Figura 2.9 se muestra una comparación con la optimización TFO y con un TCP estándar. Los resultados serán:

- Mejora de la utilización del ancho de banda de la WAN y mejor rendimiento de las aplicaciones.
- Aislamiento de los puntos finales que perjudican las condiciones de la WAN.

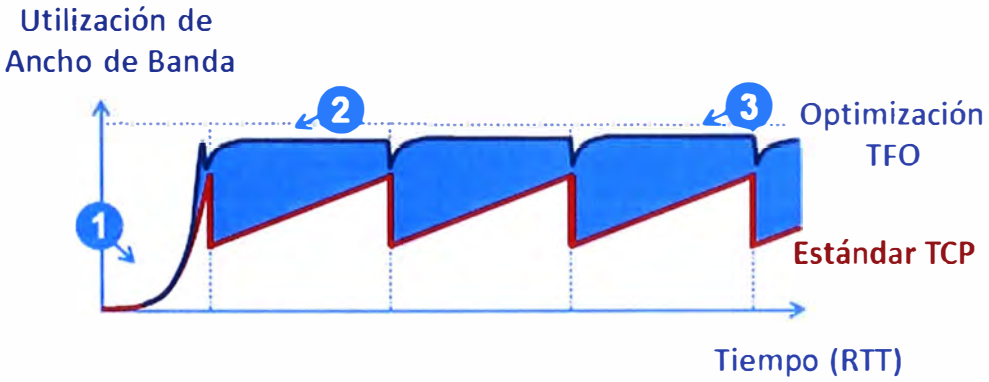

Figura 2.9 Optimización TFO (Fuente Cisco)

Nota:
1. Inicio lento corto, luego mejora
2. Uso del ancho de banda mejorado.
3. Mejor rendimiento en caso la pérdida de paquetes sea alta

a.2 Maximización del tamaño de la ventana inicial de TCP.

El optimizador incrementa el límite superior de la ventana inicial de TCP de uno o dos segmentos a dos o cuatro segmentos (aproximadamente 4Kbps). El incremento del tamaño de la ventana inicial de TCP proporciona las siguientes ventajas:

- Cuando la ventana inicial de TCP es sólo un segmento, un receptor que utiliza acuse de recibo (Acknowledgement ACK) retrasado, se ve obligado a esperar un tiempo antes de generar una respuesta ACK. Con una ventana inicial de al menos dos segmentos, el receptor genera una respuesta ACK después del segundo segmento de datos que llega, eliminando el tiempo de espera.
- Para las conexiones que transmiten sólo una pequeña cantidad de datos, una ventana

inicial grande reduce el tiempo de transmisión. Para muchos correos electrónicos (SMTP – Simple Mail Transfer Protocol, Protocolo simple de transferencia de correo) y página web (HTTP – Hypertex Transfer Protocol, Protocolo de transferencia de hipertextos), las transferencias que tienen menos de 4Kbps, una ventana inicial grande reduce el tiempo de transferencia de datos a un solo tiempo de ida y vuelta (Roundtrip Time RTT).

- Para conexiones que usan ventanas de congestiones grandes, la ventana inicial grande elimina hasta tres RTTs y un tiempo de espera de un ACK retrasado durante la primera fase lento y corto.

a.3 Incremento de almacenamiento.

El optimizador mejora el algoritmo de almacenamiento usado por el núcleo (kernel) de TCP para que los WAEs puedan más agresivamente extraer datos de los clientes y servidores de las oficinas remotas. Este incremento de almacenamiento ayuda a los dos WAEs a mantener entre ellos la participación en la conexión del enlace, incrementando la utilización del enlace.

a.4 Confirmación selectiva.

Confirmación selectiva (Selective Acknowledgment SACK) es una recuperación eficiente de pérdida de paquetes y funciones de retransmisión que permite a los clientes recuperar los paquetes perdidos más rápido que el mecanismo de recuperación por defecto que utiliza el TCP.

a.5 Incremento de la congestión binaria TCP (Binary Increase Congestion BIC TCP)

BIC TCP es un protocolo de gestión de congestión que permite recuperar más rápidamente la pérdida de los paquetes.

Cuando su red experimenta un evento de pérdida de paquetes, BIC TCP reduce el tamaño de la ventana de su receptor y establece el tamaño reducido como el nuevo valor mínimo para la ventana. BIC TCP a continuación establece el máximo valor del tamaño de la ventana tomando como referencia el tamaño de la ventana antes de producirse el evento de la pérdida de los paquetes. Debido a que la pérdida de los paquetes se produjo justo en el tamaño máximo de la ventana, la red puede transferir el tráfico sin dejar caer los paquetes cuyo tamaño está dentro de los valores mínimos y máximos de la ventana.

Si BIC TCP no registra ningún evento de pérdida de paquetes en el tamaño máximo de la ventana actualizada, el tamaño de la ventana se convierte en el nuevo mínimo. Si ocurre un nuevo evento de pérdida de paquetes, el tamaño de la ventana se convierte en el nuevo máximo. Este proceso continúa hasta que BIC TCP determina los óptimos valores, mínimos y máximo, para el tamaño de la ventana.

b. Compresión

El optimizador utiliza las siguientes tecnologías de compresión para ayudar a reducir

el tamaño de los datos transmitidos sobre la WAN:

- Eliminación de datos redundantes (Data Redundancy Elimination DRE).
- Compresión Persistente LZ (Lempel Ziv)

Estas tecnologías de compresión reducen el tamaño de los datos transmitidos por la eliminación de información redundante antes de enviar el flujo de datos acortado sobre la WAN. Al reducir la cantidad de datos transferidos, la compresión del optimizador puede reducir la utilización de la red y los tiempos de respuesta de las aplicaciones.

Cuando un dispositivo WAE utiliza la compresión para optimizar el tráfico TCP, este remplaza los datos repetidos en la secuencia con una referencia más corta, entonces envía la secuencia de datos acortada a través de la WAN. El WAE receptor utiliza su librería local redundante para reconstruir el flujo de datos antes de pasar al cliente destino o al servidor.

El esquema de compresión del optimizador se basa en una arquitectura de memoria caché compartida donde cada dispositivo WAE está involucrado en la compresión y descompresión tomando como referencia su biblioteca de la redundancia. Cuando se llena en el WAE la memoria caché que almacena la biblioteca de la redundancia, el equipo optimizador utiliza un algoritmo FIFO (First In, First Out – primero en entrar, primero en salir) para descartar los datos antiguos y hacer espacio para los nuevos.

La compresión LZ opera sobre los flujos de datos más pequeños y mantiene la historia de la compresión limitada. DRE opera con flujos significativamente grandes (por lo general de decenas a cientos de bytes o más) y mantiene un historial de compresión mucho mayor. Grandes bloques de datos redundantes es común en las operaciones de sistemas de archivos cuando los archivos son incrementalmente cambiados de una versión a otra o cuando ciertos elementos son comunes a muchos archivos, como por ejemplo los encabezados de archivos y logotipos.

c. Aceleración de aplicaciones Específicas

Además de las funciones de optimización TCP que aceleran el flujo de tráfico a través de una WAN, el optimizador de tráfico deberá contar con las siguientes características de aceleración de aplicaciones:

- Procesamiento por lotes y predicción en la operación: permite conectar un dispositivo de optimización de tráfico para transformar una secuencia de comandos en una secuencia más corta en la WAN y así reducir el tiempo de ida y vuelta (roundtrips).
- Suprime inteligentemente el mensaje: disminuye el tiempo de respuesta de las aplicaciones hacia las oficinas remotas. A pesar que TFO optimiza el tráfico en una WAN, los mensajes de protocolos entre los clientes de la oficina remota y los servidores en el centro de datos (data center) todavía puede causar un tiempo lento de respuesta de las

aplicaciones. Para resolver este problema, el optimizador de tráfico contiene los proxies (programa o dispositivo que realiza una acción en representación de otra) de aplicaciones que pueden responder a los mensajes a nivel local para que el cliente no tenga que esperar por una respuesta desde el servidor ubicado en el centro de datos. Los proxies de aplicación utilizan una variedad de técnicas incluyendo el almacenamiento en caché (conjunto de datos duplicados de otros originales), el procesamiento por lotes de comandos, la predicción y la captación previa de recursos para disminuir el tiempo de respuesta de las aplicaciones remotas.

- Sistema común de archivos de internet caché (Common Internet File System - CIFS caché): permite conectar un dispositivo optimizador de tráfico para responder a las peticiones de los clientes a partir de datos almacenados localmente en la caché en lugar de recuperar los datos de archivos y servidores de aplicaciones remotamente.
- Preposición: Permite conectar un dispositivo de optimización de tráfico para preferir un recurso de datos y mega datos anticipándose a una solicitud futura de un cliente.
- Un equipo optimizador de tráfico utiliza módulos de software con aplicaciones inteligentes aplicando estas características de aceleración.

En un típico caso de uso de aplicación CIFS, el cliente envía un gran número de solicitudes sincronizadas que requieren que el cliente espere una respuesta antes de enviar la siguiente solicitud. La compresión de los datos o tráfico a través de la WAN no es suficiente para un tiempo de respuesta aceptable.

Por ejemplo, cuando se abre un documento word de 5Mbps, se producen alrededor de 700 peticiones CIFS (550 solicitudes de lectura, además de 150 solicitudes de otras). Si todas estas peticiones se envían a través de 100ms de ida y vuelta en la WAN, el tiempo de respuesta es de al menos 70 segundos (700x0,1 segundo).

La aceleración de la aplicación del optimizador de tráfico minimiza el efecto de sincronismo del protocolo CIFS, lo que reduce el tiempo de respuesta. Cada dispositivo optimizador de tráfico utiliza una política de aplicación para que coincida el tipo de tráfico específico de una aplicación y para determinar si el tráfico de la aplicación mostrado es optimizado y acelerado.

Las aplicaciones de aceleración de un optimizador que están disponibles son las siguientes:

- CIFS: acelera el tráfico CIFS intercambiando con un servidor de archivo remoto.
- NFS (Accelerates Network File System): aceleración del sistema de archivos en la red, intercambia tráfico con un servidor de archivo remoto.
- HTTP: acelera el tráfico HTTP.
- SSL (Secure Socket Layer): aceleración encriptado del tráfico en la capa de socket

seguro (SSL) y en la seguridad de la capa de transporte (TLS Transport Layer Segurity). El acelerador SSL proporciona tráfico encriptado y descifrado dentro de los optimizadores para habilitar de extremo a extremo la optimización del tráfico. El acelerador SSL también proporciona una gestión segura de las claves y certificados encriptados.

- MAPI (Messaging Application Programming Interface, Interfaz de programación de aplicaciones de mensajería): acelera el tráfico de Exchange de Microsoft Outlook que utiliza el protocolo de interfaz de programación de aplicaciones de mensajería (MAPI). Clientes de Microsoft Outlokk 2000-2007 son compatibles. Las conexiones seguras que utilizan la autenticación de mensajes (firmas) o encriptación no son acelerados y MAPI sobre HTTP también no es acelerado.
- Video: acelera la transmisión de video en vivo por Windows Media que utilizan RTSP (Real Time Streaming Protocol, Protocolo de streaming en tiempo real) a través de TCP. El acelerador de video de forma automática divide una secuencia de video de origen de la WAN en múltiples flujos para servir a múltiples clientes en la LAN. El acelerador de video de forma automática hace que un cliente solicite un flujo UDP (User Datagram Protocol, Protocolo de datagrama de usuarios) para hacer una superposición de protocolo para utilizar TCP (si ambos, cliente y servidor permiten TCP).
- Impresión Windows: acelera el tráfico de impresión entre los clientes y un servidor de impresión de Windows situado en el centro de datos. El tráfico con firmas SMB (Server Menssage Block, Bloqueo de mensajes de servidor) no es acelerado.

2.2.4 Compresión de datos universal Lempel-Ziv (LZ)

Los algoritmos de Lempel-Ziv de compresión de datos son los algoritmos de codificación de fuentes que se diferencian de otros como son Huffman y códigos de Shannon. LZ tiene las siguientes características:

- Usan códigos variables de longitud variable, en el que ambos, tanto el número de símbolo de la fuente codificado y el número de bits codificado por un código de palabra son variables. Además, el código es variable con el tiempo.
- No requiere conocimiento previo de las fuentes estáticas, pero con el tiempo se adaptan de modo que el promedio de la longitud L del código de palabra por la letra fuente es minimizado. Tal algoritmo es llamado universal.
- Este tipo de compresores de datos son ampliamente utilizados, aunque los nuevos planes de mejora sobre estos, proporcionan un método simple para la comprensión de los algoritmos de compresión de datos universales.

Los algoritmos de compresión de datos se desarrollaron en 1977-78. El primero LZ77, usa cadena de equiparación de una ventana deslizante, mientras que el segundo LZ78, utiliza un diccionario de adaptación. LZ78 se llevó a cabo hace muchos años en el

algoritmo de compresión UNIX y en muchos otros lugares. La implementación de LZ77 es un poco más reciente (pkzip, gzip, Stacker, Microsoft Windows). LZ77 comprime mejor, pero es más robusto su ordenador.

Estos algoritmos de compresión de datos se basan en la compresión por diccionario, los cuales se pasan a explicar.

a. Compresión por diccionarios.

En la técnica de compresión de datos basada en diccionario los símbolos de la fuente o cadenas que se forman con los símbolos de la fuente se representan mediante un índice, es decir un número, que se guarda en un diccionario que se construye a partir de los datos de la fuente. Un diccionario es una lista de símbolos y cadenas de símbolos a los que se les asocia un número índice. Se puede encontrar algún ejemplo de la vida cotidiana que usa esta idea. Por ejemplo la cadena de símbolos que forma la palabra "septiembre" se puede representar por el índice 9.

La estrategia de la codificación basada en diccionario es construir un diccionario que contenga los símbolos que ocurren frecuentemente como así también cadenas de símbolos, asignándole un índice. Cuando se va leyendo la fuente y aparece un símbolo o cadena que ya está incluido en el diccionario (porque ya había aparecido antes, por eso está anotado en el diccionario), se lo codifica mediante el índice correspondiente que el diccionario le asignó. Si el símbolo o cadena no está en el diccionario entonces se lo agrega, asignándole un índice, para un posible uso futuro.

Más formalmente se dice que dada una fuente de símbolos S, un diccionario consistente de dos elementos quedando definido como D = (P, C), donde P es un conjunto finito de frases generadas con los elementos de S, y C es una función de mapeo que asigna a P un conjunto de palabras de código. Se dice que el conjunto P es completo si cualquier cadena de salida de S puede ser representada por una serie de frases de P. La función de codificación C tiene la propiedad libre de prefijo si ninguna palabra de código es prefijo de cualquier otra palabra de código. Para obtener una compresión reversible el conjunto P debe ser completo y C debe ser libre de prefijo.

El corazón de la codificación basada en diccionario es la formulación del diccionario mismo. Si el diccionario está bien construido entonces se obtiene una compresión de los datos; en caso contrario lo que se obtiene es una expansión. De acuerdo al diseño que tenga el diccionario, éste se puede clasificar en estático o adaptivo.

a.1 Diccionario estático.

En algunas aplicaciones, es suficiente conocer el alfabeto de la fuente y las cadenas relacionadas para armar un diccionario fijo, antes de efectuar la codificación. Este diccionario se usa tanto del lado del transmisor como del receptor. La ventaja de este tipo

de diccionarios es la simplicidad. La desventaja es su baja eficiencia de compresión. Además es poco flexible, es decir que una vez diseñado para una aplicación no se puede adaptar con facilidad a otra aplicación.

Un ejemplo de algoritmo estático es la codificación digrama. En esta técnica simple el diccionario contiene todos los símbolos de la fuente y varios pares de símbolos usados más frecuentemente. Para el proceso de codificación se lee de la fuente dos símbolos a la vez y se verifica si ese par de símbolos está en el diccionario. Si está entonces se lo remplaza por el índice que el diccionario tiene asignado a ese par y a continuación se lee de la fuente los dos símbolos que siguen. Si el par de símbolos no está en el diccionario entonces el primer símbolo de ese par se codifica con el índice que le corresponde y el segundo símbolo se combina con el tercero de la secuencia de entrada para formar un nuevo par. Se verifica si este nuevo par está en el diccionario y si es así se le asigna el índice correspondiente.

Esta idea de digrama puede extenderse a n-grama. En este caso el tamaño del diccionario aumenta aunque la eficiencia de compresión también.

a.2 Diccionario adaptivo

A diferencia del diccionario estático, que está armado por completo de antemano, el diccionario adaptivo no existe antes de iniciar el proceso de codificación y por otra parte una vez que se arma no tiene un tamaño fijo. En realidad sólo existe una parte inicial del diccionario al iniciarse el proceso de codificación. A medida que el proceso de codificación avanza el diccionario se va modificando según los símbolos que van saliendo de la fuente. Todos los algoritmos de diccionarios adaptivos están basados en los trabajos originales que sobre este tema hicieron Abraham Lempel y Jacobo Ziv en 1977 y 1978. El algoritmo de Lempel y Ziv de 1977 es llamado LZ77 mientras que el del año 1978 es llamado LZ78.

Una vez que se tiene el diccionario, se va examinando el texto de entrada nuevo y se va viendo si alguna cadena de símbolos de este texto coincide con alguna cadena que está guardada en el diccionario y si es así entonces se transmite el índice asociado mediante una palabra de código. Es decir que una secuencia de símbolos de entrada puede descomponerse como suma de cadenas de texto que están almacenadas en el diccionario. Esta descomposición se llama parsing (parsing viene de parse que significa análisis sintáctico.). Hay diferentes maneras de descomponer un texto como suma de cadenas. Normalmente en los algoritmos de compresión se usa un mecanismo llamado greedy parsing en donde el codificador busca dentro del texto de entrada la cadena más larga que coincide con un ítem del diccionario. Por ejemplo, si se supone que se tiene el siguiente texto de entrada: “aabbaabab” y suponiendo que el diccionario contiene las

cadenas D = {a, b, aab, abb, abab}, la secuencia de entrada puede descomponerse como: “aab-b-aab-a-b”, aunque también puede descomponerse como: “a-abb-a-abab”

Para los fines de compresión indudablemente la segunda solución es más eficiente ya que está compuesta por cuatro cadenas. Sin embargo, el método de greedy parsing (que busca las coincidencias más largas dentro del texto) conduce a la primera solución, menos eficiente porque genera cinco cadenas pero más sencilla de implementar.

b. Algoritmo de compresión LZ77

Este esquema de compresión basado en diccionario adaptivo fue desarrollado por Jacobo Ziv y Abraham Lempel y publicado en un documental en el año 1977. El algoritmo toma el nombre de las iniciales de los apellidos de los inventores y del año de publicación del trabajo. Ya que se trata de un diccionario adaptivo, antes de iniciar la codificación no existe un diccionario completo y fijo y el mismo va cambiando a medida que se va leyendo el texto de entrada para su codificación.

En el algoritmo LZ77 el diccionario se forma con una porción del texto de entrada el cual ya ha sido recientemente codificado. El texto a codificar se compara con las cadenas de símbolos que están en el diccionario. La cadena coincidente más larga que está en el diccionario es caracterizada por una terna de números, como se verá enseguida. Esta terna funciona como índice del diccionario.

Este algoritmo funciona con una ventana deslizante. Esta ventana está formada por dos partes: una ventana de búsqueda (search buffer) y una ventana de texto en avance (look-ahead buffer).

Ventana de búsqueda. Contiene los caracteres que han sido codificados recientemente y es en sí misma el diccionario.

Ventana en avance. Está a continuación de la ventana de búsqueda y contiene los caracteres a ser codificados.

La ventana se desplaza (por eso el nombre de ventana deslizante) a través del texto de entrada, desde el comienzo hasta el final, durante todo el proceso de compresión. La idea es buscar coincidencias entre cadenas de la ventana en avance y la ventana de búsqueda.

Los pasos para el desarrollo del algoritmo son los siguientes:

1. El codificador recorre la ventana de búsqueda hacia atrás, de derecha a izquierda. Busca una cadena de caracteres que sea igual a la cadena de caracteres de la ventana de adelante o a un prefijo de esta cadena. Si en el search buffer hay 2 ó más cadenas iguales se puede elegir cualquiera ya que esto no afecta al decodificador.

a) Si el codificador encuentra una cadena coincidente como se explicó antes, entonces genera una terna del tipo (puntero, longitud, caracter). Puntero es la distancia que hay

(contada en caracteres) desde el final de la ventana de búsqueda (el extremo derecho) hacia atrás, hasta el comienzo de la cadena que se ha encontrado. Longitud es la longitud de la cadena hallada. Caracter es, el caracter dentro de la ventana look-ahead, que sigue a la cadena coincidente.

b) Si no se encontró ninguna cadena coincidente entonces se genera una terna en donde puntero y longitud valen 0 y caracter es el primer caracter de la ventana de adelante.

2. Las dos ventanas (buffers) se desplazan hacia adelante una distancia igual a longitud + 1. El tamaño de la ventana de búsqueda es mucho mayor que el tamaño de la ventana en avance, lo cual resulta lógico teniendo en cuenta que la ventana de búsqueda es el diccionario en sí. En la práctica la ventana de búsqueda puede tener algunos miles de caracteres de longitud mientras que la ventana en avance tiene algunas decenas de caracteres. Para aclarar el funcionamiento del algoritmo se muestra un ejemplo. Asumiendo que la secuencia a codificar o comprimir es ACCBADACCBACCBACCGIKMOABCC. La ventana de búsqueda es de longitud 9 y la ventana en avance es de longitud 6.

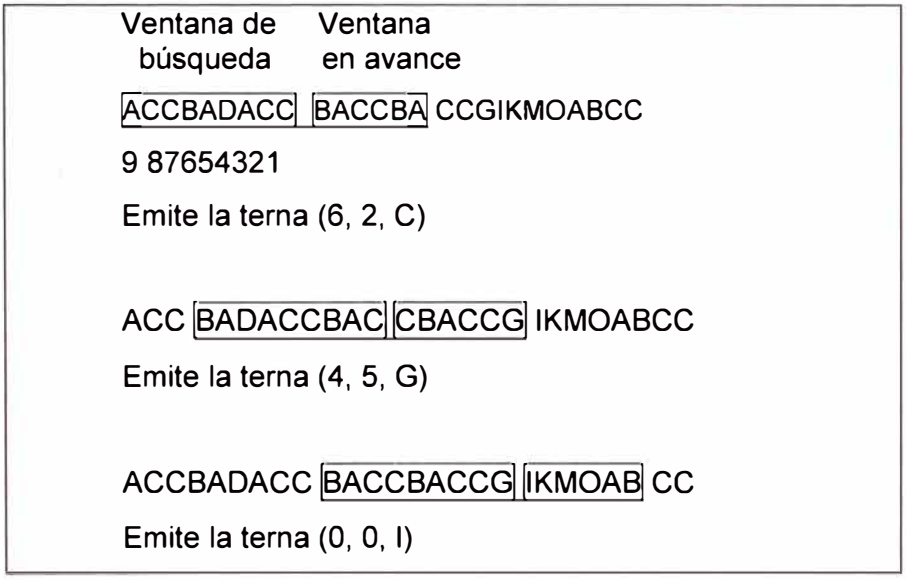

Figura 2.10 Ejemplo de codificación LZ77 (Fuente [11])

En el ejemplo de la Figura 2.10 los pasos de codificación son los siguientes:

1. En el primer esquema de la Figura 2.10 se muestra el estado inicial con la cadena completa de caracteres y las dos ventanas usadas en el algoritmo. Los símbolos de la ventana de búsqueda ya han sido codificados mientras que **los símbolos de la ventana en avance son los que hay que codificar.** Cuando el algoritmo empieza entonces la primera vez el contenido de la ventana de búsqueda se transmite sin codificar, es decir, se transmiten las letras tal como están con las palabras de código correspondientes (por ejemplo el código ASCII).

2. Siguiendo con el primer esquema de la Figura 2.10, la cadena a codificar (ventana en avance) comienza con la letra **B**. Se realiza una búsqueda de derecha a izquierda en la ventana de búsqueda, a partir de la posición 1, tratando de encontrar la letra **B**, con la esperanza de que a partir de esa letra se encuentre la coincidencia más larga posible con **BACCBA** que es el contenido de la ventana en avance. Al efectuar esta búsqueda se verifica que la letra **B** aparece en la posición 6 y la coincidencia más larga posible con el contenido de la ventana en avance es **BA**, o sea dos caracteres. El índice generado queda representado por la terna (puntero, longitud, caracter) que en este caso vale (6, 2, C). El 6 es la posición en la que se halla la **B** en la ventana de búsqueda, el 2 indica la cantidad de caracteres coincidentes y la letra **C** es el símbolo inmediatamente después de la cadena coincidente en la ventana en avance. Finalmente, la ventana completa se desplaza 3 posiciones (es decir, longitud + 1).

3. En el segundo esquema de la Figura 2.10 toda la ventana se ha desplazado 3 posiciones. El contenido de la ventana en avance es ahora **CBACCG**. Se debe buscar entonces en la ventana de búsqueda, empezando de derecha a izquierda, si hay una cadena coincidente con **CBACCG** o con un prefijo de **CBACCG**. El primer símbolo de la ventana en avance es la letra **C**, por lo que se va recorriendo la ventana de búsqueda de derecha a izquierda hasta encontrar una **C**. La primera coincidencia se da en la posición 1 de la ventana de búsqueda y la longitud coincidente es de un solo caracter. Se sigue recorriendo la ventana de búsqueda para ver si hay coincidencias más largas (recuerde que se usa el criterio greedy parsing que busca las coincidencias más largas). En la posición 4 aparece otra letra **C** y en este caso la cadena coincidente es **CBACC**. Son 5 caracteres coincidentes, aunque nótese que esta cadena supera el límite de la ventana de búsqueda y se mete en la ventana en avance. Esto es posible y luego cuando se vea la decodificación se entenderá cómo funciona. De esta manera entonces se ha hallado la máxima cadena coincidente (hay otra letra **C** en la posición 5 pero sólo genera una coincidencia de un caracter). Es decir que el valor del puntero es 4, la longitud coincidente es 5 y el próximo caracter (el que está inmediatamente después de la cadena coincidente en la ventana en avance) es la letra **G**. Por lo tanto, la terna que se transmite es (4, 5, G). La ventana completa se desplaza 6 lugares (longitud + 1).

4. En el tercer esquema de la Figura 2.10 la ventana se ha desplazado 6 lugares respecto de la posición anterior. El proceso de codificación sigue como hasta ahora. Sin embargo, en este caso no hay cadenas coincidentes entre la ventana en avance y la ventana de búsqueda. Por lo tanto la terna transmitida es (0, 0, I). Aquí se ve la utilidad del tercer valor de la terna, que permite que la ventana deslizante siga funcionando cuando no hay cadenas coincidentes. El siguiente desplazamiento de la ventana es de 1

posición.

El proceso de codificación continúa según la manera explicada. A continuación se explica el proceso de decodificación apoyándonos en la Figura 2.11

1. Inicialmente se recibe la cadena **ACCBADACC** sin codificar más la terna (6, 2, C), como se muestra en la Figura 2.11(a). El primer valor de la terna indica cuántos lugares hay que contar desde la posición extrema derecha de la ventana. En este caso son 6 posiciones, lo que lleva a la letra **B**. El segundo valor de la terna indica cuántos caracteres coincidentes hay desde la posición indicada por puntero, en este caso dos caracteres coincidentes desde la letra **B**. Por lo tanto a la cadena inicialmente recibida se le agrega la cadena **BA** más la letra **C** indicada por el tercer valor de la terna. Queda reconstruida hasta acá la cadena **ACCBADACCBAC**.

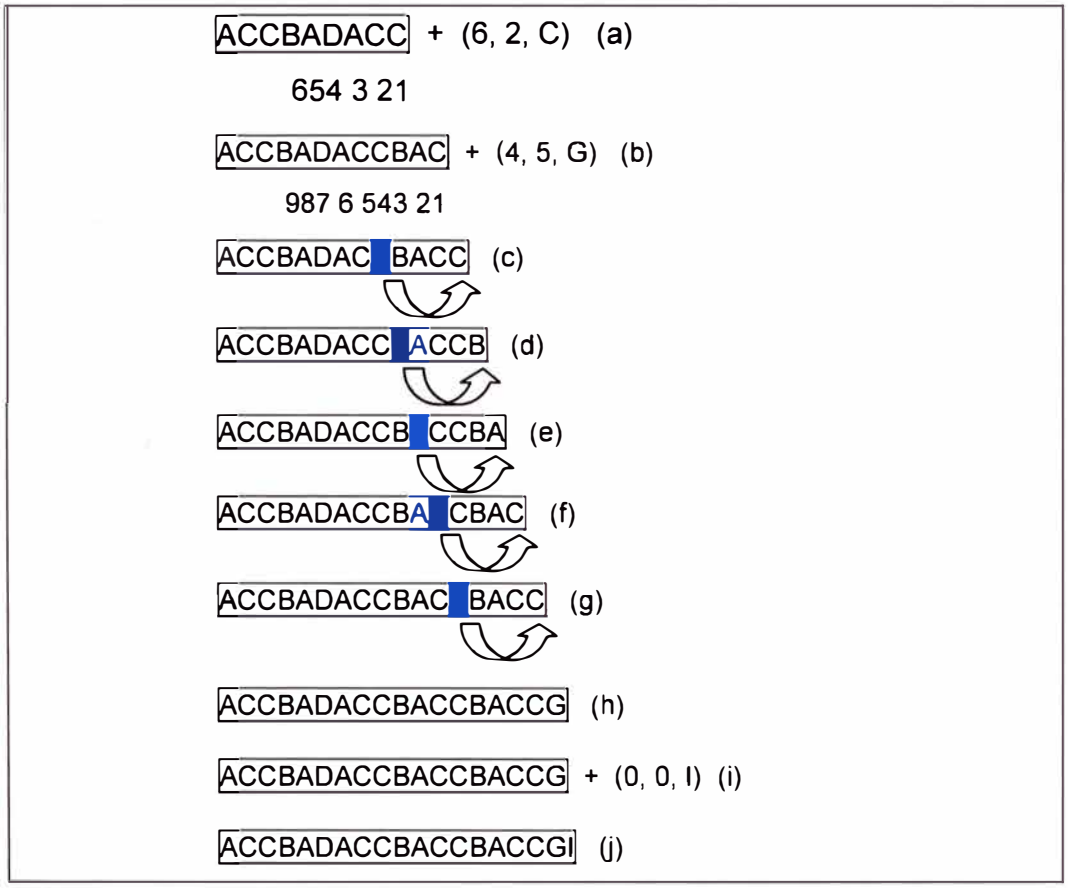

Figura 2.11 Decodificación LZ77 de la cadena codificada en la Figura 2.10 (Fuente [11])

2. A continuación, como se muestra en la Figura 2.11 (b), se recibe la terna (4, 5, G), la cual hay que decodificarla y agregar los caracteres resultantes a la cadena reconstruida hasta el momento. El primer valor de la terna es el puntero e indica cuántos lugares hay que contar desde el final de la cadena anterior, **ACCBADACCBAC**. Se cuentan entonces 4 lugares y se llega a la letra **C**. El segundo valor de la terna indica la cantidad de caracteres coincidentes a partir de esta letra **C**. Es decir que hay que agregar 5 letras contando desde la **C**. Sin embargo, parece imposible contar 5 letras coincidentes ya que

se está empezando en la posición 4 y por lo tanto no hay más que 4 letras hacia la derecha. Para poder hacerlo se copia letra por letra empezando desde la posición 4, como se muestra en la Figura 2.11 (c) hasta (g). Nótese que ahora sí es posible copiar 5 letras ya que la última **C** copiada es la que se había copiado inicialmente desde la posición 4 que indicaba el puntero. Por lo tanto ahora se forma la cadena **ACCBADACCBACCBACC**, Figura 2.11 (g), a la que finalmente se le agrega la letra **G** correspondiente al tercer valor de la terna, quedando el resultado de la Figura 2.11 (h).

3. La última terna recibida es la (0, 0, I). Ya que puntero y longitud valen cero, significa que solamente hay que agregar a la cadena que se está reconstruyendo la letra **I** de la terna, quedando formada hasta aquí la cadena **ACCBADACCBACCBACCGI** de la Figura 2.11 (j).

La compresión se pone de manifiesto cuando el segundo elemento de una terna representa una cantidad considerable de caracteres. Es decir, con un solo código se está representando a varios caracteres o letras. **En la práctica, el tercer elemento de la terna no es en realidad una letra sino el código ASCII de dicha letra**. Nótese que la cantidad de caracteres ASCII que se deben transmitir sin comprimir, en este ejemplo, es 19. Mientras que usando LZ77 se transmiten los 9 primeros códigos ASCII correspondientes a las nueve primeras letras sin comprimir y luego 3 ternas, lo que hace un total de 9 + 3 x 3 = 18. La compresión no es significativa ya que el ejemplo es muy corto y las ventanas muy pequeñas. Tomando en cuenta un código ASCII de 7 caracteres, en el primer caso se hubiesen transmitido 7 x 19 = 133 bits, mientras que en el segundo caso serían 7 x 18 = 126 bits. La relación de compresión es entonces 126/112 = 1,125. Tomando en cuenta un texto mucho más largo y ventanas también más largas la relación de compresión normalmente es mayor. Entre otras aplicaciones, el formato ZIP y la norma V.42 bis para módems están basados en LZ77.

Entre las desventajas que presenta el algoritmo se puede decir que asume que las cadenas que se repiten aparecen relativamente cerca una de otra, cuando en realidad puede ocurrir que una cadena se repita varias veces aunque en forma distanciada. Por ejemplo, la palabra mientras normalmente aparece varias veces en un texto pero en forma uniformemente distribuida lo que hace que cuando una de estas repeticiones entra en la ventana de adelante la otra repetición ya salió de la ventana de búsqueda y la compresión no se efectúa.

c. Algoritmo de compresión LZ78

Como se ha visto, el algoritmo LZ77 trabaja con una ventana deslizante de longitud fija, tanto la de búsqueda como la avance. Si dentro de un texto a comprimir la separación entre cadenas repetidas es mayor que el tamaño de la ventana de búsqueda,

el algoritmo no funcionará eficientemente. Si las ventanas se hacen más grandes, como contrapartida el proceso de búsqueda y comparación se hace más complejo a la hora de implementarlo.

En 1978, Lempel y Ziv presentaron una mejora al algoritmo LZ77 (llamándolo LZ78) eliminando la ventana deslizante. El texto que se va codificando va formando parte del diccionario por lo que en principio éste no tiene tamaño fijo.

Cada vez que se va generando un índice, la cadena codificada se agrega al diccionario. Teóricamente este algoritmo alcanza su desempeño óptimo cuando el texto codificado se acerca a infinito. Sin embargo en la práctica, un diccionario muy extenso complica la implementación del algoritmo. Por lo tanto, una vez que el diccionario alcanza un cierto tamaño prestablecido, se lo mantiene fijo en ese tamaño o bien se lo reinicia y se vuelve a empezar.

En lugar de transmitir ternas se transmiten pares. Concretamente, se transmite el puntero que indica la posición de la cadena coincidente y el caracter que sigue a la cadena coincidente. La longitud de la coincidencia no se necesita transmitir ya que el decodificador tiene el mismo diccionario y por lo tanto la conoce, como se ve a continuación enseguida.

A pesar de esta aparente mejora la relación de compresión termina siendo aproximadamente igual que en LZ77. La ventaja de LZ78 está en que se deben hacer menos comparaciones y eso simplifica la escritura del algoritmo en lenguaje de programación y reduce el tiempo de ejecución.

Un ejemplo permitirá comprender cómo funciona LZ78. Considerando la secuencia de caracteres siguiente: sir_sid_eastman_easily_teases_sea_sick_seals

El diccionario consta de tres columnas: entrada de datos, índice asignado y salida de datos, como se muestra en la Tabla 2.2. La columna de salida se forma con pares (índice, caracter actual). Inicialmente el diccionario está vació y se lo va completando a medida que se van leyendo los caracteres a codificar.

Si el nuevo símbolo que se lee no está en el diccionario entonces se lo agrega. Si ya está en el diccionario entonces se lo combina con el siguiente símbolo leído, y si esta cadena de dos símbolos no está en el diccionario entonces es agregada al diccionario. Si ya estuviese entonces se forma una cadena de tres caracteres, etc.

Tabla 2.2 Ejemplo de codificación LZ78 (Fuente [11])

Diccionario		
Entrada	**Índice**	**Salida**
S	1	(0,s)
I	2	(0,i)

R	3	(0,r)
_	4	(0,_)
Si	5	(1,i)
D	6	(0,d)
_e	7	(4,e)
A	8	(0,a)
St	9	(1,t)
M	10	(0,m)
An	11	(8,n)
_ea	12	(7,a)
Sil	13	(5,l)
Y	14	(0,y)
_t	15	(4,t)
E	16	(0,e)
As	17	(8,s)
Es	18	(16,s)
_s	19	(4,s)
Ea	20	(4,a)
_si	21	(19,i)
C	22	(0,c)
K	23	(0,k)
_se	24	(19,e)
Al	25	(8,l)
s(eof)	26	(1,eof)

En el ejemplo el primer caracter leído es s. Como no está en el diccionario entonces se lo agrega haciéndole corresponder el índice 1. El par de salida es (0, s), donde 0 significa que el caracter leído no está en el diccionario y s es el caracter que se acaba de leer. Se siguen leyendo los caracteres siguientes y se observa que hasta el cuarto caracter leído ninguno está previamente en el diccionario por lo que el primer elemento del par es 0 y el segundo elemento es el caracter leído. Cuando se lee el quinto caracter, s, resulta que ya está en el diccionario (con el índice 1), por lo que no hay que agregarlo. Se lee entonces el siguiente caracter, i, para formar la cadena si. Como esta cadena no está en el diccionario entonces se la incorpora con el índice que sigue, el 5. El par transmitido es (1, i), donde el 1 es el índice de s y la i es el último caracter leído. Es decir que en realidad se transmitió si pero con la s representada por el índice que tiene asignado en el diccionario. Es importante aclarar que el segundo elemento del par no es en realidad un caracter sino su código correspondiente, por ejemplo el que le asigna el código ASCII.

El proceso de codificación continúa de esta manera, agregándose al diccionario cadenas cada vez más largas y con un índice asociado. Justamente el efecto de

compresión se ve al formarse estas cadenas, ya que con un número índice se estará transmitiendo varios caracteres a la vez. A medida que el diccionario crece se va haciendo más eficiente la compresión. Obviamente que el diccionario deberá tener un límite. Deberá establecerse de antemano una longitud máxima y luego deberán borrarse los elementos viejos.

Para reconstruir el mensaje original el decodificador va armando el diccionario generado por el codificador. Para el ejemplo recién analizado, el decodificador recibe primero el par (0, s). El 0 le indica al decodificador que la s no está aún en el diccionario, por lo tanto ésta es agregada con índice 1, a la vez que es la salida del decodificador. Lo mismo ocurre con los siguientes caracteres que vienen con índice igual a 0. Cuando llega el quinto par, (1, i), el decodificador combina el caracter que en su diccionario tiene índice 1 (la s) con el caracter i, formando la cadena si. Esta cadena además de agregarse al diccionario con el índice que sigue, es salida del codificador. De esta manera entonces, el decodificador va recibiendo los pares y va reconstruyendo el diccionario original, a la vez que usa dicho diccionario para establecer los caracteres de salida correspondientes a la descompresión.

2.3 Protocolo de red NetFlow

Es imprescindible para una buena utilización de los recursos de red conocer el estado de la misma y sus tendencias de consumo. Para ello es necesario recurrir a ciertas tecnologías que brinden tal información, Para el caso de estudio se hace uso del protocolo de red NetFlow el cual es un protocolo propietario de Cisco. A continuación se desarrollan sus aspectos más importantes.

2.3.1 Descripción del NetFlow

Cisco NetFlow es una tecnología de flujo desarrollada por Cisco que permite el monitoreo de ancho de banda de una red. NetFlow Analyzer es un software que utiliza Cisco NetFlow para controlar el ancho de banda y se ejecuta en Windows y Linux. Dispositivos de Cisco como routers y switches pueden exportar paquete UDP mediante NetFlow. Cisco NetFlow es uno de los flujos, entre otros flujos, que se utiliza para controlar el ancho de banda de la red.

Estos paquetes de Cisco NetFlow pueden ser analizados mediante NetFlow Analyzer, para controlar el ancho de banda, para recabar información sobre los transmisores principales, aplicaciones y muchas otras características. El análisis de tráfico de las redes es uno de los usos de NetFlow Analyzer. NetFlow Analyzer proporcionar informes fácil de entender sobre el análisis de tráfico en profundidad y el monitoreo del ancho de banda.

Cisco NetFlow permite la monitorización de ancho de banda extremadamente granular y preciso al registrar el tráfico de red en la memoria caché del dispositivo. Puesto

que el tráfico en la red tiene un flujo natural, los datos contabilizados por el NetFlow, captura el tráfico IP que se está remitiendo. Se muestran algunas pantallas del NetFlow Analyzer en las Figuras 2.12 y 2.13.

Cisco NetFlow consiste en registrar datos exportados de los routers o switches de flujos de tráficos expirados con estadísticas de tráfico detallado útiles para controlar el ancho de banda y analizar el tráfico de la red. Estos flujos contienen información acerca de la fuente y destino de direcciones IP, junto con los protocolos y puertos utilizados en la comunicación extremo a extremo.

Los datos exportados por NetFlow son recolectados y analizados por NetFlow Analyzer para generar informes sobre los principales host, principales aplicaciones, principales conversaciones y comunicaciones utilizados en el ancho de banda de le red.

Cisco NetFlow combinado con Netflow Analyzer proporciona información valiosa sobre el comportamiento del tráfico y el control del ancho de banda de la red. Contar con esta información, es más fácil para tomar decisiones críticas sobre la capacidad de ancho de banda, la seguridad y el uso óptimo de la infraestructura de red.

2.3.2 Monitorización del rendimiento tradicional de SNMP

Tradicionalmente los clientes, para controlar el ancho de banda dependían casi exclusivamente de SNMP (Simple Network Management Protocol – Protocolo simple de administración de redes).

A pesar que SNMP facilita la planificación de la capacidad, hace poco para caracterizar las aplicaciones y patrones de tráfico, esenciales para la comprensión de lo bien que la red apoya el negocio. Una comprensión más granular de cómo se utiliza el ancho de banda es extremadamente importante hoy en día en redes IP. Contadores de paquetes y de interfaz de bytes son útiles, pero el conocimiento de qué direcciones IP son la fuente y destino del tráfico y qué aplicaciones son las que generan tráfico es muy valiosa.

2.3.3 Reconocimiento de Redes basada en NetFlow

La capacidad para caracterizar el tráfico IP y entender cómo y por donde fluye, es fundamental para la disponibilidad de la red, el rendimiento y solución de problemas.

El monitoreo del flujo del tráfico IP facilita la planificación más precisa de la capacidad y garantiza que los recursos se utilicen de forma adecuada para asegurar se cumplan las políticas establecidas por la organización (Figura 2.12 y 2.13).

Esto ayuda al departamento de TI (Tecnología de Información) a determinar donde aplicar Calidad de Servicio (QoS), optimizar el uso de los recursos y juega un papel vital en la seguridad de la red para detectar ataques de denegación de servicio (DoS), la red de propagación por los gusanos (informáticos) y otros eventos de la red no deseados.

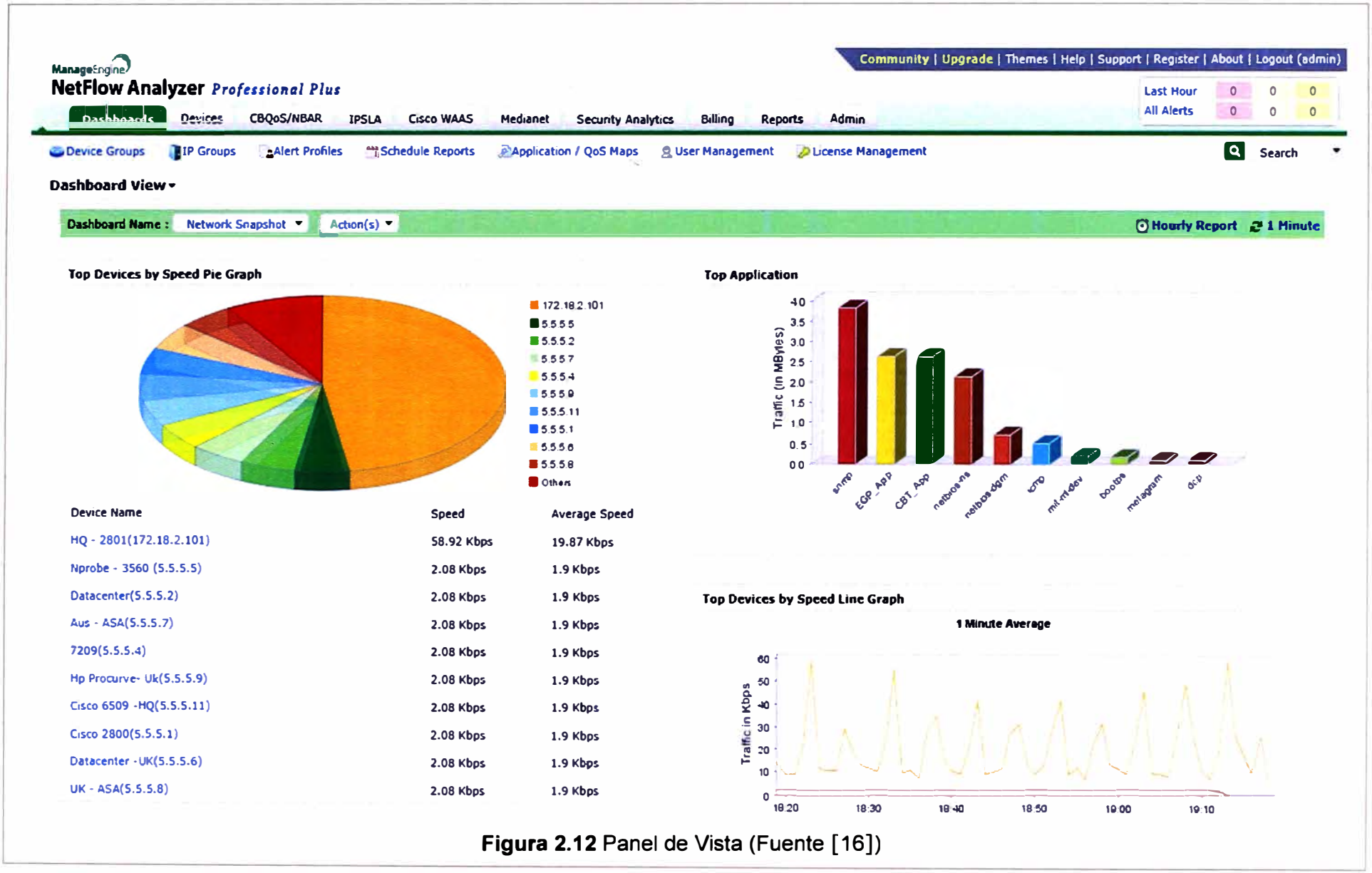

Figura 2.12 Panel de Vista (Fuente [16])

Figura 2.13 Gráfica de interfaz inteligente de tráfico (volumen). Fuente [16]

NetFlow facilita soluciones a muchos problemas comunes que enfrentan los profesionales de TI:

- Analizar las nuevas aplicaciones y su impacto en la red: Identificar las nuevas cargas de aplicaciones de red como VoIP o sitios remotos adicionados.
- Reducción en el pico de tráfico de la WAN: Utiliza estadísticas NetFlow para medir la mejora del tráfico WAN de cambios en las políticas de aplicación, conociendo quien está utilizando la red y el principal comunicador en la red.
- Solución de problemas y conocimiento de puntos críticos: Diagnosticar el rendimiento lento de la red, basura en el ancho de banda y la utilización rápidamente del ancho de banda con interfaz de comandos en línea o los reportes de herramienta.
- Detección de tráfico en la WAN no autorizada: Evita costosas actualizaciones mediante la identificación de las aplicaciones que causan congestión.
- Seguridad y detección de anomalías: NetFlow se puede utilizar para la detección de anomalías y diagnóstico de gusano junto con aplicaciones como Cisco CS_MARS.
- Validación de los parámetros de calidad de servicio (QoS): Se debe confirmar primeramente que el ancho de banda es el apropiado y ha sido asignado para cada clase de servicio (CoS) y que CoS no es excesiva o insuficiente.

2.3.4 Flujo IP

Cada paquete que se envía dentro de un router o switch es examinado por un conjunto de atributos de paquete IP. Estos atributos son los que identifican los paquetes IP o huella digital del paquete y determina si el paquete es único o similar a otros paquetes. Tradicionalmente un flujo IP se basa en un conjunto de 5 y hasta 7 atributos de paquetes IP.

A continuación se mencionó los atributos de los paquetes IP utilizados por NetFlow:

- La dirección IP de origen.
- La dirección IP de destino.
- Puerto de origen.
- Puerto de destino.
- Tipo de protocolo de capa 3.
- Clase de Servicio (CoS).
- Interfaz de router o switch.

Todos los paquetes con la misma dirección IP origen/destino, puertos origen/destino, protocolo de interfaz y clase de servicio son agrupados en un flujo, entonces los paquetes y bytes son contados. Esta metodología de toma de huellas dactilares o la determinación de un flujo es escalable porque una gran cantidad de información en la red es condensada dentro de una base de datos de información NetFlow denominada caché

NetFlow (Figura 2.14).

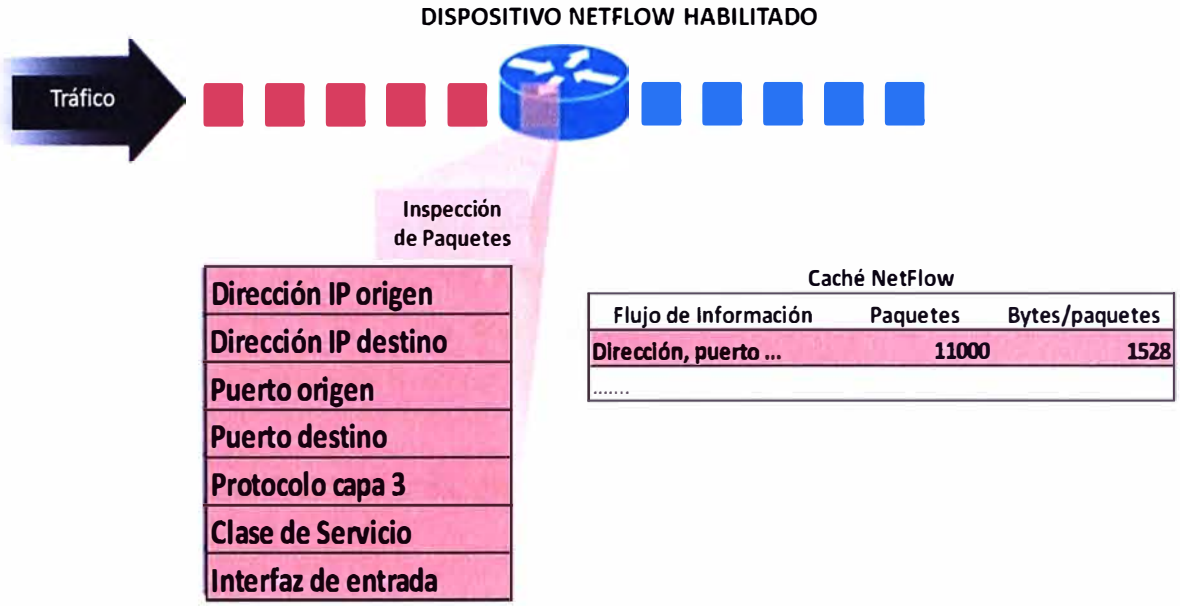

Figura 2.14 Creación de un flujo en la caché NetFlow (Fuente Cisco)

Este flujo de información es muy útil para entender el comportamiento de la red

- La dirección origen permite conocer quien está originando el tráfico.
- La dirección de destino indica quien está recepcionando el tráfico.
- Los puertos caracterizan la aplicación utilizando el tráfico.
- La clase de servicio examina la prioridad del tráfico.
- La interfaz de dispositivo informa cómo el tráfico está siendo utilizado por el dispositivo de la red.
- Los paquetes y bytes contados muestran la cantidad de tráfico.

2.3.5 Accediendo a los datos producidos por NetFlow

Hay dos métodos principales para acceder a los datos NetFlow: la interfaz de línea de comandos (CLI Command Line Interface) con comandos mostrados o la utilización de herramientas de informes de aplicación. Si se está interesado en una visión inmediata de lo que está sucediendo en su red, la CLI se puede utilizar. NetFlow CLI es muy útil para solucionar problemas.

La otra opción es exportar NetFlow a un servidor de informes o lo que se denomina el "colector NetFlow". El colector NetFlow tiene el trabajo de montaje y comprensión de los flujos de exportación y la combinación o la agregación de ellos para producir los valiosos informes utilizados para el tráfico y el análisis de la seguridad. Exportar NetFlow, a diferencia del sondeo de SNMP, arroja información periódicamente al colector de informes de NetFlow. En general, la memoria caché de NetFlow es constantemente llenada con los flujos y el software en el router o en el switch está buscando la caché para flujos que han terminado o expirado y estos flujos son exportados al servidor del colector

NetFlow. Los flujos se termina cuando la comunicación en al red ha terminado (ejemplo, un paquete contiene la flag TCP FIN). Para implementar la comunicación de datos NetFlow, se utilizan los siguientes pasos:

- NetFlow es configurado para capturar los flujos a la caché de NetFlow.
- NetFlow es configurado para enviar los flujos hacia el colector.
- La memoria caché de NetFlow está buscando los flujos que se han terminado y estos son exportados al servidor colector NetFlow.
- Aproximadamente 30 a 50 flujos son agrupados y se transportan normalmente en formato UDP (User Datagram Protocol, Protocolo de datagrama de usuario) al servidor colector NetFlow.
- El software colector NetFlow crea informes en tiempo real o históricos desde la data almacenada.

CAPÍTULO III
METODOLOGÍA PARA LA SOLUCIÓN DEL PROBLEMA

En el presente capítulo se expone la metodología para la solución de optimización de la WAN mediante la compresión de datos así como para el análisis de tráfico cursado.

Inicialmente se hace el planteamiento de la solución, luego la descripción de la solución de optimización de tráfico de datos, y la Implementación de la solución de análisis de tráfico cursado (NetFlow).

3.1 Planteamiento de la solución

En esta sección se expondrá el aspecto situacional del caso de estudio y se hará la evaluación de alternativas de solución y luego su dimensionamiento.

3.1.1 Análisis situacional

El cliente (la empresa petrolera), además de la solución de conectividad implementada mediante el cambio de tecnología y medios de acceso, y de la colocación de enlaces de respaldo, solicitó un sistema de compresión de datos que permitiera a cada una de las localidades agilizar en forma rápida la transferencia de tráfico, ahorrando el ancho de banda de cada una de las sedes.

Es para ello que esta solución constituyó un proyecto adicional, para el cual se debía realizar su adecuado dimensionamiento a fin de satisfacer los requerimientos del cliente.

Cómo ya fue descrito en el esquema de red de la empresa petrolera (Figura 1.1 capítulo I), la solución de compresión de datos debía ser aplicada a todas las sedes indicadas, es decir en total 28 sedes remotas y una sede central, cada tipo con distinto ancho de banda.

Con el propósito de evaluar la solución que se deberá ofrecer con los equipos que cubran las necesidades de cada una de las sedes de la empresa petrolera, es que se deberá contar con los datos necesarios de la cantidad de usuarios, así como de las sesiones concurrentes por cada uno de los mismos; se deberá también tener en cuenta el tipo de protocolo y la aplicación que se utilizan con mayor frecuencia.

Con este fin se realiza un levantamiento de información con la empresa petrolera obteniendo la siguiente información (con la finalidad de guardar la información de carácter privado de la empresa petrolera, los datos mostrados no son los reales,).

La Tabla 3.1 muestra dicha información.

Tabla 3.1 Datos de la empresa (Fuente Elab. Propia)

Sedes de empresa petrolera	Cantidad de Usuarios	Cantidad de sesiones concurrentes por Usuario	Tipo de Protocolo y/o aplicaciones
OFP Lima	1000	18	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima - Talara	800	14	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima - Conchán	300	12	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Operaciones Selva (Iquitos)	250	10	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima - Bayóvar	80	8	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Salaverry	4	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Unidad Norte Chiclayo	6	4	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de ventas Pucallpa	18	3	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima - Lima – Planta de Ventas Pisco	8	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Supe	8	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Chimbote	8	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Piura	8	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Mollendo	13	3	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Cerro de Pasco	3	1	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Tarapoto	13	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas	18	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP,

Sedes de empresa petrolera	Cantidad de Usuarios	Cantidad de sesiones concurrentes por Usuario	Tipo de Protocolo y/o aplicaciones
Yurimaguas			IP/TCP:5450
Lima – Planta de Ventas Cusco	18	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Juliaca	3	1	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta Aeropuerto Arequipa	2	1	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Aeropuerto Cusco	5	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Aeropuerto Trujillo	2	1	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Aeropuerto Tacna	2	1	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima - Planta de Ventas Aeropuerto Chiclayo	2	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Puerto Maldonado	8	5	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Callao	68	10	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima – Planta de Ventas Mazuko	1	1	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima - Unidad Sur	38	4	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima - Estación 7	160	18	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450
Lima - Unidad Ventas Norte Trujillo	4	2	http, ARP, ICMP, IPV6, IPV4, otros P2P, SMTP, IP/TCP:5450

3.1.2 Evaluación de alternativas

Para lograr una optimización de datos a nivel WAN, es que se hace necesario buscar una solución que cubra la información de la empresa petrolera (según tabla 3.1.), asegurando que se le brinde al cliente un servicio óptimo, con soporte posterior a la

implantación y que en caso de falla permita la continuidad de la operatividad del enlace.

Ya que la infraestructura no será de su propiedad, no existe el requerimiento de uniformización de tecnología con alguna marca específica, sin embargo, ya que el proveedor tiene un contrato corporativo con Cisco, y considerando que la red de conectividad ya implementada ha sido ejecutada con equipamiento Cisco (dispositivos de red), es que la tecnología a utilizar en la solución debía ser del mismo fabricante.

Adicionalmente, Cisco fue el primero en proveer un sistema de optimización de la WAN (denominado WAAS) que fuera transparente a la red. Esto se cumple por cuanto se preserva los detalles de la cabecera de los paquetes IP, esto incluye las direcciones IP, y los números de puerto TCP, lo cual es considerado importante para que los dispositivos y servicios intermedios funcionen de manera apropiada.

Ejemplo de los dispositivos que podrían ser afectados cuando se manipula los datos de la cabecera son los firewalls, routers, IPS (Sistemas de Prevención de Intrusos), así como técnicas de calidad de servicio (QoS).

Seguidamente se presentan las alternativas de las soluciones WAAS y el resultado de la evaluación de las mismas, es decir las que se adecúan a las necesidades del proyecto en sí. Información relativa a las técnicas de compresión usadas por el WAAS han sido desarrolladas en el capítulo II (Marco Teórico). Con la información expuesta y las necesidades de cada sede ya detalladas, en la siguiente sección se realiza el dimensionamiento de la solución.

a. WAAS appliance

Los WAAS appliance (Figura 3.1) son equipos que se utilizan como aceleradores de datos en la WAN, los cuales tienen la capacidad de optimizar y acelerar los datos aplicando las técnicas descritas en el capítulo II, se instalan en las oficinas principales y remotas y pueden ser escalables dependiendo del rango de usuarios que se necesitan[8].

Figura 3.1 WAVE (Fuente: Cisco)

La plataforma de Cisco Wide Area Application Virtualization Engine (WAVE) consta de

una cartera de aparatos de gran alcance, de redes escalables que alberga Cisco y las soluciones de optimización WAN de aceleración de aplicaciones que permiten a las oficinas remotas (sucursales) la consolidación de servidores y mejoras de rendimiento para las aplicaciones centralizadas y proporcionar a los usuarios remotos el acceso a aplicaciones, almacenamiento y contenido a través de la WAN.

Cisco WAAS appliance proporciona una plataforma unificada para la aceleración y solución de optimización WAN, incluyendo software Cisco WAAS y software Cisco de Sistema de red de contenidos y aplicación (ACNS - Application and Content Networking System).

b. WAAS Express

Cisco Waas Express son componentes que se instalan (integran) dentro de los router cisco de segunda generación (ISR G2), los cuales también trabajan para optimizar el ancho de banda en la WAN pero son usados para oficinas con pocos usuarios, la ventaja es su menor costo [9].

Cisco WAAS Express es una solución rentable de optimización WAN basada en el software Cisco IOS que aumenta la cantidad de ancho de banda disponible para las pequeñas y medianas sucursales y ubicaciones remotas, mientras que la aceleración de aplicaciones basadas en TCP que operan en un entorno WAN.

Cisco WAAS Express nativa utiliza las capacidades del software Cisco IOS y proporciona una pequeña huella, una solución rentable que se integra de forma transparente a la familia de productos Cisco ISR G2 (Integrated Services Router – Router de Servicios Integrados Segunda Generación).

Cisco WAAS Express es totalmente compatible con los módulos Cisco WAAS para los servicios-Ready Engine (SRE) y los aparatos de Cisco WAAS, y puede ser administrado por un administrador común de Cisco WAAS Central. La Figura 3.2 muestra una topología del Cisco WAAS Express.

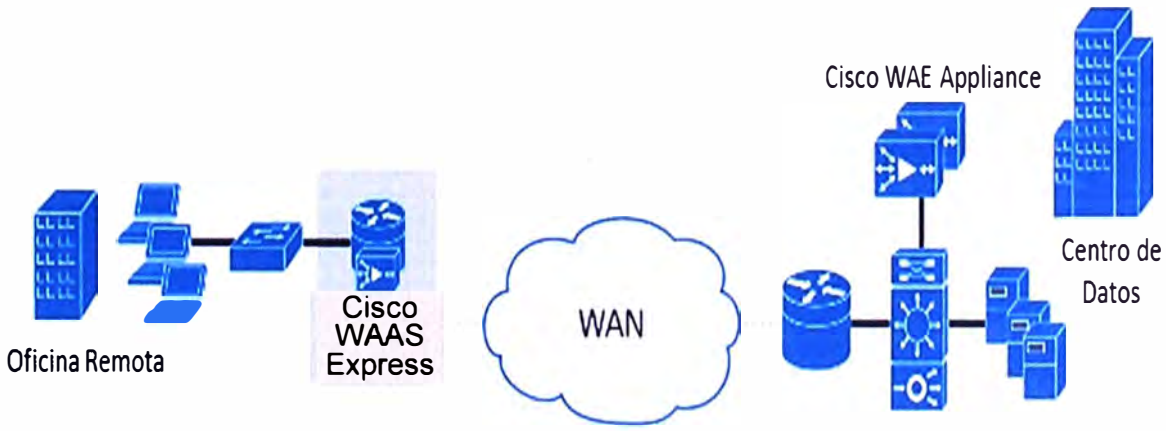

Figura 3.2 Cisco WAAS Express (Fuente: Cisco)

A continuación se mencionan algunos beneficios de Cisco WAAS Express:

- Compresión de ancho de banda: Reduce el consumo de ancho de banda y permite la escalabilidad de las oficinas remotas (sucursales) al tiempo que elimina el aumento de los costos de ancho de banda recurrentes.
- Mejora la productividad: Mitiga los efectos de la latencia WAN, mientras transfiere de datos más rápido.
- Ahorro de costes: Permite un ahorro significativo en gastos de capital (CAPEX), permitiendo una pequeña huella de las sucursales de despliegue.
- Red transparente e integrado: Utiliza las capacidades de los routers Cisco ISR G2, se integra con la seguridad, la calidad de servicio (QoS), y otros servicios nativa del software Cisco IOS.
- Facilidad de implementación: Hace fácil la implementación, con la activación del software simple en cualquier router Cisco ISR G2 ejecutando el software Cisco IOS.
- Bajo coste total de propiedad (TCO) y protección de la inversión: Ofrece protección de la inversión y la sencillez de despliegue por la interoperabilidad con los actuales dispositivos WAAS de Cisco y de gestión que proporciona por Cisco WAAS Central Manager, es totalmente compatible con un entorno mixto de Cisco WAAS Express, Cisco WAAS para los módulos SRE y Cisco WAAS appliance (equipos) en diferentes sucursales y centros de datos.

c. Virtual WAAS

El vWaas es la primera solución de optimización en la nube de la WAN. Este dispositivo virtual acelera las aplicaciones de negocios entregados desde la infraestructura de la nube privada y virtual, ayudando asegurar una experiencia óptima del usuario (Figura 3.3).

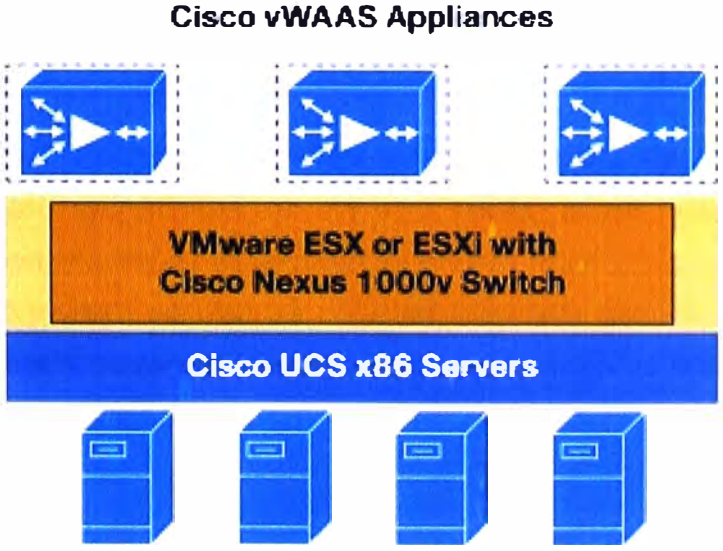

Figura 3.3 Cisco vWaas Arquitectura de implementación (Fuente Cisco)

Como se puede ver en la figura anterior, Cisco vWAAS se ejecuta en el VMware ESXi y Cisco Unified Computing System (UCS – Sistema de Informática Unificada), servidores x86, proporcionando una implementación ágil, elástica y despliegue de múltiples inquilinos [10].

Cisco vWAAS puede ser implementado de dos maneras:

- De forma transparente en el borde de la red WAN utilizando tecnología de intersección fuera de ruta como es el protocolo de comunicación de almacenamiento web (WCCP Web Cache Control Protocol), similar al despliegue de un Cisco WAAS appliance.
- En el centro de datos, junto con los servidores de aplicaciones, utilizando un servidor de red virtual basado en el marco de Cisco Nexus 1000V (switches de acceso como máquinas virtuales basado en IEEE 802.1Q), para ofrecer servicios de aplicaciones optimizados en la nube en respuesta a las instancias de servidores de aplicaciones como máquinas virtuales.

Cisco vWAAS es el único servicio de optimización WAN que soporta una demanda organizada, con operaciones basadas en políticas, en función de cada aplicación. Utilizando una política basada en la configuración en el Cisco Nexus 1000V, el servicio de Cisco vWAAS está asociado con las máquinas virtuales del servidor de aplicaciones, incluso a medida que se crean instancias o se mueven, como se muestra en la Figura 3.4.

Este enfoque permite a los proveedores de la nube ofrecer una rápida entrega de servicios de optimización WAN con una configuración mínima de la red y con poca interrupción en entornos de la nube. Los proveedores de servicios pueden utilizar vWAAS de Cisco para ofrecer un servicio de aplicaciones optimizado en la nube a través de la WAN como un servicio de valor agregado y diferenciado en sus catálogos de servicios en la nube.

Adicionalmente, la Figura 3.4 muestra una demanda organizada de Cisco vWAAS con la configuración de la red mínima con Cisco Nexus 1000V.

Cisco vWaas es totalmente compatible con Cisco WAAS appliance y con router integrados. El Cisco vWAAS Central Manager (VCM) es un appliance virtual que proporciona una gestión común de Cisco WASS virtual y físico.

Además, Cisco vWAAS admiten las características tales como la separación de los recursos informáticos y de almacenamiento con la eliminación de redundancia de datos (DRE) caché almacenada en la SAN.

Esta característica proporciona beneficios tales como la recuperación más rápida de fracasos sin perder el historial de la caché en comparación con los appliances (dispositivos) físicos.

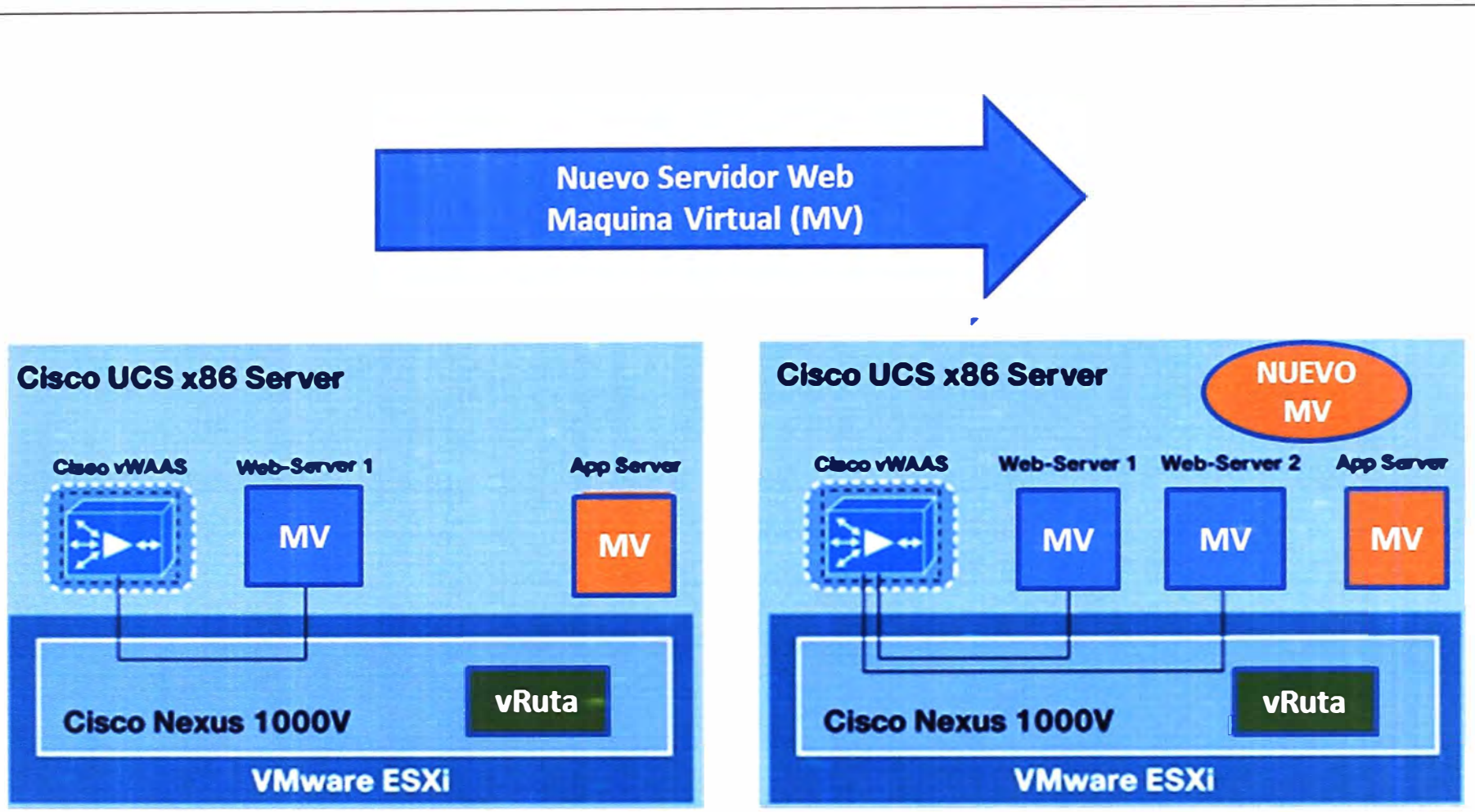

Figura 3.4 Demanda organizada de Cisco vWaas con la configuración de la red mínima con Cisco Nexus 1000V (Fuente: Cisco)

d. WAAS mobile

WAAS Mobile es una extensión de Cisco WAAS Software con beneficios de aceleración de aplicaciones para empleados itinerantes que viajan fuera de la oficina principal y de las oficinas remotas, así como a usuarios móviles que acceden a las aplicaciones alojadas en entornos públicos de la nube (Ver topología en Figura 3.5). La aceleración de las conexiones VPN móviles a través de la Internet pública trae diferentes desafíos técnicos de optimización para una oficina remota y para la WAN corporativa:

- Baja calidad de la red de conexión a la red WAN corporativa. En lugar de tener líneas WAN dedicadas entre la oficina principal y remotas, los usuarios móviles están utilizando conexiones públicas de Internet como DSL, Wi-Fi, satélites, conexión telefónica, cable o celular. Estas conexiones tienen menos ancho de banda, mayor pérdida de paquetes y latencia, y desafíos adicionales tales como retraso por tiempo compartido en entornos celulares.
- Recursos informáticos compartidos en la PC o portátil. En contraste con los usuarios de las oficinas remotas, que pueden contar con un dispositivo dedicado de esta oficina para proveer aceleración en las aplicaciones, los usuarios móviles tienen que compartir los recursos de cómputo de la portátil o de la PC, así como el software TCP con muchas otras aplicaciones del mismo equipo.
- Costo de soporte y las preocupaciones de administración. El entorno abierto de Microsoft Windows en una PC, en contraste con el ambiente controlado de un appliance (equipo), tiene una clase muy diferente de la estabilidad y los requisitos de interoperabilidad, con numerosas aplicaciones que se ejecutan en la PC, una variedad de sistemas operativos, versiones de los navegadores, aplicaciones de seguridad de punto final, y el software cliente VPN y una amplia gama de aplicaciones de negocio.

Para enfrentar estos desafíos, Cisco WAAS Mobile proporciona un rendimiento líder en las condiciones de conectividad de red más exigentes, tiene una pequeña PC, y ofrece un bajo coste total de propiedad (TCO total cost of ownership), la reducción de los costos normalmente asociados con la instalación de software cliente para las PC's de muchos usuarios. La solución también ofrece la facilidad de despliegue.

3.1.3. Conclusión

Como se puede ver, cada solución WAAS ha sido específicamente diseñada para cubrir cierta necesidad.

En esta subsección se analizan estas posibilidades a fin de que satisfagan los requerimientos del proyecto. La alternativa del Virtual WAAS básicamente es utilizada en la nube de un proveedor de servicios, y lo que se está buscando es una aplicación en cada sede.

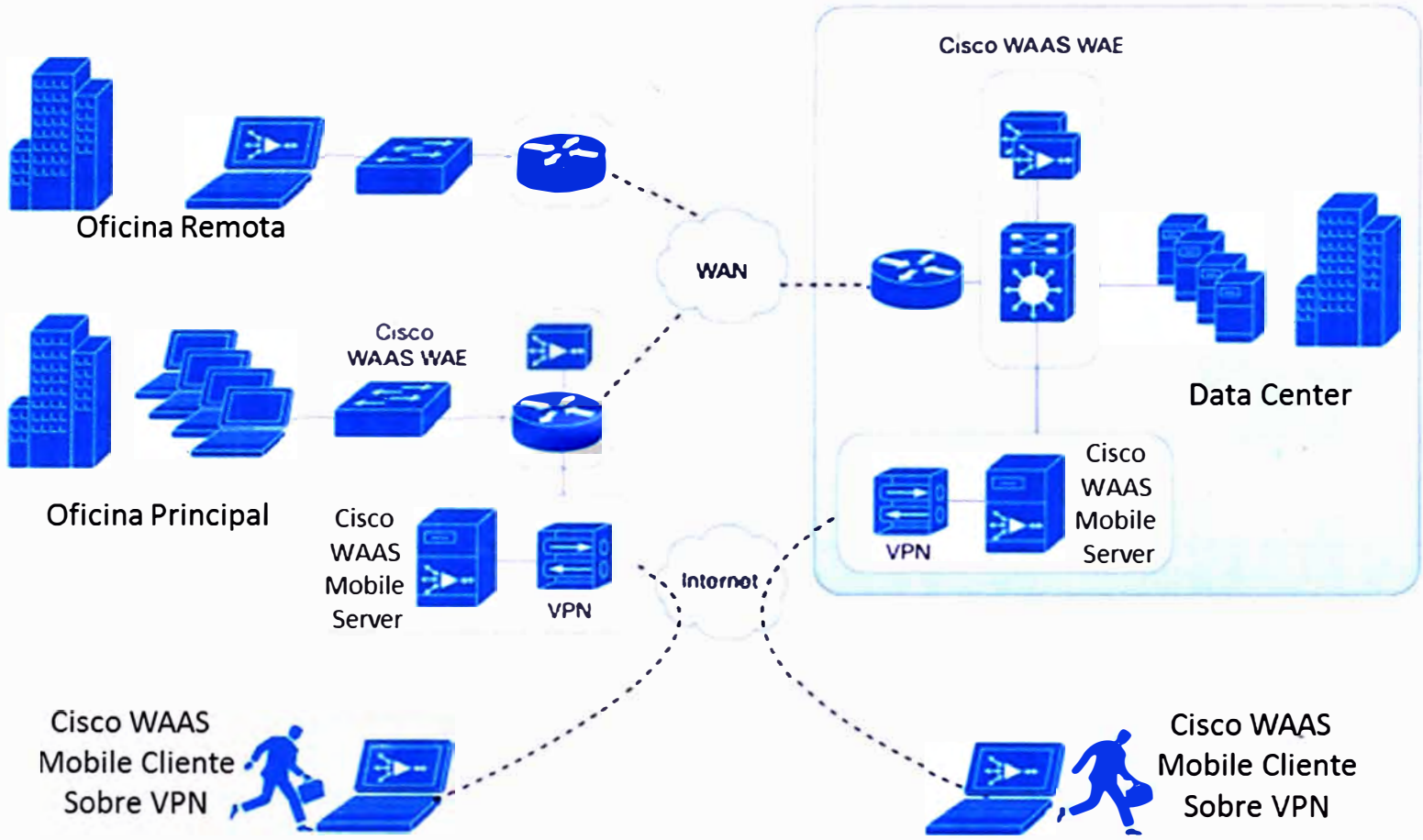

Figura 3.5 Topología de aplicación Waas Mobile (Fuente: Cisco)

Considerando que los usuarios están en oficinas fijas y no son usuarios móviles, el WAAS Mobile no sería la solución que cubra las necesidades de la empresa petrolera.

Los WAAS Express podrían haber sido consideradas para la solución de las sedes pequeñas (planta/venta) toda vez que sólo trabajan con los routers Cisco ISR G2 (2da. Generación). La solución aminora los costos, pero tiene limitantes (capacidad en lo que respecta al ancho de banda, memoria), toda vez que está solución es una aplicación que va sobre el router, compartiendo sus recursos. Sin embargo, como fue mencionado sería una solución ideal para la sedes pequeñas. A la fecha del planeamiento del proyecto (diciembre 2010), sólo se contaba con los router Cisco ISR G1 (1ra Generación). Es por ello que las sedes pequeñas son implementadas con los WAAS appliances.

Al margen de la generación de los routers, son los appliances los que cubran las necesidades de las sedes sin importar su tamaño, ya que existen distintos modelos y capacidad y no comparten recursos toda vez que son exclusivos para la gestión de aceleración de datos. Otra razón de que la solución se haya ejecutado con los WAAS appliance es que estos son escalables, pudiendo adaptarse a la demanda de usuarios según el crecimiento de las necesidades en las distintas sedes.

3.1.4 Dimensionamiento de la solución

Para el estudio, las sedes son agrupadas en tres categorías basadas en su actividad: Sede Central, Sede Operaciones y Sede Plantas/Ventas.

a. Sede Central

Es la sede donde se concentra la mayor cantidad de usuarios y la que alberga el centro de datos de la empresa petrolera. Desde esta sede se realizará la administración de todos los WAAS instalados en las distintas oficinas remotas, así como el monitoreo de los enlaces a nivel WAN.

Como la concentración de usuarios es grande, se tiene que dimensionar un enlace con ancho de banda que cubra todas sus necesidades, así como de tener en consideración las conexiones que hacen estas sedes remotas.

Al ser calificada como una sede central, en la misma se deberá instalar un equipo compresor de datos que cubra la cantidad de usuarios, así como un equipo que haga las veces de administrador central (central manager).

Para una solución de aceleradores o compresores de datos, para que funcione una conexión de un punto a otro punto, ambos tienen que contar con el equipo compresor, toda vez que al uno comprimir en un extremo, en el otro debe leer y descomprimir.

En base a lo expuesto, en la sede central es necesario un equipo appliance compresor que tenga la capacidad de cubrir los 1000 usuarios que existen en dicha sede. Adicionalmente, se deberá instalar, como ya fue mencionada, un appliance llamado

Central Manager, quien tendrá el control de todos los appliances instalados en las diferentes sedes (oficinas remotas). La Tabla 3.2 muestra los equipos appliances disponibles y que son comercializados por la empresa proveedora de servicios:

Tabla 3.2 Equipos appliances cisco

WAAS Appliance (TFO - DRE - LZ + Aplicaciones)		
Equipos Sedes	Max. Usuarios recomendados	Ancho de Banda
WAVE-294-4GB	20	10MB
WAVE-294-8GB	40	20MB
WAVE-594-8GB	75	50MB
WAVE-594-12GB	130	100MB
DATA CENTER		
Equipo Central Manager	Dispositivos WAAS Administrados	
WAVE-594	1,000	
Equipo Core	Conexiones TCP	Ancho de Banda
WAVE-7541	18,000	500MB

En base al cuadro mostrado, para la sede central se utilizará, como equipo central (core) el appliance WAVE-7541 y como Central Manager un WAVE-294-8GB (para aminorar costos), el cual es más que suficiente cubriendo los 29 dispositivos.

Cuando se procede a la instalación de cada appliance, al momento de iniciar la configuración se elige si el appliance trabajará como central manager o como optimizador (acelerador o compresor).

b. Sede Operaciones

En estas sedes se realizan trabajos de operaciones propios del negocio. Estos tienen cantidades de usuarios menor a la sede central pero que son significativos comparado con las sedes denominadas plantas/ventas. De la tabla 3.1 se evidencian cinco sedes operaciones con cantidad de usuarios igual a 80 a más. Para estas sedes, se utilizará el appliance WAVE 594-12GB.

c. Sede Plantas/Ventas

Estas sedes son las más pequeñas en lo que ha cantidad de usuario se refiere, dedicadas a las ventas de los productos que ofrece esta empresa petrolera. En base a la información de la tabla 3.1 la cantidad de usuarios no supera los 70, razón por lo cual el appliance que se propone para estas sedes serán los siguientes:

- Paras las sedes con máximo 20 usuarios, se instalará el WAVE 294-4GB (21 sedes).
- Para las sedes con máximo 40 usuarios, se instalará el WAVE 294-8GB (una sede).
- Para las sedes con máximo 75 usuarios, se instalará el WAVE 594-8GB (una sede).

3.2 Descripción de la solución de optimización de tráfico de datos

Con los equipos debidamente seleccionados y dimensionados, en esta sección se

muestra las topologías, configuración y trabajos realizados para cada caso

3.2.1 Topología

Las figuras siguientes muestran la topología de la solución WAAS. La Figura 3.6 corresponde a la Sede Central, la Figura 3.7 a la Sede Operaciones y el resto a las oficinas remotas (planta/venta).

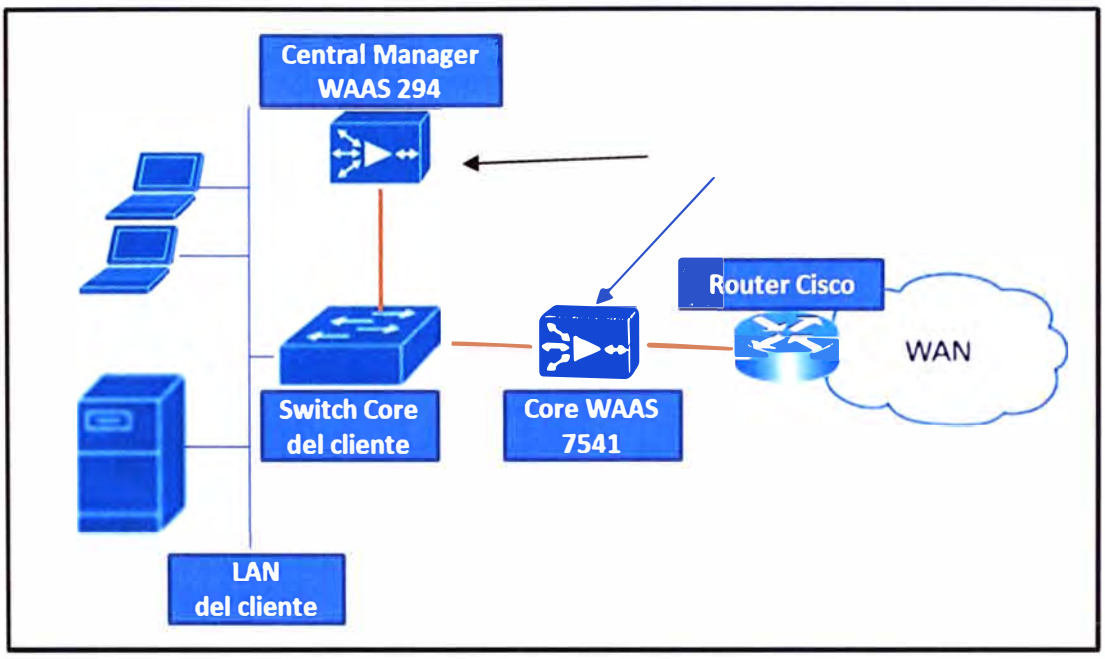

Figura 3.6 Topología de la Sede Central (Fuente: Elab. propia)

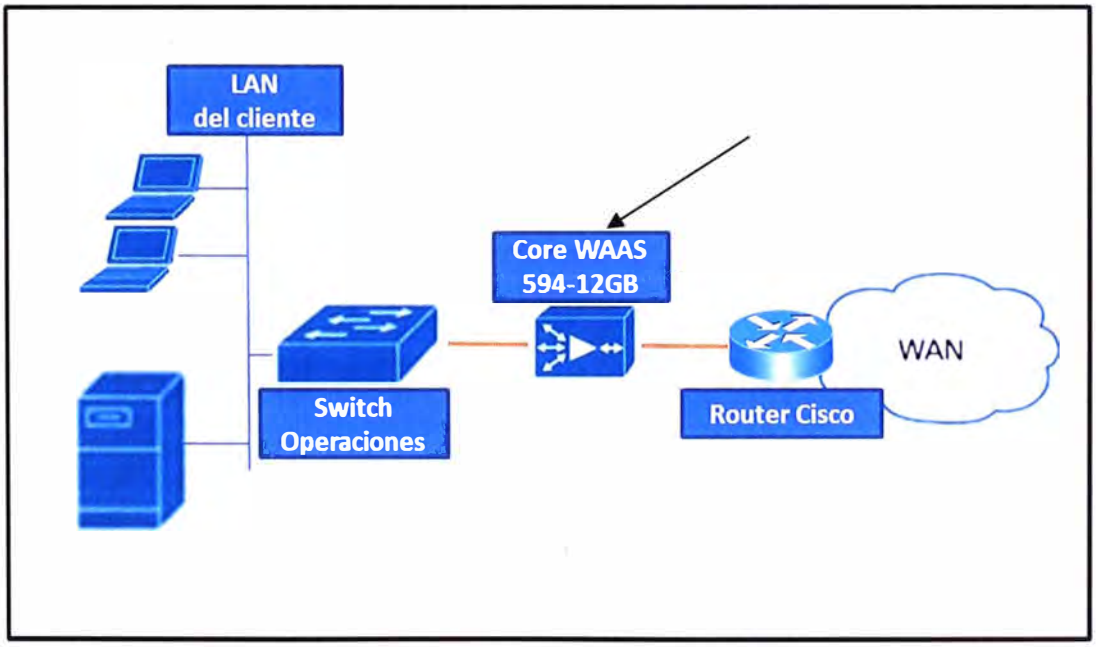

Figura 3.7 Topología de la Sede Operaciones (Fuente: Elab. propia)

La topología y la configuración son similares a todas las oficinas remotas (planta/venta), por lo cual las configuraciones aplican, tanto para la sede operaciones, como para el appliance Core WAAS de la sede central y para los appliances de las sedes planta/ventas.

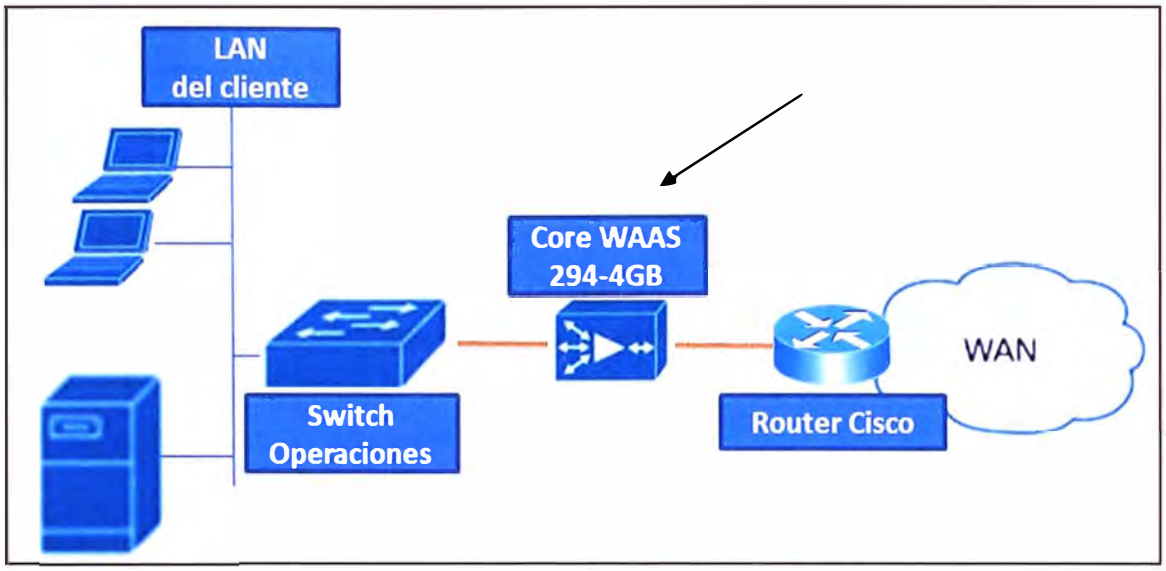

Figura 3.8 Topología para sedes remotas pequeñas, ≤20 usuarios (Fuente: Elab. propia)

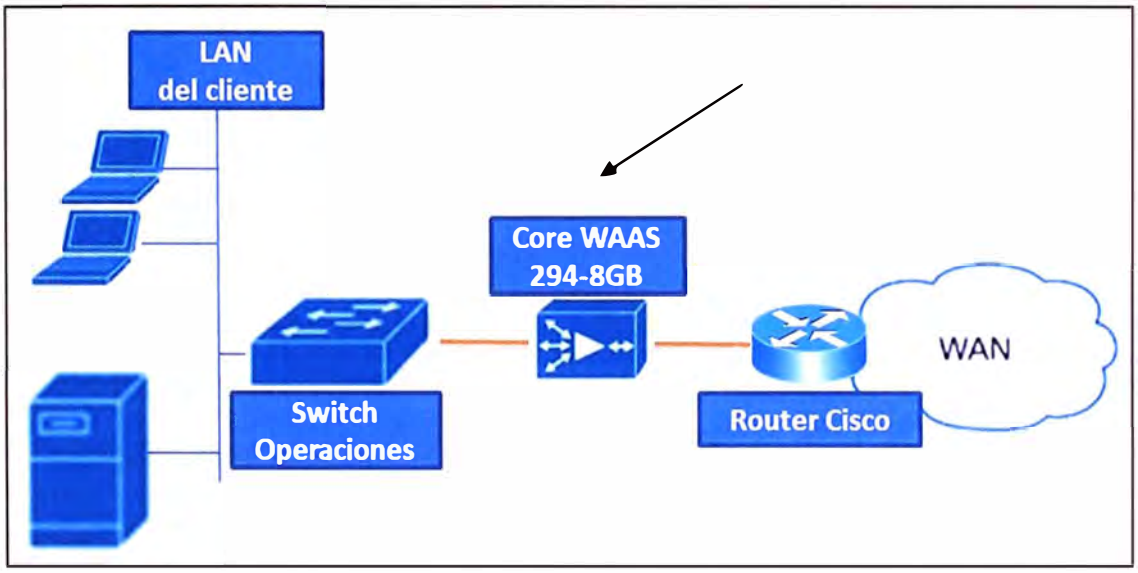

Figura 3.9 Topología para sedes remotas medianas , ≤40 usuarios (Fuente: Elab. propia)

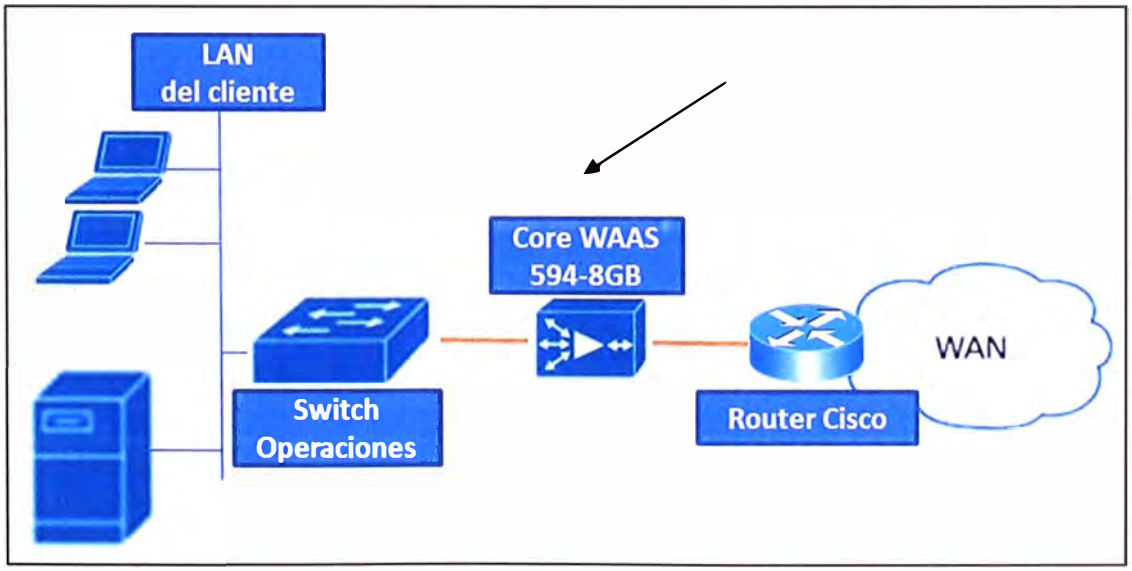

Figura 3.10 Topología para sed. remotas medianas, ≤75 usuarios (Fuente: Elab. propia)

3.2.2 Configuraciones

Las siguientes son las plantillas de configuración: Figura 3.11 configuración del Central Manager, Figura 3.12 configuración de los demás dispositivos WAAS.

Estas plantillas fueron entregadas a los equipos técnicos de implantación para la configuración de los appliances. La única diferencia entre las dos configuraciones mostradas, es que en una se califica como administrador central (Central Manager) y en las demás como acelerador "Optimizador de Datos".

```
device mode central-manager

hostname <Nombre-del-equipo>

ip domain-name <Nombre-de-Dominio>

primary-interface GigabitEthernet 1/0

interface GigabitEthernet 1/0
 ip address <direccion-IP> <mascara>
 no shutdown
 exit

ip default-gateway <IP-del-default-gateway>

clock timezone America/Lima -5 0

ntp server <IP-del-server-NTP>

no auto-register enable

cms enable


username admin password <Contrasena>
username admin privilege 15


tacacs key <contrasena>
tacacs password ascii
tacacs host <IP-del-primer-server-TACACS> primary
tacacs host <IP-del-segundo-server-TACACS>

authentication login tacacs enable primary
authentication login local enable secondary
authentication fail-over server-unreachable

banner login message " No esta permitido el ingreso de usuarios\nno
autorizados a este sistema\n"
banner enable
```

Administrador Central

Figura 3.11 configuración del Central Manager (Fuente: Propia)

```
device mode application-accelerator

hostname <Nombre-del-equipo>

ip domain-name <Nombre-de-Dominio>

primary-interface GigabitEthernet 1/0

interface GigabitEthernet 1/0
 ip address <direccion-IP> <mascara>
 no shutdown
 exit

ip default-gateway <IP-del-default-gateway>

interface InlineGroup 1/0
 inline vlan all
 no autosense
 bandwidth 100
 full-duplex
 exit


clock timezone America/Lima -5 0

ntp server <IP-del-server-NTP>

central-manager <IP-del-WAAS-Central-Manager>

no auto-register enable
cms enable

tfo tcp optimized-send-buffer 2048
tfo tcp optimized-receive-buffer 2048

accelerator http metadatacache enable
accelerator http metadatacache https enable
accelerator http metadatacache filter-extension JPG,GIF

username admin password <Contrasena>
username admin privilege 15

tacacs key <contrasena>
tacacs password ascii
tacacs host <IP-del-primer-server-TACACS> primary
tacacs host <IP-del-segundo-server-TACACS>

authentication login tacacs enable primary
authentication login local enable secondary
authentication fail-over server-unreachable

banner login message " No esta permitido el ingreso de usuarios\nno
autorizados a este sistema\n"
banner enable
```

Optimizador de datos

Figura 3.12 Configuración de los demás appliances (Fuente: propia)

3.2.3 Trabajos realizados en equipos

En base a las topologías mostradas y a la configuración realizada en cada appliance, se muestra a continuación los trabajos que se han tenido que realizar en cada equipo:

- Habilitación de la administración gráfica de la solución.
- Habilitación del funcionamiento en línea.
- La configuración incluye que todas las VLAN puedan pasar a través del WAAS.
- Se configura 100 Mbps para las interfaces del WAAS.
- Se mantienen las políticas de aceleración que vienen por defecto.

Asimismo, a continuación se muestran las pruebas que se realizarán después de la instalación y configuración de los equipos.

- Se probará la conectividad entre la sede central y las demás sedes (operaciones y planta/venta), es decir, entre el Central Manager y el WAAS remoto.
- Para este fin se necesita que el cliente (empresa petrolera) disponga de máquinas en la sede central y remota, además de servidores (FTP, Correo, Web). Se debe considerar que estos trabajos no afecten el funcionamiento actual de los servicios a través de la WAN del cliente.
- Se verificará la negociación de las velocidades, deben estar a 100 full dúplex.
- Se probará la optimización del tráfico entre sedes con aplicativos que indique el cliente, lo cual puede ser transferencia de archivos, bajar archivos de un servidor FTP o Internet.
- Se observará los gráficos en el Central Manager evidenciando el nivel de optimización.

3.2.4 Detalles técnicos el equipamiento

La Tabla 3.3 muestra las características de cada appliance que se han utilizado en la solución. La Tabla 3.4 muestra sus especificaciones de hardware.

Tabla 3.3 Características de appliances utilizados en la solución

Appliance	Características
CISCO WAVE 294 	Ideal para implementaciones en pequeñas sucursales y oficinas remotas. Soporta hasta 200 conexiones TCP (ampliable a 400). 250 GB de disco duro (HDD) de almacenamiento de datos. Dispone de 02 puertos Gigabit Ethernet. Módulo I/O de 04 puertos en línea (IOM), incluido por defecto, con facilidades de ampliación opcional de 08 puertos en línea IOM. Alberga hasta 02 cuchillas virtuales (virtual blades).
CISCO WAVE 594 	Ideal para implementaciones en pequeñas sucursales y oficinas medianas. Soporta hasta 750 conexiones TCP (ampliable a 1300). 500GB de disco duro de almacenamiento de datos (segundo disco duro opcional como redundancia). Dispone de 02 puertos Gigabit Ethernet. Proporciona 04 puertos Gigabit Ethernet de cobre, 08

	puertos de Gigabit Ethernet de cobre o 04 puertos Gigabit Ethernet de fibra SX. Ofrece una segunda fuente de alimentación opcional para una redundancia 1+1. Alberga hasta 02 cuchillas virtuales (virtual blades).
CISCO WAVE 7541 	Ideal para implementaciones en centro de datos de tamaño mediano y grandes sucursales de empresas. Suporta hasta 18000 conexiones TCP. 2.2 GB de disco duro de almacenamiento de datos con RAID-5 de redundancia (RAID, Redundant array of independent, disposición redundante de datos) Disponible de 02 puertos Gigabit Ethernet. Opción de 08 puertos Gigabit Ethernet de cobre, 04 puertos Gigabit Ethernet de fibra SX o 02 puertos de 10 Gigabit Ethernet conectable de forma pequeña (SFP+).

Después de seleccionar los appliances respectivos y descritos anteriormente, en base a los requerimientos de la empresa petrolera, se puede evidenciar el logro en la optimización del ancho de banda de la red WAN, lo cual se muestra en el capítulo IV, Figura 4.2, la misma que se detalla en dicho acápite.

3.3 Implementación de la solución de análisis de tráfico cursado (NetFlow)

Para analizar el tráfico que se está cursando en una red WAN, se necesita de un analizador de tráfico, normalmente un NetFlow Analyzer se utiliza en la sede central porque todo el tráfico de las oficinas remotas están direccionadas (configuradas) y disponibles dentro del protocolo NetFlow. La ubicación donde se implementa el NetFlow Analyzer depende de la ubicación de la solución de los informes o reportes, y también de la topología de la red. Si el servidor de recopilación de información está en una ubicación céntrica, la aplicación del NetFlow cerca de este servidor colector de informes es óptima.

NetFlow también se puede habilitar en las oficinas remotas (sucursales) con el entendimiento de que los datos de exportación utilizarán el ancho de banda del servicio en la WAN. Cerca del 1 al 5% del tráfico conmutado es usado para la exportación en el servidor de recopilación (colector).

En los routers instalados en las distintas sedes, se habilita y se configura la funcionalidad del NetFlow (sede principal, operación, planta/venta). El trabajo en esta parte de la solución es realizar el despliegue de la configuración del NetFlow en todos los dispositivos routers instalados por el proveedor, siendo responsabilidad del cliente la recolección o extracción de los diferentes tráficos de las sedes involucradas, es decir, del servidor NetFlow exportador y del NetFlow Analyzer. La extracción y el análisis del tráfico por sede, la empresa petrolera lo tiene contratado con un tercero, por eso no es parte del alcance de esta propuesta de un sistema de conectividad corporativa para una empresa petrolera el analizar dicho tráfico, solo hacer la configuración para su disponibilidad.

Tabla 3.4 Especificaciones de hardware de los appliances (Fuente: Cisco)

Características de Hardware	CISCO WAVE Appliances		
	WAVE 294	WAVE 594	WAVE 7541
DRAM	4-8 GB	8-12 GB	24 GB
Almacenamiento utilizable	250 GB	500 GB	2.2 TB
HDD máximo	1 * 250 GB HDD	Dos 500 GB	6 * 450 GB
Soporte RAID	-	RAID-1 (optional on 594)	RAID-5
Virtual blades	Hasta 2	Hasta 6	-
Interfaces de Red	Dos 10/100/1,000BASE-T	Dos 10/100/1,000BASE-T	Dos 10/100/1,000BASE-T
Fuente	One 400W AC power supply	• Una Fuente suministrada de 450W AC • Fuente redundante disponible opcional	• Dos fuentes de alimentación AC de 650 W • 1 + 1 redundancia, intercambiables en caliente
Ventilador	cinco ventiladores	Ventiladores redundantes 40 mm, intercambiables en caliente	Ventiladores redundantes 40 mm y 60 mm, intercambiables en caliente
Unidades de rack	01 (se puede utilizar como una unidad de escritorio)	1	2
Modulo I/O	04 puertos GE incluidos en línea	04 puertos / 08 puertos GE en línea (opcional)	02 puertos SFP+10 GE, 08 puertos GE en línea, o 04 puertos GE de fibra en línea (opcional)
Consola	USB, mini USB y consola serial RJ45; detección automática	USB, mini USB y consola serial RJ45; detección automática	USB, mini USB y consola serial RJ45; detección automática

Dimensiones			
Altura	42 mm (1.69 in.)	42 mm (1.69 in.)	87 mm (3.42 in.)
Ancho	429 mm (16.89 in.)	429 mm (16.89 in.)	429 mm (16.89 in.)
Profundidad	370 mm (14.55 in.)	516 mm (20.33 in.) (incluye fuente de alimentación con orejas para el rackeo)	632 mm (24.88 in.) (incluye fuente de alimentación con orejas para el rackeo)
Peso máximo	7.44 kg (16.40 lb)	10.21 kg (22.51 lb)	21.62 kg (47.66 lb)
Dimensiones de envío (con embalaje)	55 x 50.5 x 19.7 cm (21.69 x 19.88 x 7.75 in.)	67.3 x 55 x 19.7 cm (26.50 x 21.69 x 7.75 in.)	78 x 55 x 25.9 cm (30.75 x 21.69 x 10.19 in.)
Peso de envío	10.0 kg (22.0 lb)	12.93 kg (28.50 lb)	24.0 kg (53.0 lb)
Especificaciones de operación			
Entrada universal	Rango de voltaje de línea 90 a 132 VAC	Rango de voltaje de línea 90 a 132 VAC	Rango de voltaje de línea 90 a 132 VAC
Temperatura de operación	0 a 40°C (32 a 104°F)	0 a 40°C (32 a 104°F)	0 a 40°C (32 a 104°F)
Temperatura sin funcionamiento	-30 a 60°C (-22 a 140°F)	-30 a 60°C (-22 a 140°F)	-30 a 60°C (-22 a 140°F)
Humedad	En funcionamiento: 10 a 90% RH (sin condensación). Fuera de funcionamiento: de 5 a 95% RH (sin condensación)	En funcionamiento: 10 a 90% RH (sin condensación). Fuera de funcionamiento: de 5 a 95% RH (sin condensación)	En funcionamiento: 10 a 90% RH (sin condensación). Fuera de funcionamiento: de 5 a 95% RH (sin condensación)
Altitud	En funcionamiento: 3050 m (10000 pies) Fuera de funcionamiento: 4572 m (15000 pies)	En funcionamiento: 3050 m (10000 pies) Fuera de funcionamiento: 4572 m (15000 pies)	En funcionamiento: 3050 m (10000 pies) Fuera de funcionamiento: 4572 m (15000 pies)

La Figura 3.13 muestra la topología para la configuración del NetFlow como exportación de datos hacia un colector.

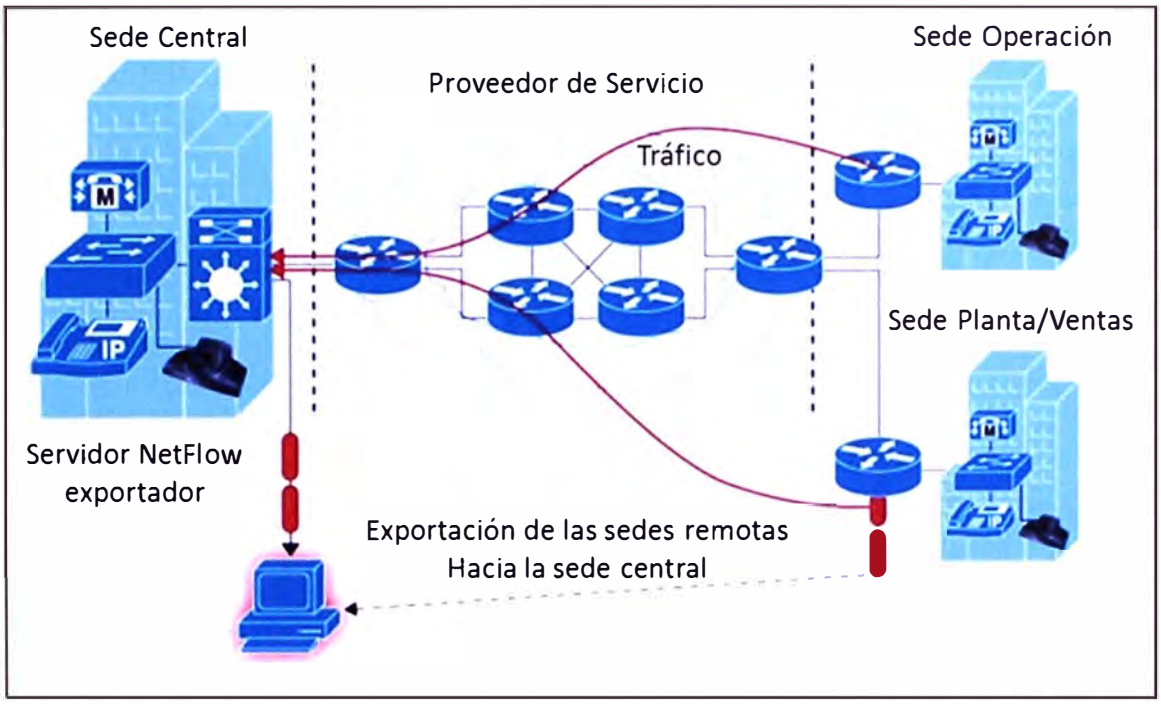

Figura 3.13 Topología para la configuración del NetFlow como exportación de datos hacia un colector (Fuente Cisco)

En la Tabla 3.5 se muestra la configuración ejecutada tanto para la oficina principal como para las oficinas remotas (sucursales):

Tabla 3.5 Configuración ejecutada (Fuente: propia)

Oficina Principal:	`ip flow-egress input-interface`
	`ip flow-cache timeout active 1`
	`ip flow-capture icmp`
	`ip flow-export source GigabitEthernet0/0`
	`ip flow-export version 9`
	`ip flow-export template options export-stats`
	`ip flow-export template options timeout-rate 4`
	`ip flow-export template options refresh-rate 40`
	`ip flow-export destination 10.1.101.51 2055`

Oficinas Remotas:	`Ip flow-cache timeout active 1`
	`ip flow-export source FastEthernet0/1`
	`ip flow-export version 9`
	`ip flow-export destination 10.1.101.51 2055`

Como se ha mencionado anteriormente en el numeral 3.3, el analizador de tráfico no forma parte del alcance de este informe, no obstante se presenta estas gráficas como ejemplos de lo que se puede obtener con esta herramienta (figuras 3.14, 3.15, 3.16 y 3.17). Las pantallas con los datos exactos son manejadas por el propio cliente así como por una tercera empresa que lleva la gestión y análisis de los tráficos generados por todas las sedes.

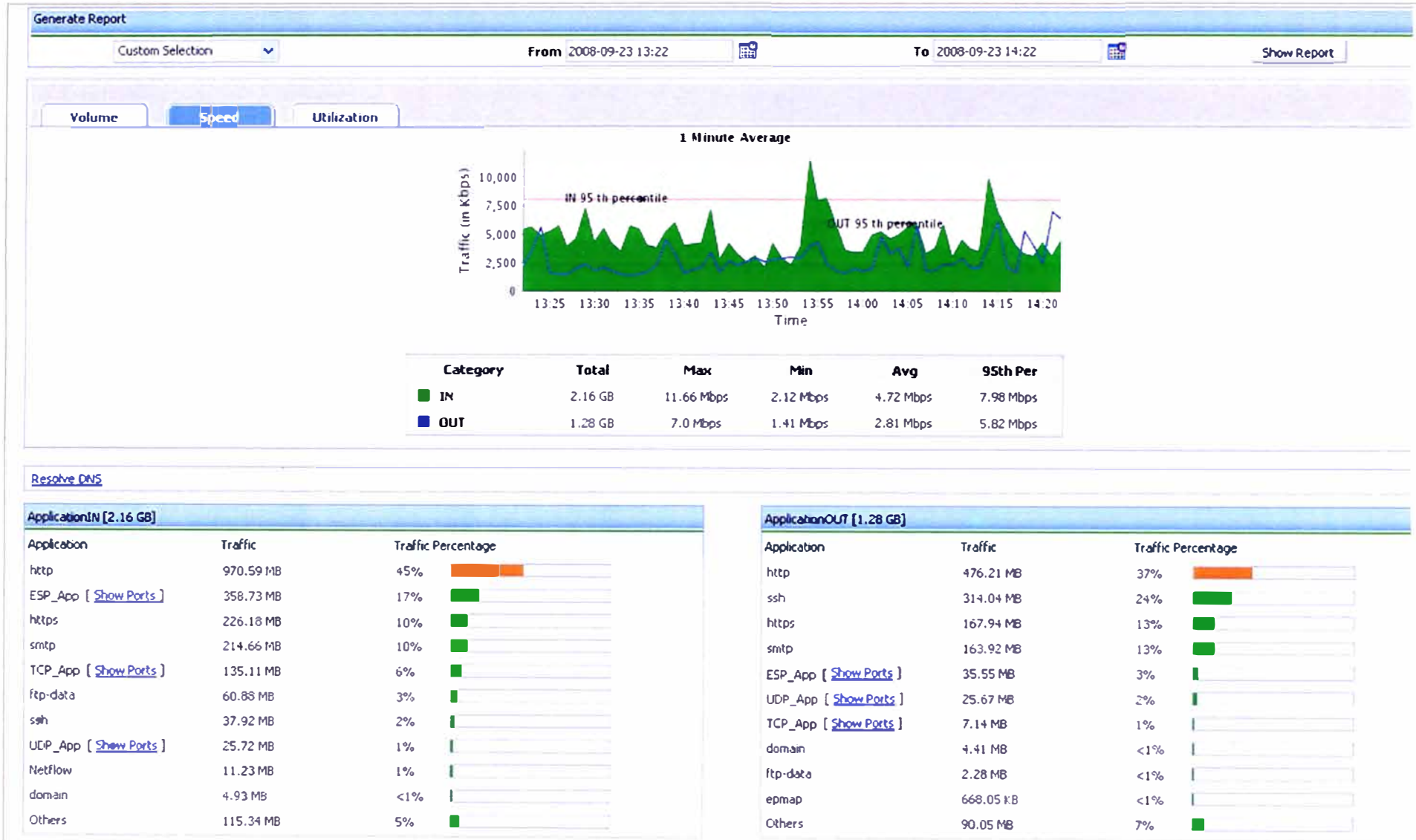

Figura 3.14 Análisis del tráfico de red (Fuente: Cisco)

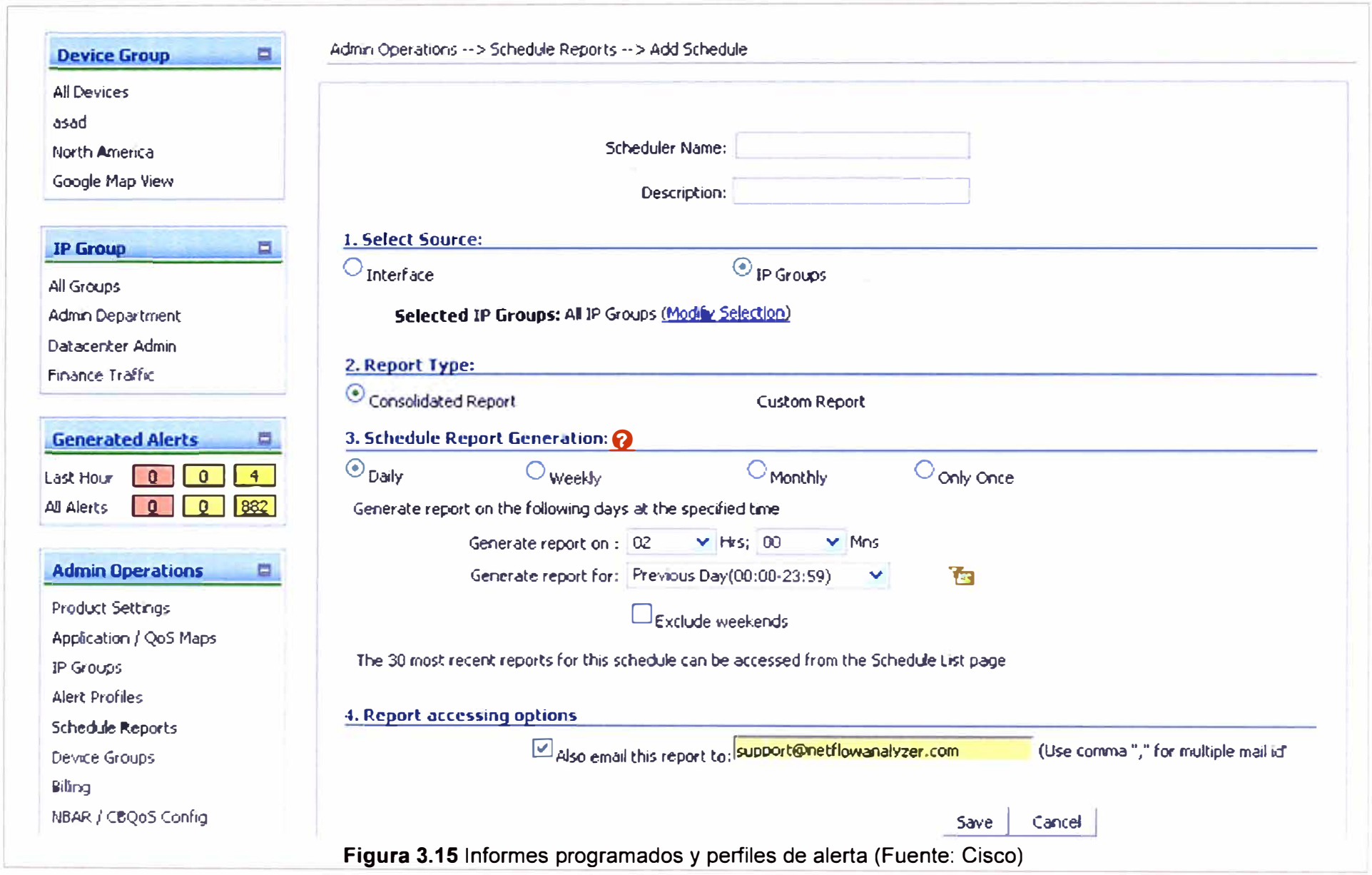

Figura 3.15 Informes programados y perfiles de alerta (Fuente: Cisco)

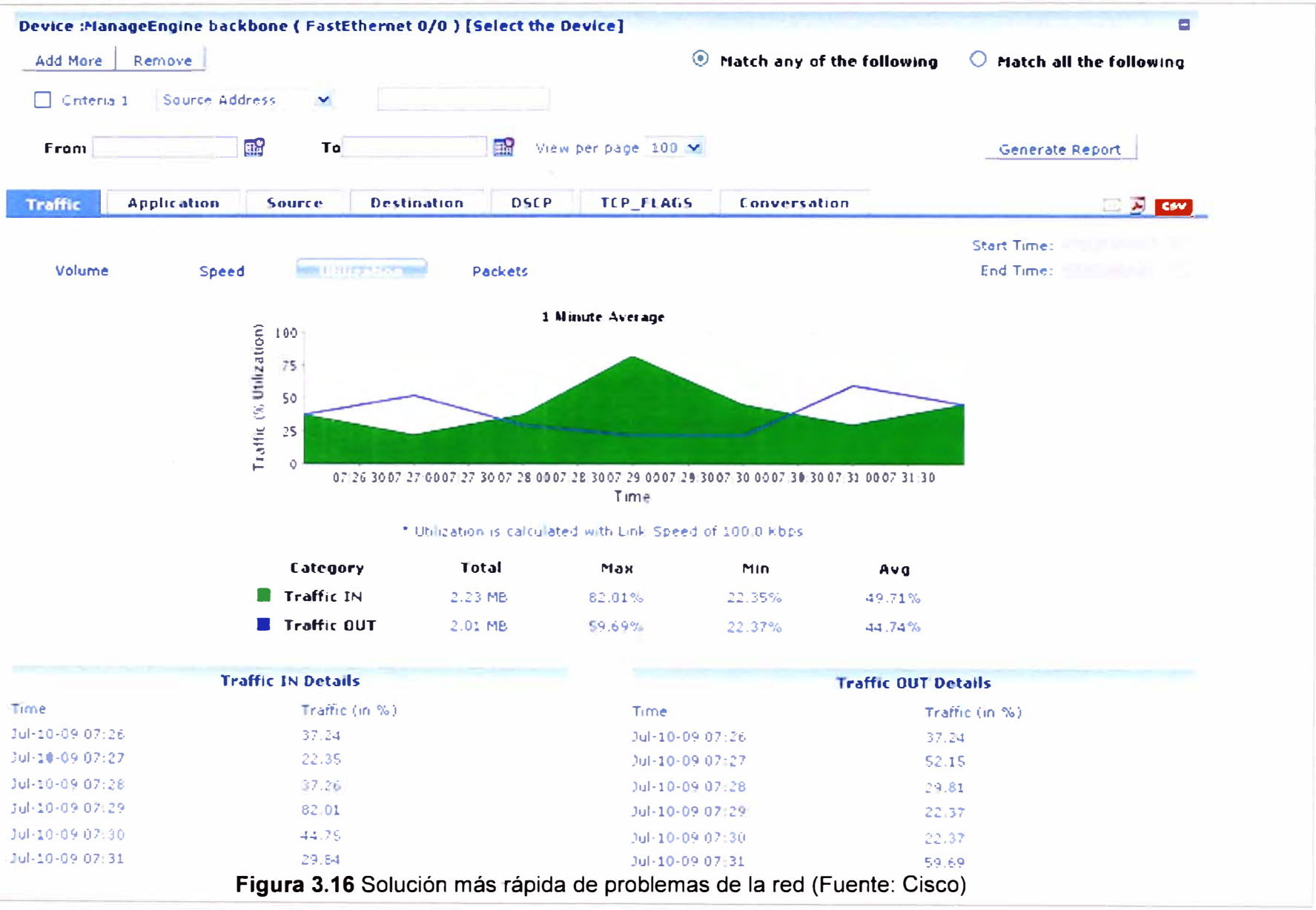

Figura 3.16 Solución más rápida de problemas de la red (Fuente: Cisco)

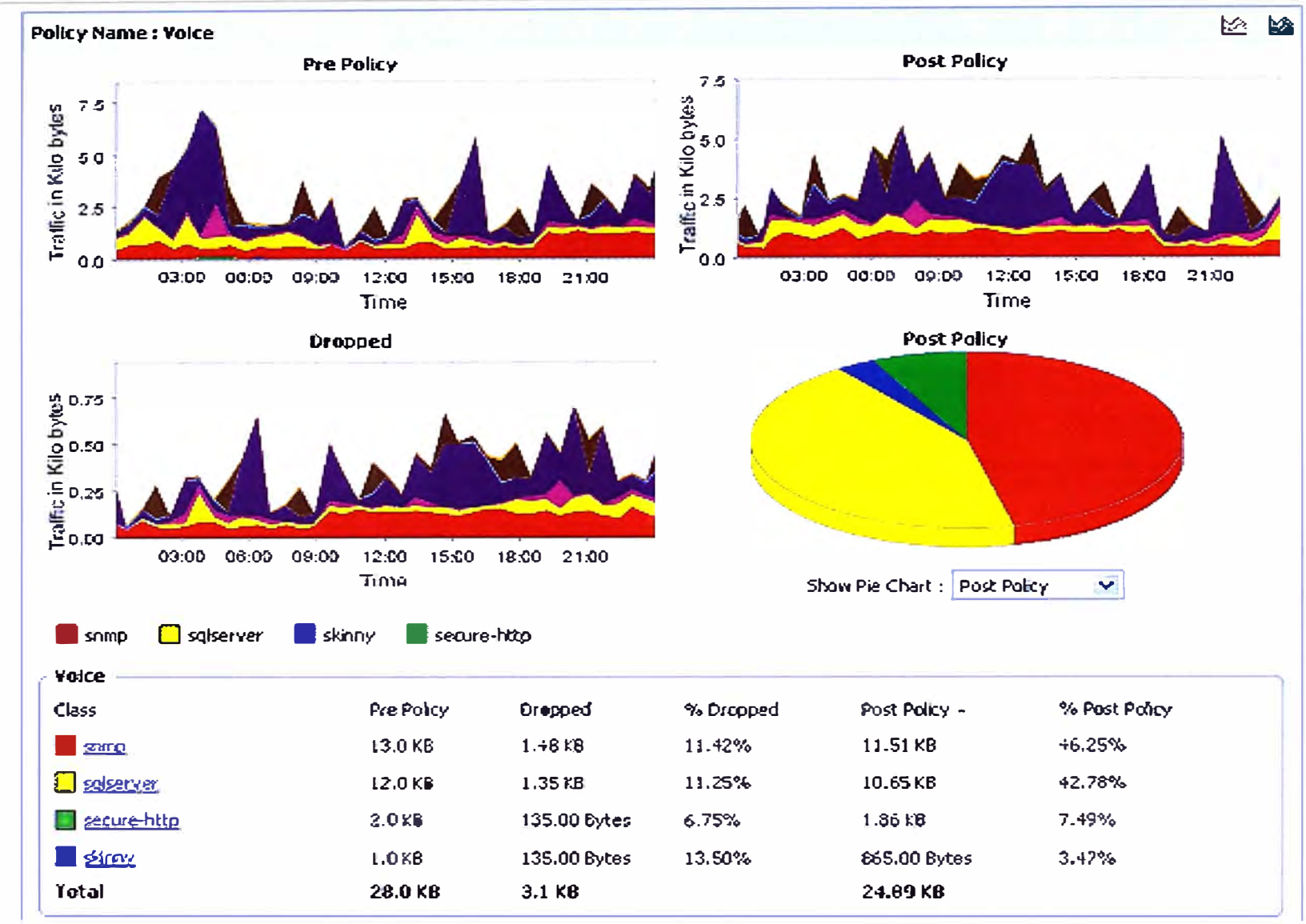

Figura 3.17 Ajuste de políticas de calidad de servicios (Fuente: Cisco)

Con el Netflow configurado y con un servidor colector se logra lo siguiente:

- **Control del ancho de banda de red:** Con informes en tiempos reales se puede controlar el ancho de banda, conociendo los principales generados de tráfico, protocolos, conversaciones y más. Asimismo se puede buscar datos específicos en función de la dirección IP, nombre de host, protocolo etc.
- **Análisis del tráfico de red**: Se controla el ancho de banda y tráfico en un nivel específico de la interfaz con una frecuencia de un minuto. El gráfico seleccionable permite acercar los picos. También se muestra los puntos de datos, que brinda detalles del tráfico entrante y saliente, como velocidad, volumen, paquetes y utilización total del ancho de banda (Figura 3.14).
- **Informes programados y perfiles de alerta**: Envía automáticamente el informe a su casilla de correo. Estos informes se pueden programar para su envío periódicamente. También se puede crear perfiles de alerta según los requisitos, las alertas pueden activar trampas SNMP o pueden enviarse como notificaciones de correo (Figura 3.15).
- **Solución más rápida de problemas de la red**: Este tipo de informe ayuda a solucionar los incidentes de la red más rápidamente. El informe permite seleccionar diferentes criterios a partir de los cuales puede generar este informe en particular. Con este informe se puede ver el tráfico, la aplicación, el origen, el destino, la conversación y mucho más para el periodo específico que seleccionó en el gráfico. Así se obtiene una visibilidad profunda de la utilización pasada del tráfico de la red y del ancho de banda. El informe se puede exportar como PDF, CSV o incluso enviarse por correo electrónico (Figura 3.16).
- **Ajuste de políticas de calidad de servicios**: Se garantiza que las aplicaciones críticas para el negocio tengan la prioridad más alta en la red. CBQoS (Class Based Quality of Service, Calidad de servicio basada en clases) hace que el rendimiento de la red sea más predecible y la utilización del ancho de banda más eficaz. CBQoS brinda visibilidad en profundidad de las políticas aplicadas a sus enlaces y de los patrones de tráfico (Figura 3.17).

CAPÍTULO IV
ANÁLISIS Y PRESENTACIÓN DE RESULTADOS

El análisis de los datos y la presentación de resultados se enfocan en las mediciones del optimizador de datos del Cisco WAAS en base a determinadas aplicaciones y protocolos.

En cuanto al Cisco NetFlow, si bien este recolectará información para ser enviado al servidor recolector, el análisis de estos datos, estaba bajo la supervisión de otra empresa, pero con el propósito de tener mayor claridad se realizará también los comentarios sobre la información en el servidor recolector.

4.1 Niveles de optimización

En la Figura 4.1 se muestra los valores en tiempo de respuesta de las aplicaciones en base a los protocolos que optimiza el Cisco WAAS. En ella se muestran los valores mínimos y máximos que se encuentran en la optimización. Esta optimización se obtiene en todas las oficinas remotas, las cuales por su uso pueden variar entre el rango mostrado. La primera columna muestra las aplicaciones, la segunda columna los protocolos y la tercera columna, la reducción en tiempo de respuesta (mínima y máxima).

Aunque no es parte de la propuesta global de un sistema de conectividad corporativa para una empresa petrolera, contar con la disponibilidad del ancho de banda para cursar tráfico de voz y video producto de su propio negocio (la empresa petrolera tiene implantado una solución de centrales IP usando adicionalmente video conferencia) esta necesidad cobra sentido en la presente solución, generando un requerimiento por parte de la empresa petrolera de optimización de datos en la red WAN, la cual especifica que se debe optimizar por lo menos la tercera parte del ancho de banda, es decir, se tiene que asegurar una optimización del orden del 30% de su tráfico de la red WAN.

En la Figura 4.2, se verifica que del total del tráfico cursado en la WAN (all traffic), la solución con Cisco WAAS logra una reducción de 45.27% del total del tráfico cursado en la WAN del cliente (tráfico original 19,794MB y tráfico optimizado 10,833MB).

Con lo mostrado en la figura, se confirma que el aumento de ancho de banda no es la única solución para los problemas de disponibilidad, sino conocer su tráfico y poder acelerar la comunicación o transferencia de datos resulta fundamental en las comunicaciones hoy en día (está información ha sido extraída en el mes de Abril 2012).

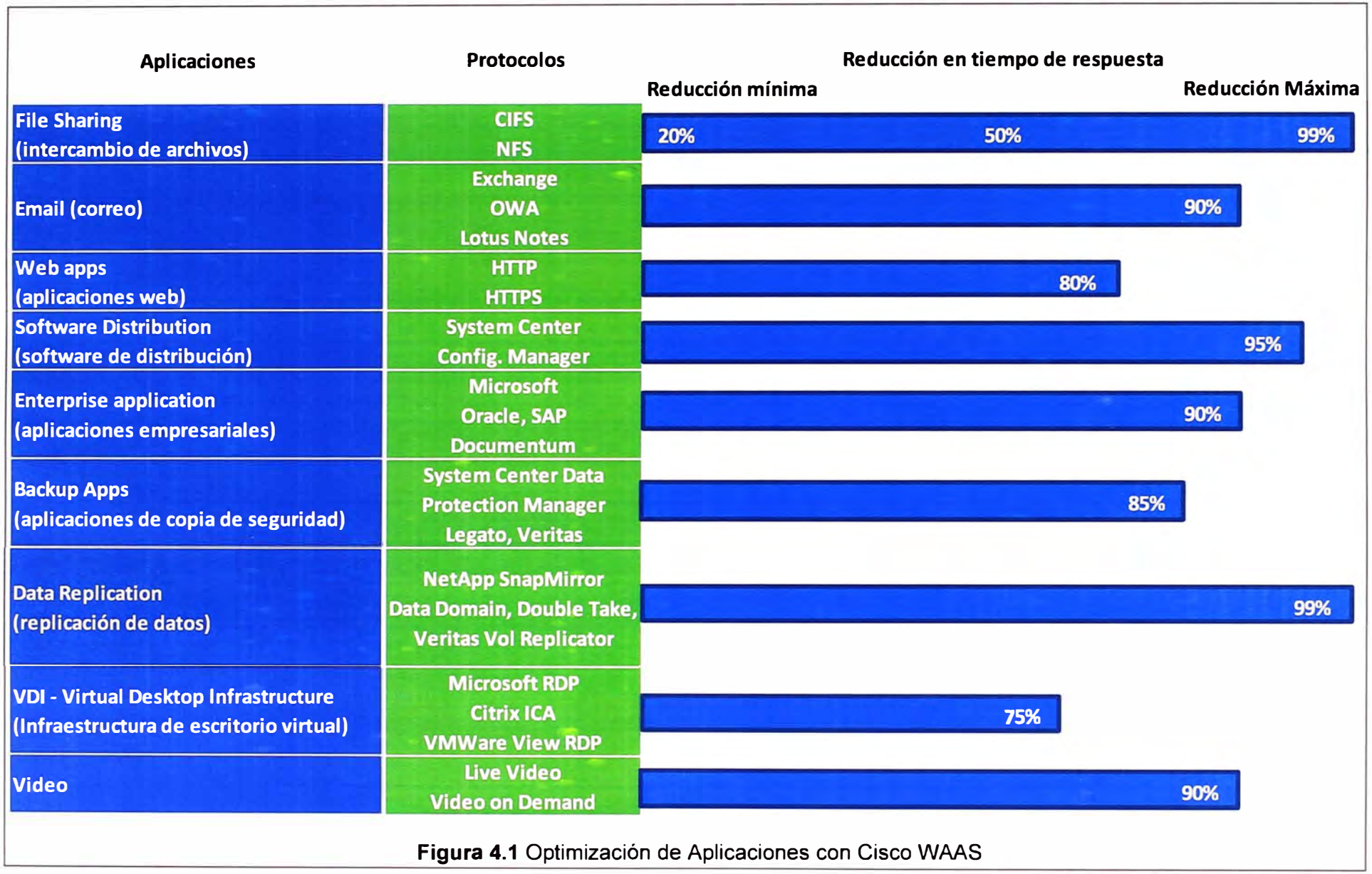

Figura 4.1 Optimización de Aplicaciones con Cisco WAAS

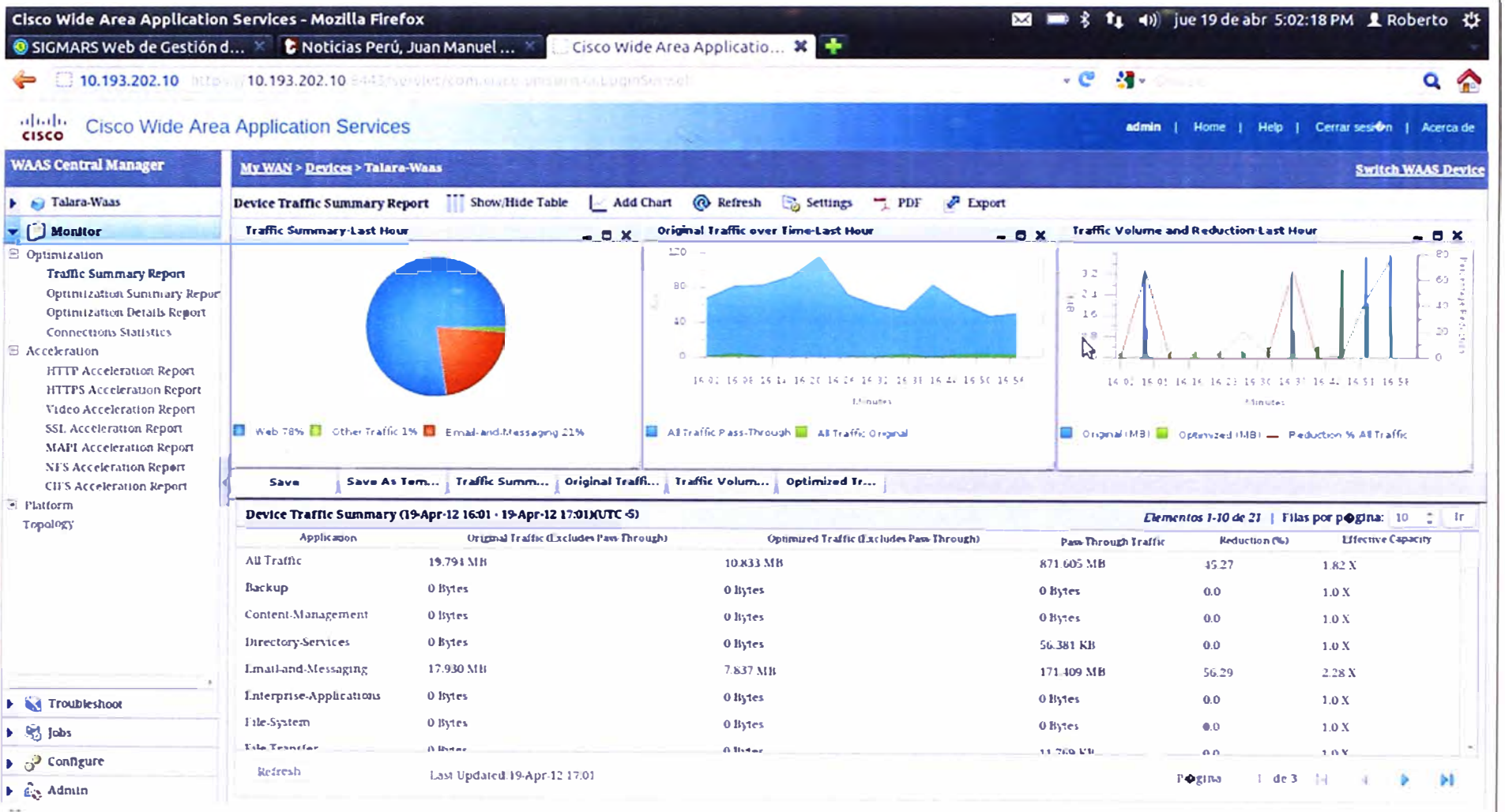

Figura 4.2 Optimización en la red WAN (Fuente: Central Manager)

Asimismo, la empresa proveedora de la solución (el proveedor), tiene en su Centro de Gestión una herramienta de monitoreo de tráfico basado en SNMP (Protocolo simple de administración de red), en la cual se puede revisar el tráfico cursado antes y después de la instalación de los optimizadores de datos (Cisco WAAS) en la sede central de la empresa petrolera, observando una mayor disponibilidad en el ancho de banda mostrado en la Figura 4.3. En esta figura, las líneas en color verde representan el tráfico saliente y las de color azul representan el tráfico entrante.

Se observa que después de la instalación del Cisco WAAS, el tráfico saliente ocupa un menor ancho de banda, logrando de esta forma una mayor disponibilidad para el envío y recepción de tráfico entre todas sus sedes.

Se debe considerar que la sede central tiene el enlace de transmisión de datos principal, el cual hace de cabecera para brindar acceso a las aplicaciones internas en su LAN y data center y es donde se ha realizado la instalación del Central Manager para la administración de los dispositivos Cisco WAAS.

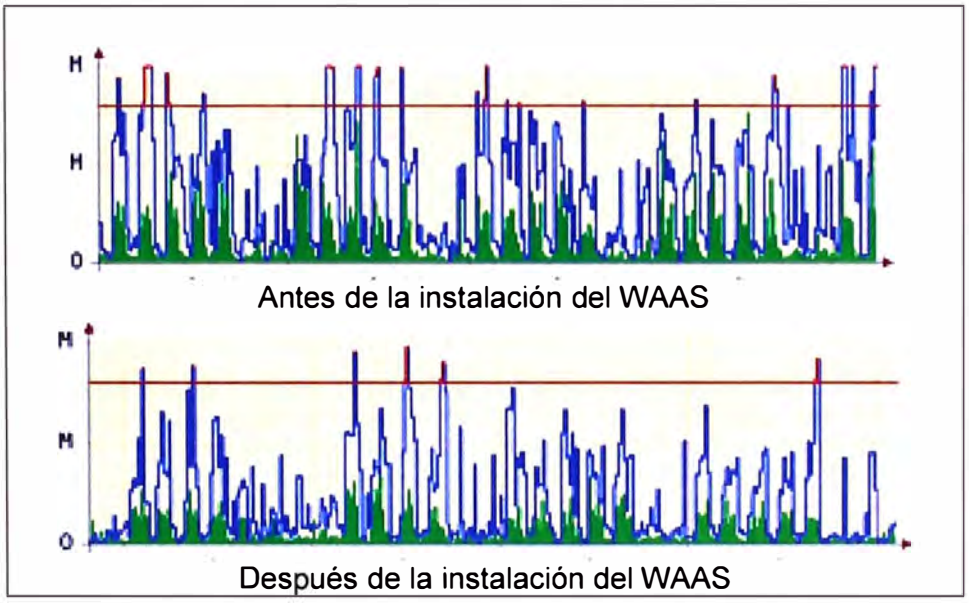

Figura 4.3 Gráficas de tráfico de la sede central (Fuente Proveedor)

La solución planteada con los appliances logra la optimización, teniendo en consideración que la compresión de datos básicamente se realiza sobre las aplicaciones mencionadas en la Figura 4.1. y según los protocolos también enunciados.

Para este análisis de compresión no se considera la variable del proceso de instalación, es decir, la instalación del cable UTP sea directo o cruzado ha sido correctamente instalado entre el router y el WAAS appliance.

La variable del proceso de fabricación de los appliance no se considera en estos resultados, por lo que se parte de la premisa que los dispositivos no cuentan con algún desperfecto de fabricación.

Tabla 4.1 Presupuesto

N°	Concepto	Cantidad	Costo Unitario (US$) sin IGV	Costo Total (US$) sin IGV
1	Estudios especiales (estimado)	1	100,000.00	100,000.00
2	Instalación para enlaces satelitales (pararrayos, etc.)	1	20,000.00	20,000.00
3	Costos de mantenimiento preventivo	1	3,000.00	3,000.00
4	Horas Hombre del Jefe de Proyecto	50	20.00	1,000.00
5	Costo Curso Capacitación - personal telefónica	1	10,000.00	10,000.00
6	Pago único - Líneas ADSL	1	1,000.00	1000.00
7	Pago mensual - Líneas ADSL	12	800.00	9,600.00
8	Instalación y Configuración de equipos WAAS (Sedes Operaciones)	1	30,000.00	30,000.00
9	Configuraciones de router durante el período de contrato	10	100.00	1,000.00
10	Inversión equipos solución de Sistema de compresión	29	6,896.55	200,000.00
11	Inversión equipos router	29	2,413.79	70,000.00
TOTAL (US$)				**445,600.00**

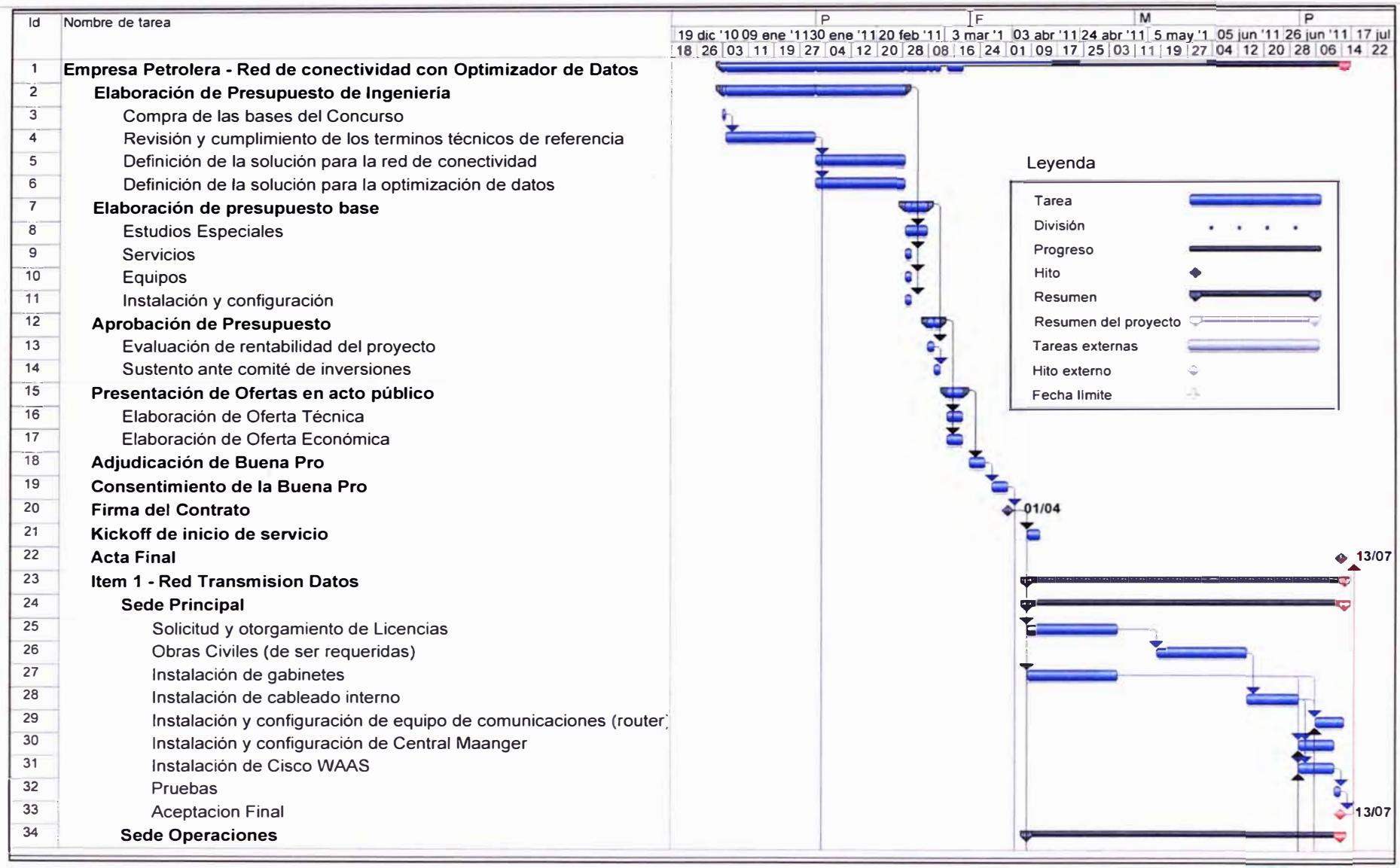

Figura 4.4 Diagrama de Gantt (página 1)

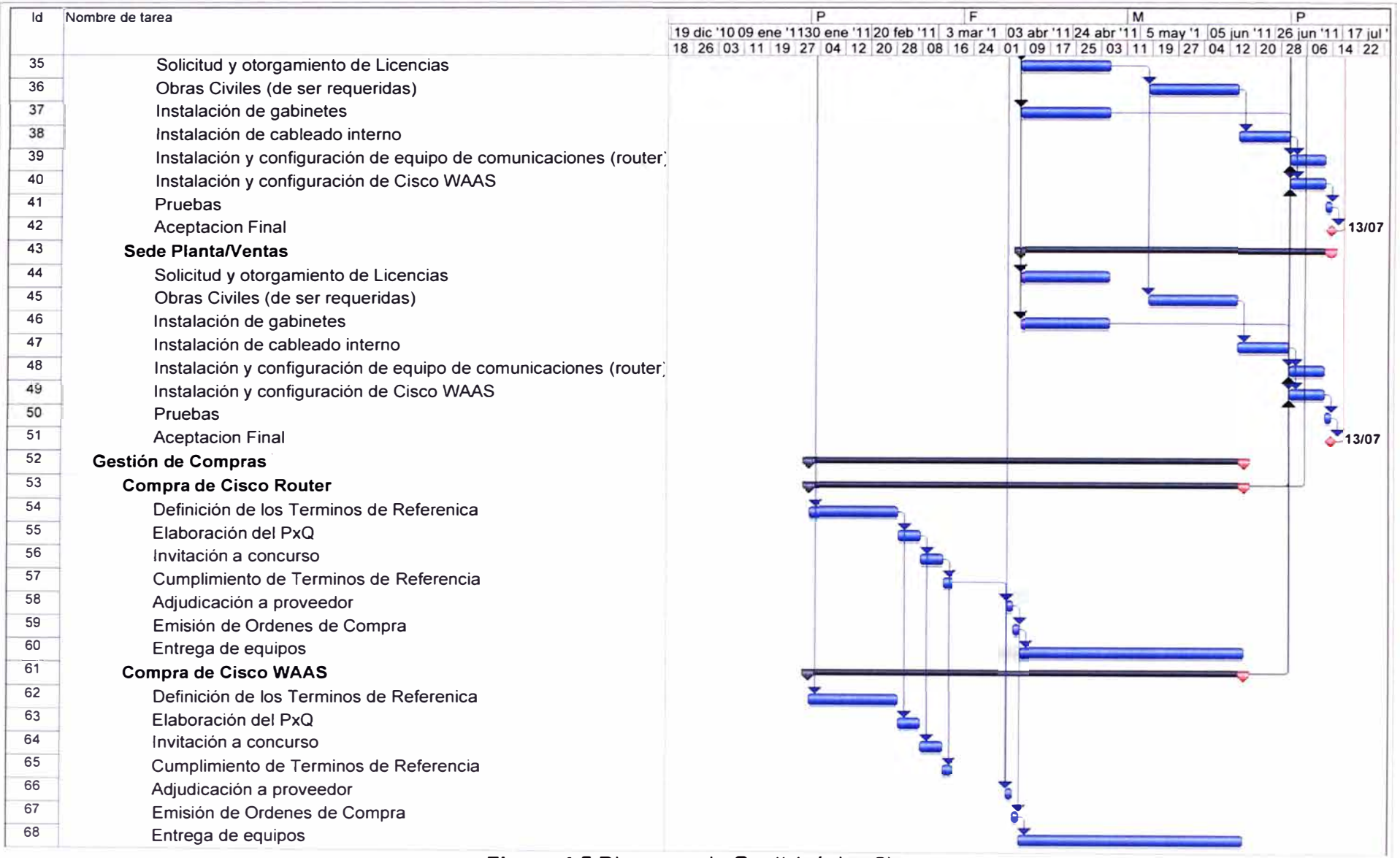

Figura 4.5 Diagrama de Gantt (página 2)

4.2 Presupuesto y tiempo de ejecución

En la Tabla 4.1 se muestra el presupuesto para la implantación respecto a la elaboración de la implementación de la solución de la red de conectividad con los dispositivos de optimización de datos.

4.3 Cronograma de trabajos

En la Figura 4.4 y 4.5 se muestra el diagrama de Gantt, donde se está considerando los tiempos desde la compra de las bases para el concurso hasta la implementación del proyecto en su totalidad (las fechas son referenciales).

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Para mejorar la transferencia de datos mediante el ancho de banda de los enlaces contratados a una empresa operadora, no siempre la solución es incrementar el ancho de banda ya que existen otras alternativas en las cuales un cliente puede mejorar la disponibilidad del ancho de banda que tiene contratado. Para esto se tiene que analizar las posibilidades y alternativas que ofrece el mercado sobre equipos y/o herramientas.

2. A la fecha de la elaboración de este informe de suficiencia, las alternativas de solución han aumentado con respecto a principios del año 2011, tiempo en el cual se inició la implantación del proyecto para una empresa petrolera.

3. Conocer el tipo de tráfico que se envía por la red WAN, el usuario que está generando el tipo de tráfico que mayor ancho de banda consume, y la frecuencia del mismo, ayuda a realizar una mejor toma de decisiones sobre las políticas internas que se puede tomar desde la oficina del Centro de Datos hacia toda la organización del cliente.

4. Si bien el proyecto en su totalidad abarcó también el diseño y la implementación de los enlaces a nivel WAN, tanto los enlaces principales como enlaces de respaldo o backup, se vio necesario limitar su alcance para este informe de suficiencia por su amplitud. Esto ayudó a conocer más los dispositivos compresores o aceleradores de datos en la WAN,

5. Si bien, el protocolo SNMP sirve para la gestión del tráfico, el cual es usado por la mayoría de las empresas operadoras, la solución de Cisco NetFlow es una herramienta que da mayores alcances sobre la utilización de la red WAN, siendo de fácil análisis y pudiendo ser administrado por el mismo cliente al interior de su Data Center (centro de datos).

6. El protocolo SNMP es utilizado para conocer si el ancho de banda está saturado, pero no puede saber si está siendo mal usado. NetFlow no remplaza al SNMP pero si ayuda de manera eficaz ofreciendo detalles que permiten determinar exactamente que está causando el problema de saturación en el ancho de banda, percibiéndose una lentitud en el servicio.

7. La solución del optimizador (compresor o acelerador) de datos, sumado con el

protocolo NetFlow, brinda una solución que conlleva a una mayor optimización de la WAN, no sólo por la compresión de los datos, sino por el análisis del tráfico y las políticas de uso que se habiliten a los diferentes usuarios de todas las sedes de la empresa petrolera.

8. En base a lo presentado en el capítulo 4, particularmente en la Figura 4.2. queda demostrado que esta solución de appliances como optimizadores o aceleradores de tráfico benefician a los usuarios que no están físicamente conectados en las oficinas principales de las empresas, logrando mejorar la eficiencia de sus gestiones propias del negocio, considerando que las grandes corporaciones siempre tienen ubicada en sus sedes principales su centro de datos (data center).

9. Esta mejora impacta en el desempeño de los usuarios finales y distantes a la oficina central, logrando mejorar su satisfacción internamente, impactando positivamente en el clima laboral y mejorando el trabajo en equipo.

10. Cabe señalar que la solución presentada en el presente informe fue calificada como ganadora en concurso público por la empresa petrolera, la cual se ha implantado, por lo cual en la Figura 4.2 se muestra fehacientemente la reducción del tráfico total, optimizándolo en una reducción del 45.27%.

11. El alcance del presente informe no considera la solución de los enlaces de transmisión de datos, se menciona que también para mejorar el nivel de disponibilidad, los enlaces principales en cada sede, se instalaron con su respectivo enlace de respaldo (backup), lo cual se describió en el capítulo I.

12. El presente informe, para los casos de problemas de disponibilidad o lentitud en los servicios de transmisión de datos a nivel WAN, confirma que se puede buscar varias alternativas de solución antes de pensar solamente en ampliar el ancho de banda, pudiendo realizar una gestión y administración del ancho de banda, una optimización bajo compresión de datos, priorización de tráfico, incluyendo políticas de seguridad con restricciones, analizando su tráfico llegando a conocer los distintos tipos de tráficos que transmite cada usuario.

Recomendaciones

1. Se recomienda que para la conexión entre el router y el Cisco WAAS se realice una buena verificación de negociación entre ambos equipos, utilizando cables directos.

2. Se recomienda que entre los equipos WAAS y el switch de la red LAN del cliente no se instale otro dispositivo, toda vez que puede fallar la negociación de los mismos, ocasionando que la optimización de los datos no sea la más óptima.

3. Se recomienda que una vez lograda la optimización de datos en las sedes, se realice

un seguimiento semanalmente para garantizar que la negociación entre los equipos Ciscos continúen.

4. Se recomienda que esta solución no se aplique a enlaces de transmisión de datos que utilicen tecnología satelital. Es conocido que para la transmisión de información, los satélites utilizan un método de compresión, por lo que al conectarse el Cisco WAAS, como appliance, este no logra su objetivo de optimización.

5. Se presento dificultades al momento de la extracción de datos bajo el protocolo NetFlow para el análisis de tráfico, considerando que el análisis del mismo no forma parte de la propuesta del sistema de conectividad corporativa para la empresa petrolera, siendo una tercera empresa la encargada de este trabajo. Se recomendó al cliente que para futuros casos debe ser el mismo proveedor quien configure el protocolo NetFlow y extraiga la información para la presentación del análisis de tráfico.

ANEXO A
GLOSARIO DE TÉRMINOS

ANEXO A GLOSARIO DE TÉRMINOS

ADSL	Línea de abonado digital asimétrica (Asymmetric Digital Subscriber Line).
ACL	Access control list (lista ed controla de acceso)
BGP	Border Gateway Protocol
BIC TCP	Incremento de la congestión binaria TCP (Binary Increase Congestion)
CE	Customer Edge
CIFS	Sistema común de archivos de internet caché (Common Internet File
CLI	Interfaz de línea de comandos (Command Line Interface)
CO	Central Office (Oficina central)
CoS	Clase de Servicio (Class of Service)
CPE	Customer Premises Equipment (Equipo terminal en local de cliente)
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
DRE	Eliminación de datos redundantes (Data Redundancy Elimination).
EFM	Ethernet in the First Mile.
FIFO	Primero en entrar, primero en salir (First In, First Out)
HTTP	Protocolo de transferencia de hipertextos (Hypertex Transfer Protocol)
IPSec	Seguridad IP
ISP	Proveedor de servicios de Internet
LAN	Red de Área Local
LSP	Label-Switched Path
LZ	Compresión Persistente LZ (Lempel Ziv)
MAN	Red de Área Metropolitana
MAPI	Interfaz de programación de aplicaciones de mensajería (Messaging Application Programming Interface)
MPLS	Multi-Protocol Label Switching
NFS	Aceleración del Sistema de Archivos en La Red (Accelerates Network File System)
NetFlow	Protocolo propietario de Cisco
PBR	Policy-Based Routing
PE	Provider Edge
PHP	Penultimate Hop Pop
PPP	Point to point Protocol
QoS	Calidad de servicio.
RD	Route Distinguisher

RTSP	Protocolo de streaming en tiempo real (Real Time Streaming Protocol)
RT	Router Target
RTT	Transferencia de datos a un solo tiempo de ida y vuelta (Roundtrip Time).
SACK	Confirmación selectiva (Selective Acknowledgment)
SLA	Service Level Agreement
SMB	Bloqueo de mensajes de servidor (Server Menssage Block)
SMTP	Protocolo simple de transferencia de correo (Simple Mail Transfer Protocol)
SNMP	Protocolo Simple de Administración de Red (Simple Network Management Protocol)
SSL	Capa de socket seguro (Secure Socket Layer)
TCP	Protocolo para el control de la transmisión (Transmission Control Protocol)
TDM	(Time-division multiplexing (Multiplexación por División de Tiempo)
TFO	TCP flow optimization
TI	Tecnología de Información
TLS	Seguridad en la capa de transporte (Transport Layer Security,)
UDP	Protocolo de datagrama de usuarios (User Datagram Protocol)
VPN	Red Privada Virtual.
VRF	Virtual Routing and Forwarding
VSAT	Very Small Aperture Terminal
WAAS	Wide Area Application Services
WAEs	Motores de Aplicaciones de Área Amplia (Wide Area Application Engines)
WAN	Red de Área Amplia
WCCP	Protocolo de Comunicación de Almacenamiento Web (Web Cache Communication Protocol)

BIBLIOGRAFÍA

[1] Gert DeLaet, Gert Schauwers, "Fundamentos de Seguridad de Redes", Cisco Press, 2004.

[2] Ernesto Ariganello, Enrique Barrientos, "Redes Cisco CCNP a Fondo. Guía de Estudios para Profesionales", Editoral RA-MA, 2010.

[3] Ina Minei, Julian Lucek, "MPLS-Enabled Applications" John Wiley & Sons Inc, 2005.

[4] Mark Lewis, "Comparing, Designing, and Deploying VPNs", Cisco Press, 2006.

[5] Alex Shneyderman and Alessio Casati, "Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems", John Wiley & Sons Inc, 2003.

[6] Cisco, "Cisco Wide Area Application Services - Configuration Guide", Cisco Systems, 2011

[7] Zach Seils, Joel Christner, "Deploying Cisco Wide Area Application Services", Cisco Press., 2006

[8] Cisco "Cisco Wide Area Application Services (WAAS) Appliances", http://www.cisco.com/en/US/products/ps6474/index.html

[9] Cisco "Cisco Wide Area Application Engine Express" Datasheet, http://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps11211/datasheet_c78-611644.pdf

[10] Cisco, "Cisco Virtual Wide Area Application Services (vWAAS)", http://www.cisco.com/en/US/products/ps11231/index.html

[11] Dpto. de Ciencia y Tecnología U.N.Quilmes "Comunicación de datos"

[12] J. Ziv and A. Lempel, "A Universal Algorithm for Sequential Data Compression" IEEE Trans. on Information Theory.

[13] A. Wyner and J. Ziv, "The sliding window Lempel-Zi algorithm is asymptotically optimal" Proc. IEEE.

[14] Cisco, "Introduction Cisco IOS NetFlow – A Technical Overview" http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps6601/prod_white_paper0900aecd80406232.html

[15] Cisco, "NetFlow Services Solutions Guide – Cisco Systems" http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/products_implementation_design_guide09186a00800d6a11.html

[16] NetFlow Analyzer http://www.manageengine.com/products/netflow/spanish/index.html