UNIVERSIDAD CATÓLICA ANDRÉS BELLO

VICERRECTORADO ACADÉMICO

DIRECCIÓN GENERAL DE LOS ESTUDIOS DE POSTGRADO

ESPECIALIZACIÓN EN INGENIERÍA DE TELECOMUNICACIONES

ANÁLISIS DE LA HERRAMIENTA NETFLOW COMO INSTRUMENTO PARA EL MANTENIMIENTO Y MEJORA DE LOS NIVELES DE CALIDAD DE SERVICIO DE LAS REDES CORPORATIVAS.

TRABAJO ESPECIAL DE GRADO PARA OBTENER EL GRADO DE ESPECIALISTA EN INGENIERÍA DE TELECOMUNICACIONES

Presentado por:

Ing. Alejandro José Iglesias Suárez

CI: V – 17.077.227

Asesor:

Ing. Berardo Di Attanasio

CI: V – 5.418.846

Caracas, Julio de 2014

DEDICATORIA

Este Trabajo de Grado está dedicado a todos aquellos que durante la realización del mismo hicieron posible su culminación.

En primer lugar a mis padres, por estar pendientes del avance del mismo así como de los hitos relacionados con él.

En segundo lugar, al profesor Berardo Di Attanasio, por aportarme valiosa documentación, sobre todo en lo relacionado con metodologías y procedimientos de investigación; así como por la ayuda para diseñar el documento final.

Finalmente, pero no menos importante, al señor Luis Ramírez por toda la valiosa ayuda que me aportó, sobre todo al permitirme utilizar el equipamiento de su academia de redes para la realización de los laboratorios requeridos por este Trabajo de Grado; así como sobre todo por el apoyo brindado durante sus distintas etapas de desarrollo, y por las ideas aportadas tanto al mismo como a futuros proyectos conjuntos.

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

LISTA DE TABLAS

DESARROLLO DE LOS RESULTADOS DEL SISTEMA NETFLOW COMO HERRAMIENTA PARA EL MANTENIMIENTO Y MEJORA DE LOS NIVELES DE CALIDAD DE SERVICIO DE LAS REDES CORPORATIVAS

AUTOR: ALEJANDRO IGLESIAS

ASESOR: BERARDO DI ATTANASIO

FECHA: JULIO 2014

RESUMEN

Las empresas poseen una serie de recursos informáticos (servidores, estaciones de trabajo, etc.), así como una serie de servicios (telefonía IP, sistemas de seguridad y de vigilancia electrónica, sistemas de impresión, sistemas de almacenamiento, etc.), que deben estar disponibles en todo momento para que sus empleados puedan utilizar los recursos que ofrecidos por la red.

Muchas empresas, que poseen más de una sucursal que deben interconectar, deben alquilar los enlaces necesarios para este fin a un ISP. Adicionalmente, muchas empresas ofrecen a sus empleados los servicios del trabajo a distancia. Estos enlaces son críticos para las empresas. Debido a esto es totalmente necesario que sean monitoreados continuamente por el personal de tecnología para conocer su comportamiento y detectar posibles problemas mediante el uso de herramientas de monitoreo y gestión adecuadas a cada una de ellas.

Se propone para este fin la utilización de la herramienta Netflow, la cual se basa en la agrupación de los paquetes entrantes o salientes a las interfaces de los dispositivos de red en grupos basados en características similares o comunes, tales como por ejemplo direcciones IP origen y destino, interfaces origen y destino, protocolos de capa de transporte, de red o de enlace de datos utilizados, etc.

Esta herramienta está instalada por defecto en todos los dispositivos CISCO de gama empresarial. Cuando se desee utilizar esta herramienta, lo único que debe ser realizado es habilitarla y configurarla de acuerdo a los parámetros deseados.

Para la consecución de los objetivos del proyecto se debe realizar una profunda investigación técnica sobre el funcionamiento y los valores arrojados por la herramienta en estudio. Se debe así mismo realizar una prueba piloto en las condiciones que más se ajusten a las redes corporativas, en la cual se pueda poner en práctica lo obtenido en la investigación teórica. Por todo ello el proyecto se propone como una investigación documental, exploratoria, factible, de simulación y de campo.

En el Capítulo IV se presenta la implementación de la topología de prueba en la cual se configuró la herramienta en análisis en el Trabajo de Grado; cuyos resultados se presentan en el Capítulo V. En base a esos resultados fueron determinadas una serie de aspectos que, divididos en dos grupos, conforman las conclusiones que se pueden extraer del trabajo realizado.

Palabras clave: *Netflow, monitoreo de redes, estudios de tráfico, seguridad en redes, calidad de servicio, redes corporativas, gestión de redes, herramientas de gestión.*

GLOSARIO DE TÉRMINOS

- ASN: *Abstract Syntax Notation,* Notación Abstracta de Sintaxis
- CIR: *Committed Information Rate*, Velocidad de Información Suscrita.
- CPU: Central Process Unit, Unidad de Procesamiento Central.
- IETF: Internet Engineering Task Force, Grupo de Trabajo de Ingeniería de Internet.
- IOS: Interworking Operating System, Sistema Operativo de Interconexión.
- IP: Internet Protocol, Protocolo de Internet.
- ISP: Internet Service Provider, Proveedor de Servicios de Internet.
- LAN: Local Area Network, Red de Área Local.
- MAC: Media Access Control, Control de Acceso al Medio.
- MIB: Management Information Base, Base de Datos de Información de Gestión.
- NMS: Network Management System, Sistema de Gestión de Redes.
- OID: Object Identifier, Identificador de Objeto.
- OSI: Open System Interconnection, Interconexión Abierta de Sistemas.
- PDU: Packet Data Unit, Paquete de Unidad de Datos
- PIR: *Peak Information Rate,* Velocidad de Información en Exceo.
- RFC: Request for Comments, Solicitud de Comentarios.
- Rmon: Remote Monitoring, Monitoreo Remoto.

- SNMP: Simplified Network Management Protocol, Protocolo Simplificado de Gestión de Redes-
- TCP: Transport Control Protocol, Protocolo de Control de Transporte.
- UDP: User Datagram Protocol, Protocolo de Datagrama de Usuario.
- BER: Bit Error Rate, Promedio de Errores de Bit.
- WAN: Wide Area Network, Red de Área Amplia.
- WLAN: Wireless Local Area Network, Red Inalámbrica de Área Local.

DEFINICIONES

Agente: es un software que, instalado en un dispositivo, es capaz de entregarle información sobre su funcionamiento a una entidad de monitoreo.

Backbone: es el núcleo de una red. Posee enlaces troncales que interconectan a diferentes enrutadores entre sí mediante el uso de enlaces de muy alta velocidad, normalmente de fibra óptica.

Catalyst: serie de conmutadores de red de capa de enlace de datos, fabricados por la empresa CISCO, que permite el intercambio de información entre distintos dispositivos de red.

Comunidad: clave utilizada en el protocolo SNMP para autenticar los permisos que una entidad tiene sobre los distintos dispositivos que forman una red de datos. Existen dos comunidades: pública y privada.

Desencapsular: consiste en eliminar los encabezados y colas de control presentes en una PDU.

Encapsular: consiste en añadir encabezados y colas con información de control a una PDU.

Ethernet: protocolo de capa de enlace de datos que define las características físicas y eléctricas de las interfaces de red de un dispositivo. Define también la velocidad de las interfaces mediante diferentes estándares. Los más comunes actualmente son *Fast Ethernet* y *Gigabit Ethernet*.

Gateway: dispositivo de red que permite la comunicación entre dos tipos diferentes de redes. Un *Gateway* muy común son los enrutadores de datos.

Modelo OSI: es un modelo de referencia surgido con el fin de estandarizar las transmisiones entre dispositivos de datos (mediante la división de los dispositivos de red en capas con funciones específicas) en la década de 1980. Aunque no se utiliza con fines de implementación, todos los desarrollos en el área de redes de datos se basan en sus definiciones.

Monitoreo de red: acción mediante la cual se vigila el comportamiento de los parámetros asociados a una red de datos y se toman las acciones correctivas que se necesiten.

MYSQL: es una base de datos que se utiliza en muchas aplicaciones diferentes tales como sistemas web. Permite obtener información muy rápidamente.

NMS: es un sistema de gestión de redes que ejecuta un protocolo de monitoreo de redes para obtener parámetros que le permitan conocer cuál es su estado y uso.

No orientado a la conexión: modo de funcionamiento de los protocolos de capa de enlace de datos mediante el cual no se establece una ruta antes de transmitir información a través de una red de datos o de voz. Un protocolo muy común que funciona de esta manera es UDP.

Orientado a la conexión: modo de funcionamiento de los protocolos de capa de enlace de datos mediante el cual se establece una ruta antes de iniciar la transferencia de información a través de una red de datos o de voz. Un protocolo muy común que funciona de esta manera es TCP.

PDU: nombre con el que se conoce a una estructura de información a ser introducida a las capas del Modelo OSI. Es un nombre genérico que se aplica a cualquiera de sus capas antes de especificar el protocolo que se utiliza.

Planificación de red: conjunto de acciones mediante las cuales se asignan los recursos de las redes en función de las aplicaciones y servicios que se prestarán con ellas.

Pool: espacio de memoria en el cual se almacena una serie valores pertenecientes a la misma variable lógica. Por ejemplo, pool de direcciones MAC, pool de flujos, etc.

Tráfico: cantidad de datos, organizados en bits, flujos u octetos, que viajan a través de una red en un período determinado de tiempo.

Trap: mensaje enviado por un agente SNMP a su NMS para indicarle el cambio en el estado de alguna de las variables que éste monitorea.

Vulnerabilidad: condición que hace que una red sea propensa a sufrir un tipo de ataque determinado, por ejemplo, el acceso no autorizado, la suplantación de identidad, la sustracción de archivos, etc.

INTRODUCCIÓN

En el presente documento se propone el trabajo titulado "Desarrollo de los resultados del sistema Netflow como herramienta para el mantenimiento y mejora de los niveles de calidad de servicio de las redes corporativas".

El proyecto se enmarca en el área del monitoreo de redes, la cual es muy importante para cualquier empresa (tanto pequeñas y medianas empresas que suelen alquilar enlaces para construir sus redes, así como grandes empresas que poseen sus propios enlaces y muchas son proveedores de servicios para otras empresas de menor tamaño).

Todas las empresas necesitan conocer el estado exacto de sus recursos de red para asegurar el buen funcionamiento de las mismas, y para asegurar que ellas se mantengan operativas la mayor cantidad de tiempo posible. Dentro de este concepto se desarrolla el presente documento: se propone el desarrollo de los resultados arrojados por una herramienta de gestión que permita a los administradores de red de las empresas realizar reportes que entreguen información sobre el uso de las redes así como el tráfico que se cursa en los enlaces que son críticos para el funcionamiento de las empresas y para el mantenimiento y mejora de sus modelos de negocios. Mediante esta herramienta, el administrador de red podrá realizar sus reportes basándose en quién observará la información contenida en ellos.

Este documento está estructurado en tres capítulos, cada uno de los cuales se encuentra dividido en secciones que pretenden desarrollar el tema propuesto en el capítulo.

En el primer capítulo se realiza el *"Planteamiento del Problema"*, en el cual se presenta la situación que llevó al autor de estas líneas a plantear la realización de este trabajo. Posee las siguientes secciones:

- Planteamiento del problema: se presentan una serie de herramientas de monitoreo en la forma de antecedentes al uso de NETFLOW. Adicionalmente se explica por qué es necesario el uso de una herramienta

diferente de las existentes en el mercado para las redes de las empresas pequeñas y medianas.

- Objetivos: se presenta el objetivo general de este documento, así como los objetivos específicos del mismo.
- Interrogantes: se presenta una serie de preguntas que inducen al desarrollo de este proyecto.
- Justificación: se intenta justificar la necesidad de desarrollar esta herramienta sobre otras existentes en el mercado para realizar el monitoreo de las redes de las empresas.
- Alcances y limitaciones: se presentan las actividades que serán realizadas y las que no, así como el marco externo en el cual será desarrollado este proyecto.

En el segundo capítulo se desarrolla el marco teórico de este documento. Se explican brevemente algunos tópicos sobre el protocolo SNMP, así como sobre algunas herramientas que sirven como antecedentes al NETFLOW de CISCO. Se explica más en detalle el funcionamiento de esta herramienta. Este capítulo posee las siguientes secciones:

- Antecedentes: se presentan varias herramientas usadas en el monitoreo de redes LAN, así como las principales características de cada una de ellas.
- Teoría de referencia: se desarrollan aspectos teóricos sobre los protocolos SNMP y NETFLOW. Se explican algunos aspectos y términos sobre el SNMP, mientras que el NETFLOW es desarrollado más extensivamente. Se presentan aspectos relacionados con la calidad de servicio, el mantenimiento y la seguridad de redes.
- Topología: se propone una topología de prueba para cumplir con los objetivos que serán planteados en el documento.

En el tercer capítulo se explica la metodología a seguir en este Trabajo de Grado, haciendo especial énfasis en los tipos de investigación en los que este

proyecto se enmarca. Se presenta también el esquema de actividades a seguir durante la ejecución de este trabajo. Posee las siguientes secciones:

- Tipo de investigación: se mencionan varios tipos de investigación que, de acuerdo al juicio de quien escribe estas líneas, y en concordancia con los autores investigados, se ajustan a la propuesta que se realiza en este documento.
- Metodología: se presentan las actividades que serán realizadas para lograr la consecución de los objetivos específicos planteados en el capítulo I. Se explica el porqué de cada una de esas actividades y se presenta en forma de gráfico una línea de tiempo en la cual se aprecian las actividades mencionadas.

Capítulo I PLANTEAMIENTO DEL PROBLEMA

El capítulo I presenta la actividad que se propone en el documento. Se divide en cinco secciones. La primera sección plantea la problemática a trabajar en el tiempo que se planteará. La segunda plantea una serie de interrogantes que conducirán a la elección de una solución a los problemas mencionados en la segunda parte del capítulo. La tercera sección introduce el objetivo general y los objetivos específicos de la investigación. La cuarta parte desarrolla una breve justificación sobre la problemática que se presenta en la sección número dos y propone una posible solución a ella. Por último, la sección 5 del capítulo menciona una serie de limitaciones que tendrá el desarrollo del trabajo.

I.1. Planteamiento del problema

Todas las empresas que utilizan los servicios informáticos como su base de negocios, pequeñas, medianas y grandes, necesitan utilizar redes para proveer aplicaciones (servidores de archivos, gestión de recursos humanos, etc.) y servicios (servidores de impresión, acceso remoto a recursos, etc.) a sus empleados.

Normalmente las empresas dividen sus redes en dos grandes niveles: la red LAN que provee los servicios a los empleados que se encuentran en su(s) sede(s), y la red WAN que les permite a los empleados acceder desde el exterior a los recursos informáticos de la empresa, así como compartir los recursos de distintas sedes.

Las grandes empresas poseen redes WAN propias que utilizan para interconectar las distintas sedes que poseen en una o en varias ciudades. Pero las pequeñas y medianas empresas suelen alquilar el acceso a un enlace de alguna tecnología de transporte a algún proveedor de servicios.

Todas las empresas, sin importar su tamaño y alcance geográfico y económico, necesitan saber cuál es el estado exacto de sus redes en cualquier momento ya que ellas son una parte crítica de su negocio y permiten que éste se mantenga en el tiempo y pueda crecer. Las redes son una parte fundamental del negocio de todas ellas; son una parte crítica de su estructura y como tal, los

dirigentes de las organizaciones necesitan controlar todos los aspectos de su operación.

Para poder cumplir con esta premisa, tanto los enlaces que forman las redes LAN como aquellos que forman las redes WAN de las empresas deben ser monitoreados continuamente por personal capacitado, propio de la empresa.

Muchas veces, cuando los enlaces de las empresas son alquilados a grandes proveedores de servicios, su estado y utilización son monitoreados por el propio ISP, siempre con el objetivo de realizar la facturación correspondiente. Sin embargo, las empresas necesitan conocer más parámetros sobre sus enlaces y redes tales como el porcentaje de uso, los errores que se han producido, el tipo de tráfico que se ha cursado, estadísticas sobre el tráfico, etc.

Las grandes empresas e ISP poseen herramientas muy poderosas, propietarias y costosas que les permiten obtener esta información. Sin embargo no existen aplicaciones en el contexto de las pequeñas y medianas empresas que ofrezcan este tipo de información.

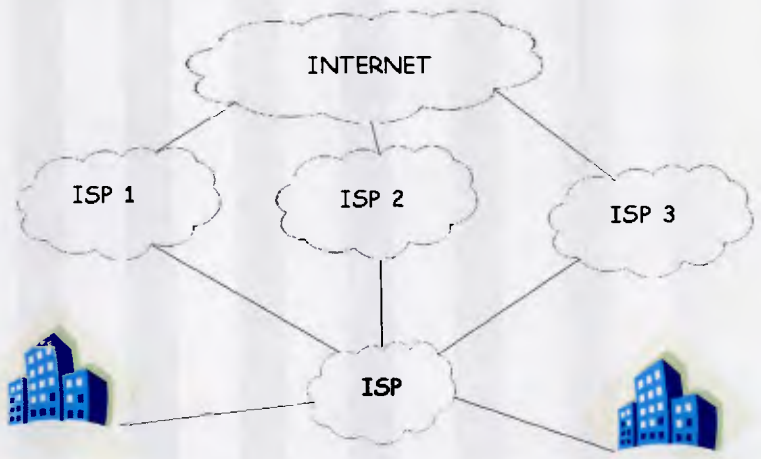

Figura 1. Internet Servicie Provider. Fuente: propia.

La Figura I-1 muestra el esquema general que siguen la mayoría de las empresas para interconectar sus sedes y para acceder a Internet. Para esto suelen contratar a un Proveedor de Servicios de Internet, el cual puede a su vez utilizar a

otros proveedores de servicio para conectarse a esta red. En el ejemplo de la Figura 1 se observa a tres ISP para acceder a Internet. Existe una estructura jerárquica, como se observa en la Figura, que garantiza la interconexión de los diferentes ISP al backbone de Internet. Sólo los proveedores que se encuentran más arriba en esa jerarquía poseen acceso a él. La posición de un ISP con respecto al backbone de Internet la define la velocidad de los enlaces que poseen. Mientras mayor sea la velocidad de estos enlaces, más directo será el acceso al núcleo de Internet.

Se extrae de lo anterior que la finalidad del trabajo es el desarrollo de una herramienta que les permita a los administradores de red de las empresas conocer el estatus de las redes internas y de los enlaces con los cuales acceden a las redes de sus proveedores de servicios de una forma práctica y sencilla.

El desarrollo se hará utilizando la herramienta NETFLOW, creada por la empresa CISCO SYSTEMS, que está instalada (pero no habilitada) por defecto en todos sus enrutadores y conmutadores con una versión de sistema operativo superior a IOS 12.2.

Con la herramienta se permite a los administradores obtener información de monitoreo sobre los datos que están siendo transmitidos directamente a través de las interfaces de los dispositivos de red, es decir, se provee a los administradores de las redes información directa sobre los datos antes de entrar a las redes de los proveedores de servicios.

I.2. Interrogantes

De acuerdo a lo mencionado anteriormente se presenta una serie de interrogantes que permiten inducir la respuesta de por qué será elegida la herramienta NETFLOW.

- Para qué será usada la red, y cómo serán usados sus recursos.
- Qué parámetros de la red deben ser monitoreados y especialmente cuidados.
- Cómo será realizada la administración, gestión y mantenimiento de la red.
- Qué partes de la red se deben monitorear.

- Qué políticas de calidad de servicio serán aplicadas a la red.
- Qué tipo de mantenimiento se debe aplicar a este tipo de redes.
- Es posible utilizar los resultados arrojados por la herramienta de monitoreo para ser presentados y ajustados bajo los requerimientos de la dirección de las empresas.
- A quién, dentro de la estructura organizativa de la empresa, serán enviados los reportes que se generen a partir de la información obtenida mediante el monitoreo de las redes corporativas.

NETFLOW permite, debido al tipo de información que entrega, generar reportes personalizados en los cuales se encuentre la información deseada por los administradores. Esta funcionalidad es la que se desea desarrollar en este Trabajo Especial de Grado. Basándose en estas preguntas, se eligió utilizar el ya mencionado NETFLOW. En la sección I.4 será explicada la razón de esta elección. En la siguiente sección se presenta el objetivo general de este trabajo, así como los objetivos específicos que permitirán cumplir con el objetivo general.

I.3. Objetivos

I.3.1. Objetivo general

Analizar la herramienta Cisco Netflow como instrumento para el mantenimiento y mejora de las políticas Calidad de Servicio asignadas por las políticas de las empresas para sus redes corporativas.

I.3.2. Objetivos específicos

1. Realizar un estudio sobre el funcionamiento del *software* CISCO NETFLOW para obtener una lista de aquellas variables de tráfico y calidad de servicio que el software es capaz de entregar.
2. Habilitar el *software* CISCO NETFLOW en un enrutador y en un conmutador para configurarlo con las características que esta herramienta es capaz de entregar.

3. Configurar el *software* CISCO NETFLOW para que sea capaz de enviar las variables configuradas previamente hacia un servidor o una estación de trabajo, para su posterior procesamiento y utilización.
4. Diseñar e implementar una topología de red de prueba en la cual se pueda poner en funcionamiento la herramienta NETFLOW de acuerdo a las configuraciones realizadas en la ejecución del tercer objetivo específico.
5. Analizar los resultados obtenidos de las pruebas realizadas para utilizarlos en el mantenimiento y mejora de la calidad de servicio asignados a la red corporativa.

I.4. Justificación

Muchas empresas crean redes LAN en sus sedes corporativas, y tienen un control absoluto sobre ellas y sobre su comportamiento. Cuando esas empresas tienen servicios tales como el acceso a Internet, ofrecer acceso remoto a los empleados que no se encuentre en algunas de las sedes de la empresa, o para compartir información y recursos entre las distintas sedes, suelen alquilar un enlace de acceso a algún proveedor de servicios (tal como CANTV, MOVISTAR, TELEFÓNICA, LEVEL 3, FRANCE TELECOM, etc.), sobre el cual no tienen control alguno debido a que no es propiedad de ellas.

Existen muchas aplicaciones comerciales, algunas gratuitas y algunas licenciadas, que permiten obtener estadísticas sobre el comportamiento y sobre el tráfico cursado en las redes LAN de las empresas.

Existen también muchas aplicaciones, propietarias, muy costosas y diseñadas a la medida de las redes que poseen los proveedores de servicios, que permiten monitorear el comportamiento de sus redes. Estas aplicaciones se diseñan en función de la tecnología presente en los distintos niveles de estas redes, y se integran dentro de ellas, muchas veces en la forma de una propia red de monitoreo.

Sin embargo, no existe comercialmente hablando, una aplicación que realice esta función en las redes de las distintas organizaciones pequeñas y medias.

Las organizaciones podrán realizar las siguientes actividades con la herramienta que será propuesta:

- Medir el tráfico saliente de sus redes hacia las redes los ISP para comprobar que la facturación que ellos (los ISP) les entrega se corresponde con la realidad del uso que hicieron del enlace contratado.
- Monitorear el tráfico que cursan las redes de las empresas a través de todos sus elementos de red para poder comprobar cuál es el estado de la red en un momento determinado, para de esta forma poder aplicar políticas de calidad de servicio que le entreguen a sus usuarios una mejor experiencia de red y se puedan mantener los procesos críticos de la empresa en funcionamiento.
- Ejecutar una aplicación desde cualquier ambiente informático, sin importar cuál es el sistema operativo que se ejecuta en las estaciones de trabajo y en los servidores de monitoreo de las empresas.

El CISCO NETFLOW es una herramienta, desarrollada por CISCO SYSTEMS, que puede ser ejecutada en cualquier ambiente que opere con dispositivos de red de este fabricante, y sus datos pueden ser consultados desde cualquier dispositivo CISCO.

Las actividades que pueden ser realizadas con el CISCO NETFLOW se listan a continuación:

- Acceder fácilmente a la herramienta de monitoreo y gestión (NETFLOW) desde cualquier estación de trabajo o servidor.
- Obtener parámetros de tráfico y calidad de servicio específicos de la red que realmente permitan resolver problemas.
- Comprobar los costos que los ISP les reflejan en las facturas.
- Administrar, gestionar y actualizar las redes con una política de calidad de servicio que le otorgue a sus usuarios una muy buena sensación al utilizar la red y que mantenga a todos procesos de las empresas operativos.

- Realizar análisis en tiempo real sobre el comportamiento de la red.
- Realizar análisis sobre el comportamiento pasado de la red.
- Realizar reportes con aquellos datos que son de interés en un momento determinado.

I.5. Alcances y limitaciones

Se define la profundidad con la que se desarrollará el proyecto que se plantea en este documento de propuesta. Se establece cuál será el alcance de este trabajo mencionando claramente cuáles serán los productos que serán entregados como parte del desarrollo final del mismo.

Se establecen también una serie de limitaciones que definen básicamente el entorno bajo el cual se desarrollará la herramienta propuesta así como también los ámbitos de aplicación de la misma. Se menciona también el mercado target del desarrollo que se plantea. Adicionalmente se mencionan aquellos desarrollos que no formarán parte de la herramienta y se justifica el porqué de esta decisión.

I.5.1. Alcance

Se pretende analizar el uso que se hace de las redes corporativas mediante la ejecución de la herramienta Netflow mediante su instalación en los dispositivos de red adecuados de las redes de las empresas para proponerla como la herramienta que permitirá realizar el monitoreo de las redes para la mejora de la calidad del servicio que éstas le ofrecen a sus empleados y para incrementar los beneficios que las redes de las organizaciones tendrán sobre su modelo de negocios.

Para realizar el análisis mencionado es necesario realizar la configuración de los dispositivos de red en los cuales será habilitada la herramienta NETFLOW. La configuración incluye tanto la configuración de red del dispositivo como la de la herramienta en cuestión.

Se realizará la configuración de red necesaria para asegurar que la herramienta sólo pueda ser configurada y consultada por personal autorizado

mediante el aprovechamiento de las herramientas de seguridad ofrecidas por el software ejecutado por los enrutadores y conmutadores del fabricante CISCO.

Se incluirá el desarrollo de una topología de prueba, en la cual se pretende probar la configuración de la herramienta CISCO NETFLOW, así como la configuración de todos los aspectos necesarios para que puedan ser obtenidas y observadas las variables que entregue la herramienta mencionada, en la cual se incluye:

- Configuración de los dispositivos de red del fabricante CISCO.
- Configuración de una red de monitoreo para asegurar que sólo los hosts y usuarios autorizados puedan tener acceso a los resultados arrojados por la herramienta NETFLOW.
- Configuración de la herramienta CISCO NETFLOW en los enrutadores de ese fabricante.
- Ordenación de los parámetros entregados por la herramienta CISCO NETFLOW de acuerdo a diferentes criterios tales como direcciones origen y destino, interfaces origen y destino, ancho de banda consumido, protocolo, aplicaciones, etc.

Los resultados anteriores serán analizados para determinar el comportamiento del tráfico cursado a través de las redes, así como para determinar posibles inconvenientes que pudieran estar presentándose en la red.

I.5.2. Limitaciones

Durante la ejecución del Trabajo Especial de Grado no serán incluidas una serie de actividades debido a diversas razones que se explican a continuación.

- No se incluirán en el análisis final aquellas variables que no son entregadas por el NETFLOW debido a que su inclusión implicaría el rediseño de la herramienta, lo cual supone el permiso por escrito del fabricante (CISCO SYSTEMS) ya que ésta es una herramienta que posee una licencia

propietaria. Se implicaría también el pago de una licencia al fabricante por el derecho de modificar su desarrollo.

- No será desarrollada ninguna aplicación externa que permita obtener la data generada en el enrutador o enrutadores donde se ejecute el NETFLOW debido a que esta acción implicaría un nivel de desarrollo que escapa del alcance del trabajo de grado así como del ámbito de las telecomunicaciones.

Existe otro tipo de limitaciones, que no son técnicas, sino más bien limitaciones temporales, económicas y geográficas.

I.5.2.1 Limitaciones temporales

Las limitaciones temporales existen debido a que el proyecto que se propone en este documento no puede ser desarrollado en un tiempo ilimitado, tiene un período de tiempo en el cual puede ser realizado.

Como se mencionará en el capítulo III, Marco Metodológico, el proyecto tiene un tiempo estimado de realización de quince semanas. En ese capítulo será mencionado cómo se distribuirá el tiempo entre las diversas actividades que es necesario realizar.

I.5.2.2 Limitaciones económicas

El producto final de este trabajo tendrá una limitación económica, debido a que la herramienta que se propone utilizar puede ser utilizada libremente en cualquier dispositivo CISCO que ejecute un *software* posterior al IOS 12.2, ésta no puede ser modificada sin un permiso escrito de esta compañía, ni sin pagar un monto de dinero determinado por el derecho a modificar un desarrollo que está patentado. Esta limitante hace que sólo formarán parte de este proyecto aquellas variables que son entregadas por la herramienta tal como CISCO la desarrolló.

Aun cuando no se requiere una inversión extra en tecnología, es una limitante que toda la infraestructura que sea monitoreada con la herramienta producto del Trabajo de Grado, sea del fabricante CISCO SYSTEMS.

I.5.2.3 Limitaciones geográficas

La herramienta usada en el presente Trabajo Especial de Grado deberá ser implementada en aquellas empresas que poseen redes basadas en la tecnología IP, y que utilizan enrutadores IP para acceder a las redes de los ISP.

La herramienta estará destinada a pequeñas y medianas empresas, ya que son ellas las que suelen cumplir con las condiciones explicadas; aunque también podrá ser implementada en las redes de las grandes empresas.

Para monitorear el tráfico dirigido hacia redes externas, esta herramienta debe ser usada en empresas con redes organizadas mediante niveles de jerarquía. Al menos deben existir dos niveles en las redes: Acceso y Distribución. El nivel de acceso es aquél al cual se conectan los dispositivos finales tales como estaciones de trabajo, teléfonos y cámaras IP; mientras que el nivel de distribución es aquél que se suele conectar con los enrutadores que proveen acceso a las redes externas. Esta condición se impone debido a que será propuesto que esta herramienta monitoree a esos enrutadores.

No existirá una limitación en cuanto a la ubicación geográfica de las sedes de las organizaciones ya que, el Netflow puede ser accedido desde cualquier sitio geográfico siempre y cuando se tenga acceso de red al dispositivo donde éste está instalado, así como con los permisos de seguridad para poder manipular y obtener datos de los enrutadores CISCO.

Capítulo II MARCO TEÓRICO

Antes de iniciar el capítulo, es necesario indicar que la bibliografía consultada para su desarrollo es la más reciente disponible. Este factor no es de importancia debido a que, a pesar de que el Trabajo de Grado está enmarcado en el sector tecnológico, está basado en un protocolo desarrollado en la época en la cual fue publicada la bibliografía. Cuando los desarrolladores del protocolo se dieron cuenta de ciertos aspectos relacionados con la utilización de los recursos de ciertas gamas de enrutadores, decidieron diseñar un nuevo protocolo, más potente, llamado *Flexible Netflow*, basado en *Netflow*. Este protocolo fue diseñado para equipos más potentes que los disponibles en las pequeñas y medianas empresas. Debido a este factor, los desarrolladores dejaron de documentar *Netflow* en beneficio del nuevo protocolo. A pesar del tiempo, la bibliografía sigue siendo totalmente válida.

Para el desarrollo del Trabajo de Grado, el capítulo se dividirá en tres secciones:

- Antecedentes: en la cual se explican algunas de las herramientas de monitoreo que existen en la actualidad, y que son usadas por diversas empresas bajo las condiciones que fueron explicadas en el capítulo I de este documento.
- Calidad de servicio, ya que es el fin último de todas las redes de datos creadas por el ser humano, y es la causa fundamental de la existencia de todas las herramientas de monitoreo que serán mencionadas en la sección de antecedentes.
- SNMP: se explica el funcionamiento del protocolo SNMP, ya que el Netflow realiza sus actividades en una forma que se contrapone con el funcionamiento de este protocolo. Son las dos formas de monitoreo de redes que existen en la actualidad.
- Netflow: se explica en detalle el funcionamiento del protocolo Netflow, el cual es la base de este Trabajo de Grado.

II.1. Antecedentes

Existen muchas aplicaciones comerciales que permiten monitorear redes y dispositivos de red. Algunas de esas tienen versiones de prueba que poseen características limitadas o proveen todas sus funciones durante un tiempo determinado. Otras aplicaciones son totalmente gratuitas. El hecho común de casi todas las herramientas que se mencionarán a continuación, y que sirven como antecedentes de este trabajo de grado es que casi ninguna tiene la profundidad en el monitoreo que sí provee la herramienta sobre la que tratará este trabajo.

II.1.1. Cisco

Cisco es una empresa dedicada a la fabricación de equipos de red fundada en el año 1984. (Cisco Systems) dice en su página web que el diseño de soluciones dirigidas hacia las necesidades y retos específicos de sus clientes ha sido una forma de concebir los negocios desde su fundación en el mencionado año.

La empresa fue fundada por Len Bosak y Sandy Lerner, ambos empleados de la universidad de Stanford por aquel entonces, para poder enviarse correos electrónicos desde sus respectivas oficinas, localizadas en distintos edificios del complejo de esa universidad, lo cual, en aquel entonces, era imposible debido a las limitaciones tecnológicas existentes.

Desde esa idea hasta el presente, CISCO SYSTEMS se ha convertido en el mayor fabricante de equipos de redes a nivel mundial, y fue uno de los pilares en el desarrollo de Internet y su enorme crecimiento.

La idea original de su fundación llevó a la empresa a inventar el enrutador multi red, base de las actuales redes LAN y WAN, y se ha convertido en el generador de muchos de los avances existentes hoy en día en ese ámbito ya que ha diseñado y desarrollado muchos de los protocolos que se utilizan como un estándar internacional.

En el reporte anual de (Cisco, 2012) se dice que las ventas durante el año 2012 de Cisco Systems fueron de 46 billones de dólares, lo cual representó un incremento de 7% con respecto al año anterior. En ese reporte se menciona que los

ingresos netos de la empresa se incrementaron en todas las áreas en las cuales ella opera con respecto al período del año 2011. Dicen que los sectores más destacados fueron el área de las redes inalámbricas (WLAN), la seguridad, y el *data center*.

Actualmente, CISCO SYSTEMS fabrica y vende equipos de red basados en el protocolo IP, y ofrece servicios relacionados con ellos. Se encargan de transportar todo tipo de datos en edificios, campus, y alrededor del mundo.

Cisco posee un negocio que extiende por todo el mundo, y una de claves de su éxito es que lo ha dividido en regiones: las Américas, Europa, Este medo y África, y la región Asia.

Actualmente las personas más importantes dentro de la dirección ejecutiva de esta empresa son:

- John Chambers: Chief Executive Officer.
- Frank Calderoni: Executive Vice President.
- Blair Christie: Senior Vice President.
- Chris Dedicoat: Presidente para la región Europa.
- Wilm Elfrink: Vicepresidente ejecutivo.

II.1.2. PRTG Network Monitor

Esta es una herramienta proveída por la empresa PAESSLER, la cual es, según se afirma en la página web de la empresa, (Paessler), es partner de importantes empresas del sector de las redes y de la informática, tales como CISCO, MICROSOFT Y VMWARE, las cuales son las empresas más importantes del mundo en el área de las redes, la informática y la virtualización de procesos respectivamente. Esto significa que entre estas empresas se comparte una gran cantidad de información y tecnología relevante para el desarrollo de nuevas aplicaciones en esas áreas.

Según se afirma en la página *web* de la empresa la aplicación PRTG *Network Monitor* es una herramienta de monitoreo basada en el CISCO NETFLOW.

Es una aplicación que debe ser descargada desde el sitio web de la compañía, e instalada en las estaciones de trabajo. Funciona como una página web que se abre inmediatamente después de ejecutar la aplicación desde el directorio en el cual se encuentra instalada.

En la Figura 2 se aprecia una vista de pantalla de esta aplicación, la cual muestra la cual está dividida en dos partes diferentes.

Figura 2. PRTG Network Monitor. Fuente: Paessler, 2013

El lado izquierdo de la pantalla muestra un gráfico en el que se analiza utilización de la red por parte de las diferentes aplicaciones que hacen uso de ella.

En el lado derecho se muestran cuatro gráficos:

- Localización de los diferentes elementos que conforman la red.

- Promedio de utilización de la red por parte de las aplicaciones que más recursos han consumido los últimos dos días.
- Promedio de utilización de la red por parte de las aplicaciones que más recursos han consumido los últimos cinco días.
- Promedio de utilización de la red por parte de las aplicaciones que más recursos han consumido los últimos seis días.

La aplicación puede ser usada para evitar la caída de la red durante períodos prolongados de tiempo, monitorea el ancho de banda de la empresa y averiguar para qué está siendo usada la misma.

La página principal de la aplicación, mostrada en la figura II-1, se divide en dos secciones. La parte izquierda muestra un análisis del uso que las aplicaciones están haciendo del procesador de la estación de trabajo, de una forma similar al análisis de los segmentos de disco duro. La parte de derecha de la página muestra información estadística sobre distintos aspectos de la estación de trabajo tal como las alarmas producidas en un período de tiempo, el uso que se hizo del CPU y el tráfico de red procesado.

Funciona recolectando información sobre las aplicaciones que se ejecuten en las estaciones de trabajo de las empresas, tanto en tiempo real como en forma de un histórico en el que se puede consultar el uso que cada aplicación ha hecho de la red.

Debe ser instalada en estaciones de trabajo que ejecuten cualquier variedad del sistema operativo Windows.

II.1.3. HP Openview

HP OPENVIEW es una suite de administración basada en nodos que utiliza SNMP para monitorear redes.

OPEN VIEW, desarrollada por (Hewlett Packaard, 2004), se utiliza sobre todo para monitorear y controlar redes, y para tomar las acciones correctivas que sean necesarias.

Entre las características que ofrece esta aplicación están:

- Monitoreo en tiempo real.
- Generación de reportes de tendencias (análisis predictivo sobre la situación futura de la red).
- Generación de mapas de red físicos y virtuales.
- Alerta sobre la producción de alarmas.

Se trata de una aplicación que corre sobre ambientes Windows, aunque existen diversos módulos de integración que permiten instalar agentes de Openview sobre algunos ambientes basados en UNIX/LINUX.

Aunque está diseñada para ser usada sobre plataformas HP, también se puede instalar en equipos de otros fabricantes, siempre teniendo en cuenta que algunas de las funciones pueden no estar operativas debido a que se utilizan algunos protocolos propietarios de HP para desarrollar algunas de las labores de monitoreo que se llevan a cabo con esta aplicación, especialmente en el caso de recolección de información sobre el dispositivo final propiamente dicho.

II.1.4. Wireshark

Wireshark es una aplicación de escritorio que puede ser instalada tanto en ambientes Windows como en ambientes basados en UNIX/LINUX. Es un analizador de protocolos que funciona como un capturador de paquetes, *sniffer*, y puede mostrar la información contenida en cada una de las capas del modelo OSI en cada uno de los paquetes.

De acuerdo a (Wireshark, 2012), existen dos versiones de esta herramienta: una versión gratuita y una versión avanzada, en la cual se permiten funciones tales como:

- Análisis gráfico de los paquetes transmitidos sobre la red.
- Generación de reportes.
- Generación de alertas.

Se asegura que la data de los paquetes esté siempre accesible por parte de los usuarios de la red, y se permite el monitoreo tanto de redes físicas como de redes virtuales.

Esta característica se da debido a que el Wireshark permite introducir la interfaz de red en la que se quiere capturar los protocolos de las tramas y paquetes transmitidos a través de ella. Estas interfaces pueden ser reales (físicas) o virtualizadas (máquinas virtuales).

Es una herramienta muy útil para realizar estudios sobre el uso que se hace de la red, así como para saber las aplicaciones que se encuentran transmitiendo data a través de ella. Sirve también para detectar posibles ataques a los sistemas informáticos al detectar el tipo de aplicaciones que se encuentran activos en los enlaces en el instante en que se ejecuta la aplicación. Sólo es capaz de realizar análisis en tiempo real, aunque permite almacenar los análisis realizados en el disco duro de las estaciones de trabajo.

En la Figura 3 se aprecia la pantalla principal de la aplicación.

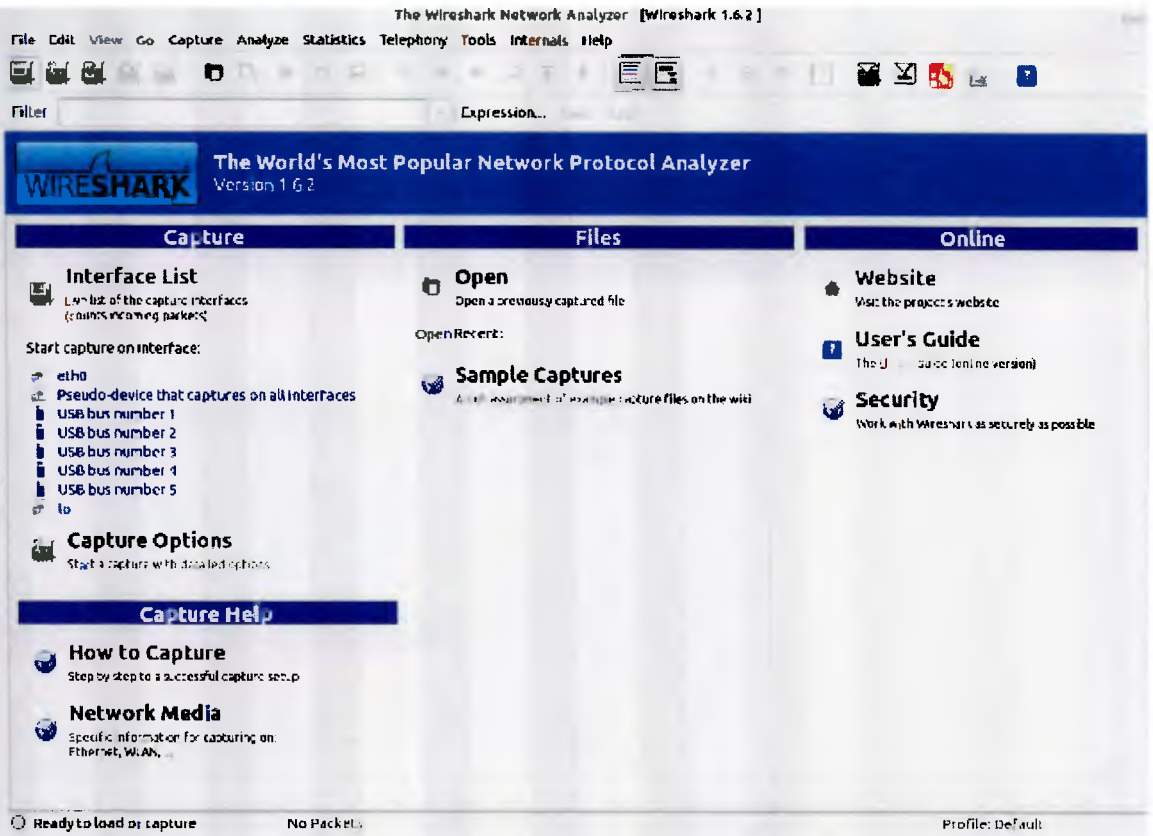

Figura 3. Wireshark. Fuente: el autor.

Desde la pantalla principal de la aplicación se pueden realizar todas las actividades disponibles en ella, aunque lo que más se aprecia debido al tamaño en que se presenta son ayudas sobre cómo utilizar la herramienta.

Para poder acceder a todos sus recursos se debe hacer uso de los distintos menús que posee en la parte superior de la pantalla.

Desde el menú *Capture* se despliegan todas las opciones disponibles sobre la captura de PDUs a través de las diferentes interfaces disponibles en el dispositivo donde se instaló la aplicación. De hecho, éste (seleccionar la interfaz) debe ser siempre el primer paso a realizar cuando se desea capturar la información que está siendo transmitida a través de ella.

En el menú *Statistics* se puede desplegar una serie de estadísticas sobre los PDU que han sido capturados. En el menú *Telephony* se dispone de una serie

de opciones sobre la voz sobre IP. Entre las actividades que pueden ser realizadas desde este menú se encuentra la captura y grabación de llamadas que se estén realizando mediante el protocolo IP en un instante determinado, así como el análisis de los protocolos que están siendo usados por ellas.

II.1.5. Datatrafic

Datatrafic es el nombre dado por (Gerencia de Tráfico - CANTV, 2010) a una aplicación web, instalada en un servidor que ejecuta el sistema operativo Sun Microsystems, que permite monitorear distintas redes.

Lo utilizan para monitorear diversos aspectos de tráfico, calidad de servicio y utilización de las redes Metro Ethernet que la corporación mantiene en el país para permitir el acceso a Internet.

Es una aplicación que se ejecuta desde cualquier estación de trabajo conectada a la red corporativa, cableada, de la corporación. El único requisito que posee es que la estación de trabajo debe tener un explorador web instalado.

Permite realizar reportes personalizados, en los que se puede elegir tanto el dispositivo de red que se va a monitorear, como las variables que se van a obtener.

Funciona mediante el protocolo SNMP, enviando solicitudes periódicas a cada dispositivo, en las cuales le interroga sobre los aspectos que es capaz de utilizar.

En los reportes se puede seleccionar la frecuencia con la que se quiere analizar la data obtenida (el tiempo transcurrido entre dos muestras que la herramienta va a colocar en el reporte solicitado), así como también permite seleccionar si se realizará el reporte por hora del día o por día de la semana. Se debe también seleccionar el período de tiempo que abarcará el reporte.

En la Figura 4 se muestra un ejemplo de un reporte realizado por esta herramienta. El reporte fue realizado el día 06/10/2010.

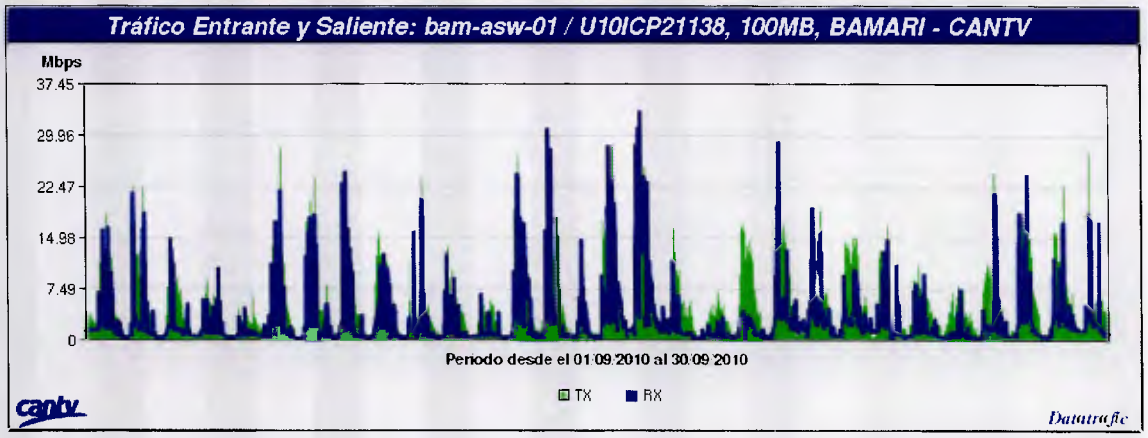

Figura 4. Análisis de tráfico utilizando la herramienta Datatrafic. Fuente: CANTV, 2010.

En la Figura II-3 se muestra una captura del tráfico cursado por un conmutador Metro Ethernet propiedad de la corporación CANTV, utilizado para el acceso al satélite Simón Bolívar. Ese reporte muestra el comportamiento seguido por el tráfico transmitido (color verde) y recibido (color azul) por el conmutador durante los 30 días continuos que van desde el 01 de septiembre de 2010 hasta el 30 de septiembre del mismo año.

Si se quiere prestar atención a algún día en particular, por ejemplo aquellos que poseen un cursado anormalmente bajo de tráfico, se puede seleccionar, desde la pantalla principal de la aplicación (no se dispone de una captura de pantalla de ella debido a que el autor no posee acceso a esa herramienta al momento de escribir el documento) un período de tiempo más corto, tal como por ejemplo 24 horas (un día), para analizar de esta forma el comportamiento hora por hora del tráfico.

Muy probablemente este comportamiento se debió a que esos días con baja actividad correspondieron a fines de semana, en los cuales suele bajar la utilización de los conmutadores debido a que la mayoría de las empresas y organizaciones no poseen actividad en esos períodos.

II.1.6. E-Health

E-Health es otra herramienta usada por (Gerencia de Tráfico - CANTV, 2010) para monitorear sus redes. Puede ser usada en redes Metro Ethernet y en redes NGN.

Realiza las mismas actividades que Datatrafic, pero tiene la capacidad extra de realizar reportes de tendencias, así como análisis predictivos que indiquen en qué momento se deberá cambiar un dispositivo debido a su colapso por la cantidad de tráfico que cursa, o debido a fallas.

Adicionalmente, E-Health trabaja usando el protocolo SNMP, y se encuentra instalado en un servidor que ejecuta el sistema operativo Sun Microsystems. Puede ser accedida desde cualquier estación de trabajo con un explorador web instalado.

Es una herramienta segura en el sentido de que exige que el usuario se identifique con un alias y una contraseña cuando intenta ejecutarla. Adicionalmente, se ejecuta bajo el protocolo https, con lo cual la data de autenticación se envía encriptada al servidor.

Para poder monitorear un dispositivo, primero debió haber sido descubierto por la aplicación, y agregado a su base de datos de dispositivos activos, con lo cual se exige que después de su configuración se ejecuten algunos pasos extra para asegurar que la herramienta pueda observar a todos los elementos de la red.

Trata a cada dispositivo como un ente dividido en partes, cada una de las cuales es un objeto monitoreable por parte de la herramienta. Así, cada elemento posee interfaces de red, procesadores, chasis, ventiladores, etc. Cada uno de esos elementos constituye una entrada para el monitoreo de la herramienta. Es una aplicación propietaria, en la cual se entregan licencias para monitorear un cierto número de elementos.

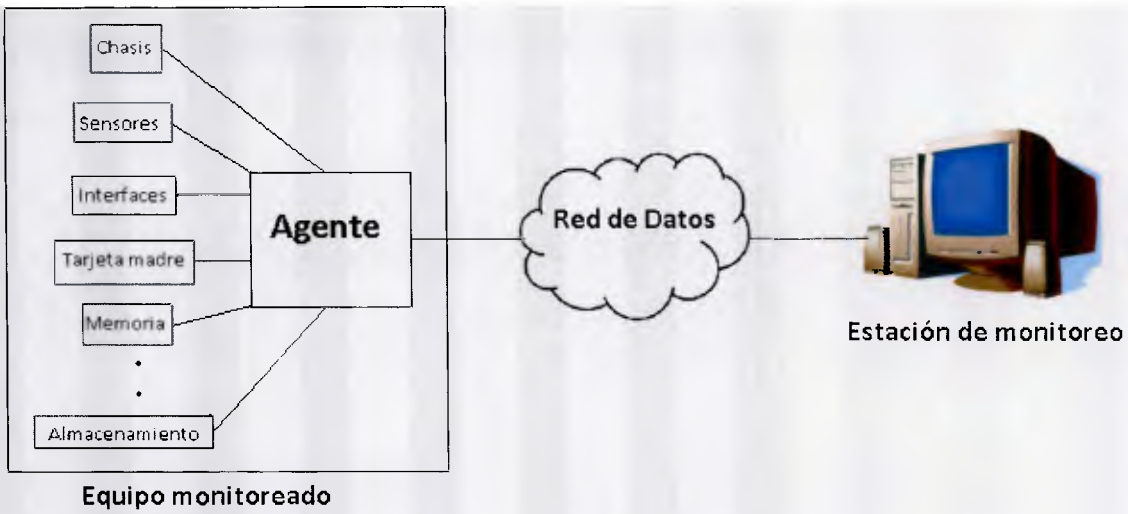

Figura 5. Funcionamiento de E-Health. Fuente: el autor, 2013.

Desde la estación de trabajo que se observa en la Figura II-4 se accede a la herramienta E-Health. Ésta es capaz de entregarle a la estación de monitoreo un reporte detallado de cada uno de los elementos de red, principalmente conmutadores de capa tres con tecnología Metro Ethernet. Este estado no se limita al hecho de informar si está inactivo o no, sino que más bien le entrega un reporte completo sobre el estado de cada uno de los dispositivos y elementos que forman a esos dispositivos.

Esta herramienta entrega toda esta información utilizando para ello el protocolo SNMP. Específicamente, el servidor en el cual se instala la aplicación es capaz de interrogar a cada uno de los elementos de la red que ha descubierto hasta ese momento sobre las MIB que ellos poseen instaladas.

Cada una de las MIB contienen información sobre el funcionamiento y estado de los elementos que forman a un dispositivo de red. Los elementos que forman el protocolo SNMP serán explicados en la sección II.2.1 "SNMP".

II.2. Referencia teórica

En esta sección se presentan algunos conceptos básicos, y el funcionamiento de dos protocolos muy importantes en el área del monitoreo de redes. En primer lugar se mencionan algunos aspectos de calidad de servicio (ya

que todo el concepto del monitoreo de redes se basa en la calidad de servicio asignada a los usuarios). A continuación se mencionan algunos conceptos relacionados con el protocolo SNMP ya que es el protocolo más utilizado actualmente en el monitoreo por su extrema sencillez, y finalmente se presenta un desarrollo de Cisco Netflow debido a que es la herramienta que será utilizada para realizar el desarrollo que se propone en este documento.

II.2.1. Calidad de Servicio (QoS)

La calidad de servicio es una serie de políticas que rigen el funcionamiento operativo de las redes de datos.

Mediante la asignación de una QoS adecuada se logra que todos lo usuarios de la redes tengan una experiencia acorde a la esperada por ellos, es decir, se logra que el ancho de banda contratado sea apreciado por todos los usuarios de las redes de una forma más o menos equitativa.

En el ámbito empresarial, la QoS tiene una función más trascendente que el simple hecho de disfrutar de rapidez en la red, lo cual, al igual que en el caso de los usuarios residenciales, es sumamente importante. Esta función es la prestación de los servicios que fueron proyectados al momento del diseño de la red.

(Cisco Systems, 2008) incluye en su material de estudio sobre redes IP, módulo III, conceptos sobre las redes convergentes. Desde hace cierto tiempo, las empresas han ido migrando su plataforma tecnológica hacia el paradigma de las redes convergentes, las cuales se definen en esa obra como la conjunción de los servicios de voz, video y datos de una empresa a través de una sola red.

Afirman que la asignación de políticas de QoS es indispensable en las redes convergentes debido a que es imprescindible la priorización y clasificación del tráfico de acuerdo al tipo de servicio que se preste en la red. Así, la voz, el video y los distintos tipos de tráfico de datos serán tratados con una prioridad diferente por parte de los dispositivos de red.

Para que la QoS pueda ser implementada en las redes empresariales, es necesario que se disponga de una red jerárquica. (Cisco Systems, 2008) explica

que una red jerárquica divide la red en capas individuales, cada una de las cuales puede estar formada por diferentes tipos de dispositivos que ejecutan funciones muy particulares. Un mismo dispositivo puede ser insertado en diferentes capas del modelo de red jerárquica, o incluso puede funcionar él mismo en varias o toda las capas que se diseñen. Se definen las siguientes capas:

- Capa de acceso: es la parte de la red en la cual se conectan los dispositivos finales, tales como PC´s, impresoras de red, cámaras IP, servidores, teléfonos IP, usuarios inalámbricos, etc. Provee acceso a los usuarios finales a los servicios ofrecidos por la propia red.
- Capa de distribución: se encarga de controlar el flujo de datos de la red mediante la aplicación de las políticas diseñadas por los administradores y gerentes de red de las empresas. Transporta los datos de los usuarios hacia su destino final o los prepara para ser enrutados hacia otra locación si fuese necesario.
- Capa de backbone: también se conoce como núcleo de la red. El núcleo es una sección de muy alta velocidad y disponibilidad que normalmente se utiliza para transportar datos entre redes diferentes y para proveer acceso a Internet a los usuarios de una red. Es muy importante que los elementos que forman el núcleo de la red sean altamente redundantes tengan un porcentaje de disponibilidad muy elevado durante todo el año, es decir, el tiempo de inactividad debe ser mínimo. Se debe garantizar que, en caso de que se produzca una falla, ésta esté lo más focalizada posible, es decir, se debe garantizar que a pesar de la falla, los usuarios tengan acceso a las redes externas de forma normal.

Antes de diseñar cualquier red basada en un modelo jerárquico como el expuesto en la página anterior, y que ejecute aspectos de QoS, se deben analizar una serie de consideraciones.

Según (Cisco Systems, 2008) se debe realizar un estudio previo del tráfico que será cursado a través de la red para determinar cuáles son los conmutadores

más adecuados para cada una de las capas de acuerdo a sus características y a los requerimientos de la red.

Afirman que es necesario realizar un análisis del flujo de tráfico considerando la segmentación de la red así como el ancho de banda cursado en cada una de los segmentos. Es necesario, según explican, estudiar profundamente la interacción entre los diferentes servidores que existen en la red.

Se asegura en este material de estudio que se debe estudiar la interacción entre los distintos grupos de trabajadores que laboran en las empresas para poder realizar la asignación adecuada de recursos.

(Barreiros & Lundqvist, 2011) afirman en su libro sobre QoS que el tráfico de voz siempre ha sido un importante paradigma en el diseño de redes con calidad de servicio, y que se ha incrementado de la tal manera que su consideración es hoy en día indispensable en el diseño de cualquier red de servicios convergentes.

Establecen en la obra referida que la QoS puede ser definida desde dos puntos de vista: local y señalización. El punto de vista local consiste en aplicar las políticas de calidad de servicio requeridas los diferentes enrutadores y conmutadores que forman la red de datos, mientras que el punto de vista de señalización consiste en marcar cada uno de los paquetes y tramas que circulan por ellos de forma que cada enrutador y conmutador presentes en la ruta que deben seguir pueda decidir qué aspectos de QoS se debe aplicar a cada uno de ellos.

Existen a su vez dos modelos mediante los cuales se puede aplicar la calidad de servicio a una red de datos, a saber:

- Servicios integrados: conocido como IntServ, fue diseñado como una forma de reserva de recursos extremo a extremo para cada uno de los flujos que circulan por la red. No fue totalmente desarrollada por la complejidad que implica su implementación. Implica el marcaje de cada uno de los paquetes con una característica determinada de acuerdo con el servicio, tipo de usuario, red a través de la cual se puede encontrar al usuario, etc. A pesar

de esta complejidad, algunas de sus características han sido trasladadas al mundo de MPLS.

- Servicios Diferenciados: conocido como DiffServ, fue diseñado como un esquema de clases. El tráfico es diferenciado en diferentes clases. Mediante este esquema cada uno de los enrutadores o conmutadores se encarga de asignar un comportamiento específico a los paquetes y tramas que procesa. Como se ve, cada dispositivo de red trabaja en forma aislada del resto, aplicando sus propias políticas a los datos que debe procesar.

Uno de los aspectos principales que debe tomarse en cuenta en la administración y configuración de la QoS es el control del tamaño de las colas de paquetes y tramas en los enrutadores y conmutadores. (Flannagan, 2001) explica en su obra sobre la gestión de la calidad de servicio en redes Cisco que uno de los principales métodos para realizar esta labor consiste en clasificar el tráfico en diferentes tipos, de acuerdo con el tipo de servicio final que cada uno de ellos transporta, y asignar a cada uno de ellos una prioridad de procesamiento diferente entre sí.

Afirma que esta clasificación le entrega a los administradores de las redes un control casi absoluto sobre los paquetes y tramas que se procesan en los dispositivos de red intermediarios y los que no, así como también el poder suficiente para denegar la transmisión de aquellos datos con las prioridades más bajas dentro de la red. Según el autor, algunos de los parámetros según los cuales se puede clasificar el tráfico de red son:

- Tipo de protocolo.
- Tamaño en bytes de los paquetes y tramas.
- Puertos TCP/UDP origen y destino.
- Fragmento o no de un paquete IP más grande, etc.

(Barreiros & Lundqvist, 2011) menciona que los siguientes son parámetros importantes que deben ser estudiados en redes con calidad de servicio:

- Retardo: es el tiempo que una trama o paquete tarda en llegar a su destino desde el momento en que fue enviada por el dispositivo final origen.
- CIR: es la cantidad de información que un dispositivo final puede transmitir hacia la red. Es un valor que se contrata a un ISP. Debería estar disponible en todo momento ya que es el parámetro por el cual los proveedores de servicio alquilan sus enlaces. Debido a esto, es uno de los parámetros más importantes que se deben estudiar cuando se analiza el comportamiento de una red con calidad de servicio.
- PIR: en muchas ocasiones los dispositivos finales y servidores deben enviar más datos a una velocidad muy grande que los que normalmente se envían. Este tráfico se comporta como una ráfaga que sobre-pasa el ancho de banda contratado al ISP. Esta sobre transmisión se conoce como PIR. Dependiendo de la tecnología que se utilice (*FRAME RELAY,* ATM, IP, MPLS, *METRO ETHERNET,* etc.) los proveedores de servicios ofrecerán un mayor o menor PIR, o simplemente no lo ofrecerán.

La empresa CISCO, líder en el mercado mundial de redes, ofrece una serie de herramientas en sus dispositivos de gama media y alta corporativa para incorporar calidad de servicio a las redes. Entre ellas *están Policy-Based Routing*, y *Commited Access Rate*.

- *Policy-Based Routing*: prove un método para marcar paquetes de acuerdo a la dirección IP origen para aplicarles aspectos de clasificación y priorización de tráfico. Trabaja en conjunto con las listas de acceso.
- *Commited Access Rate*: es el método de marcado de paquetes más comúnmente usado en los bordes de las redes. Permite controlar dos aspectos fundamentalmente: el ancho de banda que será asignado a cada paquetes, así como también la clasificación del tráfico de acuerdo a las características de QoS que hayan sido configuradas en los enrutadores. La limitación de ancho de banda de realiza de tres maneras, a saber, ancho de

banda promedio, tamaño normal de una ráfaga de datos, y tamaño en exceso de una ráfaga de datos.

II.2.2. SNMP

Como publican (Murray & Stalvig, 2008) en el artículo "SNMP: Simplified", SNMP es un protocolo que define los procedimientos necesarios para monitorear dispositivos conectados a redes IP, y es el acrónimo usado para referirse a Simple Network Management Protocol.

El monitoreo de redes es una tarea bastante compleja, para lo cual el IETF, en la década de 1980, definió el protocolo SNMP como un medio para monitorear redes complejas formadas por equipos de muchas marcas diferentes.

Hasta la fecha han sido desarrolladas tres versiones de SNMP y fue definido en el RFC 1157, el cual sustituyó el al RFC 1098. Según afirman (Case, J.; M, Fedor; M, Schoffstall;, 1990) en la publicación del IETF RFC 1157, SNMP surgió con la idea de administrar nodos en la comunidad de Internet. Los autores dicen además que la arquitectura de SNMP está basada en una colección de elementos de red y de estaciones de trabajo, las cuales monitorean y controlan a los anteriores elementos de red, los cuales son, según ellos, estaciones de trabajo y servidores que contienen agentes encargados de realizar las labores de monitoreo solicitadas por las estaciones remotas de monitoreo.

SNMP posee una base de datos que define la información genérica que todo dispositivo debe ser capaz de entregar. El mismo autor establece que existen dos versiones de esta base de datos: una pública y una privada. La porción pública de la base de datos, según el escritor, posee básicamente información relativa a las estaciones de trabajo y equipos terminales.

Existen tres versiones de SNMP: la versión 1, la versión 2 y la versión 3.

- Versión 1: proveyó la estructura básica necesaria para establecer una red de administración de la información, obtener información de los dispositivos y equipos, controlarlos, y permitir el envío de mensajes, por parte de los

equipos monitoreados, a un administrador llamado *Network Management System* (NMS).

- Versión 2: según el mismo autor, la segunda versión de SNMP ofrece varias mejoras con respecto a la primera, entre las cuales se pueden mencionar la posibilidad de enviar mensajes en grupo en vez de mensajes individuales, y le permite a los NMS enviar mensajes de solicitud y de gestión a los dispositivos que ellos monitorean.
- Versión 3: ofrece la encriptación de tanto los nombres de las comunidades públicas y privadas, así como también toda la data que se trasmite entre los dispositivos finales y los NMS.

Originalmente, SNMP fue diseñado para funcionar como un modelo de comunicación individual entre un NMS y un dispositivo final, y funcionaba de una forma no invasiva, es decir, funcionaba tratando de enviar la menor cantidad posible de paquetes a la red de forma que ésta se sobrecargara lo menos posible, así como también para añadir la menor cantidad posible de carga de operación a las estaciones de trabajo.

II.2.2.1 Extensiones MIBs

Como afirman (Murray & Stalvig, 2008) SNMP fue diseñado originalmente como una herramienta de monitoreo basada en los dispositivos. También establecen que el *Remote Monitoring* (RMON) fue diseñado originalmente como una herramienta de monitoreo basada en flujos de tráfico, la cual poseen en sus dos versiones (Rmon 1 y Rmon 2) extensiones hacia SNMP.

Según dicen los dos autores, la primera versión Rmon contenía diez grupos de extensiones enfocados en las capas físicas y de enlace de datos del Modelo OSI, usados sobre todo en el monitoreo de redes LAN basadas en *Ethernet* y en *Token Ring*.

Afirman también que la segunda versión de Rmon añadió diez grupos más que permitían monitorear las capas de red y de aplicación. Esto trae como consecuencia, según (Murray & Stalvig, 2008), el incremento de la carga de

procesamiento en los equipos y en las redes. Cuando el Rmon está completamente implementado, las extensiones de Rmon hacia SNMP proveen muchas de las funciones ofrecidas por los analizadores de red.

Toda esta actividad se realiza debido a las MIBs, las cuales son estructuras que contienen información jerárquica sobre cada uno de los dispositivos que forman la red de datos, así como sobre cada elemento que forma a esos dispositivos, organizada en objetos. Cada objeto posee un identificador de objeto único que actúa como un contador o un apuntador y facilita su ubicación y acceso.

II.2.2.2 Definiciones

Aunque frecuentemente se producen cambios en la tecnología, existen ciertas definiciones que hacen que SNMP se mantenga en el tiempo, tales como elementos de red, estación de administración, etc.

- Elemento de red: son dispositivos tales como estaciones de trabajo, *gateways*, servidores, etc.; los cuales, según afirman (Murray & Stalvig, 2008), poseen los agentes de gestión necesarios para desarrollar las funciones de administración y gestión solicitadas por las estaciones de administración. Un elemento de red es un nodo.
- Estación de monitoreo de red (NMS): según afirman (Murray & Stalvig, 2008), el NMS es un servidor que ejecuta las aplicaciones de monitoreo. Proveen los métodos para analizar y reportar información importante.
- Dispositivo de alertas SNMP: (Murray & Stalvig, 2008) dice que son dispositivos que encuestan a los dispositivos de red para recolectar información sobre ellos.
- Sondeo RMON: de acuerdo con las palabras de (Murray & Stalvig, 2008), el sondeo RMON es el acto de recolectar información sobre una red LAN para llevar a cabo actividades más sofisticadas que las desarrolladas por los agentes SNMP, así como para reportar resultados más complejos.

- Base de información de gestión; la MIB, según (Murray & Stalvig, 2008) contiene Identificadores de Objetos que contienen información sobre ellos. Tienen una estructura basada en árbol en la que cada objeto individual que es monitoreado es una rama del árbol.
- Identificador de objeto: las OID, de acuerdo a (Murray & Stalvig, 2008) identifican a objetos individuales pertenecientes a las MIB.
- Alertas: en la obra de (Murray & Stalvig, 2008) se afirma que los traps son alertas que se envían, sin una solicitud previa, desde los elementos de red hacia un administrador de red (NMS), conteniendo información importante sobre su funcionamiento.
- Comunidad: (Murray & Stalvig, 2008) aseguran que SNMP especifica dos grupos llamados comunidades que permiten el acceso a los OIDs de un sistema de gestión de red. La comunidad pública, según ellos, permite acceder a todos los elementos en un dominio SNMP.

II.2.2.3 Elementos

(Schmidt, 2005) establece en su libro sobre SNMP que este protocolo está formado por dos elementos principales: un NMS y un agente. El NMS, *Network Management System,* se encarga de controlar a cada una de las interfaces que son monitoreadas en la red.

El NMS puede interrogar a cada una de ellas acerca de su estatus, así como también tomar las acciones correctivas necesarias cuando éstas deban ser tomadas.

En forma lógica, el SNMP está formado por Management Information Base, MIB, los cuales son estructuras que permiten definir los objetos a ser monitoreados así como su comportamiento. Los agentes SNMP poseen una lista de esos objetos, cada uno de los cuales poseen la información sobre su estado operativo. Esta información es usada por el NMS para determinar el estado de salud de las redes.

Las MIB pueden ser vistas como una base de datos que contiene los objetos que los agentes rastrean. Toda la información estadística y operativa sobre un objeto que puede ser accedida por un NMS está definida en la MIB.

Los fabricantes de los equipos están autorizados por las autoridades del IETF para definir sus propias variables y MIB mediante su inclusión en la comunidad *private*.

El agente es la entidad de red que es monitoreada y controlada por el NMS. Cuando algo malo ocurre, o cuando una interfaz se encuentra caída, ésta puede enviar un mensaje de Trap hacia el NMS informando sobre esta situación. Ambos tipos de mensajes, tanto las encuestas como los trap, pueden ocurrir simultáneamente.

Cuando un NMS envía un mensaje de encuesta hacia un agente, éste responde con el parámetro solicitado. Los mensajes de trap son enviados espontáneamente por cada uno de los agentes cuando éstos tienen alguna novedad que reportarle al NMS.

En la Figura 6 se muestra la relación entre los NMS y los agentes de red.

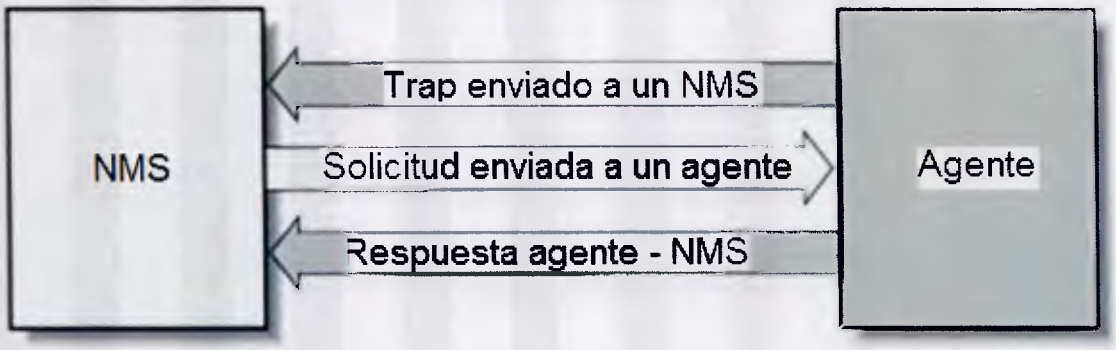

Figura 6. Mensajes entre un NMS y un agente. Fuente: (Schmidt, 2005)

Los NMS se encargan de interrogar a cada uno de los agentes en busca de información sobre su funcionamiento. Una vez recibida esta información se encargan de procesarla, analizarla, o de realizar la actividad que estén programados para realizar con ella.

Los Agentes tienen la capacidad de realizar sólo dos funciones dentro del protocolo SNMP. La primera de ellas es responder a las solicitudes de los NMS con los valores de las variables solicitadas. La segunda función consiste en enviar un mensaje de alarma (trap) a los NMS cuando se detecta cualquier problema.

II.2.2.4 Funcionamiento

(Schmidt, 2005) expone que SNMP utiliza UDP *(User Datagram Protocol)* como protocolo de capa de transporte en la trasmisión de los mensajes que deben ser enviados entre un agente y un NMS. Entre las razones de su uso se encuentran:

- Es un protocolo no orientado a la conexión, lo que significa que no se debe establecer la sesión y negociar sus parámetros antes de establecer la conexión extremo a extremo.
- Es un protocolo no confiable, debido a que no se establecen mensajes de confirmación entre los dos extremos de la conexión cuando se transmite un mensaje de data.

SNMP basa su funcionamiento en la inter-relación entre el NMS y el agente. El NMS envía un mensaje de solicitud o encuesta a un agente y espera por su respuesta. El tiempo que el NMS espera por una respuesta por parte del agente depende cómo el NMS esté configurado. Si se vence el período de espera sin la recepción de una respuesta por parte del agente SNMP, el NMS asume que el datagrama UDP se perdió y, por ende, re-envía el mismo mensaje de solicitud. El número de veces que un NMS envía el mismo mensaje también es configurable.

SNMP utiliza el puerto 161 UDP para enviar y recibir solicitudes, mientras que utiliza el puerto 162 UDP para enviar mensajes de trap. En la Figura 7 se

muestra el proceso de encapsulado / desencapsulado de un mensaje SNMP.

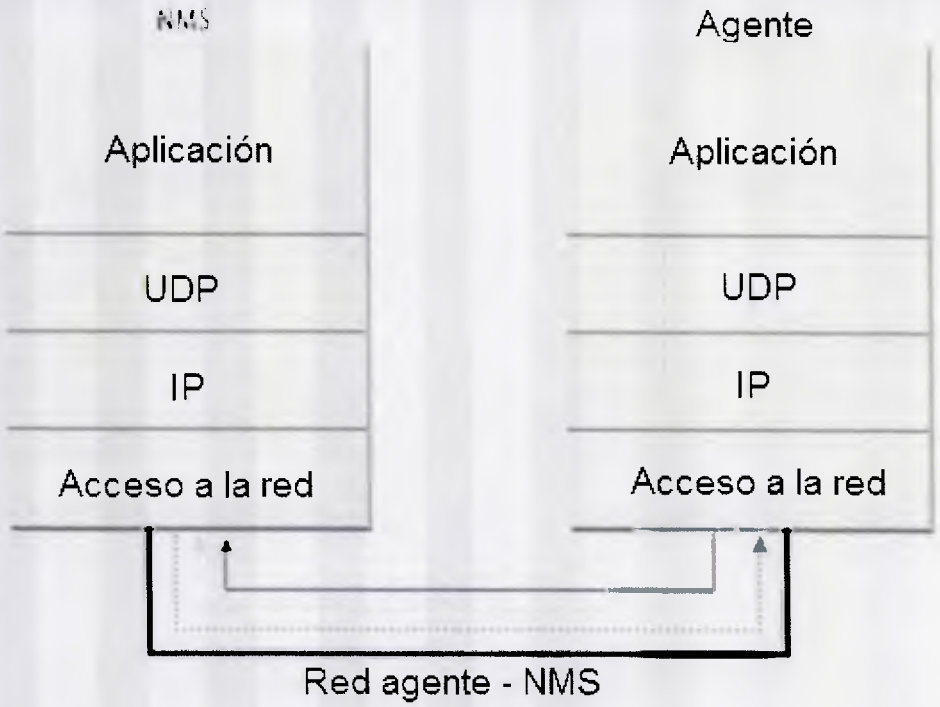

Figura 7 Capas de OSI usadas por SNMP. Fuente: (Schmidt, 2005)

En la Figura II-6 se aprecia que SNMP es un protocolo que se ejecuta en la Capa de Aplicación del Modelo de Referencia OSI. Utiliza el protocolo UDP como protocolo de Capa de Transporte debido a que, dada su naturaleza de monitoreo, no maneja información crítica para el funcionamiento de la red. Esta condición hace que no sea necesario que la información que sea transmitida por el protocolo tenga asegurada su entrega mediante los métodos de confiabilidad y corrección de errores que establece el protocolo TCP. SNMP es un protocolo No Confiable, lo cual significa que se hará el mejor esfuerzo por entregar sus mensajes, pero ésta entrega no está garantizada.

Adicionalmente, SNMP no garantiza que los mensajes enviados lleguen a su destino en el orden en el cual fueron generados. Esto no es importante para este protocolo debido a que no se maneja tráfico crítico para los usuarios finales de las redes. El interés que se tiene es que el agente informe sobre su estado en algún momento, más no importa que esta información llegue antes o después a su destino,

o el orden en el cual lo haga debido a que eventualmente el NMS se dará cuenta de que algo ha ido mal.

II.2.2.5 Estructuración de la información

SNMP estructura la información que puede ser monitoreada en objetos. (Schmidt, 2005) establece que esos objetos tienen tres partes constitutivas:

- Nombre: identifica de forma única a un objeto monitoreado. Se suele representar o bien en la forma de una cadena numérica, o bien en una forma de fácil lectura para el ser humano (usando palabras).
- Tipo y sintaxis: el tipo de datos de un objeto gestionado por SNMP está definido en una cadena del protocolo ASN.1, el cual especifica la forma en que la data se representa y transmite entre un agente y un NMS.
- Codificación: una instancia individual de un objeto monitoreado se codifica en una serie de octetos que siguen la *Basic Encoding Rules, BER,* la cual es una serie de reglas que indican la forma en que se debe codificar y decodificar la data cuando va a ser transmitida a través de una red Ethernet.

Los nombres de los objetos están definidos en una estructura jerárquica con forma de árbol, que se muestra en la Figura 8. Los objetos se representan mediante

una serie de números enteros (que constituyen los extremos de las ramas del árbol) separados entre sí mediante puntos.

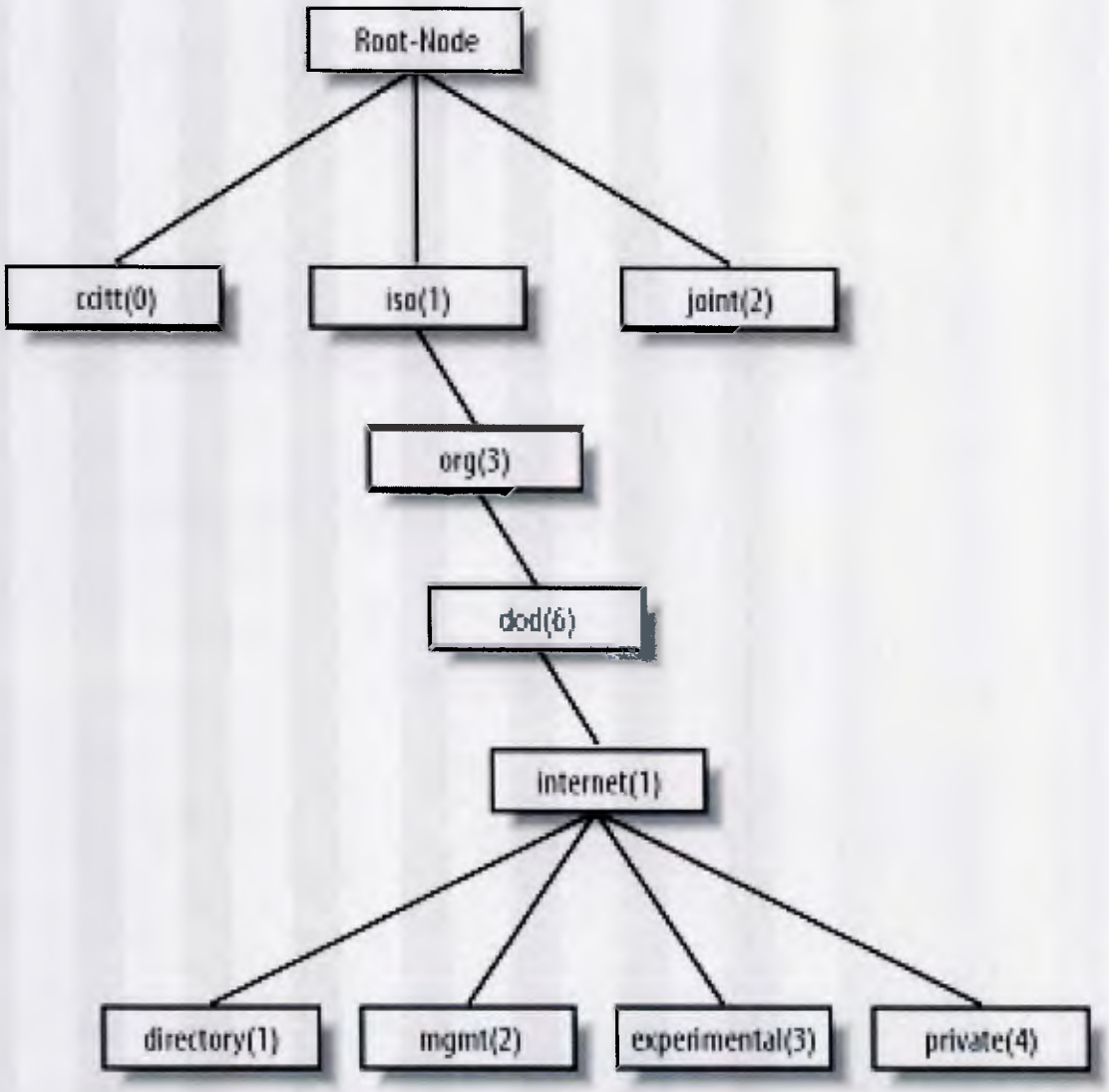

Figura 8. Nombres de los objetos en SNMP. Fuente: (Schmidt, 2005)

La mayor parte de las MIB que contienen información susceptible de ser enviada a un NMS se encuentra contenida en la comunidad pública definida por SNMP. De acuerdo al lugar en el que se encuentre cada una de esas MIB, se contendrá información de un tipo diferente. Por ejemplo, la rama Internet posee información sobre la red a la cual se encuentra conectado el dispositivo, así como también información de red del propio dispositivo. La rama Mgmt posee información

útil a la hora de administrar el sistema, tal como por ejemplo el tamaño del procesador que posee, la cantidad de memoria instalada, la capacidad del disco duro, etc.

La comunidad privada posee información que es desarrollada por las propias empresas, fabricantes de los dispositivos de red. En ella se encuentran aquellas MIBs que son propietarias de la empresa. Es información totalmente diferente a la mostrada en la comunidad pública. Para acceder a esa comunidad (privada) es necesario poseer la clave de la empresa particular. La información contenida en ella es sumamente difícil de obtener debido a que sus propietarios han invertido mucho dinero en desarrollarla.

II.2.2.6 Operaciones get - next

(Schmidt, 2005) afirma que SNMP define una secuencia de comandos que permiten enviar una serie de valores de una MIB. Esto significa que por cada objeto del que se quiera conocer su estatus, se debe generar un grupo get next.

Existen dos comandos get next:

- Get – Next Request: permite a un NMS solicitarle a un agente el valor de un objeto monitoreado por éste.
- Get – Next Response: permite al agente responderle al NMS el valor que éste solicita con el mensaje anterior.

II.2.2.7 Operaciones get – bulk

Según dice (Schmidt, 2005) en la obra que se ha venido citando hasta el momento, la segunda versión de SNMP establece los mensajes bulk, que permiten a un NMS solicitar el valor de un objeto en muchos dispositivos al mismo tiempo. Este mensaje le dice a los agentes que devuelvan la mayor parte de las respuestas solicitadas, siempre que puedan hacerlo, lo cual significa que se pueden dar respuestas incompletas. En la Figura 9 se muestra la secuencia de operaciones el comando bulk.

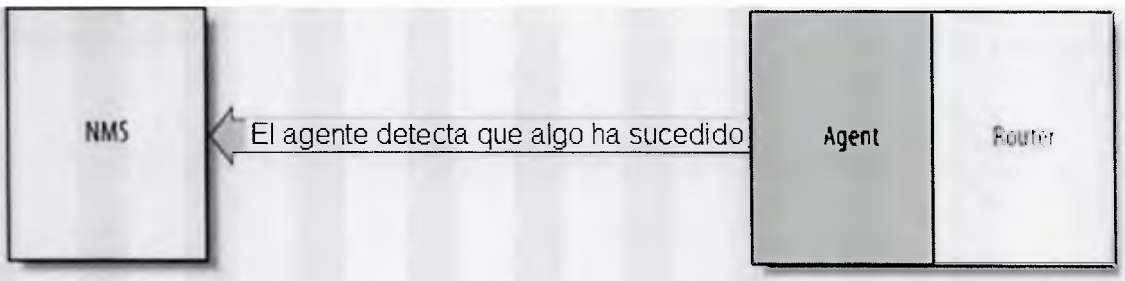

Figura 9. Operación del comando bulk. Fuente: (Schmidt, 2005)

Los NMS envían un mensaje de *Get Bulk* a los agentes registrados para solicitarles el valor de una variables o variables. En la figura se solicita el valor de *SysDescr, ifninOctets* e ifnOutOctets. Los agentes responden a esta solicitud con los valores de la descripción del sistema y el número de octetos entrantes y salientes de la interfaz.

II.2.2.8 Mensajes de trap

(Schmidt, 2005) dice que los mensajes de trap son una forma para que los agentes SNMP puedan decirle a los NMS que algo malo está ocurriendo. En la Figura 10 se muestra la secuencia de operaciones de los comandos trap.

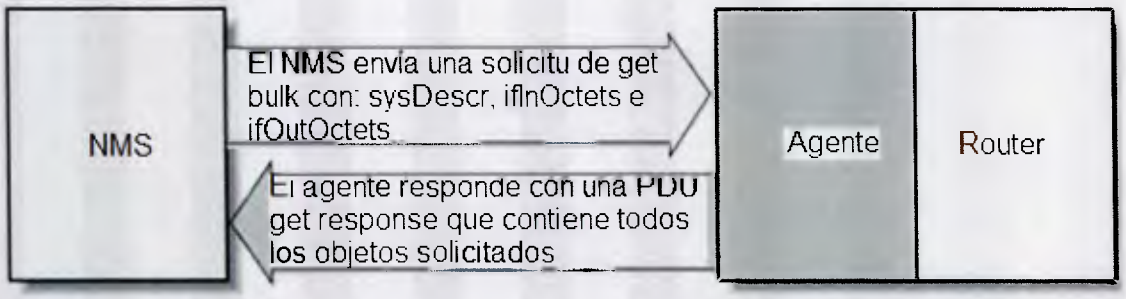

Figura 10. Operación de los comandos trap. Fuente: (Schmidt, 2005)

Cuando un agente descubre que algo no adecuado está sucediendo en su sistema, envía esta información al NMS en un mensaje de trap. En el caso de la

Figura II-9, el agente le informa al NMS que una de sus interfaces se encuentra en estado *down*, es decir, le informa que se encuentra desactivada.

El mensaje de trap se origina en los agentes y es enviado hacia un destino que normalmente es un NMS, el cual, una vez que recibe el segmento UDP, no envía una confirmación, de forma que el agente no tiene forma de saber si el NMS recibió o no el mensaje.

Entre las situaciones que los agentes reportan a los NMS se encuentran:

- Indicar que una interfaz o interfaces del dispositivo en el que funcionan los agentes, está caída.
- Indicar que una interfaz o interfaces del dispositivo en el que funcionan los agentes, ha vuelto al estado de encendido.

II.2.3. Cisco IOS Netflow

CISCO *NETFLOW* es un software que se habilita sobre el *Interworking Operating System* (IOS) desarrollado por CISCO. Según (Cisco Systems, 2007) afirma en su *datasheet* sobre la versión 9 de *Netflow*, el IOS *Netflow* provee una serie de servicios para las aplicaciones IP, entre las que se puede nombrar:

- Conteo de tráfico.
- Planificación de red.
- Seguridad.
- Monitoreo de las amenazas por denegación de servicio.
- Monitoreo de red.

El Netflow se puede definir como un medio para caracterizar la operación de las redes. En esa obra se mencionan una serie de aplicaciones, entre las que se pueden remarcar las siguientes:

- Uso de la red por parte de las distintas aplicaciones.
- Productividad de la red y utilización de sus recursos.

- El impacto que los cambios producen sobre las redes.
- Vulnerabilidades de las redes.
- Asuntos sobre la evolución a largo plazo de las redes.
- La habilidad para caracterizar el tráfico IP, y entender cómo se mueve por la red es crítico para su funcionamiento, disponibilidad, desempeño y resolución de problemas.

(Cisco Systems, Mayo 2012) afirma en su White Paper que el monitoreo del tráfico IP asegura una capacidad de planeación más precisa, y asegura así mismo que los recursos de red serán usados de una forma más apropiada de acuerdo a los intereses y metas organizacionales de las empresas.

En el documento distribuido por (Cisco Systems, Mayo 2012) se afirma que un análisis de red basado en Netflow ayuda a los gerentes y personal de IT de las empresas a determinar dónde se debe aplicar la Calidad de Servicio, optimizar el uso de los recursos y administrar la seguridad de las redes mediante la detección y prevención de distintos ataques a la seguridad lógica de los dispositivos en los que se encuentra instalada la herramienta de análisis de flujos.

(Cisco Systems, Mayo 2012) explica que con el *software Netflow* se pueden obtener las variables que se muestran a continuación.

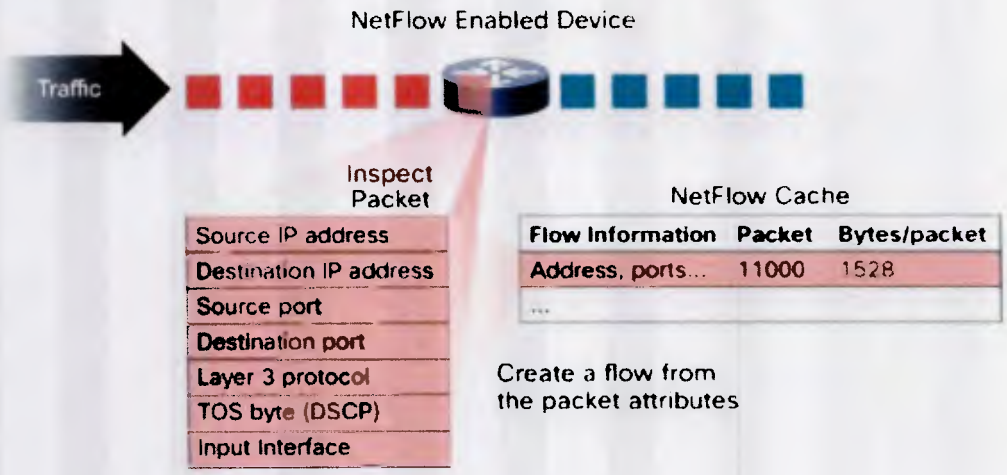

Figura 11. Data entregada por Netflow. Fuente: (Cisco Systems, Mayo 2012)

La data que se aprecia en la Figura II-10 consiste en:

- Direcciones origen y destino.
- Puertos origen y destino.
- Tipo de protocolo de capa 3.
- Clase de servicio.
- Interfaces origen y destino.

Las variables mencionadas pueden ser accedidas de dos maneras: utilizando la línea de comandos de los conmutadores y enrutadores; o utilizando una aplicación que permita realizar la actividad de monitoreo.

Figura 12. Formas de acceder a la data de Netflow. Fuente: (Cisco Systems, Mayo 2012)

Los flujos generados por *Netflow* se almacenan en una base de datos en el propio dispositivo de red, y pueden ser enviados hacia un servidor o estación de trabajo que cumpla las funciones de monitoreo. Según (Cisco Systems, Mayo 2012), a estas estaciones de trabajo o servidores se les conoce con el nombre de *Netflow Collector*.

En la Tabla **1** se muestra un ejemplo del formato de un flujo Netflow, observado en la línea de comandos del dispositivo de red.

Tabla 1. Formato de un flujo Netflow. Fuente: (Cisco Systems, Mayo 2012)

Srcif	SrcIPaddr	Dstif	DstIPaddr	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	Nexthop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.2.2	Fa0/0	10.0.227.12	11	80	10	11000	162	/24	5	[illegible]	/24	15	10.0.23.2	1528	[illegible]	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2497	15	/26	196	[illegible]	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	161	/24	180	[illegible]	/24	15	10.0.23.2	1426	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	[illegible]	/24	15	10.0.23.2	1040	24.5	[illegible]

En la tabla II-1 se aprecia el formato con el que se aprecia un conjunto de flujos con su información asociada. La información que se muestra asociada en grupos que contienen:

- IP origen y destino
- Interface origen y destino.
- Código del protocolo.
- Banderas.
- Puertos origen y destino.
- Sistema autónomo origen y destino.
- Bytes por flujo.
- Paquetes por flujo.

En el documento desarrollado por (Cisco Systems, 2007) se menciona que la salida principal de Netflow es un flujo de datos que puede ser presentado bajo distintos formatos, entre los cuales el más reciente es el formato de la versión 9, el cual se basa en muestras. En el mencionado documento se refieren una serie de ventajas sobre el uso de muestras, entre las que se pueden nombrar las siguientes:

- Se pueden añadir nuevas aplicaciones y mejoras fácilmente.
- Puede adaptarse fácilmente a desarrollos futuros.
- Utiliza estándares basados en los formatos de exportación de data desarrollados por el IETF.

(Barry, 2002) indica en su libro sobre redes que habilitar el Netflow en los enrutadores de las empresas le permite a los administradores de red tener acceso

a los flujos de paquetes de sus redes. La data de Netflow exportada hacia un servidor externo puede ser usada en una gran variedad de temas, tales como el monitoreo de seguridad, la gestión y planificación de las redes, la planificación de la capacidad de la red, facturación y el análisis del flujo de información en Internet.

Un ejemplo de planificación de la red se muestra en la Figura 13:

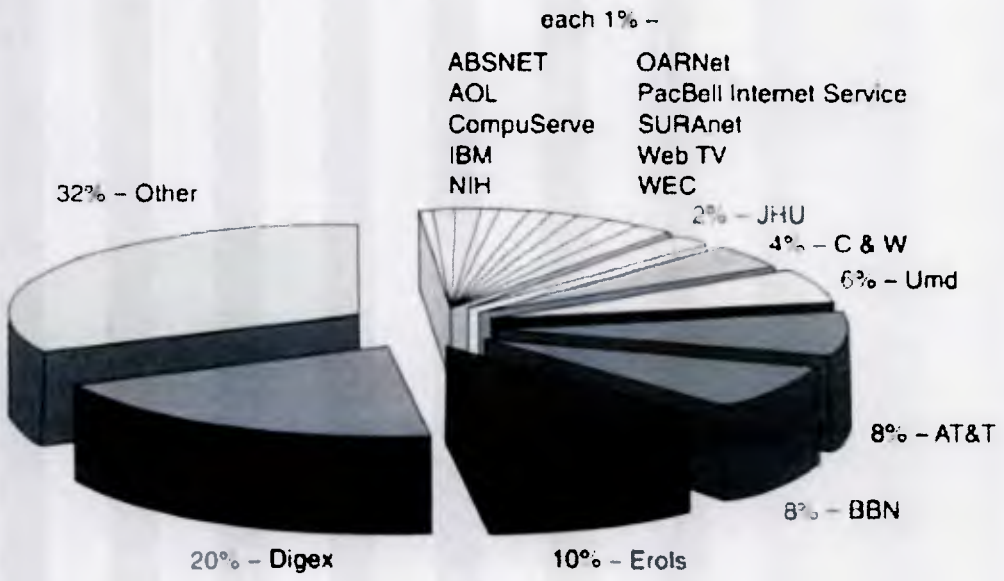

Figura 13. Planificación de capacidad. Fuente: (Barry, 2002)

El Netflow puede ser usado para planificar las redes debido a que se puede calcular la cantidad de recursos que cada aplicación utiliza de la red corporativa. Con esos cálculos es posible decidir las acciones específicas que deben ser tomadas para tratar a cada una de ellas (las aplicaciones), así como las políticas de seguridad y acceso en cada dispositivo de red.

(Solie, 2003) asegura en su libro sobre redes CISCO que *NETFLOW* permite recolectar y almacenar el conteo de la data IP transmitida sobre una red, y que puede ser usado, entre otras cosas, para realizar la facturación correspondiente a la utilización de la red.

Netflow rastrea información acerca de los flujos de paquetes IP. Estos flujos se rastrean organizándolos por protocolo, por usuario, por puerto, y por tipo de servicio.

Debido a que la data recolectada por el Netflow se almacena en la memoria de los dispositivos de red, esta herramienta incrementa la carga de procesamiento y de memoria de los mismos. Normalmente, un flujo de Netflow requiere 64 bytes de memoria. Por tanto, si se almacenan los 65536 flujos que por defecto pueden ser almacenados, se requiere una memoria DRAM de 4 MB.

Para optimizar el funcionamiento del protocolo se utiliza el *Cisco Express Forwarding*, el cual se usa para balancear la carga de paquetes, lo cual permite que los paquetes que tengan la misma dirección destino serán enviados siempre a través de la misma ruta, con lo cual se garantiza que los paquetes lleguen a su destino en el mismo orden en el que fueron transmitidos. Sin embargo, existen otros tipos de balanceo de carga que son utilizados por el Netflow, tales como el balanceo por paquete. De este párrafo se extrae que Netflow no solo permite monitorear el flujo de información que se transmite a través de una red, sino que adicionalmente establece una forma de enrutar y conmutar paquetes / tramas a su paso por un enrutador o un conmutador respectivamente.

Según se extrae de las ideas plasmadas en el White Paper sobre Netflow, publicado por (Cisco Systems, Mayo 2012), el Cisco Netflow analiza todos los paquetes que atraviesan una red en busca de ciertos parámetros de sus encabezados que le indiquen a la herramienta si el paquete es similar o diferente a otros que ha analizado previamente. Dicen que se busca principalmente siete parámetros, lo cuales se mencionan a continuación.

- Direcciones de IP origen.
- Direcciones IP de destino.
- Puertos capa 4 origen.
- Puertos capa 4 destino.

- Protocolo de capa 3 encapsulado en la trama.
- Clase de servicio.
- Interface del enrutador o conmutador a través de la cual fue recibida la trama.

Al igual que fue mencionado previamente para el caso de la conmutación y el enrutamiento de tramas, todas las que poseen parámetros similares son agrupados y puestos en una cola para ser procesados. Informan también que mediante este procedimiento se puede manejar una gran cantidad de información ya que todos los aspectos analizados son almacenados en una base de datos denominada Netflow cache.

La data se puede obtener de dos formas diferentes: usando la línea de comandos de los enrutadores y conmutadores Cisco o utilizando un servidor de recolección de data denominado Netflow Collector, el cual tiene por función, de acuerdo con el autor del documento, ensamblar, analizar y entender los flujos exportados por Netflow, para poder realizar reportes utilizables en el análisis del tráfico y la seguridad de las redes.

A diferencia de SNMP, Netflow continuamente busca la información contenida en la base de datos referida con anterioridad, para exportar esa data al Netflow Collector.

Un reporte se crea mediante los siguientes pasos:

- Netflow está configurado para capturar paquetes y tramas.
- Netflow está configurado para enviar flujos al colector.
- Netflow es interrogado acerca de los flujos almacenados en su base de datos.
- Aproximadamente treinta (30) a cincuenta (50) flujos son almacenados juntos y enviados hacia el servidor en un segmento UDP.
- El servidor crea un reporte en tiempo real o de un histórico basándose en la data recibida.

Para mantener la eficiencia de la red Netflow debe ser instalado y configurado en el sitio central de la red debido entre otras razones a que es en ese sitio en el que confluyen los datos generados por todos los sitios remotos. Sin embargo, advierten que la localización del Netflow depende también de la topología de la red y de la localización física de los servidores de monitoreo. Dicen que lo más óptimo debe ser instalar el Netflow en la locación más cercana a esos servidores. En la

Figura 14 se muestra un ejemplo sobre la localización de Netflow, recomendada por los autores del documento que se está utilizando como guía para el desarrollo de esta sección.

Figura 14. Localización de Netflow en una red. Fuente: (Cisco Systems, Mayo 2012)

En la Figura II-13 se propone que el Netflow sea habilitado en los conmutadores de frontera de la red, es decir, en su salida hacia las redes externas (las redes del ISP).

A través de esos conmutadores o enrutadores pasa todo el tráfico de la red destinado a redes externas, como la de la mencionada Figura, se organizan según una jerarquía:

- Acceso: es el nivel más bajo de las redes. En este nivel se conectan los dispositivos finales, generadores del tráfico de la red.
- Distribución: posee mayor capacidad (velocidad) de conmutación.
- Núcleo: es el backbone de las redes, se conectan con redes externas.

El *Netflow* debería ser habilitado en los dispositivos de backbone ya que son éstos los que poseen una visión completa del tráfico transmitido por las redes hacia el exterior.

En otra publicación de Cisco, (Cisco Systems, 2007), en la cual se realiza un análisis técnico sobre el *Netflow*, tratando aspectos especialmente relacionados con el uso de CPU obtenido con *Netflow*, se menciona que, para reducir el consumo de CPU y la utilización de recursos del dispositivo de red, se puede realizar un muestreo aleatorio de los paquetes y tramas que serán analizados por el *Netflow*. En este caso, según los autores del trabajo de investigación referido, sólo una porción de las tramas y paquetes conmutados por el elemento de red son utilizados para crear un flujo de datos utilizable por *Netflow* para el análisis de red. Establecen, en el mismo orden de ideas, que muchos administradores de red configuran el análisis de 1/100 tramas o de 1/1000 tramas con el objetivo de aumentar la eficiencia de la planificación. Basándose en las pruebas realizadas por el fabricante, (Cisco Systems, 2007) aseguran que cuando se usa la modalidad de 1/100 tramas, aproximadamente un 8'% del flujo de datos será convertido en un flujo de *Netflow*.

Cisco dispone varias plataformas de hardware. Los conmutadores se delimitan dentro de la plataforma *Catalyst,* la cual posee distintas series de conmutadores, tales como la 2900, 3700, 4500 y 6500.

La plataforma *Cisco Catalyst 6500* (una serie de conmutadores capa 3 de construcción modular) utiliza la modalidad de Muestras de Flujos, en la cual sólo se envía hacia el colector de la data una muestra del total de flujos de Netflow almacenados en la base de datos Netflow cache, con lo cual, según explican los autores, se reduce la utilización de CPU del conmutador así como también se reduce la utilización de la red para cuestiones de gestión y monitoreo.

En la Figura 15 se muestra el porcentaje adicional de uso que *Netflow* requiere en cuanto a recursos de CPU según la plataforma utilizada. Los autores de (Cisco Systems, 2007) dicen que las gráficas mostradas en la próxima figura fueron obtenidas después de realizar dos actividades:

- Obtener el promedio de utilización de CPU cuando se ejecutó el Netflow en cada una de las plataformas que aparecen en la figura siguiente.
- Restar ese promedio total del uso que el sistema operativo de la plataforma hace del procesador de los dispositivos de red.

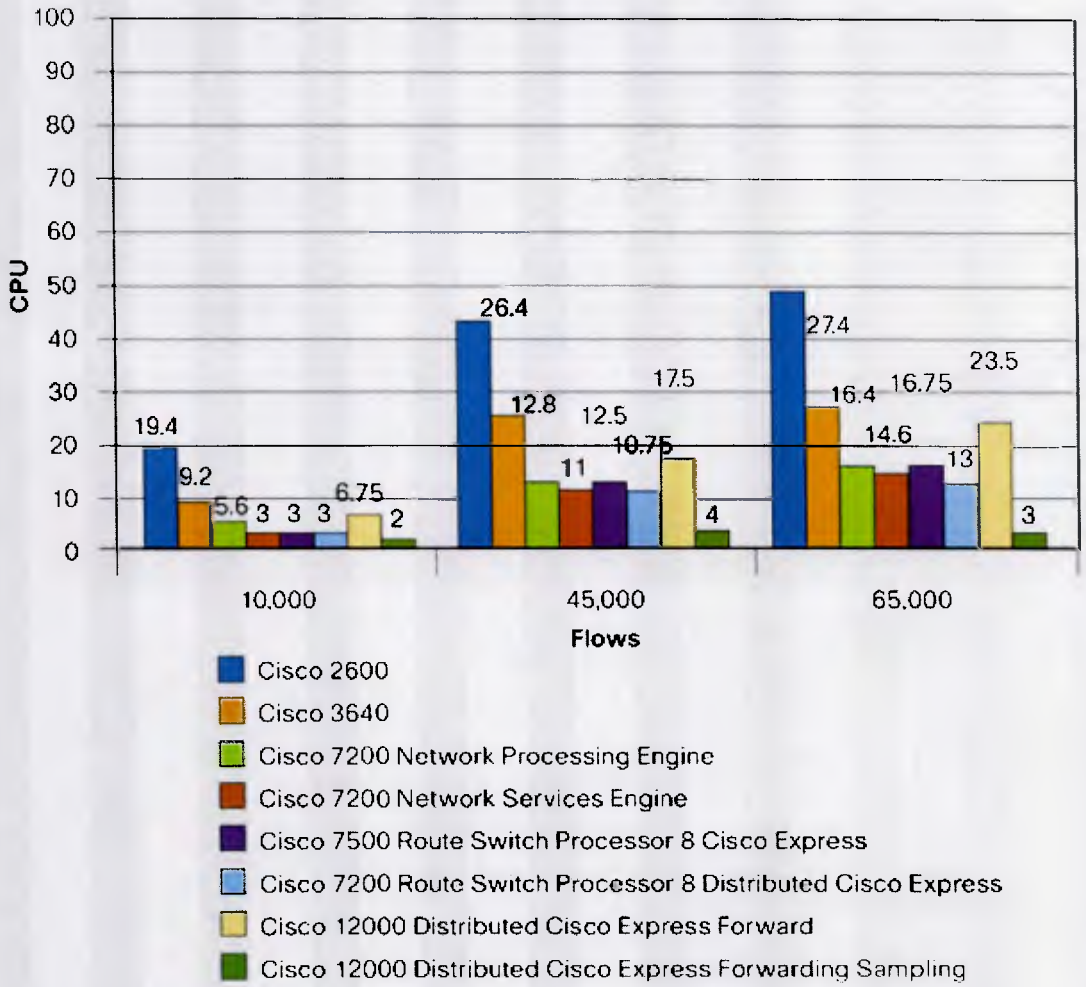

Figura 15. Utilización de recursos por plataforma. Fuente: (Cisco Systems, 2007)

En la Figura 15, todos los elementos mostrados son enrutadores pertenecientes a alguna de las plataformas desarrolladas por CISCO debido a que,

como se menciona en las obras presentadas como fuentes de esta investigación teórica, son los elementos que más comúnmente se utilizan como concentradores del tráfico en una red de datos. El único dispositivo que no es enrutador es el CISCO 3640, el cual es un conmutador capa 3, perteneciente a la plataforma Catalyst, modular, que se utiliza como un concentrador de datos en redes de gran extensión, y que permite distribuir toda la data recolectada de grandes hacia enrutadores de gran capacidad, para enviarlos hacia otras redes o hacia algún proveedor de servicios.

Dicen los autores del estudio publicado por (Cisco Systems, 2007) que, aunque el uso de *Netflow* basado en muestras no represente un gran impacto en el tráfico de red, sí puede representar una diferencia significativa en cuanto a los requerimientos de hardware que la herramienta hace del dispositivo de red en el que se encuentra instalada, de acuerdo con las características de la plataforma.

En (Cisco Systems, 2007) también opinan que el *Netflow* basado en muestras debe ser usado en sólo algunos casos y aplicaciones tales como Ingeniería de Tráfico y Planificación de Redes, pero dicen que de todas formas esta decisión debe ser realizada por los administradores y gerentes de redes en las empresas tomando en cuenta las plataformas con las que cuentan entre sus activos y tomando en cuenta la función con la que se usará el *Netflow*.

II.3. Topología

Para el desarrollo del proyecto se considera necesaria la implementación de una topología de prueba en la cual pueda ser configurada la herramienta *Netflow*, así como probados cada uno de sus parámetros y características.

Como se mencionó en la sección anterior, el lugar ideal para habilitar el *Netflow* en una red es el conmutador o el enrutador de borde, que conecta la red de la empresa con otras redes. Esto se debe a que el *Netflow* añade una carga de procesamiento elevada a los dispositivos de red, que puede ralentizar su operación.

Existe una razón más práctica y tangible para hacer esta afirmación: su habilitación en el dispositivo de borde de la red permite que se monitoreen todo el

tráfico de la red, ya que cuando se quiera acceder a recursos que están localizados fuera de ella, todo el tráfico debe pasar a través de estos dispositivos.

En la Figura 16 se muestra el esquema que será desarrollado en este Trabajo Especial de Grado.

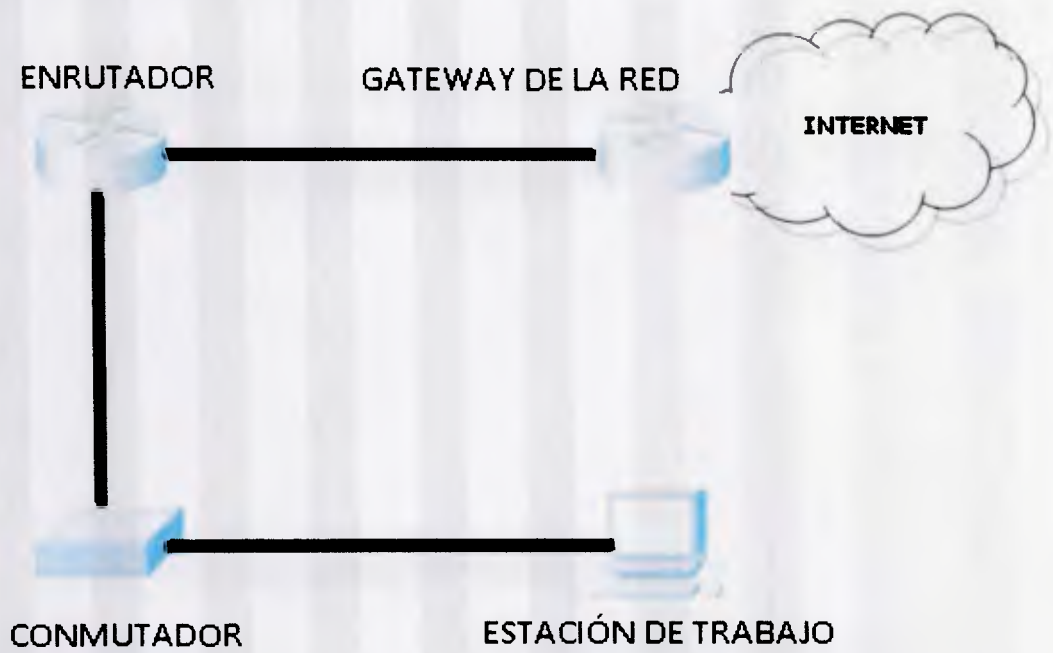

Figura 16. Topología del proyecto. Fuente: propia

En la Figura 16se observa la presencia de los siguientes dispositivos:

Tabla 2. Dispositivos a utilizar en el proyecto. Fuente: propia

DISPOSITIVO	CANTIDAD	USO
ENRUTADOR	1	RED LAN
		GATEWAY
	1	ISP
CONMUTADOR	1	RED LAN

ESTACIÓN DE TRABAJO	1	CONFIGURACIÓN DE DISPOSITIVOS DE RED

En la Tabla 2se observa la función de cada uno de los dispositivos mostrados en la Figura 16. El *Netflow* será habilitado y configurado en el enrutador que funciona como *Gateway* de la red, al cual se conecta la estación de trabajo que se aprecia en esa Figura debido a las siguientes razones:

- El router *Gateway* funciona como el *Gateway* de la red de las empresas al enrutar el tráfico hacia otras redes externas, tal como la red del proveedor de servicios. Es el punto de acceso al enlace contratado.
- Todo el tráfico destinado al proveedor de servicios debe pasar por este enrutador.
- Se trata de un punto de concentración en el cual se puede obtener la información sobre todo el uso que se haga de la red, tanto de tráfico saliente como tráfico entrante.

La Figura II-12 será usada sólo para configurar el Netflow en el enrutador de Gateway. Con la topología que se presenta en la Figura 17 se podrá exportar la data generada por la herramienta hacia un servidor de monitoreo externo.

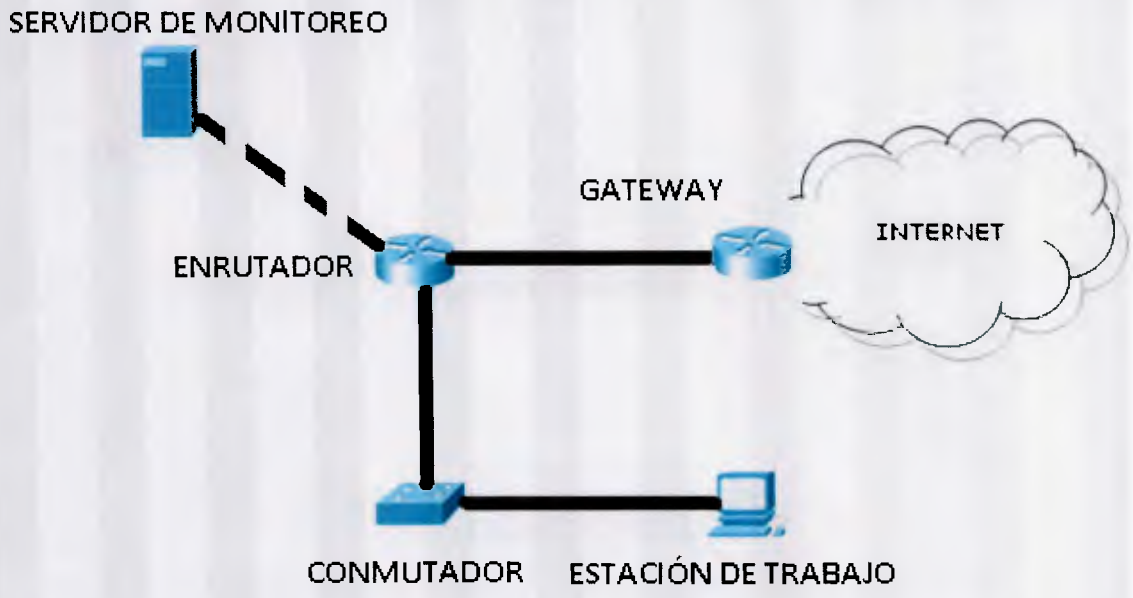

Figura 17. Topología con exportación de data. Fuente: propia

El servidor que se muestra en la Figura 17 recibirá la data exportada por el enrutador que ejecuta el *software Netflow* y podrá ser utilizado en futuros desarrollos (fuera del alcance del proyecto) para alojar una aplicación que permita obtener de forma gráfica los valores arrojados por el Netflow.

En la Tabla 3 se muestran los aspectos que deben ser configurados en cada uno de los dispositivos que forman la topología mostrada en la Figura II-13.

Tabla 3. Configuración necesaria en dispositivos de red. Fuente: propia

DISPOSITIVO	CONFIGURACIÓN
ENRUTADOR	CONFIGURACIÓN DE RED
	NETFLOW
	EXPORTACIÓN DE DATA
CONMUTADOR	CONFIGURACIÓN DE RED
ESTACIÓN DE TRABAJO	EMULADOR DE TERMINAL
	GENERADOR DE TRÁFICO
SERVIDOR	BASE DE DATOS MySQL
	CLIENTE DE MySQL

En el capítulo III se desarrolla el Marco Metodológico a aplicar durante la ejecución del presente Trabajo Especial de Grado.

Capítulo III MARCO METODOLÓGICO

El capítulo Marco Metodológico se divide en dos secciones. En la primera de ellas se selecciona el tipo de investigación que será realizado, así como también será justificada esta elección.

La segunda sección presenta la metodología o procedimiento que será realizado con el fin de cumplir con los objetivos establecidos en la sección I.2 "Objetivos".

III.1. Tipo de investigación

De acuerdo a los objetivos planteados anteriormente, los siguientes tipos de investigación serán aplicados en la ejecución del Trabajo de Grado.

Tabla 4. Tipos de investigación aplicables al Trabajo de Grado. Fuente: propia

CLASIFICACIÓN	INVESTIGACIÓN
CARÁCTER	SIMULACIÓN
	DOCUMENTAL
EXPLORATORIA	
FACTIBLE	
DE CAMPO	

Para la consecución de los objetivos del proyecto se debe realizar una profunda investigación teórica sobre el funcionamiento y los valores arrojados por la herramienta bajo estudio. Se debe, así mismo, realizar una prueba piloto en las condiciones que más se ajusten a las redes corporativas, en la cual se pueda poner en práctica lo obtenido de la investigación teórica. Por todo, ello el proyecto se propone como una investigación documental, exploratoria, factible, de simulación y de campo.

III.1.1. Investigación documental

Para la realización del Trabajo Especial de Grado se deben consultar obras relacionadas con el Cisco IOS Netflow debido a que se deben investigar una serie de aspectos relacionados con él.

Adicionalmente, se debe conocer el funcionamiento de la misma, sus actividades, procedimientos, así como las variables que es capaz de entregar.

Se debe realizar un estudio sobre qué actividades y procedimientos deben ser realizados para configurar la herramienta, así como los comandos necesarios para esto.

Adicionalmente se deben realizar un estudio sobre los dispositivos en los cuales se puede habilitar la herramienta y su ubicación en la red de las empresas en comparación con los demás elementos de la misma.

Se requiere también una serie de conocimientos sobre otros aspectos tales como el acceso a las bases de datos y la manipulación de la información contenida en ellas.

III.1.2. Investigación de simulación

El Trabajo de Grado será dividido en dos partes principales:

- Activación y configuración del Cisco Netflow en los dispositivos de red de la topología mostrada en la sección II.3 "Topología".
- Transmisión de tráfico de red real sobre la topología de prueba implementada en la sección II.3 "Topología".

La primera parte del trabajo exigirá la simulación de una red mediante la implementación de la topología mostrada en la sección II.3 "Topología". Esta simulación será realizada en dos partes:

- La primera parte de la simulación será realizada mediante el *software* de simulación de redes *CISCO PACKET TRACER*, en el cual será simulado el direccionamiento y enrutamiento necesarios en la topología.

- La segunda parte consistirá en la implementación de la topología a desarrollar en este Trabajo de Grado.

A pesar de que se trata de una implementación sobre equipos reales, el autor de estas líneas considera que se trata también de una simulación debido a que a través de esa topología será transmitido tráfico que permitirá probar las configuraciones que se lleven a cabo sobre la herramienta.

III.1.3. Investigación exploratoria

(Ferrer, 2012) afirma que las investigaciones exploratorias se dan en las primeras fases de cualquier investigación.

Se basa en la obtención de información que pueda servir para la consecución de los objetivos planteados.

Se busca información específica, según un modelo estructurado que permite obtener los datos necesarios para el desarrollo de la investigación. Puede ser comparado al guión que se prepara para el desarrollo de una entrevista a una persona.

El objetivo fundamental de las investigaciones exploratorias consiste en obtener ideas que permitan desarrollar los objetivos que persigue la investigación.

Este tipo de investigación será aplicado en las fases iniciales del Trabajo de Grado para la obtención de información sobre:

- Configuración de Netflow en los enrutadores.
- Formato de la data generada por el Netflow para su uso en un servidor de monitoreo.
- Configuración de la estructura de datos adecuada para el procesamiento de la información obtenida del Netflow.

III.1.4. Investigación de tipo factible

La (Universidad Católica Andrés Bello, 2007) afirma que una investigación de tipo factible se trata de proveer soluciones específicas a un problema

determinado después de que un proceso de investigación ha sido desarrollado en profundidad.

Se afirma en la obra que este tipo de investigación implica investigar sobre el tema elegido, explorar su funcionamiento, describir el problema que se ha planteado y proponer posibles soluciones.

Se establece también que estas investigaciones no necesariamente deben tener como producto final la implementación de las soluciones que se planteen.

Normalmente se divide en dos partes:

- Una parte descriptiva que pretende estudiar el fenómeno de investigación para determinar las necesidades del hecho a investigar.
- Una fase proyectiva que implica el desarrollo de un modelo que permita satisfacer las demandas de la situación investigada.

El Trabajo de Grado dispondrá de las dos fases de este tipo de investigación. La fase descriptiva consistirá en el estudio de Netflow para obtener aspectos específicos del estándar tales como el formato con el que la data generada se transmite hacia los servidores de monitoreo, e incluirá otros aspectos más operativos tales como, por ejemplo, los procedimientos necesarios para configurar la herramienta de monitoreo en los dispositivos seleccionados, así como también para observar la información recolectada por ésta.

En el caso particular del Trabajo de Grado, sí se realizará la implementación de las soluciones que se planteen a la problemática planteada. Se analizarán los datos arrojados por la herramienta y se propondrá la realización de una herramienta de monitoreo y gestión como parte de otros trabajos futuros.

III.1.5. Investigación de campo

(Muñoz, 1998) afirma que en las investigaciones de campo todas las actividades se desarrollan en el ambiente en el cual se desenvuelven los fenómenos y situaciones que se investigan.

Los resultados de este tipo de investigaciones suelen estar complementados con un estudio documental que permitan sustentar con una base teórica los aspectos que se presentan.

Las investigaciones de campo que se aplican a estudios sobre sistemas informáticos y de red suelen presentar sus resultados en una profunda investigación documental previa que permita justificar cada una de las soluciones que se presente en un análisis teórico.

El proyecto se enmarca dentro de una investigación de campo ya que busca, mediante las investigaciones mencionadas anteriormente, obtener una serie de datos relacionados con el Netflow para, sin manipularlos ni modificarlos, analizarlos y proponer soluciones a los posibles comportamientos que presenten, así como proponer la herramienta que se ha planteado.

Una parte muy importante del Trabajo de Grado será la obtención de la data generada por el Netflow (en la forma de un monitoreo del tráfico TCP/IP) debido a que el fin último del proyecto será su análisis para presentar soluciones como base de los reportes que puedan ser generados a partir del mismo.

La única forma de conocer el funcionamiento de la herramienta así como el formato de la data generada por ella es recolectando la data transmitida a través de la red. Adicionalmente, la única forma de cumplir con lo expresado en párrafos anteriores es configurando el Netflow en un ambiente de laboratorio y capturando la data que genera.

Sin estas actividades, las investigaciones presentadas con anterioridad no servirían de nada ya que se tratará de una simple recolección de datos sin un objetivo distinto al académico. Para que la recolección de información que se planteó tenga sentido práctico es necesario que se realice la recolección de datos que se obtiene con las investigaciones de campo ya que es ella la que permite aplicar la teoría en una solución práctica.

III.2. Metodología

La presentación de los resultados del proyecto se dividirá en dos partes que se listan en la siguiente tabla:

Tabla 5. Actividades generales del proyecto. Fuente: propia

PARTE	TEMA	ACTIVIDAD
Investigación teórica	Netflow	Funcionamiento
		Configuración
Simulación	Netflow	Direccionamiento de red
		Configuración de Netflow.
		Exportación de data.

Cada una de las actividades presentadas en la tabla III.2 se basa en los objetivos específicos presentados en la sección I.3 "Objetivos". Cada uno de los objetivos específicos planteados exige la realización de una serie de actividades.

El primer objetivo específico mencionado en la sección I.3.2 "Objetivos específicos" incluye la realización de las siguientes actividades:

Tabla 6. Objetivo específico número uno. Fuente: propia

OBJETIVO ESPECÍFICO NÚMERO 1	ACTIVIDADES
Realizar un estudio teórico sobre Netflow	Estudiar los elementos de la herramienta Cisco Netflow.

OBJETIVO ESPECÍFICO NÚMERO 1	ACTIVIDADES
	Estudiar otras herramientas que utilicen Netflow como base de su funcionamiento.
	Estudiar el funcionamiento de la herramienta Cisco Netflow.
	Estudiar el formato de los mensajes generados por Cisco Netflow.
	Estudiar las variables monitoreadas por la herramienta Cisco Netflow.

El primer objetivo específico es un objetivo de estudio. Consiste en el estudio de la herramienta Netflow, sus elementos, su arquitectura, su funcionamiento, así como también algunas aplicaciones que se basan en ella. Permite conocer cuáles son las bondades y características del Netflow que serán útiles para el desarrollo del proyecto que se plantea en este documento.

El segundo objetivo específico se trata sobre la configuración de Netflow e incluye las siguientes actividades:

Tabla 7. Objetivo específico número dos del proyecto. Fuente: propia

OBJETIVO ESPECÍFICO NÚMERO DOS	ACTIVIDADES
Habilitar Netflow en un enrutador y en un conmutador	Habilitar el Netflow en el enrutador de la topología mostrada en la sección II.3 "Topología"
	Habilitar Netflow en el conmutador de la topología mostrada en la sección II.3 "Topología"

Este objetivo tiene por función habilitar el Netflow en los enrutadores y conmutadores de la topología a desarrollar en este proyecto, en las interfaces adecuadas para los efectos de este Trabajo Especial de Grado.

El tercer objetivo específico prevé la configuración del Netflow en los enrutadores y conmutadores, y sus actividades se muestran en la siguiente tabla:

Tabla 8. Objetivo específico número tres del proyecto. Fuente: propia

OBJETIVO ESPECÍFICO NÚMERO TRES	ACTIVIDADES
Configurar Netflow en un enrutador y en un conmutador	Configurar una interface para capturar el tráfico entrante o saliente.
	Activar el filtro para distinguir entre protocolos, puertos y direcciones origen y destino en los flujos.
	Exportar la data obtenida hacia una dirección externa

Este objetivo tiene como función configurar el Netflow con todos los parámetros necesarios para que pueda capturar el tráfico que pasa a través de las interfaces en las cuales se encuentre habilitado. También se pretende exportar la data capturada por el protocolo en las interfaces hacia un servidor externo en el cual se pueda recuperar esa data y utilizarla para los fines planteados en el siguiente objetivo específico, cuyas actividades se muestran en la siguiente tabla:

Tabla 9. Objetivo específico número cuatro. Fuente: propia

OBJETIVO ESPECÍFICO NÚMERO CUATRO	ACTIVIDADES
	Diseño de un esquema de red que pueda ser utilizado en una red

Diseñar e implementar una topología de red de prueba.	corporativa. Debe incluir una simulación para probar conectividad de red.
	Implementación del esquema mediante el uso de dispositivos de red del fabricante Cisco. Se debe incluir la conexión de cada uno de ellos mediante la utilización de los cables adecuados.

Tabla 10. Objetivo específico número cinco. Fuente: propia

OBJETIVO ESPECÍFICO NÚMERO CUATRO	ACTIVIDADES
Analizar los resultados obtenidos de las pruebas realizadas.	Recopilar la data arrojada por la herramienta Netflow. Clasificarla de acuerdo a los parámetros más convenientes.
	Análisis e interpretación de la data recopilada..

Con este objetivo específico se pretende dar cumplimiento al objetivo general del proyecto, es decir, éste es el objetivo que inspira la ejecución de este Trabajo Especial de Grado.

En la Tabla 11 se muestra la duración estimada que tendrá cada una de las actividades que han sido mencionadas a lo largo de esta sección del documento.

Tabla 11. Duración estimada de las actividades. Fuente: propia

ACTIVIDAD	SEMANAS
Estudiar los elementos de la herramienta Cisco Netflow.	3
Estudiar otras herramientas que utilicen Netflow como base de su funcionamiento.	
Estudiar el funcionamiento de la herramienta Cisco Netflow.	
Estudiar el formato de los mensajes generados por Cisco Netflow.	
Estudiar las variables monitoreadas por la herramienta Cisco Netflow.	
Habilitar el Netflow en el enrutador de la topología mostrada en la sección II.3 "Topología"	4
Habilitar Netflow en el conmutador de la topología mostrada en la sección II.3 "Topología"	
Configurar una interface para capturar el tráfico entrante o saliente.	
Activar el filtro para distinguir entre protocolos, puertos y direcciones origen y destino en los flujos.	
Recolección de la data capturada por Netflow.	3
Análisis de la data capturada por Netflow.	2
Obtención de conclusiones y soluciones a partir de la data capturada por la herramienta Netflow.	6

Como se observa en la Tabla 11, el proyecto cuya realización se propone en este documento tiene una duración estimada de 18 semanas, lo cual supone una duración aproximada de dos trimestres académicos.

En la siguiente página se observa en forma gráfica el desarrollo temporal que el autor de estas líneas estima tendrá cada una de las actividades mostradas en la Tabla 11.

En esa página se observa que existe una actividad extra, que no se muestra en la tabla III.7, la cual es la escritura del documento final del Trabajo Especial de Grado.

La causa de que esta actividad se prolongue durante todo el período de tiempo es que, de esta forma, se permitirá que todos los detalles que vayan surgiendo durante la ejecución del problema sean considerados en el documento final.

Será además más fácil correlacionar los datos que vayan surgiendo durante la ejecución del proyecto con respecto al uso y configuración de la herramienta Netflow.

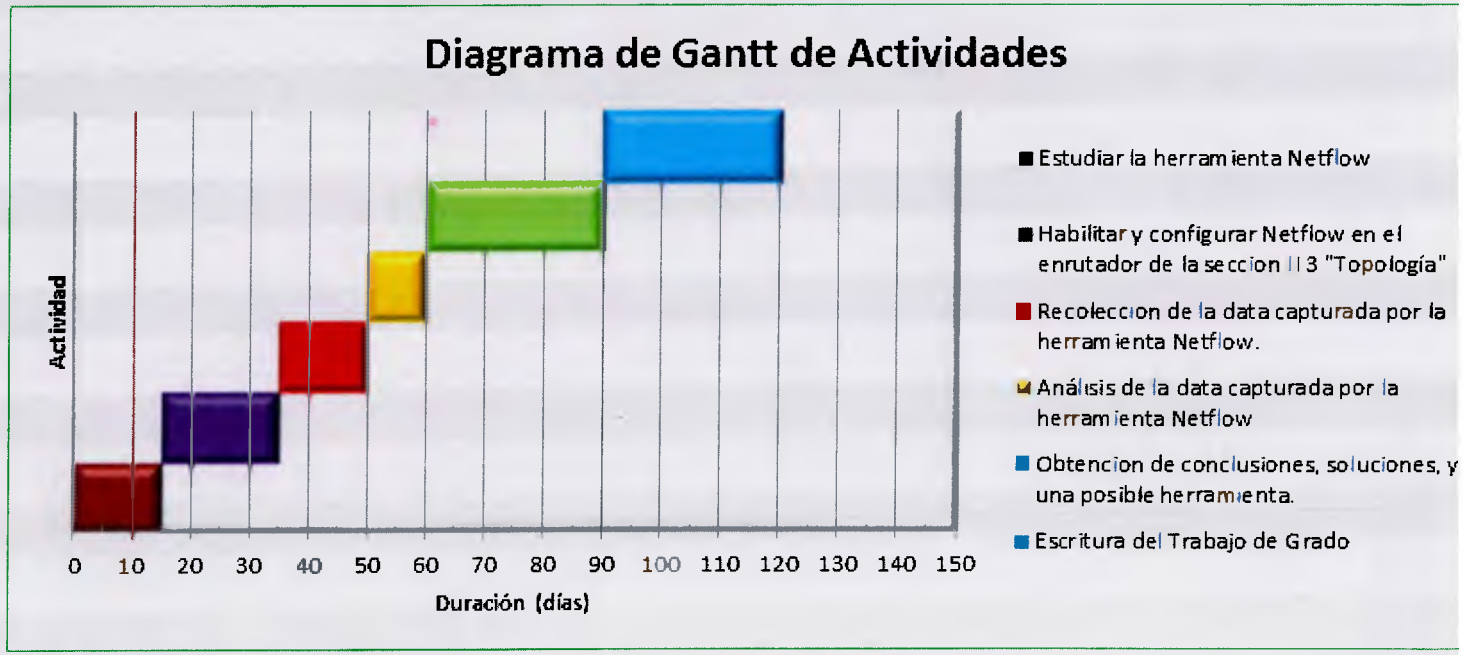

Figura 18. Diagrama de Gantt del proyecto. Fuente: propia

En la Tabla 12 se muestra la lista de actividades mostradas en la figura III.8, así como los períodos de validez para cada una de ellas.

Tabla 12. Lista de actividades del proyecto. Fuente: propia

Nombre de la tarea	Duración
Estudiar la herramienta Netflow	15 días
Habilitar y configurar Netflow en el enrutador de la sección II.3 "Topología"	20 días
Recolección de la data capturada por la herramienta Netflow.	15 días
Análisis de la data capturada por la herramienta Netflow	10 días
Obtención de conclusiones, soluciones, y una posible herramienta.	30 días
Escritura del Trabajo de Grado	30 días

Para el desarrollo del Trabajo de Grado serán seguidas las consideraciones éticas establecidas en el (Colegio de Ingenieros de Venezuela, 2012), especialmente las siguientes:

- "Artículo 2 (ilegalidad): Violar o permitir que se violen las leyes, ordenanzas y reglamentaciones relacionadas con el cabal ejercicio profesional."
- "Artículo 18 (autoría): Utilizar estudios, proyectos, planos, informes u otros documentos, que no sean el dominio público, sin la autorización de sus autores y/o propietarios."
- "Artículo 19 (secreto): Revelar datos reservados de índole técnico, financiero o profesionales, así como divulgar sin la debida autorización, procedimientos, procesos o características de equipos protegido por patentes o contratos que establezcan las obligaciones de guardas de secreto profesional. Así como utilizar programas, discos, cintas u otros medios de información, que no sea de dominio público, sin la debida autorización de sus autores y/o propietarios, o utilizar sin autorización de códigos de acceso de otras personas, en provecho propio."

Capítulo IV PROCEDIMIENTO APLICADO

Para el desarrollo del Trabajo de Grado instaló y configuró una topología de prueba cuya arquitectura se muestra en la Figura 19.

Fueron utilizados los siguientes dispositivos y elementos consumibles:

- Enrutador: Cisco 2900.
- Conmutador: Cisco 2950 y Cisco 1900.
- Cable serial con reloj conectado en fábrica.
- Cables UTP categoría 5E directos.

En el 0 "**DISPOSITIVOS Y MATERIALES UTILIZADOS**" será presentada una referencia de todos los dispositivos y cables utilizados.

Mediante el procedimiento que será explicado en las diferentes secciones del capítulo se pretende simular el tráfico de red de una empresa formada por dos sedes, conectadas mediante una topología de estrella a un enrutador principal que actúe como punto de concentración del tráfico proveniente de ambas; punto de entrada y salida a la red; así como punto de conexión con los diferentes ISP que la empresa tenga contratados.

Es en este enrutador central donde será habilitado y configurado el Netflow ya que, como se explicó en la sección II.2.3, Figura 14, el protocolo debe ser habilitado en los enrutadores de backbone. Se debe recordar que un enrutador de backbone, entre otras, tiene como función ser el punto de salida hacia redes externas, de forma que todo el tráfico saliente de la red pase por él. Uno de los objetivos que se tiene en cuenta al habilitar Netflow en una red es precisamente, de acuerdo a la sección I.4, contabilizar el tráfico saliente de la red hacia los enlaces externos contratados a los diferentes ISP.

IV.1. Topología

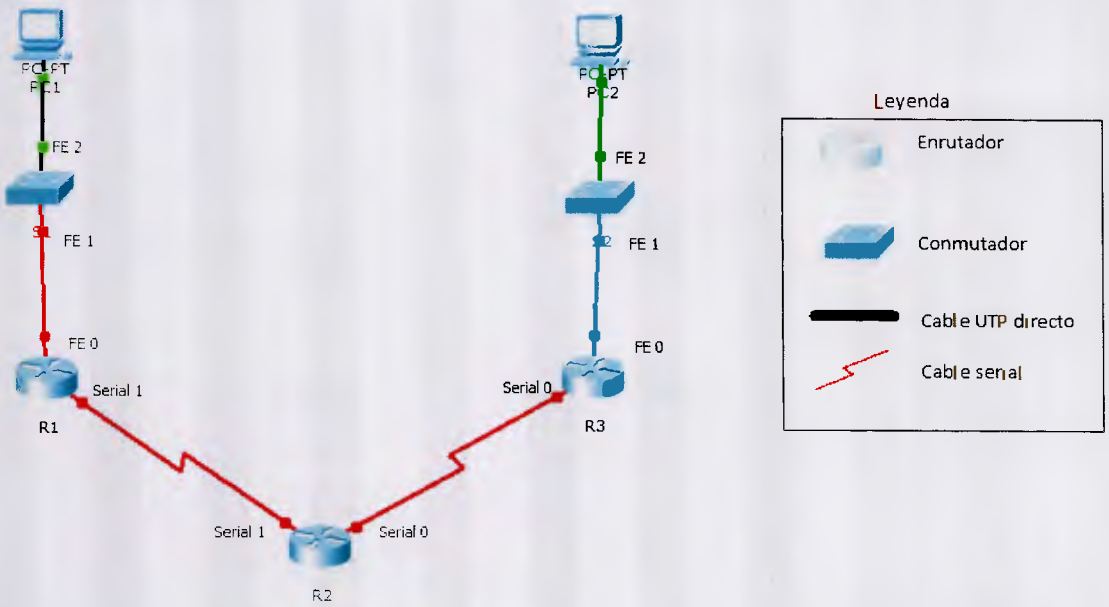

Figura 19 Topología utilizada durante la fase de pruebas

La topología mostrada en la Figura 19 fue montada sobre un *boundle* estudiantil, el cual es un *rack* vendido por CISCO SYSTEMS a las academias autorizadas para impartir los cursos CCNA, preparados y distribuidos por la propia empresa.

Los *boundles* normalmente están formados por tres enrutadores y tres conmutadores, de la serie elegida por cada academia. Fueron diseñados para que los estudiantes de las distintas academias puedan desarrollar las topologías de práctica establecidas en los distintos laboratorios de redes diseñados por CISCO SYSTEMS para los cursos CCNA.

Debido a que sólo se requerían dos conmutadores para realizar la prueba del Trabajo de Grado, el tercer conmutador fue removido de la configuración, la cual se muestra en la Figura 20.

Figura 20 Rack móvil de dispositivos de red

El enrutador superior fue llamado Sede_1, el enrutador del medio ISP, y al enrutador inferior se le dio el nombre de Sede_2.

En la Figura 21 se muestra la conexión de los cables seriales entre los tres conmutadores, así como de los cables UTP entre los conmutadores y los enrutadores.

Figura 21 Vista de la conexión entre dispositivos

En la Figura 22 se observa la conexión de un PC a un dispositivo de red (tanto enrutador como conmutador) mediante el uso de un cable serial de consola, el cual se observa en la Figura 23.

Figura 22 Vista de la conexión de una computadora al conmutador

Figura 23 Cable serial de consola

La conexión entre los enrutadores fue realizada a través de cables seriales, como se aprecia en la Figura 19. En la Figura 24 se aprecia una vista de los cables seriales utilizados durante la fase de pruebas del Trabajo de Grado.

Figura 24 Cable serial

IV.2. Configuración de red

Una vez realizada la instalación de la topología según las imágenes mostradas en la sección IV.1, se realizó la configuración de red necesaria para que

los dispositivos mostrados en la Figura 19 (en general cualquiera que se conectase a la topología) tuvieran conectividad a nivel de red y pudieran intercambiar archivos y solicitudes entre ellos.

La configuración de red fue realizada en:

- PC.
- Enrutadores.
- Conmutadores.

IV.2.1. PC

Consistió en la configuración de la tarjeta de red con los parámetros de conectividad que ella soporta: dirección IP, máscara de sub-red y puerta de enlace predeterminada. A pesar de que las tarjetas de red instaladas en los PCs modernos soportan el protocolo DHCP (para obtener configuraciones de red de forma automática mediante el intercambio de una serie de mensajes con el servidor DHCP al cual se encuentren conectadas), debido a que éste no es el tema central del Trabajo de Grado (y no afectará ni cambiará los resultados finales del Trabajo su no utilización), la configuración fue realizada de forma manual.

En la Figura 25 se muestra la configuración de red de un PC conectado al primer enrutador (Sede_1).

La conexión del PC fue realizada al puerto FE 1 del conmutador 2950 mediante la utilización de un cable UTP directo, categoría 5E.

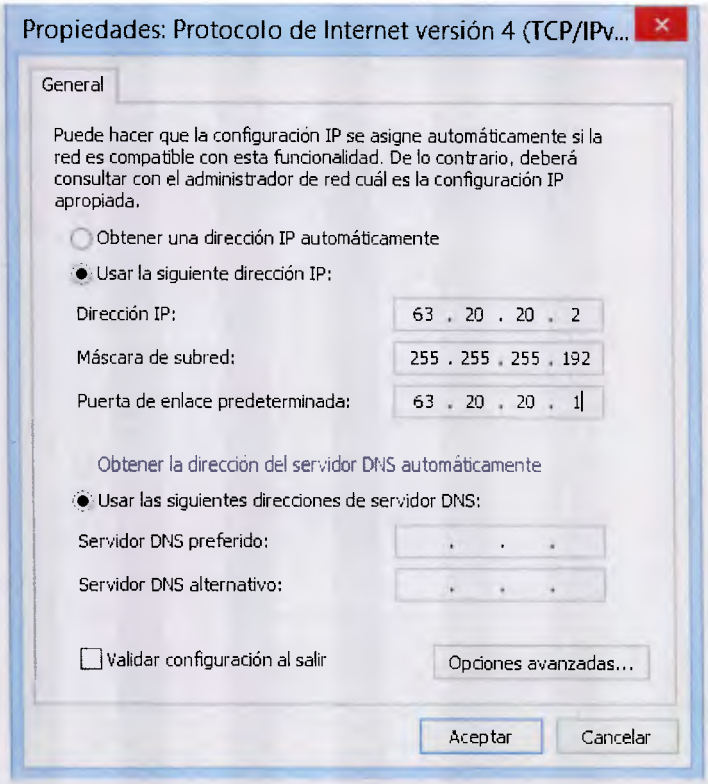

Figura 25 Configuración de red de la primera PC

Si se quisiera conectar más PC´s al enrutador Sede_1, se les podría asignar direcciones IP ubicadas en el rango 63.20.20.2 – 63.20.20.62, con máscara de sub-red 255.255.255.192, y puerta de enlace predeterminada 63.20.20.1 (tal como se muestra en la Figura 25.

En la Figura 26 se muestra la configuración de red de un PC conectado al tercer enrutador (Sede_2).

La conexión del PC fue realizada al puerto FE 1 del conmutador 1900 mediante la utilización de un cable UTP directo, categoría 5E.

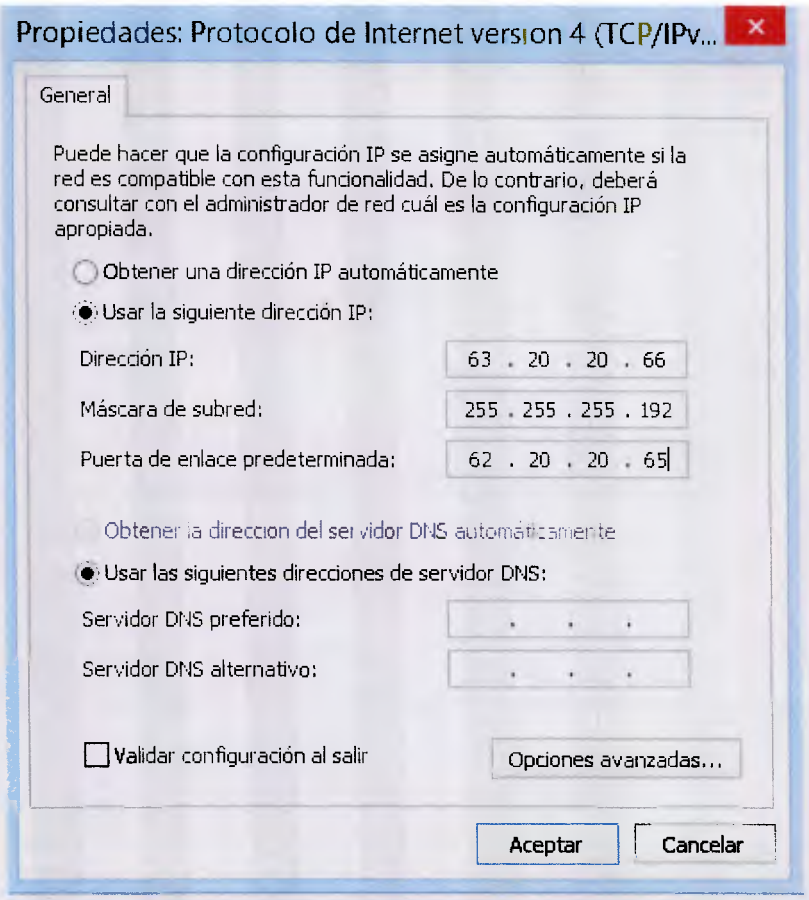

Figura 26 Configuración de red de la segunda PC

Si se quisiera conectar más PC´s al enrutador Sede_2, se les podría asignar direcciones IP ubicadas en el rango 63.20.20.67 – 63.20.20.190, con máscara de sub-red 255.255.255.192, y puerta de enlace predeterminada 63.20.20.65 (tal como se muestra en la Figura 26.

IV.2.2. Enrutador Sede_1

El enrutador Sede_1 se utiliza como punto de concentración del tráfico proveniente de la primera sede de la empresa cuyo tráfico fue simulado mediante esta topología.

Fueron cargadas dos configuraciones en este enrutador, a saber:

- Configuración básica: formada por nombre de host, claves de acceso a los modos de operación y direcciones IP en las interfaces a utilizar.

- Protocolo de enrutamiento: fue utilizado el protocolo de enrutamiento OSPF debido a que es un protocolo muy potente preparado para cursar una gran cantidad de tráfico y para soportar cambios frecuentes en las topologías.

En la Tabla 13 se muestra el contenido presente en el enrutador Sede_1 una vez configurado completamente, en lo que se denomina "Archivo de configuración en ejecución":

Tabla 13 Archivo de configuración del enrutador Sede_1

```
Current configuration : 1031 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Sede_1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Mo.g$2hEHphSCiFPC18RnjQoo81
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
no ip dhcp use vrf connected
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
```

```
speed auto
!
interface FastEthernet0/1
ip address 63.20.20.1 255.255.255.192
duplex auto
speed auto
!
interface Serial0/1/0
no ip address
shutdown
no fair-queue
clockrate 2000000
!
interface Serial0/1/1
ip address 10.15.32.2 255.255.255.252
clockrate 2000000
!
router ospf 1001
log-adjacency-changes
network 10.15.32.0 0.0.0.3 area 3000
network 63.20.20.0 0.0.0.63 area 3000
!
ip classless
!
ip http server
!
control-plane
!
line con 0
password ajiglesias_tesis_2013
login
line aux 0
line vty 0 5
password acceso_tesis_2013
login
!
end
```

En la Tabla 13 se aprecian los siguientes aspectos de la configuración:

- Contraseñas de los modos de operación: los dispositivos de red Cisco configurables por consola poseen diferentes modos de operación protegidos por contraseña para diferenciar las operaciones que se puede realizar, dando por resultado un incremento de la seguridad (al permitir o eliminar operaciones de acuerdo a los privilegios que se disponga).
- Información de direccionamiento: se muestran tanto las interfaces que no tienen información de red cargada como aquellas que sí la tienen. En las interfaces seriales se añade así mismo la velocidad de reloj configurada para el enrutador. Por un error de *software* (sin ningún tipo de incidencia sobre el funcionamiento del enrutador o sobre los resultados del Trabajo de Grado), el sistema operativo cargó también una velocidad de reloj para una interface serial sin información de direccionamiento.
- Protocolo de enrutamiento: como ya se dijo fue utilizado OSPF. El *software* del enrutador muestra tanto las redes a las que el protocolo le presta servicio como los parámetros de configuración del mismo (el área de enrutamiento y el número de sistema autónomo).
- Los servicios activados y desactivados en el enrutador.

IV.2.3. Enrutador Sede_2

El enrutador Sede_2 se utiliza como punto de concentración del tráfico proveniente de la segunda sede de la empresa cuyo tráfico fue simulado mediante esta topología.

Fue cargado con exactamente la misma configuración que el enrutador Sede_1, variando únicamente la información de direccionamiento de las interfaces y la información de enrutamiento en el protocolo OSPF.

En la Tabla 14 se muestra el contenido del Archivo de Configuración en Ejecución del enrutador Sede_2:

Tabla 14 Archivo de configuración del enrutador Sede_2

```
Current configuration : 995 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Sede_2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$qbhL$MWQFBdnsBSef6XyrW0Ezb.
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
no ip dhcp use vrf connected
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 63.20.20.65 255.255.255.240
duplex auto
speed auto
!
interface Serial0/1/0
ip address 10.15.32.6 255.255.255.252
!
```

```
interface Serial0/1/1
no ip address
clockrate 2000000
!
router ospf 1001
log-adjacency-changes
network 10.15.32.4 0.0.0.3 area 3000
network 63.20.20.64 0.0.0.15 area 3000
!
no ip classless
!
no ip http server
!
control-plane
!
line con 0
password ajiglesias_tesis_2013
login
line aux 0
line vty 0 5
password acceso_tesis_2013
login
!
end
```

IV.2.4. Enrutador ISP

El enrutador ISP posee, además de los parámetros observados en los enrutadores Sede_1 y Sede_2, la información de Netflow, y el módulo CEF habilitado (el cual, según se recordará de la sección II.2.3, se recomienda esté habilitado para reducir la carga de procesamiento a nivel de operaciones de red en el enrutador o conmutador donde el Netflow funcione).

Tabla 15 Archivo de configuración del enrutador ISP

```
Current configuration : 1344 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Lef6$xxE8cd7A86OX88Ekw1UbY.
!
no aaa new-model
ip cef
!
ip flow-cache entries 100000
ip flow-cache timeout inactive 30
ip flow-cache timeout active 45
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
voice-card 0
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/1/0
ip address 10.15.32.5 255.255.255.252
ip flow ingress
no fair-queue
clock rate 64000
!
interface Serial0/1/1
ip address 10.15.32.1 255.255.255.252
ip flow ingress
clock rate 64000
```

```
!
router ospf 1001
log-adjacency-changes
network 10.15.32.0 0.0.0.3 area 3000
network 10.15.32.4 0.0.0.3 area 3000
!
ip forward-protocol nd
!
ip flow-aggregation cache as
!
ip flow-top-talkers
top 5
sort-by bytes
match input-interface Serial0/1/1
match protocol udp
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
password ajiglesias_tesis_2013
login
line aux 0
line vty 0 5
password acceso_tesis_2013
login
!
scheduler allocate 20000 1000
end

ISP#
```

IV.3. Explicación de los procedimientos aplicados

En las secciones IV.2.2, IV.2.3 y IV.2.4 se presentaron las configuraciones aplicadas a cada uno de los enrutadores mostrados en la topología de la Figura 19. Los conmutadores no fueron configurados debido a que no poseen importancia para las configuraciones requeridas por el Trabajo de Grado. En esta sección se

explicará la configuración de los enrutadores de sedes (Sede_1 y Sede_2); así como del enrutador de concentración de datos (ISP).

IV.3.1. Configuración de básica

La configuración básica de un dispositivo de red CISCO configurable a través de la línea de comandos (como lo son todos los dispositivos de la gama empresarial de la empresa) consiste en darle al dispositivo un nombre de host, establecer contraseñas para los distintos modos de operación de la memoria del dispositivo; y establecer así mismo una contraseña para limitar el acceso desde el exterior (mediante la utilización de protocolos de acceso remoto tales como Telnet y SSH).

Toda la configuración básica se puede realizar desde el modo de "Configuración Global".

El nombre de host (*hostname*) se especifica mediante el comando:

- hostname "Nombre de dispositivo"

Existen dos modos de operación básicos en un dispositivo CISCO. El Modo de Ejecución Privilegiado es el primero disponible cuando se enciende el dispositivo y, por tanto, debe ser protegido mediante el uso de una contraseña (encriptada por razones de seguridad para que cualquier persona con acceso a la memoria del enrutador, tal como el lector de este documento, no pueda identificarla y por tanto ingresar al dispositivo) mediante el uso de los siguientes dos comandos:

- line console 0
- enable secret "Contraseña"
- login

Para proteger el modo de "Configuración Global" (desde el cual se pueden realizar todas las configuraciones requeridas en cualquier dispositivo CISCO) se utiliza el siguiente comando:

- password "Contraseña"

Para proteger el acceso remoto desde otros dispositivos de red se utilizan los siguientes comandos:

- line vty 0 4
- password "Contraseña"

El primer comando implica existe en este dispositivo la posibilidad de realizar cinco sesiones simultáneas remotas de conexión al mismo, y se están protegiendo todas mediante una contraseña. Un buen ejercicio académico consiste en proteger cada una de ellas con una contraseña diferente para incrementar la seguridad del dispositivo.

Es de hacer notar que al haber introducido el comando "enable secret", se habilita el servicio de encriptación de contraseñas, y todas las contraseñas del dispositivo deben aparecer en su memoria como una serie de símbolos ininteligibles al lector.

El siguiente paso consiste en configurar las interfaces del dispositivo. En el caso de los enrutadores Sede_1 y Sede_2, fueron configuradas una interfaz *Fast Ethernet* y una interfaz Serial.

La interfaz *Fast Ethernet* tiene como función conectarse a conmutadores y es la que provee conectividad de red a todos los dispositivos que se conecten a la topología. Se configura con una dirección IP mediante los siguientes comandos:

- interface fastethernet "Nombre de la interfaz"
- ip address "x.y.z.w" "a.b.c.d"

El término x.y.z.w corresponde a la dirección IP asignada a la interfaz en configuración. Una dirección IP tiene un formato compuesto por cuatro grupos de dígitos (entre 0 y 255) separados por un signo de punto. Un ejemplo clásico de dirección IP es 192.168.0.1.

El término a.b.c.d corresponde a la Máscara de Subred asignada a la interfaz en configuración. Este término se utiliza para cuantificar cuántos

dispositivos podrán ser conectados a la red creada. Un ejemplo cásico de máscara de subred es 255.255.255.0.

Cuando se configuren interfaces seriales, además de éstos, se debe configurar la velocidad de reloj que utilizará la interfaz para sincronizarse y para crear los enlaces, mediante el siguiente comando:

- clock rate "Velocidad"

IV.3.2. Configuración de enrutamiento

Una vez configurados de forma básica (si se tienen varios enrutadores en una misma topología, como es el caso del Trabajo de Grado), es necesario configurar las rutas que cada paquete seguirá en su camino hacia su destino. Existen dos formas de hacerlo: mediante rutas estáticas en las que el configurador debe introducir manualmente cada uno de los caminos que será seguidos por cada paquete en función de su destino; y mediante protocolos de enrutamiento, en lo que será este programa el que seleccione la mejor ruta en función de los parámetros grabados en su algoritmo de funcionamiento. En el caso del Trabajo de Grado fue seleccionado el protocolo de enrutamiento OSPF.

Para configurar OSPF (en realidad cualquier protocolo de enrutamiento) se debe ingresar al modo de Configuración Global. Una vez en este modo de operación se deben introducir los siguientes comandos:

- router ospf "Número de proceso"
- network a.b.c.d area "Número de área"

Para configurar el protocolo de enrutamiento OSPF en un dispositivo CISCO se deben poseer tres parámetros:

- Número de proceso: es el identificador asignado por el operativo al proceso que el programa OSPF ejecuta en la memoria del dispositivo de red.
- Red: es la red que será publicada por el OSPF. La red es el resultado de aplicar la operación lógica *and* entre una dirección IP y la máscara de subred asociada a ella.

- Número de área: es el identificador del grupo de trabajo que en informática se conoce como "Sistema Autónomo". Todos los enrutadores de una topología OSPF deben pertenecer al mismo sistema autónomo debido a que en caso contrario no serán procesados los mensajes enviados por las instancias del protocolo ejecutadas en otros enrutadores. Es el número de pertenencia al grupo de enrutamiento, y el que garantiza que los dos enrutadores en los que se procesa un mensaje, pertenecen a la misma red.

IV.3.3. Configuración de *Netflow*

Lo único que debe hacerse para configurar *Netflow* es habilitarlo en las interfaces donde será utilizado, mediante los siguientes comandos:

- ip flow ingress
- ip flow egress

Mediante el primer comando se configura a la interfaz para realice el conteo de los flujos entrantes a la misma; mientras que con el segundo se realiza el conteo de lo saliente. En el caso de que se quiera, por ejemplo, saber el flujo de tráfico hacia un enlace exterior, se debe utiliza la segunda opción planteada.

Una vez habilitado *Netflow* en las interfaces donde será aplicado, los administradores de red ya pueden realizar sus labores de análisis. Sin embargo, por facilidad, es muy recomendable configurar además una serie de opciones para organizar la data recolectada por el programa. Las siguientes opciones fueron configuradas en los enrutadores utilizados para el Trabajo de Grado.

Para no sobrecargar la memoria del enrutador (por muy elevada que sea siempre será limitada, y debe estar disponible para otras tareas más primordiales como por ejemplo las propias labores de enrutamiento), se debe limitar el número de flujos que serán almacenados antes de descartarlos o de enviarlos hacia un servidor externo, mediante el siguiente comando:

- ip flow-cache entries "Número de entradas"

Otras actividades uese deben realizar, también para optimizar el uso de memoria, procesador, y recursos en el propio enrutador, es limitar la cantidad de tiempo que una entrada puede permanecer activa e inactiva en el caché del protocolo:

- ip flow-cache timeout inactive "Cantidad de segundos"
- ip flow-cache timeout active "Cantidad de minutos"

Un flujo activo es aquel que está actualizándose, es decir, con el comando lo que se especifica es la cantidad de tiempo que la interfaz debe permanecer enviando flujos hacia las entradas disponibles en el caché.

Un flujo inactivo es aquél que no está actualizándose. El comando especifica la cantidad de tiempo que una entrada en el caché de *Netflow* que no está recibiendo nuevos flujos, puede permanecer en la memoria.

Un paso que debe ser seguido cuando se desea agrupar los flujos de datos de *Netflow* según diferentes clasificaciones, es utilizar los "Esquemas de Agregación", con lo cual, mediante el siguiente comando, permite separar cada tipo de flujo en diferentes espacios de memoria en el enrutador (en diferentes cachés). En el caso del Trabajo de Grado se realizó la separación por sistema autónomo ya que no se tenía especial interés en otros tipos de clasificaciones tales como dominios de enrutamiento u otros.

- Ip flow-aggregation cache as

Aunque las optimizaciones anteriores no son necesarias para el funcionamiento de *Netflow* (debido a que como se dijo al inicio de esta sección, sólo es necesario habilitarlo), sí es recomendable utilizarlas por la elevada carga de trabajo que esta herramienta produce sobre los enrutadores mientras está operativa en ellos, sobre todo cuando se introducen aspectos como la clasificación del tráfico. Consultar la Figura 15.

La interfaz del enrutador debe saber que tiene que organizar los flujos de datos que reciba o envíe (de acuerdo a como haya sido configurado *Netflow* en ella) Para ello se organizan los flujos en "Topes" mediante el siguiente comando:

- Ip flow-top-talkers

Una vez dada la orden de organizar los flujos se le debe indicar a la herramienta cuántos flujos va a añadir en cada muestra presentada mediante el siguiente comando:

- Top "Número de flujos"

Cuando se habilita *Netflow* se tiene en mente qué tipo de data queremos extraer del sistema (si son los bytes transmidos / recibidos, los errores, los protocolos, los descartes, etc.). En el Trabajo de Grado fueron utilizados dos criterios de organización: bytes y protocolo de capa de Transporte, mediante los tres siguientes comandos:

- sort-by "Criterio de organización"
- match input-interface "Nombre de la Interfaz"
- match protocol "Protocolo"

En el siguiente capítulo del Trabajo de Grado serán presentados los resultados obtenidos de aplicar esta plantilla de configuración a la topología presentada en este capítulo.

Capítulo V RESULTADO Y ANÁLISIS DE RESULTADOS

El capítulo desarrollará los resultados obtenidos de aplicar la plantilla de configuración presentada a lo largo de la sección IV.2.

Una vez construida la topología desarrollada en la sección IV.1, se aplicó el siguiente comando de visualización en la consola del enrutador R2, el cual funciona como la salida de la empresa hacia otras redes externas.

- show ip chache flow

En el 0 se hace una referencia completa a los comandos de visualización disponibles en la herramienta Netflow.

Mediante el comando presentado en el capítulo fueron obtenidas capturas para diferentes protocolos de red, los cuales serán desarrollados en la sección V.1.

V.1. Protocolos capturados

El comando *show ip cache flow* arrojó como resultado la captura de los flujos que estaban siendo transmitidos y recibidos por las distintas interfaces del enrutador R2 al momento de su ejecución. Fueron capturados los siguientes protocolos:

- ICMP
- Telnet
- FTP
- HTTP
- TFTP

En la FIGURA 27 se aprecia la captura de una transmisión de mensajes pertenecientes al protocolo ICMP, los cuales se usan para verificar la disponibilidad de un sistema remoto, así como para comprobar la inexistencia de problemas de conectividad de capa de Red en el sistema emisor del mensaje.

```
R2#show ip cache flow
IP packet size distribution (79 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .063 .936 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 2 added
  91 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  1 active, 1023 inactive, 2 added, 2 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
UDP-other            1       0.0         5    32      0.0       0.2      15.6
Total:               1       0.0         5    32      0.0       0.2      15.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/1/0       10.0.0.10       Local         209.165.200.151 01 0000 0800    74
R2#
```

FIGURA 27. Captura del protocolo ICMP

La FIGURA 27 muestra que fue transmitido un mensaje *ping*, perteneciente al protocolo ICMP. Este protocolo establece que se enviará una ráfaga de cinco mensajes, cada uno con un tamaño de 32 bytes.

Se puede apreciar que los mensajes fueron enviados desde la interfaz serial cuya dirección IP es 10.0.0.10; hacia la dirección 209.165.200.151, correspondiente a una interfaz lógica (virtual) conocida como "Interfaz de *Loopback*", que se usa para:

- Probar conectividad de red en los enrutadores CISCO sin la necesidad de general tráfico de red hacia el exterior, simulando la existencia de una interfaz con un enlace hacia un ISP.
- Descartar aquellos paquetes que no interesa mantener en la memoria del enrutador por cualquier razón, tal como la existencia de errores en su encabezado de capa de red.

Se aprecia finalmente que no se especifica ningún protocolo de capa de Transporte en la captura presentada en la FIGURA 27.

En la FIGURA 28 se aprecia la captura de una transmisión utilizando el protocolo TFTP, el cual se utiliza para realizar la descarga de archivos desde un servidor instalado en un sistema informático o de red. Este protocolo funciona bajo el modelo cliente – servidor.

```
R2#show ip cache flow
IP packet size distribution (234 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .042 .944 .012 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 22 added
  412 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          10       0.0         4    46      0.0       1.2       5.7
TCP-FTP              2       0.0         3    40      0.0       1.0       1.1
UDP-TFTP             4       0.0         1    58      0.0       0.0      15.5
UDP-other            2       0.0         5    32      0.0       0.2      15.6
ICMP                 2       0.0        83    60      0.0      88.4      15.3
Total:              20       0.0        11    55      0.0       9.6       9.1
```

FIGURA 28. Captura del protocolo TFTP

La FIGURA 28 la captura de las transmisiones correspondientes a una secuencia de solicitud más respuesta en el protocolo TFTP. Consultar la sección V.2.

Se puede identificar que en la secuencia capturada fueron transmitidos un total de veinte flujos. De ellos, ocho corresponden a la transmisión capturada; mientras que el resto corresponde a actividades residuales que la estación de trabajo estaba realizando con respecto a otras transmisiones realizadas (transmisiones Telnet e ICMP).

Aunque no se menciona explícitamente en la tabla resumen, se puede comprobar en la FIGURA 28 que un mensaje TFTP utiliza el protocolo UDP de capa de Transporte para realizar el control de sus transmisiones extremo a extremo.

En la Tabla 16 se observa la cantidad de bytes transmitidos en esta captura, con respecto al protocolo TFTP.

Tabla 16. Datos de flujos con paquetes TFTP

PROTOCOLO	TOTAL DE FLUJOS	PAQUETES POR FLUJO	BYTES POR PAQUETE
FTP	2	3	40
TFTP	4	1	58
OTRO	2	5	32

En la FIGURA 29 se aprecia la captura de la transmisión realizada utilizando el protocolo HTTP. Esta transmisión se realizó utilizando un navegador web.

Se aprecia en la FIGURA 29 que el WWW, nombre con el que *Netflow* identifica al protocolo HTTP debido a que es su aplicación más conocida y común, utiliza el protocolo de capa de Transporte TCP para el control de sus transmisiones.

Fueron capturados seis flujos pertenecientes a este protocolo, con un total de seis paquetes agrupados, tres por flujo.

En la Tabla 17 se observa la cantidad de bytes almacenados en los flujos que reflejados por la FIGURA 28.

```
R2#show ip cache flow
IP packet size distribution (252 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .039 .948 .011 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  0 active, 4096 inactive, 28 added
  482 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          10       0.0         4    46      0.0       1.2       5.7
TCP-FTP              4       0.0         3    45      0.0       1.0       8.1
TCP-WWW              4       0.0         3    45      0.0       1.0       8.3
TCP-other            2       0.0         3    45      0.0       1.0       8.5
UDP-TFTP             4       0.0         1    58      0.0       0.0      15.5
UDP-other            2       0.0         5    32      0.0       0.2      15.6
ICMP                 2       0.0        83    60      0.0      88.4      15.3
Total:              28       0.0         9    54      0.0       7.1       9.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
R2#_
```

FIGURA 29. Captura del protocolo HTTP

Tabla 17. Datos correspondientes al protocolo HTTP

PROTOCOLO	TOTAL DE FLUJOS	PAQUETES POR FLUJO	BYTES POR PAQUETE
HTTP	4	3	45
OTRO	2	2	58

En la FIGURA 30 se aprecia una captura global en la que se almacenan todos los protocolos que, al momento de ser realizada, estaban siendo transmitidos desde las estaciones de trabajo hacia la red instalada.

```
IP packet size distribution (252 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .039 .948 .011 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 28 added
  476 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          10      0.0         4    46      0.0       1.2       5.7
TCP-FTP              4      0.0         3    45      0.0       1.0       8.1
TCP-WWW              4      0.0         3    45      0.0       1.0       8.3
TCP-other            1      0.0         3    40      0.0       1.0       1.5
UDP-TFTP             4      0.0         1    58      0.0       0.0      15.5
UDP-other            2      0.0         5    32      0.0       0.2      15.6
ICMP                 2      0.0        83    60      0.0      88.4      15.3
Total:              27      0.0         9    54      0.0       7.4       9.2

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/1/1       10.0.0.138      Se0/1/0       10.0.0.10       06 C00D 0D3D     3
R2#
```

FIGURA 30. Captura de varios protocolos I

Se aprecia la transmisión de mensajes bajo los protocolos Telnet, FTP, TFTP, HTTP e ICMP. Consultar la sección V.2 para más información sobre su presencia en esta captura.

Puede ser notado que fueron realizadas tres transmisiones desde la interfaz Serial 0/1/1 hacia la interfaz Serial 0/1/0. Consultar la sección V.2.

Los datos fueron enviados desde el puerto de capa de Transporte C00D (valor hexadecimal correspondiente a 49165 en decimal) hacia el puerto 0D3D (valor correspondiente al 3389 decimal). Consultar la sección V.2.

En la Tabla 18 se aprecia el total de bytes capturados en la FIGURA 29.

Tabla 18. Captura de diferentes protocolos I

PROTOCOLO	TOTAL DE FLUJOS	PAQUETES POR FLUJO	BYTES POR PAQUETE
Telnet	10	4	46
FTP	4	3	45
HTTP	4	3	45
OTRO	1	3	40
TFTP	4	1	58
ICMP	2	83	60

En la FIGURA 31 se aprecia otra captura similar a la mostrada en la FIGURA 30.

La principal diferencia entre las dos ilustraciones mencionadas es que en la FIGURA 30 sólo se capturó una transmisión; mientras que en la FIGURA 31 fueron capturadas dos transmisiones realizadas desde la interfaz Serial 0/1/1 hacia la interfaz Serial 0/1/0.

Adicionalmente, en la captura de la FIGURA 31 no se capturó la entrada correspondiente a "TCP – OTHER". Consultar la sección V.2.

```
R2#show ip cache flow
IP packet size distribution (246 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .040 .947 .012 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 26 added
  441 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          10       0.0         4    46      0.0       1.2       5.7
TCP-FTP              4       0.0         3    45      0.0       1.0       8.1
TCP-WWW              2       0.0         3    40      0.0       1.0       1.5
UDP-TFTP             4       0.0         1    58      0.0       0.0      15.5
UDP-other            2       0.0         5    32      0.0       0.2      15.6
ICMP                 2       0.0        83    60      0.0      88.4      15.3
Total:              24       0.0        10    55      0.0       8.2       9.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/1/0       10.0.0.10       Se0/1/1       10.0.0.138      06 C009 0050     3
Se0/1/0       10.0.0.10       Se0/1/1       10.0.0.138      06 C008 0050     3
```

FIGURA 31. Captura de varios protocolos II

En la Tabla 19 se aprecia el total de bytes almacenados en los flujos capturados en la FIGURA 31.

Tabla 19. Captura de diferentes protocolos II

PROTOCOLO	TOTAL DE FLUJOS	PAQUETES POR FLUJO	BYTES POR PAQUETE
Telnet	10	4	46
FTP	4	3	45
HTTP	2	3	40
TFTP	4	1	58
ICMP	2	83	60

No serán realizados mayores comentarios sobre el contenido de la Tabla 19 debido a que éste es similar al de la Tabla 18, variando los valores de los diferentes campos.

V.2. Análisis de resultados

El protocolo ICMP varía su funcionamiento de acuerdo al sistema operativo instalado en el sistema informático desde el cual se construye un mensaje que siga este protocolo. Por ejemplo, las implementaciones basadas en cualquier distribución de *kernel* LINUX envían mensajes en primer plano hasta que el usuario ordena detener esta operación; pero los sistemas *WINDOWS* envían cinco mensajes en primer plano para que el usuario tenga acceso a las estadísticas del resultado de los mensajes. Sin embargo, en segundo plano, el sistema continúa enviando mensajes a la dirección IP especificada en la construcción del mensaje.

Por esta razón se observa que en las figuras FIGURA 28, FIGURA 29, FIGURA 30 y FIGURA 31 fueron capturados 166 mensajes en vez de los cinco que se aprecian en la FIGURA 27.

V.2.1. Seguridad

Se aprecia en las cinco gráficas que el primer uso que se le puede dar a *Netflow* es la identificación de inconvenientes en la seguridad de la red al detectar los protocolos que la misma está procesando en cada instante particular.

En el caso del Trabajo de Grado, en la red sólo debían aparecer los protocolos HTTP, FTP, TFTP, e ICMP debido a que no existen en las estaciones de trabajo del laboratorio utilizado otras aplicaciones. Sólo está instalado un navegador web y un cliente TFTP. Al no estar estas estaciones de trabajo conectadas a la red corporativa de la academia, ni a Internet, la red no debe procesar ningún protocolo perteneciente a otras aplicaciones diferentes a las mencionadas. Por esta razón, si existiera en las capturas presentadas otros protocolos adicionales, podríamos decir sin temor a errores que existe un problema de seguridad en la red y habría que pensar en la existencia de virus en las estaciones de trabajo.

Se aprecia en las figuras de la sección V.1 las direcciones IP de los encabezados de capa de red de los diferentes mensajes capturados por *Netflow*. Al conocer el esquema de direccionamiento aplicado en la red (consultar la sección IV.2.1), se debe comparar las direcciones que pueden ser asignadas en los diferentes rangos que se pueden crear a partir de él (el esquema de direccionamiento) con las direcciones efectivas transmitidas por la red.

Si existe en la red alguna dirección IP que no está contenida dentro de ninguno de los rangos que pueden ser creados a partir del esquema efectivamente aplicado a la red, se puede considerar una de las siguientes afirmaciones:

- Existe un intruso en la red: una estación de trabajo que no pertenece a la red se encuentra conectada a ella, transmitiendo mensajes pertenecientes a diferentes aplicaciones que potencialmente tienen la capacidad de provocar destrozos en el sistema informático instalado.
- Existe algún tipo de *software* malicioso instalado en alguna de las estaciones de trabajo de la red transmitiendo sus mensajes, con la potencialidad de provocar destrozos en el sistema y de robar información.

Las capturas mostradas en las figuras de la sección V.1 pueden proveer así mismo información importante sobre los protocolos que, estando autorizados, están corriendo en la red.

Es importante conocer el funcionamiento de cada protocolo. Por ejemplo, lo básico de todos los protocolos utilizados en el laboratorio instalado para la realización del Trabajo de Grado es que funcionan bajo el modelo cliente – servidor. Este modelo especifica que todas las conexiones se originan en una estación de trabajo (que funciona como cliente), y que deben ser respondidas por otra estación de trabajo (que funcione como servidor).

En las figuras de la sección V.1 se aprecia que:

- Existen paquetes con la denominación "*TCP – OTHER*".
- Existen paquetes con la denominación "*UDP-OTHER*".

El protocolo TFTP utiliza el protocolo de capa de transporte UDP para su funcionamiento. Como protocolo que sigue el modelo cliente – servidor, éste se basa en que una estación de trabajo (cliente) envía una solicitud a otra estación de trabajo (servidor) para descargar un archivo contenido en alguno de sus directorios.

Existen dos tipos de mensajes principales: los mensajes de solicitud y respuesta intercambiados entre el cliente y el servidor (incluyendo aspectos del establecimiento, mantenimiento y cierre de la sesión entre ambos); y los mensajes relacionados mediante los cuales se intercambia propiamente la información solicitada.

Los diferentes paquetes en los que viajan los archivos solicitados por el cliente son transmitidos por el servidor mediante un tipo de conexión conocida como "relacionada". Una conexión relacionada es aquella que, sin ser propiamente la conexión original, está relacionada con ésta.

En el caso de TFTP, las conexiones relacionadas son aquellas conexiones originadas como consecuencia del intercambio de mensajes entre un cliente y un servidor; es decir, la transferencia propiamente dicha de los archivos.

Por esta razón, toda comunicación mediante TFTP debe poseer un número igual o mayor de conexiones relacionadas (UDP – OTHER) que de conexiones originales (UDP – TFTP).

HTTP, que opera con el protocolo de capa de Transporte TCP, trabaja de forma similar. Los mensajes de solicitud y de respuesta (sólo texto) se envían mediante conexiones "originales".

Una página web está formada por texto, imágenes, audio, video, etc. Toda la parte multimedia de la misma es muy pesada (son archivos de gran tamaño) en comparación con el texto de la misma. Por esta razón, el servidor transmite el código HTML de las páginas web en dos partes: el relacionado con el texto mediante conexiones "originales" y el relacionado con la parte multimedia en conexiones "relacionadas".

Se extrae de esto que, al igual que con el protocolo TFTP, toda conexión HTTP debe estar formada por dos tipos de conexiones: la "original" (TCP-HTTP), y un número igual o superior de paquetes "relacionados" (TCP-OTHER).

El aspecto que se debe tener en cuenta es que, si en la captura que *Netflow* realice se encuentran paquetes TCP-OTHER o UDP-OTHER, pero no se encuentran las conexiones originales TCP-HTTP y UDP-TFTP, podríamos estar en presencia de una amenaza de seguridad o de algún *software* malicioso en la red debido a que este tipo de conexiones no se pueden crear si no existe una solicitud previa desde el sistema.

Adicionalmente, se debe verificar que el origen y el destino de las conexiones "originales" y de las relacionadas sean contrarios debido a que todas las conexiones relacionadas de cualquier protocolo que siga el modelo cliente – servidor debe ser originada en el destino de las conexiones originales (es decir, todas las conexiones relacionadas se originan en el servidor y van dirigidas al cliente). Si esto no sucede, podríamos estar en presencia de alguno de los problemas de seguridad ya mencionados previamente.

El último aspecto de seguridad que se debe tomar en cuenta es el tiempo en el que los flujos permanecen activos en la base de datos *Netflow Collector.* Mientras más tiempo permanezca un flujo activo, hay un problema de seguridad debido a que se trata de un espacio de memoria que permanece abierto para ser modificado por el ente que acceda a éste (tanto autorizado como no autorizado).

En las figuras de la sección V.1 se aprecia que el tiempo en el que los flujos correspondientes al protocolo ICMP permanecen activos en la memoria del enrutador es mucho mayor que el tiempo en el que los demás protocolos capturados permanecen activos. Esto se debe a que, como se dijo al principio de la sección en curso, el sistema operativo *WINDOWS* mantiene una línea de comunicación abierta con el destino de la conexión durante un tiempo posterior a la entrega del resultado de la operación al usuario. Cuando se detecte esta situación (tiempo activo del flujo muy elevado) se debe bloquear este protocolo en la red debido a que es una fuente muy común de ataques a la seguridad por parte de quienes tienen intereses ocultos

en la red. Adicionalmente, representa una forma muy básica de ataques a la seguridad de la red mediante lo que se conoce como "denegación de servicio", que consiste en bombardear al sistema con mensajes para ocupar toda su atención y recursos en responderlos.

V.2.2. Tráfico

A partir de la información suministrada en las figuras de la sección V.1, compendiadas en las tablas de la misma sección, se puede calcular:

- La cantidad de datos transmitidos por la red hacia el exterior.
- La velocidad utilizada por esos datos para salir de la red corporativa.

Ninguno de los dos datos se puede obtener directamente de la información ofrecida por *Netflow*, sino que debe ser calculada a partir de ella.

Referirse a la Tabla 16. En ella se observa que fueron capturados 1920 bits pertenecientes al protocolo FTP, 1856 bits correspondientes al protocolo TFTP, Y 2560 bits correspondientes a la conexión relacionada de TFTP. Se aprecia por ende que la transmisión consistió en descargar un archivo de 2.56 Kb.

Referirse a la Tabla 17. Se aprecia que fueron capturados 4320 bits correspondientes a solicitudes de un navegador para cargar una página web determinada; así como también 1856 bits de conexiones relacionadas.

En este caso, las conexiones relacionadas no tienen nada que ver con la carga de las imágenes y videos que existen en cualquier página web. Debido a que la red creada con el laboratorio del Trabajo de Grado no estaba conectada a la red corporativa de la academia y, por tanto, no tenía acceso a Internet; las conexiones relacionadas no son más que las respuestas erróneas a esos mensajes de solicitud indicando que no se encuentra el destino solicitado.

Los mensajes de error en Internet se transmiten utilizando el protocolo IGMP. Sin embargo, debido a que los enrutadores CISCO conocen que la solicitud que se realiza pertenece al protocolo HTTP (aunque son dispositivos de capa de Red tienen la capacidad de inspeccionar el contenido de la capa de Aplicación de

los mensajes y determinar el protocolo que está encapsulado en ella debido a una característica de seguridad conocida como *Access List*), generan la respuesta de error bajo este protocolo para que la estación de trabajo no tenga que decodificar el contenido del protocolo IGMP, el cual podría no estar instalado en ella.

En las tablas Tabla 18 y Tabla 19 se muestra la misma información que en las primeras dos analizadas, expandiendo la información a todos los protocolos capturados por *Netflow* de forma simultánea; por lo que no vale la pena realizar el análisis nuevamente.

También se puede determinar la velocidad utilizada por las diferentes transmisiones en su camino hacia las redes externas. Éste suele ser el objetivo principal de las empresas ya que los ISP suelen alquilar velocidad de enlaces sobre capacidad transmitida.

Para determinar la velocidad utilizada por cada protocolo o aplicación se debe aplicar la siguiente ecuación:

$$Velocidad = \frac{Data\ transmitida}{Unidad\ de\ tiempo}$$ Ecuación V-1. Cálculo básico de velocidad

La "data transmitida" mencionada en la $Velocidad = \frac{Data\ transmitida}{Unidad\ de\ tiempo}$ Ecuación V-1 corresponde a la analizada a lo largo de esta sección. La "unidad de tiempo" corresponde al campo *"Flows / Sec"*, que puede ser consultado en las ilustraciones FIGURA 27, FIGURA 28, FIGURA 29,FIGURA 30 y FIGURA 31.

Si se analizan las mencionadas ilustraciones se observa que en todas ellas el campo "*Flows / Sec*" tiene un valor de cero, a pesar de que los campos correspondientes a cantidad de data sí poseen valores.

Esto se debe a que para que este valor *"Flows / Sec"* sea diferente de cero, por cuestiones de diseño de la herramienta, se debe realizar una transmisión de forma continuada en el tiempo.

Debido a que todas las transmisiones realizadas fueron transmisiones de prueba, transmisiones que tuvieron una duración limitada, este valor no fue registrado por la herramienta.

Si se hubiera realizado el llamado "ping de la muerte" (que consiste en enviar solicitudes ICMP bajo este formato de forma continua e ininterrumpida en el tiempo hacia cualquier dirección IP), el campo en cuestión tendría un valor diferente de cero, al menos en la fila correspondiente al protocolo ICMP.

En el caso de las capturas correspondientes al protocolo TFTP, para que el valor del campo *"Flows / Sec"* fuera distinto de cero, se debería haber realizado la descarga de un archivo de más de 100 KB (800 Kb).

Aplicando el correspondiente análisis a las capturas del protocolo HTTP, se ve que la condición es que la red de laboratorio hubiese tenido acceso a la red corporativa y, por ende, a Internet.

Este hecho se debe a que *Netflow* fue diseñado para su utilización en ambientes de producción real, en los cuales la transmisión de data es mucho mayor que la utilizada en un laboratorio de prueba.

Es decir, para que el enrutador donde se encuentre habilitado *Netflow* calcule (en vez de recopilar, como sucede con el resto de estadísticas presentadas a lo largo de la sección V.1) el valor del campo *"Flows / Sec"*, el enrutador debe transmitir volúmenes de tráfico reales.

En el Capítulo V serán presentadas las conclusiones y recomendaciones que se desprenden de la información provista y analizada a lo largo del Capítulo V.

Capítulo VI CONCLUSIONES Y RECOMENDACIONES

El capítulo se divide en dos secciones:

- Conclusiones, en la que se presenta y desarrollan las conclusiones obtenidas como consecuencia del trabajo realizado en los capítulos Capítulo IV y Capítulo V.
- Recomendaciones, en la cual se presenta una serie de recomendaciones tendientes a mejorar los resultados obtenidos en el Trabajo de Grado.

VI.1. Conclusiones

Se presentan dos grupos de conclusiones. El primer grupo está basado en los objetivos específicos en los cuales se basa el Trabajo de Grado: se presenta como mínimo una conclusión por cada objetivo específico. El segundo grupo, llamado general, son conclusiones basadas en la experiencia obtenida con la realización del trabajo de grado, que no tienen nada que ver, de forma explícita, con los objetivos específicos planteados en la sección I.3.2.

VI.1.1. Conclusiones basadas en los objetivos específicos

Basándose en los objetivos específicos (en orden ascendente), se pueden enunciar las siguientes conclusiones:

1. El *software Netflow* funciona mediante la recopilación de información procedente de los encabezados de los paquetes IP transmitidos en las redes corporativas. Deben ser utilizadas técnicas adicionales para evitar que el protocolo (que hace una gran utilización de los recursos físicos de procesamiento disponibles en los dispositivos de red) tenga un impacto negativo (de ralentización) en la operación de los elementos donde se habilite.
2. El protocolo *Netflow* viene instalado por defecto en los dispositivos de red de la gama corporativa de CISCO. Consultar la sección II.2.3. Deben ser utilizadas configuraciones adicionales para que la herramienta funcione como desea el administrador de la red.

3. En consonancia con la conclusión número dos, se debe realizar una profunda personalización del protocolo mediante la introducción de una plantilla de configuración adecuada a los intereses de monitoreo y gestión de la red corporativa. Mientras más exhaustiva sea esa configuración, más personalizada estará la herramienta y, por tanto, los datos recopilados podrán ser utilizados con mayor eficiencia por el equipo de redes de la empresa.
4. Debe ser diseñada e implementada una topología física y lógica en las empresas. Se debe estudiar de forma cuidadosa en qué parte de esa topología será habilitado y configurado *Netflow*.
5. Los resultados obtenidos de las pruebas realizadas, y explicadas en el Capítulo V, indican que el protocolo debe ser habilitado sólo en aquellos casos en los cuales las redes corporativas se encuentran en un estado de producción, con una transmisión normal de datos para este tipo de redes.

La primera conclusión de esta sección induce la necesidad de habilitar el uso de técnicas de conmutación avanzadas en los dispositivos de red donde *Netflow* se habilite (entendiendo como conmutación al hecho de recibir, procesar y transmitir datos).

Como se ha dicho previamente a lo largo del trabajo de grado, *Netflow* hace una gran utilización de recursos de los dispositivos de red. El objetivo principal de éstos debe ser la prestación de los servicios disponibles en la red corporativa. Su monitoreo debe ser una herramienta que funciones para la red, no al revés. Debido a esto, se debe optimizar el funcionamiento de las funciones básicas de los dispositivos.

La segunda y tercera conclusiones afirman que se debe configurar completamente el protocolo *Netflow* para asegurar que los datos que recopile sean realmente los que al administrador de la red le interesa estudiar. Esto permite, así mismo, evitar que el protocolo consuma recursos excesivos de los dispositivos de red.

No basta con habilitar el protocolo en los dispositivos de red; ya que los administradores tienen la intención de monitorear la red corporativa, lo cual se consigue filtrando y clasificando la data que el *Netflow* recopila mediante la aplicación de alguna plantilla de configuración.

Se debe recordar que el objetivo fundamental del trabajo de grado es estudiar el protocolo *Netflow* para su uso como herramienta de monitoreo y gestión de las redes corporativas. La personalización (configuración) de la misma permite clasificar la data recopilada por ésta mediante algún criterio establecido en su configuración (consultar la sección IV.2).

La cuarta conclusión implica que antes de decidir la utilización de *Netflow* (y en general de cualquier protocolo o sistema de monitoreo) es necesario diseñar una topología de red (tanto física como lógica) que permita la comunicación de los diferentes elementos conectados mediante la red corporativa.

Será luego de que se tenga claro el diseño a implementar que se podrá estudiar el protocolo de monitoreo a utilizar, así como el elemento de la red en el que será implementado (habilitado).

Se puede dar el caso de que, mediante una topología totalmente diferente a la topología de producción utilizada en la red corporativa, se decida utilizar una topología en paralelo (física o lógica) para el monitoreo de la red.

En cualquier caso, es necesario e indispensable que la topología de la misma sea decidida antes de la implementación de cualquier protocolo de monitoreo (en particular *Netflow*), ya que una vez decidida aquella es que se puede pensar en la habilitación y configuración del mismo (recuérdese que el objetivo de la red, como se indicó previamente, es servir a las aplicaciones instaladas en ella y no a su monitoreo. El monitoreo debe ser un medio secundario utilizado para mantener a la red en óptimas condiciones.

La quinta conclusión confirma lo expresado en el Capítulo V (se repite el mismo razonamiento en la próxima sección, como conclusiones generales del trabajo de grado). *Netflow* debe ser utilizado sólo en redes operativas, no en redes

experimentales. La cantidad de data que el protocolo está diseñado para manejar hace que en cualquier ambiente de laboratorio, en el cual sólo se corren algunas aplicaciones para probar el funcionamiento del protocolo, no se obtengan los resultados deseados.

La herramienta está diseñada para recopilar la gran cantidad de data y protocolos que se transmiten de forma normal en cualquier red corporativa. Por esta razón, cuando se transmiten unos pocos datos experimentales, la herramienta no los captura. Consultar la sección V.2.

Al agrupar patrones similares contenidos en el encabezado IP de la data que circula por la red, *Netflow* "cuenta" la información asociada a éstos. Cuando sólo circulan pocos paquetes de un determinado protocolo, *Netflow* no lo refleja debido a que no ha agrupado información suficiente en su base de datos.

Si se quiere implementar como una prueba antes de su ejecución real, es ideal que se haga en una red de producción comercial real, simulando redes mediante el concepto de las interfaces virtuales. De esta forma no se afecta a la producción real de la red, y se obtienen los resultados deseados desde el principio.

En la próxima sección se desarrollan conclusiones obtenidas en base al trabajo práctico realizado, que no tienen nada que ver con los objetivos específicos del trabajo de grado. El autor del mismo considera que es necesario plasmarlas en el documento debido a que se mencionan aspectos importantes que deben ser tomados en cuenta antes de iniciar la migración hacia *Netflow*.

VI.1.2. Conclusiones generales

De forma general, basándose en la experiencia obtenida al realizar el trabajo de grado, se pueden enunciar las siguientes conclusiones:

1. El protocolo *Netflow* puede y debe ser utilizado como herramienta de medición y clasificación de tráfico en redes corporativas basadas en la tecnología LAN.
2. El protocolo debe ser usado en ambientes de producción empresarial normal, con flujos de tráfico corrientes. No debería ser usado en ambientes de

laboratorio debido a que, por su diseño, no serán aprovechadas todas sus características. Consultar la sección V.2.

3. A pesar de que viene instalado por defecto en todos los sistemas operativos IOS 12.2 o superior, se debe tener cuidado de la plataforma en la que se utilice la herramienta debido al gran uso de recursos que ella hace.
4. *Netflow* tiene aplicaciones que van más allá del clásico monitoreo de los flujos de tráfico.
5. Para realizar una gestión completa de la red corporativa, se deben utilizar los datos arrojados por *Netflow* en el cálculo de otros parámetros. A modo de ejemplo, consultar la $Velocidad = \frac{Data\ transmitida}{Unidad\ de\ tiempo}$ Ecuación V-1.
6. De acuerdo al tamaño de la red corporativa, así como de acuerdo al tipo de plataforma utilizada, *Netflow* pudiera no ser la herramienta de gestión adecuada a utilizar en el monitoreo de la red. Consultar la sección VI.2.
7. Para la adecuada gestión de la red es necesario disponer de personal especializado que se encargue de analizar los datos arrojados por *Netflow*, los cuales por sí mismos no plantean las acciones que son necesarias para corregir las diferentes situaciones que pudieran estar sucediendo en la red.

La primera conclusión confirma la idea básica del Trabajo de Grado: el *Netflow* puede ser utilizado como herramienta de monitoreo en las redes corporativas de las pequeñas y medianas empresas. Esta conclusión implica que si se aplican las técnicas de monitoreo adecuadas, el protocolo es la herramienta de gestión de redes adecuada para ser aplicada en las empresas referidas debido a la gran cantidad de información entregada por este protocolo.

Se especifica en esa afirmación que el protocolo debe ser usado en redes basadas en la tecnología LAN. Esto se debe fundamentalmente a que los enrutadores y conmutadores en los cuales se recomienda la habilitación de este protocolo están diseñados y optimizados para su funcionamiento en este tipo de redes.

Se menciona en el segundo punto de la sección que *Netflow* debe ser utilizado en ambientes corporativos. Esta herramienta no está diseñada para la captura de pequeños flujos de tráfico, sino para grandes cantidades.

Está optimizada para la captura de protocolos utilizados en ambientes reales, tales como HTTP, FTP, etc. (todos ellos utilizados en el Trabajo de Grado). Se debe utilizar en ambientes en los cuales se garantizará un flujo de tráfico extenso, normal en ambientes corporativos que, al fin y al cabo, es donde el protocolo funciona de forma más óptima.

La tercera conclusión afirma que se debe tener cuidado en la plataforma donde se utilizará el protocolo *Netflow*. Esto se debe a que la herramienta hace un extenso uso de los recursos de *hardware* (CPU, memoria flash, etc.) disponibles en el dispositivo de red. No debería ser utilizado cuando los valores físicos instalados en el mismo son pequeños. Se debe recordar que la prioridad de la red no es su monitoreo mediantes ninguna aplicación, sino más bien el servicio a los usuarios conectados con sus dispositivos finales a ella.

Si la plataforma que se posee es básica y realmente se necesita monitorear la transmisión de datos desde ella hacia el exterior, consultar la sección VI.2.

Según la cuarta afirmación de la sección, *Netflow* posee aplicaciones que van más allá del monitoreo propio de la red. Analizando los datos presentados en el Capítulo V se puede apreciar que a partir de estos datos pueden ser desarrolladas aplicaciones que permitan mantener la seguridad de la red (consultar la sección V.2).

A partir de estos datos se pueden diseñar aplicaciones que permitan realizar un control más estricto de las operaciones en la empresa (controlando las horas de actividad de cada estación de trabajo), las actividades realizadas por los trabajadores durante sus horas laborales (sin invadir su privacidad personal), detectando qué protocolos se transmiten desde cada estación de trabajo y comparándola con los que deben ser transmitidos de acuerdo con los roles de cada una; etc.

La quinta afirmación establece que, para encontrar una utilidad completa, así como explotar todas posibilidades del protocolo, se debe realizar cálculos a partir de la data capturada por éste. El mero datos de cuántos flujos circulan por la red no es suficiente para hacer un estudio completo sobre el tráfico que circula a través de la misma.

Debido a este hecho la herramienta muestra datos adicionales, tal como se aprecia en las tablas Tabla 16,Tabla 17,Tabla 18 yTabla 19. La información que realmente importa se debe calcular a partir de los datos presentados en las tablas referidas. No es suficiente conocer qué protocolos se transmiten en la red (a no ser que se esté realizando un estudio de seguridad de la misma); sino que se desea conocer cuántos datos se transmiten de cada protocolo.

La próxima sentencia afirma que *Netflow* pudiera no ser la herramienta de monitoreo y gestión adecuada. De acuerdo a la plataforma de red disponible en la empresa (así como, obviamente, del tamaño de la red a servir), se puede dar el caso de que la herramienta idónea sea el *Flexible Netflow*, sucesor de *Netflow*, con mejores prestaciones y utilización de los recursos físicos del dispositivo de red debido a la forma en la que captura los datos.

Esta afirmación debe ser tomada en cuenta junto con la tercera conclusión presentada en la sección. Realmente debe ser realizado un profundo estudio de las características de *hardware* disponibles en los dispositivos de red antes de decidir la variedad de *Netflow* que será utilizada.

Finalmente, la última conclusión establece que no es suficiente el hecho de habilitar y configurar *Netflow*, así como una herramienta basada en ella. Si la empresa realmente desea monitorear y conocer el estado de su red corporativa (así como tomar decisiones basándose en ese estado) debe disponer de personal especializado capaz de interpretar los datos que dicha herramienta arroje. De acuerdo al tamaño de la empresa y de la red propia, podría ser un extenso grupo o unas pocas personas (incluso una).

La herramienta o cualquiera de las aplicaciones que se diseñen a partir de ella, a pesar la extensión de los reportes que genere, no son capaces de tomar

decisiones y aplicarlas en base a los datos que aparecen en dichos reportes. Se pueden automatizar lo más posible e incluir la mayor cantidad de datos, pero siempre será necesaria una persona que los analice y utilice para el correcto funcionamiento de la red.

VI.2. Recomendaciones

La sección propone algunas actividades que se consideran de utilidad a raíz del Trabajo de Grado. Estas recomendaciones no están relacionadas con los objetivos del mismo, sino que se consideran adicionales a los mismos, pero así mismos necesarias para el buen funcionamiento de las redes de monitoreo basadas en *Netflow* (en general cualquier red de datos).

1. Desarrollar de una aplicación web que genere reportes personalizados a partir de la data capturada por *Netflow*.
2. Diseñar y desarrollar de una aplicación web que capture los tiempos de actividad de las estaciones de trabajo de la red.
3. Utilizar de la herramienta Flexible Netflow para el monitoreo de redes en las cuales existe una gran demanda de usuarios, así como en aquellas redes formadas por dispositivos superiores de la gama Catalyst de CISCO.
4. Activar la función de conmutación avanzada "CISCO Express Forwarding" cuando se utilice Netflow como herramienta de monitoreo de la red.
5. Configurar en las estaciones de trabajo conectadas a la red la actividad por permisos.

La primera recomendación de la sección implica el diseño y desarrollo de una aplicación que, basándose en la data creada por *Netflow*, la presente en la forma de reportes de acuerdo con las características seleccionadas por los usuarios finales de estos reportes que, de acuerdo a las conclusiones presentadas en la sección VI.1, debe ser personal especializado.

Se recomienda que el acceso a esta aplicación sea a través de un navegador *web*, con lo cual se obtiene independencia del sistema operativo en la

estación de trabajo desde la cual se realiza la consulta. Aunque implica un alto grado de desarrollo debido a las variables informáticas involucradas en el tratamiento y manipulación de la información, es lo ideal cuando se tienen aplicaciones que siguen el modelo cliente – servidor debido a que, normalmente, los servidores y las estaciones de trabajo ejecutan sistemas operativos diferentes.

Como segunda acción, se recomienda utilizar *Flexible Netflow* para el monitoreo de las redes con plataformas CISCO avanzadas. Ejemplo de estas plataformas son las series 4500, 6500 y 7200 (conmutación); así como la serie ASR (enrutamiento).

Esto se debe a que ellas están preparadas para transmitir data a una velocidad mucho mayor que las series corporativas más económicas, con lo cual el *Netflow* puro deja de ser útil. Se requiere de un nuevo esquema de captura para no comprometer el funcionamiento de la red, el cual es provisto por el mencionado protocolo.

La tercera recomendación establece activar la herramienta CISCO *Express Forwarding*, la cual es una técnica diseñada por CISCO para incrementar la velocidad de las redes y de los dispositivos mediante la reducción de la cantidad de información que aparece en los encabezados de cada una de las transmisiones realizadas.

Esta recomendación implica que el procesador del enrutador o conmutador esté más libre para la ejecución de tareas adicionales (tales como *Netflow*) en períodos de gran actividad de la red. Permite no comprometer los recursos de *hardware* disponibles en perjuicio de la actividad de red. Ya se ha mencionado que *Netflow* hace un uso intensivo del procesador, memoria *flash*, etc.

Finalmente, es muy recomendable establecer en todas las estaciones de trabajo la actividad por permisología. Esto implica que el usuario de las estaciones de trabajo requiera una contraseña y privilegios determinados para poder realizar cualquier actividad que pueda ser considerada de administración (instalación de *software,* ejecución de consultas, acceso remoto a dispositivos, etc.

Constituye una muy buena medida de seguridad ya que se asegurará que el usuario, de forma consciente o inconsciente, no tenga la capacidad de introducir a la red corporativa ningún protocolo que no esté permitido dentro de ella.

Un punto muy asociado a esta recomendación es el establecimiento de una "Política de Seguridad". Existe mucha documentación disponible acerca de ella. Se recomienda que, antes de ejecutar la recomendación propiamente dicha, se cree y ejecute una política de seguridad clara y concisa para establecer claramente lo que cada usuario puede transmitir hacia la red (protocolos permitidos y no permitidos), así como también las actividades que éste puede realizar dentro de la misma.

ANEXO I. DISPOSITIVOS Y MATERIALES UTILIZADOS

En el anexo se presentan las características de los dispositivos utilizados en el Trabajo de Grado. Fueron utilizados:

6. Enrutador CISCO 2900.
7. Conmutador CISCO 2950.
8. Conmutador CISCO 1900.
9. Cable serial.
10. Cable UTP categoría 5E.

Para más información sobre las configuraciones aplicadas a cada dispositivo consultar el Capítulo IV "PROCEDIMIENTO APLICADO". Se presentan en el anexo los *datasheet* de cada dispositivo, provistos por CISCO. Se presentarán los *datasheet* de los tres dispositivos utilizados. Los *datasheet* se encuentran en idioma inglés, ya que es el utilizado por la empresa CISCO en todas sus publicaciones.

1. Cisco 2900

La serie de enrutadores CISCO 2900 pertenece a una gama de productos denominada ISR: *Integrated Services Router.* De acuerdo con (CISCO SYSTEMS, s.f.), la serie de enrutadores está diseñada para cumplir con los requerimientos de las redes de las pequeñas y medianas empresas que hoy en día hacen vida económica. Dicen que la plataforma es capaz de desarrollar servicios virtualizados cuando así sea requerido.

En la próxima página se presenta el *datasheet* de la plataforma, provisto por CISCO.

Data Sheet

Cisco 2900 Series Integrated Services Routers

Cisco® 2900 Series Integrated Services Routers build on 25 years of Cisco innovation and product leadership. The new platforms are architected to enable the next phase of branch-office evolution, providing rich media collaboration and virtualization to the branch while maximizing operational cost savings The Integrated Services Routers Generation 2 platforms are future-enabled with multicore CPUs, support for high- capacity digital signal processors (DSPs) for future enhanced video capabilities, high- powered service modules with improved availability, Gigabit Ethernet switching with enhanced Power over Ethernet (PoE), and new energy monitoring and control capabilities while enhancing overall system performance. Additionally, a new Cisco IOS® Software Universal image and Services-Ready Engine module enable you to decouple the deployment of hardware and software, providing a flexible technology foundation that can quickly adapt to evolving network requirements. Overall, the Cisco 2900 Series offer unparalleled total cost of ownership savings and network agility through the intelligent integration of market-leading security, unified communications, wireless, and application services.

Figure 1. Cisco 2900 Series Integrated Services Routers

Product Overview

Cisco 2900 Series builds on the best-in-class offering of the existing Cisco 2800 Series Integrated Services

Routers by offering four platforms (Figure 1): the Cisco 2901, 2911, 2921, and 2951 Integrated Services Routers.

All Cisco 2900 Series Integrated Services Routers offer embedded hardware encryption acceleration, voice- and video-capable digital signal processor (DSP) slots, optional firewall, intrusion prevention, call processing, voicemail, and application services. In addition, the platforms support the industries widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, copper and fiber GE.

Key Business Benefits

The Integrated Services Routers Generation 2 (ISR G2) provide superior services integration and agility. Designed for scalability, the modular architecture of these platforms enables you to grow and adapt with your business needs. Table 1 lists the business benefits of the Cisco 2900 Series.

Table 1. Key Business Benefits of the Cisco 2900 Series Integrated Services Routers

Benefits	Description
Services Integration	• The Cisco 2900 Series ISRs offer increased levels of services integration with voice, video, security, wireless, mobility, and data services, enabling greater efficiencies and cost savings.
Services On Demand	• A single Cisco IOS® Software Universal image is installed on each ISR G2. The Universal image contains **all** of the Cisco IOS Software technology sets which can be activated with a software license. This allows your business to quickly deploy advanced features without downloading a new Cisco IOS Software image. Additionally, larger default memory is included to support the new capabilities. • The Cisco Services Ready Engine (SRE) enables a new operational model which allows you to reduce capital expenditures (CapEx) and deploy a variety of application services as needed on a single integrated compute services module.
High Performance with Integrated Services	• The Cisco 2900 Series enables deployment in high speed WAN environments with concurrent services enabled up to 75 Mbps. • A multigigabit fabric (MGF) enables high-bandwidth module-to-module communication without compromising routing performance.
Network Agility	• Designed to address customer business requirements, the Cisco 2900 Series modular architecture offers increased capacity and performance as your network needs grow. • Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency.
Energy Efficiency	• The Cisco 2900 Series architecture provides energy-saving features that include the following: ◦ The Cisco 2900 Series offers intelligent power management and allows the customer to control power to the modules based on the time of day. Cisco EnergyWise technology will be supported in the future. ◦ Services integration and modularity on a single platform performing multiple functions, optimizes raw materials consumption and energy usage. ◦ Platform flexibility and ongoing development of both hardware and software capabilities lead to a longer product lifecycle, lowering all aspects of the total cost of ownership, including materials and energy use. ◦ High efficiency power supplies are provided with each platform.

Investment Protection	• The Cisco 2900 Series maximizes investment protection: ◦ Reuse of a broad array of existing modules supported on the original Integrated Services Routers provides a lower cost of ownership. ◦ A rich set of Cisco IOS Software features carried forward from the original Integrated Services Routers and delivered in a single universal image. ◦ Flexibility to adapt as your business needs evolve.

Platform Architecture and Modularity

The Cisco 2900 Series is architected to meet the application demands of today's branch offices with design flexibility for future applications. The modular architecture is designed to support increasing bandwidth requirements, time-division multiplexing (TDM) interconnections, and fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE (ePoE). Table 2 lists the architectural features and benefits of the Cisco 2900 Series.

Table 2. Architectural Features and Benefits

Architectural Feature	Benefits
Modular Platform	• The Cisco 2900 Series ISRs are highly modular platforms with several types of module slots to add connectivity and services for varied branch-office network requirements. • The ISRs offer an industry-leading breadth of LAN and WAN connectivity options through modules to accommodate field upgrades for future technologies without requiring a platform replacement.
Processors	• The Cisco 2900 Series are powered by high-performance multi-core processors that can support the growing demands of high-speed WAN connections to the branch-office while also running multiple concurrent services.
Embedded IP Security (IPSec) VPN Hardware Acceleration	• Embedded hardware encryption acceleration is enhanced to provide higher scalability, which combined with an optional Cisco IOS Security license, enables WAN link security and VPN services (IPSec acceleration). • The onboard encryption hardware replaces and outperforms the advanced integration modules (AIMs) of previous generations.

Architectural Feature	Benefits
Multigigabit Fabric (MGF)	• The Cisco 2900 Series introduces an innovative multigigabit fabric (MGF) that allows for efficient module-to-module communication, enabling tighter services interactions across modules while reducing the overhead on the route processor.
TDM Interconnectivity Fabric	• Unified communications services in the branch office are significantly enhanced with the use of a TDM interconnectivity fabric in the system architecture, allowing for scaling of DS-0 channel capacity.
Integrated Gigabit Ethernet Ports	• All onboard WAN ports are 10/100/1000 Gigabit Ethernet WAN routed ports. • One of the three 10/100/1000 Ethernet WAN ports on the Cisco 2921 and 2951 supports Small Form-Factor Pluggable (SFP)-based connectivity in lieu of a RJ-45 port and enabling fiber connectivity.
Innovative Universal-Serial-Bus (USB)-Based Console Access	• A new, innovative USB console port offers management connectivity for devices without a serial port such as modern laptop computers. • Traditional console and auxiliary ports are also available.
Optional Integrated Power Supply for Distribution of PoE and Universal DC Power Supply	• An optional upgrade to the internal power supply provides inline power (802.3af-compliant PoE and Cisco Inline Power) to integrated switch modules. • On the Cisco 2911, 2921, and 2951, an optional DC power supply will be available in the future that extends deployment into central offices and industrial environments.
Optional External Redundant Power Supply (RPS)	• The Cisco 2911, 2921, and 2951 allow for power redundancy through the use of an external RPS device, thereby decreasing network downtime and protecting the network from power-supply failures. • Redundant power on the Cisco 2900 Series is supported through the Cisco RPS 2300 Redundant Power System. You can use the Cisco RPS 2300 to provide redundant power for Cisco 2900 Series ISRs as well as Cisco Catalyst® switches. • In order to use the Cisco RPS 2300, an external RPS adapter is required (configurable option) to connect the platform to the external RPS.

PoE Boost	• When connected to an external RPS device, the Cisco 2911, 2921, and 2951 can operate in a PoE boost configuration in lieu of redundant power mode - whereby the power capacity of the platform is increased to twice the normal level to power additional PoE ports.
Designed for Flexible Deployments	• The Cisco 2911 and 2951 are designed for NEBS environments. • The 2911 is 12" deep and has an optional fan filter for deployments in a variety of environments. An assembly that provides front-to-back airflow is also available for 23" racks.

Modularity Features and Benefits

The Cisco 2900 Series provides significantly enhanced modular capabilities (refer to Table 3) offering investment protection for customers. Most of the modules available on previous generations of Cisco routers, such as the Cisco 2800 Series, are supported on the Cisco 2900 Series. Additionally, modules can be used on other supported Cisco platforms to provide maximum investment protection. Taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

A complete list of supported modules, including a list of supported SFPs for the Cisco 2900 Series, is available at:

http://www.cisco.com/go/2900.

Table 3. Modularity Features and Benefits

ISR Modules	Benefits
Cisco Service Module	• Each service module slot offers high-data-throughput capability: ◦ Up to 4 Gbps aggregate toward the route processor. ◦ Up to 2 Gbps aggregate to other module slots over MGF. • Service module (SM) slots are highly flexible with support for double-wide service modules (SM-Ds), which are Service Modules that require two SM slots. SM-Ds in the Cisco 2921 and 2951 provide flexibility for higher-density modules. • A service module slot replaces the network module and the extension module for voice/fax (EVM) slots and is offered on Cisco 2911, 2921, and 2951 ISRs. • An adapter module enables backward compatibility with existing network modules, enhanced network modules (NMEs), and EVMs. • Service module slots provide twice the power capabilities relative to the network-module slots, allowing for flexibility for higher-scale and better-performance modules. • Power to service module slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.
ISR Modules	**Benefits**
Cisco Unified Computing System™ (Cisco UCS®) E-Series Servers	Cisco UCS E-Series Servers are next-generation power-optimized, general-purpose x86 64-bit blade servers that provide: • Integrated networking • Virtualization optimization • Four- or six-core Intel Xeon processors • Hardware RAID 0, 1, and 5 support • Cisco Integrated Management Controller (IMC)
Cisco UCS E-Series Network Compute Engine (NCE)	The Cisco UCS E-Series Network Compute Engine is a series of compute modules that are both price- and power-optimized for hosting a variety of Cisco network applications and other applications: • Integrated networking • Virtualization-ready • Two-core Intel processors • Cisco IMC

Cisco Internal Services Module (ISM)	• A single ISM slot provides flexibility to integrate intelligent service modules on an internal slot within the chassis • Each ISM slot offers high-data-throughput capability: ◦ Up to 4 Gbps aggregate toward the route processor. ◦ Up to 2 Gbps aggregate to other module slots over the MGF. • The ISM replaces the AIM slot; existing AIM modules are not supported in the ISM slot. • Power to ISM slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.
Cisco High-Density Packet Voice Digital Signal Processor (DSP) Module (PVDM3) Slots on Motherboard 	• PVDM3 slots natively support PVDM3 modules, providing support for richer density for rich-media voice and video. • Each PVDM3 slot connects back to the system architecture through a 2 Gbps aggregate link through the MGF. • Investment protection for PVDM2 modules is supported through an adapter module. • Power to the PVDM slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.
Compact Flash Slots	• Two external Compact Flash slots are available on the Cisco 2900 Series Integrated Services Routers. Each slot can support high-speed storage densities upgradeable to 4 GB in density.
USB 2.0 Ports	• Two high-speed USB 2.0 ports are supported. The USB ports enable secure token capabilities and storage.

Cisco IOS Software

Cisco 2900 Series Integrated Services Routers deliver innovative technologies running on industry-leading Cisco IOS Software. Developed for wide deployment in the world's most demanding enterprise, access, and service provider networks, the Integrated Services Routers Generation 2 platforms are supported on Cisco IOS Software releases 15M&T. Release 15.0(1)M is available immediately and provides support for a comprehensive portfolio of Cisco technologies, including the functionality and features delivered in releases 12.4 and 12.4T. New innovations in 15.0(1)M span multiple technology areas, including security, voice, high availability, IP Routing and Multicast, quality of service (QoS), IP Mobility, Multiprotocol Label Switching (MPLS), VPNs, and embedded management.

Cisco IOS Software Licensing and Packaging

A single Cisco IOS Universal image encompassing all Cisco IOS Software technology feature sets is delivered with the platforms. You can enable advanced features by activating a software license on the Universal image. In previous generations of access routers, these feature sets required you to download a new software image. Technology packages and feature licenses, enabled through the Cisco software licensing infrastructure, simplify software delivery and decrease the operational costs of deploying new features.

Four major technology licenses are available on the Cisco 2900 Series Integrated Services Routers; you can activate the licenses through the Cisco software activation process identified at http://www.cisco.com/go/sa. The four licenses are as follows:

- IP Base: This technology package is available as default.
- Data
- Unified Communications
- Security (SEC) or Security with No Payload Encryption (SEC-NPE)

```
R2#show ip cache flow
IP packet size distribution (79 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .063 .936 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 2 added
  91 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  1 active, 1023 inactive, 2 added, 2 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
UDP-other            1       0.0         5    32      0.0       0.2      15.6
Total:               1       0.0         5    32      0.0       0.2      15.6

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/1/0       10.0.0.10       Local         209.165.200.151 01 0000 0800    74
R2#
```

FIGURA 27. Captura del protocolo ICMP

La FIGURA 27 muestra que fue transmitido un mensaje *ping*, perteneciente al protocolo ICMP. Este protocolo establece que se enviará una ráfaga de cinco mensajes, cada uno con un tamaño de 32 bytes.

Se puede apreciar que los mensajes fueron enviados desde la interfaz serial cuya dirección IP es 10.0.0.10; hacia la dirección 209.165.200.151, correspondiente a una interfaz lógica (virtual) conocida como "Interfaz de *Loopback*", que se usa para:

- Probar conectividad de red en los enrutadores CISCO sin la necesidad de general tráfico de red hacia el exterior, simulando la existencia de una interfaz con un enlace hacia un ISP.
- Descartar aquellos paquetes que no interesa mantener en la memoria del enrutador por cualquier razón, tal como la existencia de errores en su encabezado de capa de red.

Se aprecia finalmente que no se especifica ningún protocolo de capa de Transporte en la captura presentada en la FIGURA 27.

En la FIGURA 28 se aprecia la captura de una transmisión utilizando el protocolo TFTP, el cual se utiliza para realizar la descarga de archivos desde un servidor instalado en un sistema informático o de red. Este protocolo funciona bajo el modelo cliente – servidor.

```
R2#show ip cache flow
IP packet size distribution (234 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .042 .944 .012 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 22 added
  412 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          10      0.0         4    46      0.0       1.2       5.7
TCP-FTP              2      0.0         3    40      0.0       1.0       1.1
UDP-TFTP             4      0.0         1    58      0.0       0.0      15.5
UDP-other            2      0.0         5    32      0.0       0.2      15.6
ICMP                 2      0.0        83    60      0.0      88.4      15.3
Total:              20      0.0        11    55      0.0       9.6       9.1
```

FIGURA 28. Captura del protocolo TFTP

La FIGURA 28 la captura de las transmisiones correspondientes a una secuencia de solicitud más respuesta en el protocolo TFTP. Consultar la sección V.2.

Se puede identificar que en la secuencia capturada fueron transmitidos un total de veinte flujos. De ellos, ocho corresponden a la transmisión capturada; mientras que el resto corresponde a actividades residuales que la estación de trabajo estaba realizando con respecto a otras transmisiones realizadas (transmisiones Telnet e ICMP).

Aunque no se menciona explícitamente en la tabla resumen, se puede comprobar en la FIGURA 28 que un mensaje TFTP utiliza el protocolo UDP de capa de Transporte para realizar el control de sus transmisiones extremo a extremo.

En la Tabla 16 se observa la cantidad de bytes transmitidos en esta captura, con respecto al protocolo TFTP.

Tabla 16. Datos de flujos con paquetes TFTP

PROTOCOLO	TOTAL DE FLUJOS	PAQUETES POR FLUJO	BYTES POR PAQUETE
FTP	2	3	40
TFTP	4	1	58
OTRO	2	5	32

En la FIGURA 29 se aprecia la captura de la transmisión realizada utilizando el protocolo HTTP. Esta transmisión se realizó utilizando un navegador web.

Se aprecia en la FIGURA 29 que el WWW, nombre con el que *Netflow* identifica al protocolo HTTP debido a que es su aplicación más conocida y común, utiliza el protocolo de capa de Transporte TCP para el control de sus transmisiones.

Fueron capturados seis flujos pertenecientes a este protocolo, con un total de seis paquetes agrupados, tres por flujo.

En la Tabla 17 se observa la cantidad de bytes almacenados en los flujos que reflejados por la FIGURA 28.

```
R2#show ip cache flow
IP packet size distribution (252 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .039 .948 .011 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  0 active, 4096 inactive, 28 added
  482 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          10       0.0         4    46      0.0       1.2       5.7
TCP-FTP              4       0.0         3    45      0.0       1.0       8.1
TCP-WWW              4       0.0         3    45      0.0       1.0       8.3
TCP-other            2       0.0         3    45      0.0       1.0       8.5
UDP-TFTP             4       0.0         1    58      0.0       0.0      15.5
UDP-other            2       0.0         5    32      0.0       0.2      15.6
ICMP                 2       0.0        83    60      0.0      88.4      15.3
Total:              28       0.0         9    54      0.0       7.1       9.4

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
R2#_
```

FIGURA 29. Captura del protocolo HTTP

Tabla 17. Datos correspondientes al protocolo HTTP

PROTOCOLO	TOTAL DE FLUJOS	PAQUETES POR FLUJO	BYTES POR PAQUETE
HTTP	4	3	45
OTRO	2	2	58

En la FIGURA 30 se aprecia una captura global en la que se almacenan todos los protocolos que, al momento de ser realizada, estaban siendo transmitidos desde las estaciones de trabajo hacia la red instalada.

```
IP packet size distribution (252 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .039 .948 .011 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 28 added
  476 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          10       0.0         4    46      0.0       1.2       5.7
TCP-FTP              4       0.0         3    45      0.0       1.0       8.1
TCP-WWW              4       0.0         3    45      0.0       1.0       8.3
TCP-other            1       0.0         3    40      0.0       1.0       1.5
UDP-TFTP             4       0.0         1    58      0.0       0.0      15.5
UDP-other            2       0.0         5    32      0.0       0.2      15.6
ICMP                 2       0.0        83    60      0.0      88.4      15.3
Total:              27       0.0         9    54      0.0       7.4       9.2

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/1/1       10.0.0.138      Se0/1/0       10.0.0.10       06 C00D 0D3D     3
R2#
```

FIGURA 30. Captura de varios protocolos I

Se aprecia la transmisión de mensajes bajo los protocolos Telnet, FTP, TFTP, HTTP e ICMP. Consultar la sección V.2 para más información sobre su presencia en esta captura.

Puede ser notado que fueron realizadas tres transmisiones desde la interfaz Serial 0/1/1 hacia la interfaz Serial 0/1/0. Consultar la sección V.2.

Los datos fueron enviados desde el puerto de capa de Transporte C00D (valor hexadecimal correspondiente a 49165 en decimal) hacia el puerto 0D3D (valor correspondiente al 3389 decimal). Consultar la sección V.2.

En la Tabla 18 se aprecia el total de bytes capturados en la FIGURA 29.

Tabla 18. Captura de diferentes protocolos I

PROTOCOLO	TOTAL DE FLUJOS	PAQUETES POR FLUJO	BYTES POR PAQUETE
Telnet	10	4	46
FTP	4	3	45
HTTP	4	3	45
OTRO	1	3	40
TFTP	4	1	58
ICMP	2	83	60

En la FIGURA 31 se aprecia otra captura similar a la mostrada en la FIGURA 30.

La principal diferencia entre las dos ilustraciones mencionadas es que en la FIGURA 30 sólo se capturó una transmisión; mientras que en la FIGURA 31 fueron capturadas dos transmisiones realizadas desde la interfaz Serial 0/1/1 hacia la interfaz Serial 0/1/0.

Adicionalmente, en la captura de la FIGURA 31 no se capturó la entrada correspondiente a "TCP – OTHER". Consultar la sección V.2.

```
R2#show ip cache flow
IP packet size distribution (246 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .040 .947 .012 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 26 added
  441 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet          10       0.0         4    46      0.0       1.2       5.7
TCP-FTP              4       0.0         3    45      0.0       1.0       8.1
TCP-WWW              2       0.0         3    40      0.0       1.0       1.5
UDP-TFTP             4       0.0         1    58      0.0       0.0      15.5
UDP-other            2       0.0         5    32      0.0       0.2      15.6
ICMP                 2       0.0        83    60      0.0      88.4      15.3
Total:              24       0.0        10    55      0.0       8.2       9.0

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Se0/1/0       10.0.0.10       Se0/1/1       10.0.0.138      06 C009 0050     3
Se0/1/0       10.0.0.10       Se0/1/1       10.0.0.138      06 C008 0050     3
```

FIGURA 31. Captura de varios protocolos II

En la Tabla 19 se aprecia el total de bytes almacenados en los flujos capturados en la FIGURA 31.

Tabla 19. Captura de diferentes protocolos II

PROTOCOLO	TOTAL DE FLUJOS	PAQUETES POR FLUJO	BYTES POR PAQUETE
Telnet	10	4	46
FTP	4	3	45
HTTP	2	3	40
TFTP	4	1	58
ICMP	2	83	60

No serán realizados mayores comentarios sobre el contenido de la Tabla 19 debido a que éste es similar al de la Tabla 18, variando los valores de los diferentes campos.

V.2. Análisis de resultados

El protocolo ICMP varía su funcionamiento de acuerdo al sistema operativo instalado en el sistema informático desde el cual se construye un mensaje que siga este protocolo. Por ejemplo, las implementaciones basadas en cualquier distribución de *kernel* LINUX envían mensajes en primer plano hasta que el usuario ordena detener esta operación; pero los sistemas *WINDOWS* envían cinco mensajes en primer plano para que el usuario tenga acceso a las estadísticas del resultado de los mensajes. Sin embargo, en segundo plano, el sistema continúa enviando mensajes a la dirección IP especificada en la construcción del mensaje.

Por esta razón se observa que en las figuras FIGURA 28, FIGURA 29, FIGURA 30 y FIGURA 31 fueron capturados 166 mensajes en vez de los cinco que se aprecian en la FIGURA 27.

V.2.1. Seguridad

Se aprecia en las cinco gráficas que el primer uso que se le puede dar a *Netflow* es la identificación de inconvenientes en la seguridad de la red al detectar los protocolos que la misma está procesando en cada instante particular.

En el caso del Trabajo de Grado, en la red sólo debían aparecer los protocolos HTTP, FTP, TFTP, e ICMP debido a que no existen en las estaciones de trabajo del laboratorio utilizado otras aplicaciones. Sólo está instalado un navegador web y un cliente TFTP. Al no estar estas estaciones de trabajo conectadas a la red corporativa de la academia, ni a Internet, la red no debe procesar ningún protocolo perteneciente a otras aplicaciones diferentes a las mencionadas. Por esta razón, si existiera en las capturas presentadas otros protocolos adicionales, podríamos decir sin temor a errores que existe un problema de seguridad en la red y habría que pensar en la existencia de virus en las estaciones de trabajo.

Se aprecia en las figuras de la sección V.1 las direcciones IP de los encabezados de capa de red de los diferentes mensajes capturados por *Netflow*. Al conocer el esquema de direccionamiento aplicado en la red (consultar la sección IV.2.1), se debe comparar las direcciones que pueden ser asignadas en los diferentes rangos que se pueden crear a partir de él (el esquema de direccionamiento) con las direcciones efectivas transmitidas por la red.

Si existe en la red alguna dirección IP que no está contenida dentro de ninguno de los rangos que pueden ser creados a partir del esquema efectivamente aplicado a la red, se puede considerar una de las siguientes afirmaciones:

- Existe un intruso en la red: una estación de trabajo que no pertenece a la red se encuentra conectada a ella, transmitiendo mensajes pertenecientes a diferentes aplicaciones que potencialmente tienen la capacidad de provocar destrozos en el sistema informático instalado.
- Existe algún tipo de *software* malicioso instalado en alguna de las estaciones de trabajo de la red transmitiendo sus mensajes, con la potencialidad de provocar destrozos en el sistema y de robar información.

Las capturas mostradas en las figuras de la sección V.1 pueden proveer así mismo información importante sobre los protocolos que, estando autorizados, están corriendo en la red.

Es importante conocer el funcionamiento de cada protocolo. Por ejemplo, lo básico de todos los protocolos utilizados en el laboratorio instalado para la realización del Trabajo de Grado es que funcionan bajo el modelo cliente – servidor. Este modelo especifica que todas las conexiones se originan en una estación de trabajo (que funciona como cliente), y que deben ser respondidas por otra estación de trabajo (que funcione como servidor).

En las figuras de la sección V.1 se aprecia que:

- Existen paquetes con la denominación "*TCP – OTHER*".
- Existen paquetes con la denominación "*UDP-OTHER*".

El protocolo TFTP utiliza el protocolo de capa de transporte UDP para su funcionamiento. Como protocolo que sigue el modelo cliente – servidor, éste se basa en que una estación de trabajo (cliente) envía una solicitud a otra estación de trabajo (servidor) para descargar un archivo contenido en alguno de sus directorios.

Existen dos tipos de mensajes principales: los mensajes de solicitud y respuesta intercambiados entre el cliente y el servidor (incluyendo aspectos del establecimiento, mantenimiento y cierre de la sesión entre ambos); y los mensajes relacionados mediante los cuales se intercambia propiamente la información solicitada.

Los diferentes paquetes en los que viajan los archivos solicitados por el cliente son transmitidos por el servidor mediante un tipo de conexión conocida como "relacionada". Una conexión relacionada es aquella que, sin ser propiamente la conexión original, está relacionada con ésta.

En el caso de TFTP, las conexiones relacionadas son aquellas conexiones originadas como consecuencia del intercambio de mensajes entre un cliente y un servidor; es decir, la transferencia propiamente dicha de los archivos.

Por esta razón, toda comunicación mediante TFTP debe poseer un número igual o mayor de conexiones relacionadas (UDP – OTHER) que de conexiones originales (UDP – TFTP).

HTTP, que opera con el protocolo de capa de Transporte TCP, trabaja de forma similar. Los mensajes de solicitud y de respuesta (sólo texto) se envían mediante conexiones "originales".

Una página web está formada por texto, imágenes, audio, video, etc. Toda la parte multimedia de la misma es muy pesada (son archivos de gran tamaño) en comparación con el texto de la misma. Por esta razón, el servidor transmite el código HTML de las páginas web en dos partes: el relacionado con el texto mediante conexiones "originales" y el relacionado con la parte multimedia en conexiones "relacionadas".

Se extrae de esto que, al igual que con el protocolo TFTP, toda conexión HTTP debe estar formada por dos tipos de conexiones: la "original" (TCP-HTTP), y un número igual o superior de paquetes "relacionados" (TCP-OTHER).

El aspecto que se debe tener en cuenta es que, si en la captura que *Netflow* realice se encuentran paquetes TCP-OTHER o UDP-OTHER, pero no se encuentran las conexiones originales TCP-HTTP y UDP-TFTP, podríamos estar en presencia de una amenaza de seguridad o de algún *software* malicioso en la red debido a que este tipo de conexiones no se pueden crear si no existe una solicitud previa desde el sistema.

Adicionalmente, se debe verificar que el origen y el destino de las conexiones "originales" y de las relacionadas sean contrarios debido a que todas las conexiones relacionadas de cualquier protocolo que siga el modelo cliente – servidor debe ser originada en el destino de las conexiones originales (es decir, todas las conexiones relacionadas se originan en el servidor y van dirigidas al cliente). Si esto no sucede, podríamos estar en presencia de alguno de los problemas de seguridad ya mencionados previamente.

El último aspecto de seguridad que se debe tomar en cuenta es el tiempo en el que los flujos permanecen activos en la base de datos *Netflow Collector.* Mientras más tiempo permanezca un flujo activo, hay un problema de seguridad debido a que se trata de un espacio de memoria que permanece abierto para ser modificado por el ente que acceda a éste (tanto autorizado como no autorizado).

En las figuras de la sección V.1 se aprecia que el tiempo en el que los flujos correspondientes al protocolo ICMP permanecen activos en la memoria del enrutador es mucho mayor que el tiempo en el que los demás protocolos capturados permanecen activos. Esto se debe a que, como se dijo al principio de la sección en curso, el sistema operativo *WINDOWS* mantiene una línea de comunicación abierta con el destino de la conexión durante un tiempo posterior a la entrega del resultado de la operación al usuario. Cuando se detecte esta situación (tiempo activo del flujo muy elevado) se debe bloquear este protocolo en la red debido a que es una fuente muy común de ataques a la seguridad por parte de quienes tienen intereses ocultos

en la red. Adicionalmente, representa una forma muy básica de ataques a la seguridad de la red mediante lo que se conoce como "denegación de servicio", que consiste en bombardear al sistema con mensajes para ocupar toda su atención y recursos en responderlos.

V.2.2. Tráfico

A partir de la información suministrada en las figuras de la sección V.1, compendiadas en las tablas de la misma sección, se puede calcular:

- La cantidad de datos transmitidos por la red hacia el exterior.
- La velocidad utilizada por esos datos para salir de la red corporativa.

Ninguno de los dos datos se puede obtener directamente de la información ofrecida por *Netflow*, sino que debe ser calculada a partir de ella.

Referirse a la Tabla 16. En ella se observa que fueron capturados 1920 bits pertenecientes al protocolo FTP, 1856 bits correspondientes al protocolo TFTP, Y 2560 bits correspondientes a la conexión relacionada de TFTP. Se aprecia por ende que la transmisión consistió en descargar un archivo de 2.56 Kb.

Referirse a la Tabla 17. Se aprecia que fueron capturados 4320 bits correspondientes a solicitudes de un navegador para cargar una página web determinada; así como también 1856 bits de conexiones relacionadas.

En este caso, las conexiones relacionadas no tienen nada que ver con la carga de las imágenes y videos que existen en cualquier página web. Debido a que la red creada con el laboratorio del Trabajo de Grado no estaba conectada a la red corporativa de la academia y, por tanto, no tenía acceso a Internet; las conexiones relacionadas no son más que las respuestas erróneas a esos mensajes de solicitud indicando que no se encuentra el destino solicitado.

Los mensajes de error en Internet se transmiten utilizando el protocolo IGMP. Sin embargo, debido a que los enrutadores CISCO conocen que la solicitud que se realiza pertenece al protocolo HTTP (aunque son dispositivos de capa de Red tienen la capacidad de inspeccionar el contenido de la capa de Aplicación de

los mensajes y determinar el protocolo que está encapsulado en ella debido a una característica de seguridad conocida como *Access List*), generan la respuesta de error bajo este protocolo para que la estación de trabajo no tenga que decodificar el contenido del protocolo IGMP, el cual podría no estar instalado en ella.

En las tablas Tabla 18 y Tabla 19 se muestra la misma información que en las primeras dos analizadas, expandiendo la información a todos los protocolos capturados por *Netflow* de forma simultánea; por lo que no vale la pena realizar el análisis nuevamente.

También se puede determinar la velocidad utilizada por las diferentes transmisiones en su camino hacia las redes externas. Éste suele ser el objetivo principal de las empresas ya que los ISP suelen alquilar velocidad de enlaces sobre capacidad transmitida.

Para determinar la velocidad utilizada por cada protocolo o aplicación se debe aplicar la siguiente ecuación:

$$Velocidad = \frac{Data\ transmitida}{Unidad\ de\ tiempo}$$ Ecuación V-1. Cálculo básico de velocidad

La "data transmitida" mencionada en la $Velocidad = \frac{Data\ transmitida}{Unidad\ de\ tiempo}$ Ecuación V-1 corresponde a la analizada a lo largo de esta sección. La "unidad de tiempo" corresponde al campo *"Flows / Sec"*, que puede ser consultado en las ilustraciones FIGURA 27, FIGURA 28, FIGURA 29,FIGURA 30 y FIGURA 31.

Si se analizan las mencionadas ilustraciones se observa que en todas ellas el campo "*Flows / Sec*" tiene un valor de cero, a pesar de que los campos correspondientes a cantidad de data sí poseen valores.

Esto se debe a que para que este valor *"Flows / Sec"* sea diferente de cero, por cuestiones de diseño de la herramienta, se debe realizar una transmisión de forma continuada en el tiempo.

Debido a que todas las transmisiones realizadas fueron transmisiones de prueba, transmisiones que tuvieron una duración limitada, este valor no fue registrado por la herramienta.

Si se hubiera realizado el llamado "ping de la muerte" (que consiste en enviar solicitudes ICMP bajo este formato de forma continua e ininterrumpida en el tiempo hacia cualquier dirección IP), el campo en cuestión tendría un valor diferente de cero, al menos en la fila correspondiente al protocolo ICMP.

En el caso de las capturas correspondientes al protocolo TFTP, para que el valor del campo *"Flows / Sec"* fuera distinto de cero, se debería haber realizado la descarga de un archivo de más de 100 KB (800 Kb).

Aplicando el correspondiente análisis a las capturas del protocolo HTTP, se ve que la condición es que la red de laboratorio hubiese tenido acceso a la red corporativa y, por ende, a Internet.

Este hecho se debe a que *Netflow* fue diseñado para su utilización en ambientes de producción real, en los cuales la transmisión de data es mucho mayor que la utilizada en un laboratorio de prueba.

Es decir, para que el enrutador donde se encuentre habilitado *Netflow* calcule (en vez de recopilar, como sucede con el resto de estadísticas presentadas a lo largo de la sección V.1) el valor del campo *"Flows / Sec"*, el enrutador debe transmitir volúmenes de tráfico reales.

En el Capítulo V serán presentadas las conclusiones y recomendaciones que se desprenden de la información provista y analizada a lo largo del Capítulo V.

Capítulo VI CONCLUSIONES Y RECOMENDACIONES

El capítulo se divide en dos secciones:

- Conclusiones, en la que se presenta y desarrollan las conclusiones obtenidas como consecuencia del trabajo realizado en los capítulos Capítulo IV y Capítulo V.
- Recomendaciones, en la cual se presenta una serie de recomendaciones tendientes a mejorar los resultados obtenidos en el Trabajo de Grado.

VI.1. Conclusiones

Se presentan dos grupos de conclusiones. El primer grupo está basado en los objetivos específicos en los cuales se basa el Trabajo de Grado: se presenta como mínimo una conclusión por cada objetivo específico. El segundo grupo, llamado general, son conclusiones basadas en la experiencia obtenida con la realización del trabajo de grado, que no tienen nada que ver, de forma explícita, con los objetivos específicos planteados en la sección I.3.2.

VI.1.1. Conclusiones basadas en los objetivos específicos

Basándose en los objetivos específicos (en orden ascendente), se pueden enunciar las siguientes conclusiones:

1. El *software Netflow* funciona mediante la recopilación de información procedente de los encabezados de los paquetes IP transmitidos en las redes corporativas. Deben ser utilizadas técnicas adicionales para evitar que el protocolo (que hace una gran utilización de los recursos físicos de procesamiento disponibles en los dispositivos de red) tenga un impacto negativo (de ralentización) en la operación de los elementos donde se habilite.
2. El protocolo *Netflow* viene instalado por defecto en los dispositivos de red de la gama corporativa de CISCO. Consultar la sección II.2.3. Deben ser utilizadas configuraciones adicionales para que la herramienta funcione como desea el administrador de la red.

3. En consonancia con la conclusión número dos, se debe realizar una profunda personalización del protocolo mediante la introducción de una plantilla de configuración adecuada a los intereses de monitoreo y gestión de la red corporativa. Mientras más exhaustiva sea esa configuración, más personalizada estará la herramienta y, por tanto, los datos recopilados podrán ser utilizados con mayor eficiencia por el equipo de redes de la empresa.
4. Debe ser diseñada e implementada una topología física y lógica en las empresas. Se debe estudiar de forma cuidadosa en qué parte de esa topología será habilitado y configurado *Netflow*.
5. Los resultados obtenidos de las pruebas realizadas, y explicadas en el Capítulo V, indican que el protocolo debe ser habilitado sólo en aquellos casos en los cuales las redes corporativas se encuentran en un estado de producción, con una transmisión normal de datos para este tipo de redes.

La primera conclusión de esta sección induce la necesidad de habilitar el uso de técnicas de conmutación avanzadas en los dispositivos de red donde *Netflow* se habilite (entendiendo como conmutación al hecho de recibir, procesar y transmitir datos).

Como se ha dicho previamente a lo largo del trabajo de grado, *Netflow* hace una gran utilización de recursos de los dispositivos de red. El objetivo principal de éstos debe ser la prestación de los servicios disponibles en la red corporativa. Su monitoreo debe ser una herramienta que funciones para la red, no al revés. Debido a esto, se debe optimizar el funcionamiento de las funciones básicas de los dispositivos.

La segunda y tercera conclusiones afirman que se debe configurar completamente el protocolo *Netflow* para asegurar que los datos que recopile sean realmente los que al administrador de la red le interesa estudiar. Esto permite, así mismo, evitar que el protocolo consuma recursos excesivos de los dispositivos de red.

No basta con habilitar el protocolo en los dispositivos de red; ya que los administradores tienen la intención de monitorear la red corporativa, lo cual se consigue filtrando y clasificando la data que el *Netflow* recopila mediante la aplicación de alguna plantilla de configuración.

Se debe recordar que el objetivo fundamental del trabajo de grado es estudiar el protocolo *Netflow* para su uso como herramienta de monitoreo y gestión de las redes corporativas. La personalización (configuración) de la misma permite clasificar la data recopilada por ésta mediante algún criterio establecido en su configuración (consultar la sección IV.2).

La cuarta conclusión implica que antes de decidir la utilización de *Netflow* (y en general de cualquier protocolo o sistema de monitoreo) es necesario diseñar una topología de red (tanto física como lógica) que permita la comunicación de los diferentes elementos conectados mediante la red corporativa.

Será luego de que se tenga claro el diseño a implementar que se podrá estudiar el protocolo de monitoreo a utilizar, así como el elemento de la red en el que será implementado (habilitado).

Se puede dar el caso de que, mediante una topología totalmente diferente a la topología de producción utilizada en la red corporativa, se decida utilizar una topología en paralelo (física o lógica) para el monitoreo de la red.

En cualquier caso, es necesario e indispensable que la topología de la misma sea decidida antes de la implementación de cualquier protocolo de monitoreo (en particular *Netflow*), ya que una vez decidida aquella es que se puede pensar en la habilitación y configuración del mismo (recuérdese que el objetivo de la red, como se indicó previamente, es servir a las aplicaciones instaladas en ella y no a su monitoreo. El monitoreo debe ser un medio secundario utilizado para mantener a la red en óptimas condiciones.

La quinta conclusión confirma lo expresado en el Capítulo V (se repite el mismo razonamiento en la próxima sección, como conclusiones generales del trabajo de grado). *Netflow* debe ser utilizado sólo en redes operativas, no en redes

experimentales. La cantidad de data que el protocolo está diseñado para manejar hace que en cualquier ambiente de laboratorio, en el cual sólo se corren algunas aplicaciones para probar el funcionamiento del protocolo, no se obtengan los resultados deseados.

La herramienta está diseñada para recopilar la gran cantidad de data y protocolos que se transmiten de forma normal en cualquier red corporativa. Por esta razón, cuando se transmiten unos pocos datos experimentales, la herramienta no los captura. Consultar la sección V.2.

Al agrupar patrones similares contenidos en el encabezado IP de la data que circula por la red, *Netflow* "cuenta" la información asociada a éstos. Cuando sólo circulan pocos paquetes de un determinado protocolo, *Netflow* no lo refleja debido a que no ha agrupado información suficiente en su base de datos.

Si se quiere implementar como una prueba antes de su ejecución real, es ideal que se haga en una red de producción comercial real, simulando redes mediante el concepto de las interfaces virtuales. De esta forma no se afecta a la producción real de la red, y se obtienen los resultados deseados desde el principio.

En la próxima sección se desarrollan conclusiones obtenidas en base al trabajo práctico realizado, que no tienen nada que ver con los objetivos específicos del trabajo de grado. El autor del mismo considera que es necesario plasmarlas en el documento debido a que se mencionan aspectos importantes que deben ser tomados en cuenta antes de iniciar la migración hacia *Netflow*.

VI.1.2. Conclusiones generales

De forma general, basándose en la experiencia obtenida al realizar el trabajo de grado, se pueden enunciar las siguientes conclusiones:

1. El protocolo *Netflow* puede y debe ser utilizado como herramienta de medición y clasificación de tráfico en redes corporativas basadas en la tecnología LAN.
2. El protocolo debe ser usado en ambientes de producción empresarial normal, con flujos de tráfico corrientes. No debería ser usado en ambientes de

laboratorio debido a que, por su diseño, no serán aprovechadas todas sus características. Consultar la sección V.2.

3. A pesar de que viene instalado por defecto en todos los sistemas operativos IOS 12.2 o superior, se debe tener cuidado de la plataforma en la que se utilice la herramienta debido al gran uso de recursos que ella hace.
4. *Netflow* tiene aplicaciones que van más allá del clásico monitoreo de los flujos de tráfico.
5. Para realizar una gestión completa de la red corporativa, se deben utilizar los datos arrojados por *Netflow* en el cálculo de otros parámetros. A modo de ejemplo, consultar la $Velocidad = \frac{Data\ transmitida}{Unidad\ de\ tiempo}$ Ecuación V-1.
6. De acuerdo al tamaño de la red corporativa, así como de acuerdo al tipo de plataforma utilizada, *Netflow* pudiera no ser la herramienta de gestión adecuada a utilizar en el monitoreo de la red. Consultar la sección VI.2.
7. Para la adecuada gestión de la red es necesario disponer de personal especializado que se encargue de analizar los datos arrojados por *Netflow*, los cuales por sí mismos no plantean las acciones que son necesarias para corregir las diferentes situaciones que pudieran estar sucediendo en la red.

La primera conclusión confirma la idea básica del Trabajo de Grado: el *Netflow* puede ser utilizado como herramienta de monitoreo en las redes corporativas de las pequeñas y medianas empresas. Esta conclusión implica que si se aplican las técnicas de monitoreo adecuadas, el protocolo es la herramienta de gestión de redes adecuada para ser aplicada en las empresas referidas debido a la gran cantidad de información entregada por este protocolo.

Se especifica en esa afirmación que el protocolo debe ser usado en redes basadas en la tecnología LAN. Esto se debe fundamentalmente a que los enrutadores y conmutadores en los cuales se recomienda la habilitación de este protocolo están diseñados y optimizados para su funcionamiento en este tipo de redes.

Se menciona en el segundo punto de la sección que *Netflow* debe ser utilizado en ambientes corporativos. Esta herramienta no está diseñada para la captura de pequeños flujos de tráfico, sino para grandes cantidades.

Está optimizada para la captura de protocolos utilizados en ambientes reales, tales como HTTP, FTP, etc. (todos ellos utilizados en el Trabajo de Grado). Se debe utilizar en ambientes en los cuales se garantizará un flujo de tráfico extenso, normal en ambientes corporativos que, al fin y al cabo, es donde el protocolo funciona de forma más óptima.

La tercera conclusión afirma que se debe tener cuidado en la plataforma donde se utilizará el protocolo *Netflow*. Esto se debe a que la herramienta hace un extenso uso de los recursos de *hardware* (CPU, memoria flash, etc.) disponibles en el dispositivo de red. No debería ser utilizado cuando los valores físicos instalados en el mismo son pequeños. Se debe recordar que la prioridad de la red no es su monitoreo mediantes ninguna aplicación, sino más bien el servicio a los usuarios conectados con sus dispositivos finales a ella.

Si la plataforma que se posee es básica y realmente se necesita monitorear la transmisión de datos desde ella hacia el exterior, consultar la sección VI.2.

Según la cuarta afirmación de la sección, *Netflow* posee aplicaciones que van más allá del monitoreo propio de la red. Analizando los datos presentados en el Capítulo V se puede apreciar que a partir de estos datos pueden ser desarrolladas aplicaciones que permitan mantener la seguridad de la red (consultar la sección V.2).

A partir de estos datos se pueden diseñar aplicaciones que permitan realizar un control más estricto de las operaciones en la empresa (controlando las horas de actividad de cada estación de trabajo), las actividades realizadas por los trabajadores durante sus horas laborales (sin invadir su privacidad personal), detectando qué protocolos se transmiten desde cada estación de trabajo y comparándola con los que deben ser transmitidos de acuerdo con los roles de cada una; etc.

La quinta afirmación establece que, para encontrar una utilidad completa, así como explotar todas posibilidades del protocolo, se debe realizar cálculos a partir de la data capturada por éste. El mero datos de cuántos flujos circulan por la red no es suficiente para hacer un estudio completo sobre el tráfico que circula a través de la misma.

Debido a este hecho la herramienta muestra datos adicionales, tal como se aprecia en las tablas Tabla 16,Tabla 17,Tabla 18 yTabla 19. La información que realmente importa se debe calcular a partir de los datos presentados en las tablas referidas. No es suficiente conocer qué protocolos se transmiten en la red (a no ser que se esté realizando un estudio de seguridad de la misma); sino que se desea conocer cuántos datos se transmiten de cada protocolo.

La próxima sentencia afirma que *Netflow* pudiera no ser la herramienta de monitoreo y gestión adecuada. De acuerdo a la plataforma de red disponible en la empresa (así como, obviamente, del tamaño de la red a servir), se puede dar el caso de que la herramienta idónea sea el *Flexible Netflow*, sucesor de *Netflow*, con mejores prestaciones y utilización de los recursos físicos del dispositivo de red debido a la forma en la que captura los datos.

Esta afirmación debe ser tomada en cuenta junto con la tercera conclusión presentada en la sección. Realmente debe ser realizado un profundo estudio de las características de *hardware* disponibles en los dispositivos de red antes de decidir la variedad de *Netflow* que será utilizada.

Finalmente, la última conclusión establece que no es suficiente el hecho de habilitar y configurar *Netflow*, así como una herramienta basada en ella. Si la empresa realmente desea monitorear y conocer el estado de su red corporativa (así como tomar decisiones basándose en ese estado) debe disponer de personal especializado capaz de interpretar los datos que dicha herramienta arroje. De acuerdo al tamaño de la empresa y de la red propia, podría ser un extenso grupo o unas pocas personas (incluso una).

La herramienta o cualquiera de las aplicaciones que se diseñen a partir de ella, a pesar la extensión de los reportes que genere, no son capaces de tomar

decisiones y aplicarlas en base a los datos que aparecen en dichos reportes. Se pueden automatizar lo más posible e incluir la mayor cantidad de datos, pero siempre será necesaria una persona que los analice y utilice para el correcto funcionamiento de la red.

VI.2. Recomendaciones

La sección propone algunas actividades que se consideran de utilidad a raíz del Trabajo de Grado. Estas recomendaciones no están relacionadas con los objetivos del mismo, sino que se consideran adicionales a los mismos, pero así mismos necesarias para el buen funcionamiento de las redes de monitoreo basadas en *Netflow* (en general cualquier red de datos).

1. Desarrollar de una aplicación web que genere reportes personalizados a partir de la data capturada por *Netflow*.
2. Diseñar y desarrollar de una aplicación web que capture los tiempos de actividad de las estaciones de trabajo de la red.
3. Utilizar de la herramienta Flexible Netflow para el monitoreo de redes en las cuales existe una gran demanda de usuarios, así como en aquellas redes formadas por dispositivos superiores de la gama Catalyst de CISCO.
4. Activar la función de conmutación avanzada "CISCO Express Forwarding" cuando se utilice Netflow como herramienta de monitoreo de la red.
5. Configurar en las estaciones de trabajo conectadas a la red la actividad por permisos.

La primera recomendación de la sección implica el diseño y desarrollo de una aplicación que, basándose en la data creada por *Netflow*, la presente en la forma de reportes de acuerdo con las características seleccionadas por los usuarios finales de estos reportes que, de acuerdo a las conclusiones presentadas en la sección VI.1, debe ser personal especializado.

Se recomienda que el acceso a esta aplicación sea a través de un navegador *web*, con lo cual se obtiene independencia del sistema operativo en la

estación de trabajo desde la cual se realiza la consulta. Aunque implica un alto grado de desarrollo debido a las variables informáticas involucradas en el tratamiento y manipulación de la información, es lo ideal cuando se tienen aplicaciones que siguen el modelo cliente – servidor debido a que, normalmente, los servidores y las estaciones de trabajo ejecutan sistemas operativos diferentes.

Como segunda acción, se recomienda utilizar *Flexible Netflow* para el monitoreo de las redes con plataformas CISCO avanzadas. Ejemplo de estas plataformas son las series 4500, 6500 y 7200 (conmutación); así como la serie ASR (enrutamiento).

Esto se debe a que ellas están preparadas para transmitir data a una velocidad mucho mayor que las series corporativas más económicas, con lo cual el *Netflow* puro deja de ser útil. Se requiere de un nuevo esquema de captura para no comprometer el funcionamiento de la red, el cual es provisto por el mencionado protocolo.

La tercera recomendación establece activar la herramienta CISCO *Express Forwarding*, la cual es una técnica diseñada por CISCO para incrementar la velocidad de las redes y de los dispositivos mediante la reducción de la cantidad de información que aparece en los encabezados de cada una de las transmisiones realizadas.

Esta recomendación implica que el procesador del enrutador o conmutador esté más libre para la ejecución de tareas adicionales (tales como *Netflow*) en períodos de gran actividad de la red. Permite no comprometer los recursos de *hardware* disponibles en perjuicio de la actividad de red. Ya se ha mencionado que *Netflow* hace un uso intensivo del procesador, memoria *flash*, etc.

Finalmente, es muy recomendable establecer en todas las estaciones de trabajo la actividad por permisología. Esto implica que el usuario de las estaciones de trabajo requiera una contraseña y privilegios determinados para poder realizar cualquier actividad que pueda ser considerada de administración (instalación de *software*, ejecución de consultas, acceso remoto a dispositivos, etc.

Constituye una muy buena medida de seguridad ya que se asegurará que el usuario, de forma consciente o inconsciente, no tenga la capacidad de introducir a la red corporativa ningún protocolo que no esté permitido dentro de ella.

Un punto muy asociado a esta recomendación es el establecimiento de una "Política de Seguridad". Existe mucha documentación disponible acerca de ella. Se recomienda que, antes de ejecutar la recomendación propiamente dicha, se cree y ejecute una política de seguridad clara y concisa para establecer claramente lo que cada usuario puede transmitir hacia la red (protocolos permitidos y no permitidos), así como también las actividades que éste puede realizar dentro de la misma.

ANEXO I. DISPOSITIVOS Y MATERIALES UTILIZADOS

En el anexo se presentan las características de los dispositivos utilizados en el Trabajo de Grado. Fueron utilizados:

6. Enrutador CISCO 2900.
7. Conmutador CISCO 2950.
8. Conmutador CISCO 1900.
9. Cable serial.
10. Cable UTP categoría 5E.

Para más información sobre las configuraciones aplicadas a cada dispositivo consultar el Capítulo IV "PROCEDIMIENTO APLICADO". Se presentan en el anexo los *datasheet* de cada dispositivo, provistos por CISCO. Se presentarán los *datasheet* de los tres dispositivos utilizados. Los *datasheet* se encuentran en idioma inglés, ya que es el utilizado por la empresa CISCO en todas sus publicaciones.

1. Cisco 2900

La serie de enrutadores CISCO 2900 pertenece a una gama de productos denominada ISR: *Integrated Services Router.* De acuerdo con (CISCO SYSTEMS, s.f.), la serie de enrutadores está diseñada para cumplir con los requerimientos de las redes de las pequeñas y medianas empresas que hoy en día hacen vida económica. Dicen que la plataforma es capaz de desarrollar servicios virtualizados cuando así sea requerido.

En la próxima página se presenta el *datasheet* de la plataforma, provisto por CISCO.

Data Sheet

Cisco 2900 Series Integrated Services Routers

Cisco® 2900 Series Integrated Services Routers build on 25 years of Cisco innovation and product leadership. The new platforms are architected to enable the next phase of branch-office evolution, providing rich media collaboration and virtualization to the branch while maximizing operational cost savings The Integrated Services Routers Generation 2 platforms are future-enabled with multicore CPUs, support for high- capacity digital signal processors (DSPs) for future enhanced video capabilities, high- powered service modules with improved availability, Gigabit Ethernet switching with enhanced Power over Ethernet (PoE), and new energy monitoring and control capabilities while enhancing overall system performance. Additionally, a new Cisco
IOS® Software Universal image and Services-Ready Engine module enable you to
decouple the deployment of hardware and software, providing a flexible technology foundation that can quickly adapt to evolving network requirements. Overall, the Cisco
2900 Series offer unparalleled total cost of ownership savings and network agility through the intelligent integration of market-leading security, unified communications, wireless, and application services.

Figure 1. Cisco 2900 Series Integrated Services Routers

Product Overview

Cisco 2900 Series builds on the best-in-class offering of the existing Cisco 2800 Series Integrated Services

Routers by offering four platforms (Figure 1): the Cisco 2901, 2911, 2921, and 2951 Integrated Services Routers.

All Cisco 2900 Series Integrated Services Routers offer embedded hardware encryption acceleration, voice- and video-capable digital signal processor (DSP) slots, optional firewall, intrusion prevention, call processing, voicemail, and application services. In addition, the platforms support the industries widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, copper and fiber GE.

Key Business Benefits

The Integrated Services Routers Generation 2 (ISR G2) provide superior services integration and agility. Designed for scalability, the modular architecture of these platforms enables you to grow and adapt with your business needs. Table 1 lists the business benefits of the Cisco 2900 Series.

Table 1. Key Business Benefits of the Cisco 2900 Series Integrated Services Routers

Benefits	Description
Services Integration	• The Cisco 2900 Series ISRs offer increased levels of services integration with voice, video, security, wireless, mobility, and data services, enabling greater efficiencies and cost savings.
Services On Demand	• A single Cisco IOS® Software Universal image is installed on each ISR G2. The Universal image contains **all** of the Cisco IOS Software technology sets which can be activated with a software license. This allows your business to quickly deploy advanced features without downloading a new Cisco IOS Software image. Additionally, larger default memory is included to support the new capabilities. • The Cisco Services Ready Engine (SRE) enables a new operational model which allows you to reduce capital expenditures (CapEx) and deploy a variety of application services as needed on a single integrated compute services module.
High Performance with Integrated Services	• The Cisco 2900 Series enables deployment in high speed WAN environments with concurrent services enabled up to 75 Mbps. • A multigigabit fabric (MGF) enables high-bandwidth module-to-module communication without compromising routing performance.
Network Agility	• Designed to address customer business requirements, the Cisco 2900 Series modular architecture offers increased capacity and performance as your network needs grow. • Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency.
Energy Efficiency	• The Cisco 2900 Series architecture provides energy-saving features that include the following: ◦ The Cisco 2900 Series offers intelligent power management and allows the customer to control power to the modules based on the time of day. Cisco EnergyWise technology will be supported in the future. ◦ Services integration and modularity on a single platform performing multiple functions, optimizes raw materials consumption and energy usage. ◦ Platform flexibility and ongoing development of both hardware and software capabilities lead to a longer product lifecycle, lowering all aspects of the total cost of ownership, including materials and energy use. ◦ High efficiency power supplies are provided with each platform.

Investment Protection	• The Cisco 2900 Series maximizes investment protection: ◦ Reuse of a broad array of existing modules supported on the original Integrated Services Routers provides a lower cost of ownership. ◦ A rich set of Cisco IOS Software features carried forward from the original Integrated Services Routers and delivered in a single universal image. ◦ Flexibility to adapt as your business needs evolve.

Platform Architecture and Modularity

The Cisco 2900 Series is architected to meet the application demands of today's branch offices with design flexibility for future applications. The modular architecture is designed to support increasing bandwidth requirements, time-division multiplexing (TDM) interconnections, and fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE (ePoE). Table 2 lists the architectural features and benefits of the Cisco 2900 Series.

Table 2. Architectural Features and Benefits

Architectural Feature	Benefits
Modular Platform	• The Cisco 2900 Series ISRs are highly modular platforms with several types of module slots to add connectivity and services for varied branch-office network requirements. • The ISRs offer an industry-leading breadth of LAN and WAN connectivity options through modules to accommodate field upgrades for future technologies without requiring a platform replacement.
Processors	• The Cisco 2900 Series are powered by high-performance multi-core processors that can support the growing demands of high-speed WAN connections to the branch-office while also running multiple concurrent services.
Embedded IP Security (IPSec) VPN Hardware Acceleration	• Embedded hardware encryption acceleration is enhanced to provide higher scalability, which combined with an optional Cisco IOS Security license, enables WAN link security and VPN services (IPSec acceleration). • The onboard encryption hardware replaces and outperforms the advanced integration modules (AIMs) of previous generations.

Architectural Feature	Benefits
Multigigabit Fabric (MGF)	• The Cisco 2900 Series introduces an innovative multigigabit fabric (MGF) that allows for efficient module-to-module communication, enabling tighter services interactions across modules while reducing the overhead on the route processor.
TDM Interconnectivity Fabric	• Unified communications services in the branch office are significantly enhanced with the use of a TDM interconnectivity fabric in the system architecture, allowing for scaling of DS-0 channel capacity.
Integrated Gigabit Ethernet Ports	• All onboard WAN ports are 10/100/1000 Gigabit Ethernet WAN routed ports. • One of the three 10/100/1000 Ethernet WAN ports on the Cisco 2921 and 2951 supports Small Form-Factor Pluggable (SFP)-based connectivity in lieu of a RJ-45 port and enabling fiber connectivity.
Innovative Universal-Serial-Bus (USB)-Based Console Access	• A new, innovative USB console port offers management connectivity for devices without a serial port such as modern laptop computers. • Traditional console and auxiliary ports are also available.
Optional Integrated Power Supply for Distribution of PoE and Universal DC Power Supply	• An optional upgrade to the internal power supply provides inline power (802.3af-compliant PoE and Cisco Inline Power) to integrated switch modules. • On the Cisco 2911, 2921, and 2951, an optional DC power supply will be available in the future that extends deployment into central offices and industrial environments.
Optional External Redundant Power Supply (RPS)	• The Cisco 2911, 2921, and 2951 allow for power redundancy through the use of an external RPS device, thereby decreasing network downtime and protecting the network from power-supply failures. • Redundant power on the Cisco 2900 Series is supported through the Cisco RPS 2300 Redundant Power System. You can use the Cisco RPS 2300 to provide redundant power for Cisco 2900 Series ISRs as well as Cisco Catalyst® switches. • In order to use the Cisco RPS 2300, an external RPS adapter is required (configurable option) to connect the platform to the external RPS.

PoE Boost	• When connected to an external RPS device, the Cisco 2911, 2921, and 2951 can operate in a PoE boost configuration in lieu of redundant power mode - whereby the power capacity of the platform is increased to twice the normal level to power additional PoE ports.
Designed for Flexible Deployments	• The Cisco 2911 and 2951 are designed for NEBS environments. • The 2911 is 12" deep and has an optional fan filter for deployments in a variety of environments. An assembly that provides front-to-back airflow is also available for 23" racks.

Modularity Features and Benefits

The Cisco 2900 Series provides significantly enhanced modular capabilities (refer to Table 3) offering investment protection for customers. Most of the modules available on previous generations of Cisco routers, such as the Cisco 2800 Series, are supported on the Cisco 2900 Series. Additionally, modules can be used on other supported Cisco platforms to provide maximum investment protection. Taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

A complete list of supported modules, including a list of supported SFPs for the Cisco 2900 Series, is available at:

http://www.cisco.com/go/2900.

Table 3. Modularity Features and Benefits

ISR Modules	Benefits
Cisco Service Module 	• Each service module slot offers high-data-throughput capability: ◦ Up to 4 Gbps aggregate toward the route processor. ◦ Up to 2 Gbps aggregate to other module slots over MGF. • Service module (SM) slots are highly flexible with support for double-wide service modules (SM-Ds), which are Service Modules that require two SM slots. SM-Ds in the Cisco 2921 and 2951 provide flexibility for higher-density modules. • A service module slot replaces the network module and the extension module for voice/fax (EVM) slots and is offered on Cisco 2911, 2921, and 2951 ISRs. • An adapter module enables backward compatibility with existing network modules, enhanced network modules (NMEs), and EVMs. • Service module slots provide twice the power capabilities relative to the network-module slots, allowing for flexibility for higher-scale and better-performance modules. • Power to service module slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.
ISR Modules	**Benefits**
Cisco Unified Computing System™ (Cisco UCS®) E-Series Servers	Cisco UCS E-Series Servers are next-generation power-optimized, general-purpose x86 64-bit blade servers that provide: • Integrated networking • Virtualization optimization • Four- or six-core Intel Xeon processors • Hardware RAID 0, 1, and 5 support • Cisco Integrated Management Controller (IMC)
Cisco UCS E-Series Network Compute Engine (NCE)	The Cisco UCS E-Series Network Compute Engine is a series of compute modules that are both price- and power-optimized for hosting a variety of Cisco network applications and other applications: • Integrated networking • Virtualization-ready • Two-core Intel processors • Cisco IMC

Cisco Internal Services Module (ISM)	• A single ISM slot provides flexibility to integrate intelligent service modules on an internal slot within the chassis • Each ISM slot offers high-data-throughput capability: ◦ Up to 4 Gbps aggregate toward the route processor. ◦ Up to 2 Gbps aggregate to other module slots over the MGF. • The ISM replaces the AIM slot; existing AIM modules are not supported in the ISM slot. • Power to ISM slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.
Cisco High-Density Packet-Voice Digital Signal Processor (DSP) Module (PVDM3) Slots on Motherboard 	• PVDM3 slots natively support PVDM3 modules, providing support for richer density for rich-media voice and video. • Each PVDM3 slot connects back to the system architecture through a 2 Gbps aggregate link through the MGF. • investment protection for PVDM2 modules is supported through an adapter module. • Power to the PVDM slots can be managed by extensions similar to the Cisco EnergyWise framework, so your organization can reduce energy consumption in your network infrastructure. Full EnergyWise support will be available in future software releases.
Compact Flash Slots	• Two external Compact Flash slots are available on the Cisco 2900 Series Integrated Services Routers. Each slot can support high-speed storage densities upgradeable to 4 GB in density.
USB 2.0 Ports	• Two high-speed USB 2.0 ports are supported. The USB ports enable secure token capabilities and storage.

Cisco IOS Software

Cisco 2900 Series Integrated Services Routers deliver innovative technologies running on industry-leading Cisco IOS Software. Developed for wide deployment in the world's most demanding enterprise, access, and service provider networks, the Integrated Services Routers Generation 2 platforms are supported on Cisco IOS Software releases 15M&T. Release 15.0(1)M is available immediately and provides support for a comprehensive portfolio of Cisco technologies, including the functionality and features delivered in releases 12.4 and 12.4T. New innovations in 15.0(1)M span multiple technology areas, including security, voice, high availability, IP Routing and Multicast, quality of service (QoS), IP Mobility, Multiprotocol Label Switching (MPLS), VPNs, and embedded management.

Cisco IOS Software Licensing and Packaging

A single Cisco IOS Universal image encompassing all Cisco IOS Software technology feature sets is delivered with the platforms. You can enable advanced features by activating a software license on the Universal image. In previous generations of access routers, these feature sets required you to download a new software image. Technology packages and feature licenses, enabled through the Cisco software licensing infrastructure, simplify software delivery and decrease the operational costs of deploying new features.

Four major technology licenses are available on the Cisco 2900 Series Integrated Services Routers; you can activate the licenses through the Cisco software activation process identified at http://www.cisco.com/go/sa. The four licenses are as follows:

- IP Base: This technology package is available as default.
- Data
- Unified Communications
- Security (SEC) or Security with No Payload Encryption (SEC-NPE)

For additional information and details about Cisco IOS Software licensing and packaging on Cisco 2900 Series

Integrated Services Routers, please visit http://www.cisco.com/go/2900l.

Key Branch-Office Services

The Cisco Integrated Services Routers are industry-leading platforms that offer unprecedented levels of services integration. Designed to meet the requirements of the branch office, these platforms provide a complete solution with voice, video, security, mobility and application services. Businesses enjoy the benefit of deploying a single device that meets all their needs, reducing capital and operational expenses.

Cisco UCS E-Series Servers: Integrated Network, Compute, and Storage

Cisco UCS E-Series Servers, part of the Cisco Unified Computing System (Cisco UCS), are next-generation, power-optimized, general-purpose x86 64-bit blade servers designed to be deployed in Cisco Integrated Services Routers Generation 2 (ISR G2) and the Cisco 4451-X Integrated Services Router.

These price-to-performance optimized single-socket blade servers balance simplicity, performance, reliability, and power efficiency and are well suited for applications and infrastructure services typically deployed in small and branch offices. By using the Cisco ISR G2 as the blade server chassis, you can now deploy a single converged networking and computing platform designed specifically for remote- and branch-office infrastructure consolidation.

Cisco UCS E-Series Servers deliver next-generation Intel Xeon processor E5-2400 and E3-1100 product family technology in combination with integrated remote lights-out management in a blade-server form factor. These powerful processors deliver multiple cores and threads in a reduced-power envelope, providing improved performance and better energy efficiency than preceding models, making them an excellent platform for

introducing virtualization into the branch office. The innovative, zero-footprint form factor of the Cisco UCS E-Series

Servers in conjunction with the Intel Xeon processor E5-2400 and E3-1100 product families offers significantly lower total cost of ownership (TCO), increased business agility, and greater reliability when compared to standalone rack-mount and tower servers.

Cisco UCS E-Series Server modules are available in two form factors. The first is a singlewide blade server powered by a high-performance yet power-efficient Intel Xeon processor E3 v1 or v2 with four cores, up to 16 GB of RAM, and two TB of local storage. The second is a doublewide blade server powered by a high-performance Intel Xeon processor E5-2400 with up to six cores and support for up to 48 GB of RAM and three TB of local storage.

Unified Communications, Collaboration, and Voice-Gateway Services

The Cisco 2900 Integrated Services Router is the foundation for collaboration in the small and midsize branch office, serving as a critical component of a Cisco's video architecture (Medianet) and enterprise Unified Communications solution. With embedded voice services and a wide range of supported telephony interfaces, the Cisco 2900 Series delivers maximum deployment flexibility for the distributed enterprise. Unified communications is enabled through a rich signaling and media-processing infrastructure, including a variety of protocols, media interworking, signal and media security, transcoding, conferencing, and QoS. Cisco Integrated Services Routers also feature a wide range of voice-gateway interfaces, supporting a broad array of signaling and physical network interfaces.

The Cisco 2900 Series enables a full range of existing and emerging video services, with scaling improvements to support Cisco TelePresence® conferencing, security, and session control. The Cisco Unified Border Element extends these capabilities for business-to-business TelePresence communications. The Cisco 2900 Series adds support for the new Cisco High-Density Packet Voice Digital Signal Processor (DSP) Module (PVDM3), which has been optimized for voice and video support. The new PVDM3 modules support all voice-gateway functions of earlier generations of PVDMs and add higher density and more processing power to support emerging rich-media applications. The Cisco 2900 Series provides 2 or 3 onboard PVDM3 slots, depending on the platform.

Cisco Unified Communications Manager Express and Survivable Remote Site Telephony

The Cisco Integrated Services Routers natively provide optional unified communications services within the Cisco IOS Software, minimizing the IT hardware footprint and total cost of ownership at the branch office. Cisco Unified Communications Manager Express (CME) provides a broad range of IP private-branch-exchange (PBX) and key-system features integrated into the router for the small and midsize branch office. Cisco Survivable Remote Site Telephony (SRST), also inherently available in Cisco IOS Software, and an option on the Cisco 2900 Series, helps ensure that branch-office employees have uninterrupted telephony services and features, even if the connection to a centralized Cisco Unified Communications Manager is disrupted.

Coupled with Cisco Unity® Express, the integrated solution for voicemail, Automated Attendant, and interactive voice response (IVR), the Cisco 2900 Series offers the branch office a complete range of unified communications services while delivering industry-leading security within a single platform.

VoiceXML Application Services

The Cisco 2900 Series also supports standards-certified VoiceXML browser services. VoiceXML is an open-standard markup language used to create voice-enabled web browsers and IVR applications. Just as HTML enables you to retrieve data with a PC, VoiceXML enables you to retrieve data using voice or dual-tone-multifrequency (DTMF) telephony input. The Cisco 2900 Series can deliver a much higher range of concurrent voice-gateway services combined with VoiceXML browser services, for up to 200 sessions on the Cisco 2951.

Cisco Unified Border Element

The Cisco Unified Border Element capabilities supported on the Cisco 2900 Series address the emerging requirements in an IP-centric interconnect for branch-office unified communications between enterprises and service provider networks. Cisco Unified Border Element provides intelligent border-element functions such as physical and logical ingress and egress demarcation points, signaling and media control, and consolidated security and management features. The Cisco 2900 Series supports higher scale than previously provided on the Cisco 2800 Series, up to three times the number of sessions.

Integrated Network Security for Data, Voice, Video, and Mobility

Security is essential to protect a business' intellectual property while also ensuring business continuity and providing the ability to extend the corporate workplace to employees who need anytime, anywhere access to company resources. As part of the Cisco' SAFE architectural framework that allows organizations to identify, prevent, and adapt to network security threats, the Cisco 2900 Series Integrated Services Routers facilitate secure business transactions and collaboration.

The Cisco IOS Software Security technology package for the Cisco 2900 Series offers a wide array of common security features such as advanced application inspection and control, threat protection, and encryption architectures for enabling more scalable and manageable VPN networks. The Cisco 2900 Series offers onboard hardware-based encryption acceleration to provide greater IPSec throughput with less overhead for the route processor when compared with software-based encryption solutions. Cisco Integrated Services Routers offer a comprehensive and adaptable security solution for branch offices that includes features such as:

- **Secure connectivity:** Secure collaborative communications with Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), or Enhanced Easy VPN
- **Integrated threat control:** Responding to sophisticated network attacks and threats using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, Cisco IOS IPS, Cisco IOS Content Filtering, and Flexible Packet Matching (FPM)
- **Identity management:** Intelligently protecting endpoints using technologies such as authentication, authorization, and accounting (AAA) and public key infrastructure (PKI)

Detailed information about the security features and solutions supported on the Cisco 2900 Series is available at http://www.cisco.com/go/routersecurity.

Wireless and Mobility Services

Wireless LAN/WAN

The Cisco Integrated Services Routers supporting the Cisco Unified Wireless Architecture enable deployment of secure, manageable wireless LANs (WLANs) optimized for remote sites and branch offices, including fast secure mobility, survivable authentication, and simplified management. The Cisco Wireless LAN Controller Module on the Cisco 2900 Series allows small and medium-sized businesses (SMBs) and enterprise branch offices to cost-effectively deploy and manage secure WLANs. Cisco Wireless LAN Controllers work in conjunction with Cisco lightweight access points and the Cisco Wireless Control System (WCS) to provide system-wide WLAN functions, managing up to 6, 12, and 25 access points.

Wireless WAN

Cisco third-generation (3G) wireless WAN (WWAN) modules combine traditional enterprise router functions, such as remote management, advanced IP services such as voice over IP (VoIP), and security, with mobility capabilities of 3G WAN access. Using high-speed 3G wireless networks, routers can replace or complement existing landline infrastructure, such as dialup, Frame Relay, and ISDN. Cisco 3G solutions support 3G standards High-Speed Packet Access (HSPA) and Evolution Data Only/Evolution Data Optimized (EVDO) providing you with a true multipath WAN backup and the ability to rapidly deploy primary WAN connectivity. For more information about 3G solutions on Cisco Integrated Services Routers, please visit http //www.cisco.com/go/3g

Integrated LAN Switching

The Cisco 2900 Integrated Services Routers (Cisco 2911 through Cisco 2951) support the new, enhanced Cisco SM-X Layer 2/3 EtherSwitch® Service Modules, which greatly expand router capabilities by integrating industry-

leading Layer 2 or Layer 3 switching with feature sets identical to those found in the Cisco Catalyst 2960 and Catalyst 3650-X Series Switches performing local line-rate switching and routing.

The new, enhanced Cisco SM-X Layer 2/3 EtherSwitch Service Modules take advantage of the increased power capabilities on the Cisco 2900 ISRs. They support PoE+, MACsec, and Cisco TrustSec® technology. Additionally, the enhanced Cisco EtherSwitch modules enable the newest Cisco power initiatives, Cisco EnergyWise™ technology, Cisco Enhanced Power over Ethernet (ePoE), per-port PoE power monitoring, and RPS-enabled PoE boost. These technologies allow you to meet increased endpoint power requirements without increasing the total power consumption of the branch office.

Application Services

As organizations continue to centralize and consolidate their branch-office IT infrastructure in an effort to reduce cost and complexity, they are challenged to provide an excellent user experience, ensure continuous service availability, and deliver business-relevant applications when and where they are needed. To address these challenges, the Cisco 2900 Series provides the capability to host Cisco, third-party, and custom applications on a portfolio of high-performance Cisco Services Ready Engine (SRE) modules that transparently integrate into the router. The modules have their own processors, storage, network interfaces, and memory that operate independently of the host router resources, helping to ensure maximum concurrent routing and application performance while reducing physical space requirements, lowering power consumption, and consolidating management.

Application Acceleration

The Cisco 2900 Series seamlessly combines industry leading security, Cisco IOS Software-based traffic control and visibility, with Cisco application acceleration solutions. Cisco IOS Software features such as NBAR, IP SLA, and NetFlow provide visibility and monitoring of traffic patterns and application performance while Cisco IOS Software features such as QoS, ACLs, and PfR intelligently control the traffic to maximize the quality of the user experience and employee productivity. The user experience can be further enhanced through the addition of a Cisco WAAS Network Module which can be used to securely provide more advanced WAN optimization techniques such as TCP optimization, caching, compression, and application acceleration. Cisco Integrated Services Routers combined with Cisco WAAS Network Modules, provide optimal performance for applications delivered from a central data center to branch-office users. The solution allows you to consolidate costly server, storage, and backup infrastructure into data centers while maintaining LAN-like service levels for remote users.

Cisco UCS E-Series Network Compute Engine

Cisco UCS E-Series Network Compute Engines are the newest E-Series brand of products that are price- and power-optimized, general-purpose x86 64-bit compute modules designed to be deployed in Cisco ISR G2 routers (Figure 1) and Cisco 4400 Series ISR networking platforms.

The first compute module in this series delivers a high-performance yet power-efficient Intel Pentium Processor B925C (4-MB cache, 2.00 GHz) product family with two cores in combination with integrated remote lights-out management in a service-module form factor. The innovative, zero-footprint form factor of the Cisco UCS E- Series Network Compute Engine offers significantly lower TCO, increased business agility, and greater reliability when deploying network applications in the remote and branch office.

Cisco Services Ready Engine

The Cisco Services Ready Engine solution is available in a Service Module (SM) and Internal Service Module (ISM) form factor. The Service Module hardware offers up to a seven times performance improvement over the

previous generation Network Modules and provides a multi-core x86-64 processor. The SRE modules also support up to 1 terabyte of storage, RAID configurations, hardware-assisted virtualization and cryptography options. The Cisco SRE module enables on-demand provisioning of branch-office applications on the Cisco 2900 Series platforms so that you can deploy the right application, at the right time, in the right place. The hardware and software decoupling provided by the service-ready deployment model enables applications to be provisioned on
the module at the time of their installation or remotely anytime thereafter. Supported solutions include Cisco Wide Area Application Services (WAAS), Cisco Unity Express, Cisco Application Extension Platform (AXP), Cisco Wireless LAN Controller (WLC), Cisco Video Surveillance, and other applications under development. The Service Ready Engine enables organizations of various sizes to future-proof their network by allowing them to quickly deploy new branch-office applications without deploying new hardware, reducing the cost of rolling out branch- office services.

WAAS Express

Organizations today face several unique wide area network (WAN) challenges: the need to provide employees with constant access to centrally located information, the requirement to continuously back up and replicate mission-critical data to centrally managed data centers, the desire to provide satisfactory experience for IP phone and video communication, and the mandate to control bandwidth costs without sacrificing application availability and performance.

Cisco WAAS Express is designed to help organizations address these challenges. Cisco WAAS Express extends the Cisco WAAS product portfolio with a small-footprint, cost-effective Cisco IOS Software-based software solution integrated into the ISR G2 to offer bandwidth optimization and application acceleration capabilities. Cisco WAAS Express increases remote user productivity, reduces WAN bandwidth costs, and offers investment protection by interoperating with existing Cisco WAAS infrastructure. Cisco WAAS Express is unique in providing network transparency, improving deployment flexibility with on-demand service enablement, and integrating with native Cisco IOS Software-based services such as security, NetFlow, and QoS.

Cisco WAAS Express is fully interoperable with WAAS on SM-SRE modules, WAAS appliances and can be managed by a common WAAS Central Manager.

Cisco WAAS Express is available in Cisco IOS Software from Release 15.1(2)T1.

Further information on Cisco WAAS Express can be found at
http://www.cisco.com/en/US/products/ps11211/index.html.

Medianet for 2900 ISRs

As video becomes pervasive in an organization and more video devices are used, new demands are placed on the network. It can be challenging to accommodate video needs while reducing complexity, planning for capacity, and providing the best possible user experience.

Smarter Network, Endpoints, and Services

Traditional IP networks need to evolve to medianets to accommodate these changes. A medianet is an end-to-end IP architecture that helps to enable pervasive media experiences.

The medianet architecture includes a smarter network, smarter endpoints, shared media services, cloud services, and shared media services.

More Medianet Benefits

A medianet reduces total cost of ownership and scales video through features such as auto-configuration and media monitoring. At the same time, it helps to ensure a quality user experience while optimizing bandwidth use and efficiency.

For more information on Medianet for 2900ISR, please go to http://www.cisco.com/en/US/netsol/ns1094/index.html.

Managing Your Integrated Services Routers

Network management applications are instrumental in lowering operating expenses (OpEx) while improving network availability by simplifying and automating many of the day-to-day tasks associated with managing an end- to-end network. Day-one device support provides immediate manageability support for the Integrated Services Router, enabling quick and easy deployment, monitoring, and troubleshooting from Cisco and third-party applications.

Organizations rely on Cisco, third-party, and in-house developed network management applications to achieve their OpEx and productivity goals. Underpinning those applications are the embedded management features available in every Integrated Services Router. The new Integrated Services Routers continue a tradition of broad and deep manageability features such as IP service-level agreement (IP SLA), Cisco IOS Embedded Event Manager (EEM), and NetFlow which allow you to know the status of your network at all times. These features, along with Simple Network Management Protocol (SNMP) and syslog, enable your organization's management applications.

Refer to Tables 4 and 5 below for details about network management and manageability support on Cisco 2900 Series Integrated Services Routers.

Table 4. Cisco 2900 ISR G2 Series IOS Software Features and Protocols Support

Feature	Support
Protocols	IPv4, IPv6, Static Routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN.
Encapsulation	Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.
Traffic Management	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Advanced Routing (NBAR).

Note: For a more comprehensive list of features supported in Cisco IOS Software refer to the Feature Navigator tool at http://www.cisco.com/go/fn.

Table 5 lists the embedded management features available with Cisco IOS Software.

Table 5. Embedded Management Features Available with Cisco IOS Software

Feature	Description
Cisco IOS Web Services Management Agent (WSMA)	The Web Services Management Agent (WSMA) defines a mechanism through which you can manage a network device, retrieve configuration data information, and upload and manipulate new configuration data. WSMA uses XML- based data encoding that is transported by the Simple Object Access Protocol (SOAP) for the configuration data and protocol messages.
Cisco IOS Embedded	Cisco IOS Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS Software device. It offers the ability to monitor events and take informational,

Event Manager (EEM)	corrective, or any desired EEM action when the monitored events occur or when a threshold is reached.
Cisco IOS IP Service-Level Agreement (IPSLA)	Cisco IOS IP Service-Level Agreements (SLAs) enable you to assure new business-critical IP applications, as well as IP services that use data, voice, and video in an IP network.
SNMP, Remote Monitoring (RMON), syslog, NetFlow, and TR-069	Cisco 2900 Series Integrated Services Routers also support SNMP, Remote Monitoring (RMON), syslog, NetFlow, and TR-069 in addition to the embedded management features previously mentioned.

The Cisco network management applications listed in Table 6 are standalone products that you can download or purchase to manage your Cisco network devices. The applications are built specifically for the different operational phases; you can select the ones that best fit your needs.

Table 6. Network Management Applications

Operational Phase	Application	Description
Device staging and configuration	Cisco Configuration Professional	Cisco Configuration Professional is a GUI device-management tool for Cisco IOS Software-based access routers. This tool simplifies router, security, unified communications, wireless, WAN, and basic LAN configuration through easy-to-use wizards.
Network-wide deployment, configuration, monitoring, and troubleshooting	CiscoWorks LMS	CiscoWorks LAN Management Solution (LMS) is a suite of integrated applications for simplifying day-to-day management of a Cisco end-to-end network, lowering OpEx while increasing network availability. CiscoWorks LMS offers network managers an easy-to-use web-based interface for configuring, administering, and troubleshooting the Cisco Integrated Services Routers, using new instrumentation such as Cisco IOS EEM Generic Online Diagnostics (GOLD). In addition to supporting basic platform services of the Integrated Services Router, CiscoWorks also provides added-value support for the Cisco Services Ready Engine, enabling the management and distribution of software images to the SRE, thereby reducing the time and complexities associated with image management.
Network-wide staging, configuration, and compliance	CiscoWorks NCM	CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements.
Security staging, configuration, and monitoring	Cisco Security Manager	Cisco Security Manager is a leading enterprise-class application for managing security. It delivers provisioning of firewall, VPN, and intrusion-prevention-system (IPS) services across Cisco routers, security appliances, and switch service modules. The suite also includes the Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) for monitoring and mitigation.
Voice configuration and provisioning	Cisco Unified Provisioning Manager	Cisco Unified Provisioning Manager provides a reliable and scalable web-based solution for managing a company's crucial next-generation communications services. It manages unified communications services in an integrated IP telephony, voicemail, and messaging environment.
Staging, deployment, and changes of licenses	Cisco License Manager	Easily manage Cisco IOS Software activation and licenses for a wide range of Cisco platforms running Cisco IOS Software as well as other operating systems with the secure client-server application Cisco License Manager.
Staging, deployment, and changes to configuration and image files	Cisco Configuration Engine	Cisco Configuration Engine is a secure network management product that provides zero-touch image and configuration distribution through centralized, template-based management.

Summary

As your business strives to lower the total cost of ownership in running your network and increase your overall employee productivity with more centralized and collaborative network applications, you will need more intelligent branch-office solutions. The Cisco 2900 Series offers these solutions by providing enhanced performance and increased modular density to support multiple services. The Cisco 2900 Series is designed to consolidate the functions of many separate devices into a single, compact system.

Table 7. Cisco 2900 Integrated Services Router Product Specifications

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Services and Slot Density				
Embedded Hardware-Based Cryptography and Acceleration	Yes	Yes	Yes	Yes
Cisco Unified SRST Sessions	35	50	100	250
Cisco Unified CCME Sessions	35	50	100	150
Total Onboard WAN 10/100/1000 Ports	2	3	3	3
RJ-45-Based Ports	2	3	3	3
SFP-Based Ports (use of SFP port disables the corresponding RJ-45 port)	0	0	1	1
Service Module Slots	0	1	1	2
Double-Wide Service Module Slots (use of a double-wide slot will occupy all single-wide service module slots in a 2900)	0	0	1	1
EHWIC Slots	4	4	4	4
Double-Wide EHWIC Slots (use of a double-wide EHWIC slot will consume two EHWIC slots)	2	2	2	2
ISM Slots	1	1	1	1
Onboard DSP (PVDM) Slots	2	2	3	3
Memory DDR2 ECC DRAM – Default	512 MB	512 MB	512 MB	512 MB
Memory (DDR2 ECC DRAM) – Maximum	2 GB	2 GB	2 GB	2 GB
Compact Flash (External) – Default	slot 0: 256 MB slot 1: none	slot 0: 256 MB slot 1: none	slot 0: 256 MB slot 1: none	slot 0: 256 MB slot 1: none
Compact Flash (External) – Maximum	slot 0: 4 GB slot 1: 4 GB	slot 0: 4 GB slot 1: 4 GB	slot 0: 4 GB slot 1: 4 GB	slot 0: 4 GB slot 1: 4 GB
External USB 2.0 Flash Memory Slots (Type A)	2	2	2	2
USB Console Port (Type B) (up to 115.2 kbps)	1	1	1	1
Serial Console Port	1	1	1	1
Serial Auxiliary Port	1	1	1	1
Power-Supply Options	AC and PoE	AC, PoE, and DC	AC, PoE, and DC	AC, PoE, and DC
RPS Support (External)	No	Cisco RPS 2300	Cisco RPS 2300	Cisco RPS 2300
Power Specifications				
AC Input Voltage	100 to 240 VAC auto ranging	100 to 240 VAC auto ranging	100 to 240 VAC auto ranging	100 to 240 VAC auto ranging
AC Input Frequency	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz
AC Input Current Range AC Power Supply (Maximum)	1.5 to 0.6A	2.2 to 1.0A	3.4 to 1.4A	3.4 to 1.4A
AC Input Surge Current	<50A	<50A	<50A	<50A
Typical Power (No Modules) (Watts)	40	50	60	70
Maximum Power with AC Power Supply (Watts)	150	210	320	340
Maximum Power with PoE	175	250	370	405

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Power Supply (Platform Only) (Watts)				
Maximum End-Point PoE Power Available from PoE Power Supply (Watts)	130	200	280	370
Maximum End-Point PoE Power Capacity with PoE Boost (Watts)	N/A	750	750	750
DC Input Voltage	N/A	24 to 60 Vdc, autoranging positive or negative	24 to 60 Vdc, autoranging positive or negative	24 to 60 Vdc, autoranging positive or negative
DC Input Current	N/A	(MAX) 8A (24V) 3.5A (60V)	(MAX) 12A (24V) 5A (60V)	(MAX) 12A (24V) 5A (60V)
Physical Specifications				
Dimensions (H x W x D)	1.75 x 17.25 x 17.3 in. (44.5 x 438.2 x 439.4 mm)	3.5 x 17.25 x 12 in. (88.9 x 438.2 x 304.8 mm)	3.5 x 17.25 x 18.5 in. (88.9 x 438.2 x 469.9 mm)	3.5 x 17.25 x 18.5 in. (88.9 x 438.2 x 469.9 mm)
Rack Height	1RU (rack unit)	2RU	2RU	2RU
Rack-Mount 19 in. (48.3 cm) EIA	Included	Included	Included	Included
Rack-Mount 23 in. (58.4 cm) EIA	Optional	Optional	Optional	Optional
Wall-Mount (refer to installation guide for approved orientation)	Yes	Yes	No	No
Weight with AC Power Supply (No Modules)	13.4 lb (6.1 kg)	18 lb (8.2 kg)	29 lb (13.2 kg)	29 lb (13.2 kg)
Weight with AC PoE Power Supply (No Modules)	14.3 lb (6.5 kg)	19 lb (8.6 kg)	30 lb (13.6 kg)	30 lb (13.6 kg)
Typical Weight Fully Configured	16 lb (7.3 kg)	21 lb (9.5 kg)	34 lb (15.5 kg)	34 lb (15.5 kg)
Airflow	Front to side	Side to side	Back and Side to Front	Back and Side to Front
Optional Airflow Kit	N/A	Front to back	N/A	N/A
Environmental Specifications				
Operating Conditions				
Temperature: 5,906 feet (1,800m) Maximum Altitude	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Temperature: 9,843 feet (3,000m) Maximum Altitude	32 to 77°F (0 to 25°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Temperature: 13,123 feet (4,000m) Maximum Altitude	N/A	32 to 86°F (0 to 30°C)	32 to 86°F (0 to 30°C)	32 to 86°F (0 to 30°C)
Temperature: Short-Term (per NEBS) 5906 feet (1,800m) Maximum Altitude	N/A	23°F to 122°F (-5 to 50°C)	N/A	23°F to 122°F (-5 to 50°C)
Altitude	10,000 ft (3,000m)	13,000 ft (4,000m)	10,000 ft (3,000m)	13,000 ft (4,000m)
Relative Humidity	10 to 85%	5 to 85%	10 to 85%	5 to 85%
Short-Term (per NEBS) Humidity	N/A	5% to 90%, but not to exceed 0.024 kg water/kg of dry air	N/A	N/A
Acoustic: Sound Pressure (Typical/Maximum)	41/53 dBA	51.8/62.9 dBA	54.4/67.4 dBA	54.4/67.4 dBA
Acoustic: Sound Power (Typical/Maximum)	49/61 dBA	58.5/70.3 dBA	62.6/74.5 dBA	62.6/74.5 dBA
Non-Operating Conditions				
Temperature	-40 to 158°F (-40 to 70°C)	-40 to 176°F (-40 to 80°C)	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)
Relative Humidity	5 to 95%	5 to 95%	5 to 95%	5 to 95%

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Altitude	15,000 ft (4,570m)	15,000 ft (4,570m)	15,000 ft (4,570m)	15,000 ft (4,570m)
Regulatory Compliance				
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1
Telecom	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive

Supported Modules

The Cisco 2900 Series supports a wide range of modules that span industry-leading breadth of services at the branch office. For a list of modules supported on the Cisco 2900 Series, please visit: http://www.cisco.com/en/US/products/ps10537/products_relevant_interfaces_and_modules.html.

Ordering Information

The Cisco 2900 Series Integrated Services Routers are orderable and shipping. For information about how to order the Cisco 2900 Series, please visit the Cisco 2900 Series Ordering Guide. To place an order, visit the Cisco Ordering Home Page and refer to Table 8, which provides basic ordering information. For additional product numbers, including the Cisco 2900 Series bundle offerings, please check the Cisco 2900 Series Integrated Services Router Price List or contact your local Cisco account representative.

Table 8. Cisco 2900 Series Basic Ordering Information

Product Name	Product Description
CISCO2901/K9	Cisco 2901 with 2 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
CISCO2911/K9	Cisco 2911 with 3 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
CISCO2921/K9	Cisco 2921 with 3 onboard GE, 4 EHWIC slots, 3 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
CISCO2951/K9	Cisco 2951 with 3 onboard GE, 4 EHWIC slots, 3 DSP slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base
SL-29-DATA-K9	Data License for Cisco 2901-2951
SL-29-UC-K9	Unified Communications License for Cisco 2901-2951
SL-29-SEC-K9	Security License for Cisco 2901-2951

Cisco Integrated Services Router Migration Options

Cisco 2900 Series Integrated Services Routers are included in the standard Cisco Technology Migration Program (TMP). Refer to http://www.cisco.com/go/tmp and contact your local Cisco account representative for program details.

Warranty Information

The Cisco 2900 Series Integrated Services Routers have a ninety (90) day limited liability warranty.

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies. For more information, please visit http://www.cisco.com/go/services

Cisco SMARTnet® technical support for the Cisco 2900 Series is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access rights to Cisco.com technical libraries for technical assistance, electronic commerce, and product information
- 24-hour access to the industry's largest dedicated technical support staff

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

2. Cisco 2950

(CISCO SYSTEMS, s.f.) afirma en el *datasheet* del dispositivo *CATALYST 2950* que éste es un conmutador de veinticuatro puertos, *standalone*, gestionado, que provee conectividad a los usuarios de redes medianas y pequeñas.

Explican que posee una aplicación de gestión centralizada que permite, valga la redundancia, simplificar la gestión y administración de este dispositivo.

Según se menciona en el referido documento, el dispositivo posee las siguientes características:

11. Veinticuatro puertos *Fast Ethernet*.
12. 1 unidad de rack.
13. Transmisión de data de video y servicios de voz a la velocidad del cable.
14. Imagen de sistema operativo estándar.
15. Ideal para la conectividad de computadores de usuario final.

En la próxima página se presenta el *datasheet* del dispositivo.

Cisco Catalyst 2950 Series Intelligent Ethernet Switches for Metro Access (Enhanced Image)

Product Over view

The Cisco Catalyst® 2950 Series Intelligent Ethernet switches is an affordable line of fixed-configuration Fast Ethernet and Gigabit Ethernet switches that extend intelligence to the metro access edge, enabling service breadth, availability, security, and manageability. Key components of the Cisco Metro Ethernet Switching portfolio, these switches are ideal for service providers looking to deliver profitable Ethernet services to the residential and small-office, home-office (SOHO) market. Featuring advanced rate limiting, voice virtual LAN (VLAN) support, and multicast management, these switches enable a variety of residential metro services such as Internet access, voice over IP (VoIP), and broadcast video.

The Cisco Catalyst 2950 Series Intelligent Ethernet switches consists of the following devices—which are only available with the Enhanced Image (EI) software for the Cisco Catalyst 2950 Series:

- Cisco Catalyst 2950G-48 Switch—
48 10/100 ports and 2 gigabit interface converter (GBIC)-based Gigabit Ethernet ports
- Cisco Catalyst 2950G-24 Switch—
24 10/100 ports and 2 GBIC ports
- Cisco Catalyst 2950G-24-DC Switch—24 10/100 ports, 2 GBIC ports, and DC power
- Cisco Catalyst 2950G-12 Switch—
12 10/100 ports and 2 GBIC ports
- Cisco Catalyst 2950T-24 Switch—
24 10/100 ports and 2 fixed 10/100/1000BaseT uplink ports
- Cisco Catalyst 2950C-24 Switch—
24 10/100 ports and 2 fixed 100BaseFX uplink ports
- Catalyst 2950ST-24-LRE—24 LRE and 2 Gigabit Ethernet ports (user can select either 10BaseT/100BaseTX/1000BaseT Ethernet Ports or Small Form Factor Pluggable (SFP) Transceivers)
- Catalyst 2950ST-8-LRE—8 LRE and 2 Gigabit Ethernet ports (user can select either 10BaseT/100BaseTX/1000BaseT Ethernet Ports or Small Form Factor Pluggable (SFP) Transceivers)

The two built-in Gigabit Ethernet ports on the Cisco Catalyst 2950G-12, 2950G-24, and 2950G-48 accommodate a range of GBIC transceivers, including the Cisco Course Wave Division Multiplexing (CWDM) GBIC Solution, Cisco GigaStack® GBIC, 1000BaseSX, 1000BaseLX/LH, 1000BaseZX and 1000BaseT GBICs. The dual GBIC-based Gigabit Ethernet implementation provides customers with tremendous deployment flexibility— allowing them increased availability with the redundant uplinks. High levels of resiliency can also be implemented by deploying dual redundant Gigabit Ethernet uplinks, UplinkFast and

Per-VLAN Spanning Tree Plus (PVST+) for uplink load balancing. This Gigabit Ethernet flexibility makes the Cisco Catalyst 2950 Series switches an ideal metro access edge complement to the Cisco 7600 Series Internet Router and Cisco Catalyst 6500 Series of metro Ethernet switches.

Intelligence at the Metro Access Edge: Enabling Profitable Ethernet Services

Service providers that address the residential and SOHO market face the continual challenge of offering compelling value-added services.

Although alternative broadband technologies such as DSL can offer bandwidth at speeds ranging up to 1.5 Mbps, the monthly subscriber fees for such speeds can be out of reach for most users. As a result, compelling high-quality services such as high-speed Internet access, VoIP, or broadcast video are often not viable propositions over these technologies. However, in the metro, service providers are discovering that high-performance, Ethernet access over fiber-optic networks can easily provide cost-effective bandwidth of 10 to 100 Mbps. By taking advantage of the simplicity and cost benefits of Ethernet, revenue growth via voice, video, and data services becomes a reality. When considering the deployment of Ethernet services, service providers must consider the following issues:

- Building cost-effective, highly available, scalable metro Ethernet networks
- Providing profitable new services while reducing operational and capital costs
- Having the network flexibility to move up market to enterprise and small and medium- sized business services

These issues are especially relevant at the metro access edge. As service providers look to provide profitable Ethernet services such as high-speed Internet access, voice, and video, Cisco intelligent functionality such as advanced quality of service (QoS), granular rate limiting, and multicast management are essential in the provider's customer-located equipment. In addition, availability and security concerns at the access edge are addressed with intelligent features such as subsecond Spanning Tree Protocol (STP) convergence and 802.1x support. With Cisco Catalyst 2950 Series Intelligent Ethernet switches, Cisco delivers the ideal balance of affordability and intelligence, enabling profitable Ethernet service breadth, availability, security and manageability.

Most important, the Cisco Catalyst 2950 Series is a key component of the Cisco Metro Ethernet Switching portfolio. As such, service providers are assured that they can offer a range of residential and commercial services over the same network. For regional metro, metro aggregation, and metro access, Cisco Metro Ethernet Switching enables service providers to deliver profitable, comprehensive Ethernet services. With the effective integration of existing WAN services such as Frame Relay and ATM, Cisco Metro Ethernet Switching offers an unmatched breadth of service delivery mechanisms. Cisco also helps service providers minimize total cost of ownership for new services with its extensive automated operations support. Through technology leadership, financial stability, and a commitment to customer support, Cisco ensures service success from "start to scale."

Service Breadth Through Advanced Quality of Service, Rate Limiting, and Voice/ Multicast Features

To achieve profitability, service providers that serve the residential and SOHO markets must offer value-added services such as voice and video in addition to basic high-speed Internet connectivity to increase revenue per subscriber. But these services are compelling only when service quality matches that of competing voice and video offerings.

The Cisco Catalyst 2950 Series offers superior and highly granular QoS to ensure that network traffic is classified and prioritized, and that congestion is avoided in the best possible manner. The Cisco Catalyst 2950 Series can classify, reclassify, police (determine if the packet is in or out of predetermined profiles and affect actions on the packet), and mark or drop the incoming packets before the packet is placed in the shared buffer. Packet classification allows the network elements to discriminate between various traffic flows and enforce policies based on Layer 2 and Layer 3 QoS fields.

To implement QoS, first, the Cisco Catalyst 2950 Series switches identify traffic flows, or packet groups, and classify or reclassify these groups using either the Differentiated Services Code Point (DSCP) field or the 802.1p class-of-service (CoS) field, or both. Classification and reclassification can be based on criteria as specific as the source/destination IP address, source/destination Media Access Control (MAC) address, or the Layer 4 Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port. At the ingress, the Cisco Catalyst 2950 Series can also perform policing and marking of the packet.

After the packet goes through classification, policing, and marking, it is then assigned to the appropriate queue before exiting the switch. The Cisco Catalyst 2950 Series supports four egress (outgoing port) queues per port, which allows the service provider to be more discriminating and specific in assigning priorities for the various applications. At the egress, the switch performs Weighted Round Robin (WRR) or strict priority scheduling to determine the order in which the queues are processed. The WRR queuing algorithm ensures that the lower-priority packets are not entirely starved for bandwidth and are serviced without compromising the priority settings administered by the network manager. Strict priority scheduling ensures that the highest-priority packets are always serviced first, ahead of all other traffic.

In terms of rate limiting, the Cisco Catalyst 2950 Series is capable of allocating bandwidth based on several criteria, including MAC source address, MAC destination address, IP source address, IP destination address, and TCP/UDP port number. Bandwidth allocation is essential in network environments requiring service-level agreements (SLAs), or when it is necessary for the network manager to control the bandwidth given to certain subscribers. The Cisco Catalyst 2950 Series supports up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port. Traffic policing can be done in 1-Mbps increments on Fast Ethernet ports and 8-Mbps increments on Gigabit Ethernet ports, giving the network manager very granular control of network bandwidth.

In addition, the Cisco Catalyst 2950 Series provides key voice and video service features with voice VLAN (auxiliary VLAN) for VoIP services and hardware-based Internet Group Management Protocol (IGMP) snooping, allowing the switch to "listen in" on the IGMP conversation between hosts and routers. When a switch hears an IGMP join request from a host for a given multicast group, the switch adds the host port number to the Group Destination Address (GDA) list for that group. And, when the switch hears an IGMP leave request, it removes the host port from the list. Together with the superior QoS and rate-limiting features mentioned previously, service providers can build a flexible network with the Cisco Catalyst 2950 Series to provide voice, video, and data services all in one network architecture.

Service Availability through Resiliency Enhancements and Network Redundancy

The Cisco Catalyst 2950 Series provides a rich set of resiliency enhancement features to ensure quick failover recovery and create a high-availability network. The IEEE 802.1w Rapid Spanning Tree standard allows the service provider to achieve subsecond spanning tree convergence times to maximize network stability and reliability. The

IEEE 802.1s Multiple Spanning Tree standard can be deployed in conjunction with 802.1w to improve the scalability of the STP by grouping VLANs into spanning tree instances, as well as to provide backward compatibility to devices running the 802.1D STP.

In addition, service providers can enable Bridge Protocol Data Unit (BPDU) guard and Spanning Tree Root Guard (STRG) to enhance the reliability of their networks. BPDU guard allows the service provider to shut down STP PortFast-enabled interfaces to avoid receiving BPDUs from their customers' networks. STRG prevents customer devices outside of the service provider's network from becoming STP root nodes.

The Cisco Catalyst 2950 Series enables the service provider to construct a highly redundant network. PVST+ allows the service provider to implement Layer 2 load-sharing on redundant links, efficiently utilizing the extra capacity inherent in a redundant design. Service providers can also utilize Cisco EtherChannel® technology to aggregate up to 4 Gbps through Gigabit EtherChannel technology and up to 1.6 Gbps through Fast EtherChannel technology. The Cisco EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches and to routers.

In addition to resiliency and network redundancy advantages, the Cisco Catalyst 2950 Series enables metro network scalability at the access edge through its support of Cisco CWDM GBIC Solution. This solution allows service providers to scale their bandwidth without deploying additional fiber. The service provider can scale up to eight gigabits of bandwidth on a pair of single-mode fibers at distances up to 120 km. With the support for Cisco CWDM GBICs on the Cisco Catalyst 2950 Series, service providers can aggregate multiple Cisco Catalyst 2950 Series switches to easily upgrade network bandwidth with existing fiber infrastructure.

Metro network scalability is also enhanced by the Cisco Catalyst 2950 Series support of 4096 VLAN IDs and 256 active VLANs per switch.

Service Security Through Cisco Access Control Parameters and Enhanced Security Features

The Cisco Catalyst 2950 Series offers enhanced data security through the use of access control parameters (ACPs). By denying packets based on source and destination MAC addresses, IP addresses, or TCP/UDP ports, users can be restricted from sensitive portions of the network. Also, because all ACP lookups are done in hardware, forwarding performance is not compromised when implementing ACP-based security in the network.

Service providers can also implement higher levels of data security by supporting private VLAN edge. This feature provides security and isolation between ports on a switch, ensuring that traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port. Local Proxy Address Resolution Protocol (ARP) works in conjunction with private VLAN edge to minimize broadcasts and maximize available bandwidth.

With the Cisco Catalyst 2950 Series, service providers can implement high levels of console security. Multilevel access security on the switch console and the Web-based management interface prevents unauthorized users from accessing or altering switch configuration. Terminal Access Controller Access Control System (TACACS+) authentication enables centralized access control of the switch and restricts unauthorized users from altering the configuration.

Service providers are also able to enhance their network security by adding 802.1x port-based authentication for authenticating individual customers, and port security with MAC address aging for limiting the concurrent MAC addresses allowed per port.

Service Management Through Cisco IE 210 0 Series and SNMP

The Cisco Catalyst 2950 Series provides outstanding service management capabilities via Cisco IE 2100 Series Intelligence Engine support and Simple Network Management Protocol (SNMP). Service providers will be able to integrate the Cisco Catalyst 2950 Series seamlessly into their operations support systems (OSSs) and enable improved flow-through provisioning.

The Cisco IE 2100 Series network device allows service providers to effectively manage a network of Cisco IOS® devices, including the Cisco Catalyst 2950 Series. It is a completely self-contained unit that includes a task-oriented Web graphical user interface (GUI), a programmable extensible markup language (XML) interface, configuration template management, and an embedded repository. Network operators can use the Web GUI to quickly turn existing Cisco IOS command-line interface (CLI) configuration files into reusable templates. The Cisco IE 2100 Series supports easy integration into existing customer OSS/business support system (BSS) and provisioning systems via its external repository support and the event-based Cisco IOS XML interface that effectively "workflow-enables" Cisco device deployment.

Service providers also can manage the Cisco Catalyst 2950 Series using SNMP version 2 and version 3, and the Telnet interface for comprehensive in-band management. A CLI-based management console provides detailed out-of-band management.

A comprehensive set of Management Information Bases (MIBs) is provided for the service provider to collect traffic information on the Cisco Catalyst 2950 Series for various billing methods.

Figure 1
Cisco Catalyst 2950 Series Intelligent Ethernet Switches

Feature	Benefit
Service Breadth	
Advanced QoS	• This feature enables end-to-end QoS in the network by extending the QoS trust boundary to the edge of the network. • The switches support configuring QoS ACPs on all ports to ensure proper policing and marking on a per-packet basis using ACPs. Up to four ACPs per switch are supported in configuring either QoS ACPs or security filters.
	QoS Classification Support at Ingress • The switches support QoS classification of incoming packets for QoS flows based on Layer 2, Layer 3, and Layer 4 fields. • The following Layer 2 fields or a combination can be used for classifying incoming packets to define QoS flows: source MAC address, destination MAC address, 16-bit Ethertype. • The following Layer 3 and 4 fields or a combination can be used to classify incoming packets to define QoS flows: source IP address, destination IP address, TCP source or destination port number, UDP source or destination port number.
	QoS Metering/Policing at Ingress • Support for metering/policing of incoming packets restricts incoming traffic flows to a certain rate. • The switches support up to 6 policers per Fast Ethernet port, and 60 policers on a Gigabit Ethernet port. • The switches offer granularity of traffic flows at 1 Mbps on Fast Ethernet ports, and 8 Mbps on Gigabit Ethernet ports. QoS Marking at Ingress • The switches support marking/remarking packets based on state of policers/ meters. • The switches support marking/remarking based on the following mappings: from DSCP to 802.1p, and 802.1p to DSCP. • The switches support 14 well-known and widely used DSCP values. • The switches support classifying or reclassifying packets based on default DSCP per port. • The switches support classifying or reclassifying frames based on default 802.1p value per port. • The switches support 802.1p override at ingress.

Feature	Benefit
Service Breadth	
Advanced QoS (continued)	QoS Scheduling Support at Egress • Four queues per egress port are supported in hardware. • The WRR queuing algorithm ensures that low-priority queues are not starved. • Strict-priority queue configuration ensures that time-sensitive applications such as voice always follow an expedited path through the switch fabric.
Granular rate limiting	• The switch supports up to 6 policers per Fast Ethernet port and up to 60 policers on a Gigabit Ethernet port. • The switch offers granularity of traffic flows at 1 Mbps on Fast Ethernet ports and 8 Mbps on Gigabit Ethernet ports. • The switch offers the ability to limit data flows based on MAC source/ destination address, IP source/destination address, TCP/UDP port numbers, or any combination of these fields. • The switch offers the ability to manage data flows asynchronously upstream and downstream from the end station or on the uplink.
Voice and video services	• The IGMP snooping feature allows the switch to "listen in" on the IGMP conversation between hosts and routers. When a switch hears an IGMP join request from a host for a given multicast group, the switch adds the host port number to the GDA list for that group. And, when the switch hears an IGMP leave request, it removes the host port from the list. • Multicast VLAN registration (MVR) continuously sends multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons. • IGMP filtering provides the control of the set of multicast groups to which a user on a switch port can belong. • Voice VLAN (auxiliary VLAN) support for VoIP application allows the creation
Resiliency and reliability	• IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) takes advantage of point-to-point wiring and provides rapid convergence of the spanning tree independent of spanning-tree timers. Reconfiguration of the spanning tree can occur in less than one second, a feature that is critical for networks carrying delay-sensitive traffic such as voice and video. • IEEE 802.1s Multiple Spanning Tree (MSTP), which uses RSTP for rapid convergence, enables VLANs to be grouped into a spanning-tree instance, with each instance having a spanning-tree topology independent of other spanning-tree instances. This architecture provides for multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances required to support a large number of VLANs. • Cisco UplinkFast/BackboneFast technologies ensure quick failover recovery, enhancing overall network stability and reliability.

Feature	Benefit
Service Breadth	
Resiliency and reliability (continued)	• Cisco CrossStack UplinkFast (CSUF) technology provides increased redundancy and network resiliency through fast spanning-tree convergence (less than two seconds) across a stack of switches using Cisco GigaStack GBICs in an independent stack backplane cascaded configuration. • Redundant stacking connections provide support for a redundant loopback connection for top and bottom switches in an independent stack backplane cascaded configuration. • BPDU guard shuts down STP PortFast-enabled interfaces when BPDUs are received to avoid accidental spanning tree topology changes. • STRG prevents edge devices not in the network administrator's control from becoming STP root nodes. • Command switch redundancy enabled in the Cisco Cluster Management Suite (CMS) Software allows customers to designate a backup command switch that takes over cluster management functions if the primary command switch fails. • Unidirectional link detection (UDLD) detects and disables unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults. Aggressive UDLD allows precautionary disabling of port on bidirectional links. • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance. • Support for Cisco's optional RPS 300 Redundant Power System provides superior internal power source redundancy for up to six Cisco networking devices, resulting in improved fault tolerance and network uptime.
Redundancy	• Bandwidth aggregation up to 4 Gbps through Cisco Gigabit EtherChannel technology and up to 1.6 Gbps through Cisco Fast EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches, to routers and individual servers. • IEEE 802.1D STP support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • PVST+ allows for Layer 2 load sharing on redundant links to efficiently utilize the extra capacity inherent in a redundant design. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices.
Scalability	• CWDM GBIC solution support allows for the scaling of bandwidth without deploying additional fiber. It provides scalability of up to eight Gigabits of bandwidth on a pair of single-mode fibers to reach distances up to 100–120 km. • Support for up to 4096 VLAN Ids with 250 active VLANs per switch, and up to 64 spanning tree instances per switch.

Feature	Benefit
Service Security	
Network-wide security features	• Filtering of incoming traffic flows based on Layer 2, Layer 3, or Layer 4 ACPs prevents unauthorized data flows. Up to four ACPs are supported in configuring either QoS or security filters. – The following Layer 2 ACPs or a combination can be used for security classification of incoming packets: source MAC address, destination MAC address, and 16-bit Ethertype. – The following Layer 3 and Layer 4 fields or a combination can be used for security classification of incoming packets: source IP address, destination IP address, TCP source or destination port number, UDP source, or destination port number. • Private VLAN edge provides security and isolation between ports on a switch, ensuring that voice traffic travels directly from its entry point to the aggregation device through a virtual path and cannot be directed to a different port. • IEEE 802.1x for dynamic port-based security. • Support for "secure ports" prevents unauthorized stations from accessing the switch by restricting the number of concurrent MAC addresses allowed to access the port. Up to 132 addresses can be configured per port. • STRG prevents edge devices not in the network administrator's control from becoming STP root nodes. • The STP PortFast/ BPDU guard feature disables access ports with STP PortFast enabled upon reception of a BPDU, and increases network reliability, manageability, and security. • Multilevel security on console access prevents unauthorized users from altering the switch configuration. • TACACS+ and Remote Access Dial-In User Service (RADIUS) authentication enables centralized control of the switch and restricts unauthorized users from altering the configuration.
Service Management	
Superior manageability	• Cisco IE 2100 support for flow- through provisioning and integration with OSS applications via programmatical interfaces. • SNMP v1, v2c, v3, and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management. • Manageable through CiscoWorks network management software on a per-port and per-switch basis providing a common management interface for Cisco routers, switches, and hubs. • Comprehensive MIBs enable the service provider to collect traffic information on the Cisco Catalyst 2950 Series for various billing methods.

Feature	Benefit
Service Management	
Superior manageability (continued)	• An embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events) for enhanced traffic management, monitoring, and analysis. • The switch supports all nine RMON groups through the use of a Cisco SwitchProbe® Analyzer (Switched Port Analyzer [SPAN]) port, permitting traffic monitoring of a single port, a group of ports, or the entire switch from a single network analyzer or RMON probe. • RSPAN (Remote SPAN) allows network administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network. • The Domain Name System (DNS) provides IP address resolution with user-defined device names. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all switches within the intranet. • Multifunction LEDs per port for port status, half-duplex/full-duplex, 10BaseT/100BaseTX/1000BaseT indication, as well as switch-level status LEDs for system, redundant power supply, and bandwidth utilization provide a comprehensive and convenient visual management system.
Ease of use and ease of deployment	• Autoconfiguration eases deployment of switches in the network by automatically configuring multiple switches across a network via a boot server. • Autosensing on each non-GBIC port detects the speed of the attached device and automatically configures the port for 10-, 100-, or 1000-Mbps operation, easing the deployment of the switch in mixed 10, 100, and 1000BaseT environments. • Autonegotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Cisco Discovery Protocol Versions 1 and 2 enable a CiscoWorks network management station to automatically discover the switch in a network topology. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches. • Support for dynamic VLAN assignment through implementation of VLAN Membership Policy Server (VMPS) client functionality provides flexibility in assigning ports to VLANs. • Dynamic Trunking Protocol (DTP) enables dynamic trunk configuration across all ports in the switch. • Port Aggregation Protocol (PAgP) automates the creation of Cisco Fast EtherChannel or Gigabit EtherChannel groups, enabling linking to another switch, router, or server. • IEEE 802.3z-compliant 1000BaseSX, 1000BaseLX/LH, 1000BaseZX, and 1000BaseT physical interface support through a field-replaceable GBIC module provides customers unprecedented flexibility in switch deployment.

Ease of use and ease of deployment (continued)

- The default configuration stored in Flash memory ensures that the switch can be quickly connected to the network and can pass traffic with minimal user intervention.
- The switches support nonstandard Ethernet frame sizes (mini-giants) up to 1542 bytes (configurations with GBIC ports only).

Product Specifications

(See separate Cisco Catalyst 2950 LRE data sheet for Catalyst 2950ST-24-LRE and Catalyst 2950ST-8-LRE product specifications)

Feature	Description
Performance	• 13.6-Gbps switching fabric • 6.8-Gbps maximum forwarding bandwidth • Forwarding rates based on 64-byte packets • Cisco Catalyst 2950G-48: 10.1-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-24 and 2950G-24-DC: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950G-12: 4.8-Mpps wire-speed forwarding rate • Cisco Catalyst 2950T-24: 6.6-Mpps wire-speed forwarding rate • Cisco Catalyst 2950C-24: 3.9-Mpps wire-speed forwarding rate • 32-MB maximum packet buffer shared by all ports • 16-MB DRAM and 8-MB Flash memory • Configurable up to 8000 MAC addresses • Configurable maximum transmission unit (MTU) of up to 1530 bytes (Cisco Catalyst 2950G
Management	• BRIDGE-MIB • CISCO-CDP-MIB • CISCO-CLUSTER-MIB • CISCO-CONFIG-MAN-MIB • CISCO-FLASH-MIB • CISCO-IMAGE-MIB • CISCO-MAC-NOTIFICATION-MIB • CISCO-MEMORY-POOL-MIB • CISCO-PAGP-MIB • CISCO-PING-MIB • CISCO-PROCESS-MIB • CISCO-PRODUCTS-MIB • CISCO-RTTMON-MIB • CISCO-STACKMAKER-MIB • CISCO-STP-EXTENSIONS-MIB

Feature	Description
Management (continued) • CISCO-SYSLOG-MIB • CISCO-TCP-MIB • CISCO-VLAN-MEMBERSHIP-MIB • CISCO-VTP-MIB • ENTITY-MIB • IANAifType-MIB • IF-MIB (RFC 1573) • OLD-CISCO-CHASSIS-MIB • OLD-CISCO-CPU-MIB • OLD-CISCO-INTERFACES-MIB • OLD-CISCO-IP-MIB • OLD-CISCO-MEMORY-MIB	• OLD-CISCO-SYSTEM-MIB • OLD-CISCO-TCP-MIB • OLD-CISCO-TS-MIB • CISCO-PAGP-MIB • CISCO-UDLD-MIB • RFC1213-MIB (MIB-II) • RFC1398-MIB (ETHERNET-MIB) • RMON-MIB (RFC 1757) • RS-232-MIB • SNMPv2-MIB • SNMPv2-SMI • SNMPv2-TC • TCP-MIB • UDP-MIB
Standards	• IEEE 802.1x support • IEEE 802.1w • IEEE 802.1s • IEEE 802.3x full duplex on 10BaseT, 100BaseTX, and 1000BaseT ports • IEEE 802.1D STP • IEEE 802.1p class-of-service (CoS) prioritization • IEEE 802.1Q VLAN • IEEE 802.3 10BaseT specification • IEEE 802.3u 100BaseTX specification • IEEE 802.3ab 1000BaseT specification • IEEE 802.3z 1000BaseX specification

Feature	Description
Standards (continued)	• 1000BaseX (GBIC) • 1000BaseSX • 1000BaseLX/LH • 1000BaseZX • 1000Base-CWDM GBIC 1470 nm • 1000Base-CWDM GBIC 1490 nm • 1000Base-CWDM GBIC 1510 nm • 1000Base-CWDM GBIC 1530 nm • 1000Base-CWDM GBIC 1550 nm • 1000Base-CWDM GBIC 1570 nm • 1000BaseE-CWDM GBIC 1590 nm • 1000Base-CWDM GBIC 1610 nm • RMON I and II standards • SNMPv1, SNMPv2c, and SNMPv3
Year 2000 (Y2K) compliance	• Y2K compliant
Connectors and cabling	• 10BaseT ports: RJ-45 connectors; two-pair Category 3, 4, or 5 unshielded twisted-pair (UTP) cabling • 100BaseTX ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 1000BaseT ports: RJ-45 connectors; two-pair Category 5 UTP cabling • 100BaseFX ports: MT-RJ connectors, 50/125 or 62.5/125 micron multimode fiber-optic cabling • 1000BaseSX, -LX/LH, -ZX GBIC-based ports: SC fiber connectors, single-mode or multimode fiber • Cisco GigaStack GBIC ports: copper-based Cisco GigaStack cabling • Management console port: 8-pin RJ-45 connector, RJ-45-to-RJ-45 rollover cable with RJ-45-to-DB9 adapter for PC connections; for terminal connections, use RJ-45-to-DB25 female data-terminal-equipment (DTE) adapter (can be ordered separately from Cisco, part number ACS-DSBUASYN=)
MT-RJ patch cables for Cisco Catalyst 2950C-24 Switch	**Type of Cable** — **Cisco Part Number** 1-meter, MT-RJ-to-SC multimode cable — CAB-MTRJ-SC-MM-1M 3-meter, MT-RJ-to-SC multimode cable — CAB-MTRJ-SC-MM-3M 5-meter, MT-RJ-to-SC multimode cable — CAB-MTRJ-SC-MM-5M 1-meter, MT-RJ-to-ST multimode cable — CAB-MTRJ-ST-MM-1M 3-meter, MT-RJ-to-ST multimode cable — CAB-MTRJ-ST-MM-3M 5-meter, MT-RJ-to-ST multimode cable — CAB-MTRJ-ST-MM-5M

Feature	Description
Power connectors	Customers can provide power to a switch by using either the internal power supply or the Cisco RPS 300. The connectors are located at the back of the switch. **Internal Power Supply Connector** • The internal power supply is an auto-ranging unit. • The internal power supply supports input voltages between 100 and 240 VAC. • Use the supplied AC power cord to connect the AC power connector to an AC power outlet. **Cisco RPS Connector** • The connector offers connection for an optional Cisco RPS 300 that uses AC input and supplies DC output to the switch. • The connector offers a 300-watt redundant power system that can support six external network devices and provides power to one failed device at a time. • The connector automatically senses when the internal power supply of a connected device fails and provides power to the failed device, preventing loss of network traffic. • When the internal power supply has been brought up or replaced, the Cisco RPS 300 automatically stops powering the device. • Attach only the Cisco RPS 300 (model PWR300-AC-RPS-N1) to the redundant power supply receptacle.
Indicators	• Per-port status LEDs: link integrity, disabled, activity, speed, and full-duplex indications • System status LEDs: system, RPS, and bandwidth utilization indications
Dimensions and weight (H x W x D)	• 1.72 x 17.5 x 9.52 in. (4.36 x 44.5 x 24.18 cm) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, 2950G-24, and 2950G-24-DC) • 1.72 x 17.5 x 13 in. (4.36 x 44.5 x 33.02 cm) (Cisco Catalyst 2950G-48) • 1.0 rack-unit high • 6.5 lb. (3.0 kg) (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, 2950G-24, and 2950G-24-DC) • 10 lb. (4.5 kg) (Cisco Catalyst 2950G-48)
Environmental ranges	• Operating temperature: 32 to 113 F (0 to 45 C) • Storage temperature: –13 to 158 F (–25 to 70 C) • Operating relative humidity: 10 to 85% (noncondensing) • Operating altitude: Up to 10,000 ft. (3000m) • Storage altitude: Up to 15,000 ft. (4500m) • Not intended for use on top of desktops or in open office environments
Power requirements	• Power consumption: 30W maximum, 102 BTUs per hour (Cisco Catalyst 2950T-24, 2950C-24, 2950G-12, 2950G-24, and 2950G-24-DC) • Power consumption: 45W maximum, 154 BTUs per hour (Cisco Catalyst 2950G-48) • AC input voltage/frequency: 100 to 127/200 to 240 VAC (autoranging), 50 to 60 Hz • DC input voltages – RPS input: +12V @ 4.5 A – DC input for 2950G-24-DC: –36 to –72 VDC @ 1A

Feature	Description
Mean time between failure (MTBF) – Predicted	• 482,776 hours (Cisco Catalyst 2950G-12) • 468,884 hours (Cisco Catalyst 2950G-24) • 479,086 hours (Cisco Catalyst 2950G-24-DC) • 159,026 hours (Cisco Catalyst 2950G-48) • 297,144 hours (Cisco Catalyst 2950T-24) • 268,292 hours (Cisco Catalyst 2950C-24)
Fiber-port specifications for Cisco Catalyst 2950C-24 Switch	Fiber-port power levels: • Optical transmitter wavelength: 1300 nanometers • Optical receiver sensibility: –14 dBm2 • Optical transmitter power: –19 to –14 dBm • Transmit: –19 to –14 dBm
Regulatory Agency Approvals	
Safety certifications	• UL 1950/CSA 22.2 No. 950 • IEC 950-EN 60950 • AS/NZS 3260, TS001 • CE Marking
Electromagnetic emissions certifications	• FCC Part 15 Class A • EN 55022: 1998 Class A (CISPR22 Class A) • EN 55024: 1998 (CISPR24) • VCCI Class A • AS/NZS 3548 Class A • CE Marking • CNS 13438 • BSMI Class A • MIC
NEBS	• Bellcore • GR-1089-CORE • GR-63-CORE • SR-3580 Level 3
Warranty	• Limited lifetime warranty

Service and Support

The services and support programs described in the table below are available as part of the Cisco Desktop Switching Service and Support solution, and are available directly from Cisco and through resellers

Service and Support	Features	Benefits
Cisco Advanced Services		
Cisco Total Implementation (TIS)—available Cisco **Packaged Total Implementation Solutions (Packaged TIS)—available through resellers**	• Project management • Site survey, configuration deployment • Installation, text, and cutover • Training • Major moves, adds, changes • Design review and product staging	• Supplements existing staff **Solutions direct from** • Ensures functionality meets needs • Mitigates risk
Technical Support Services		

Cisco SMARTnet™ and SMARTnet Onsite Support direct from Technical Assistance Center (TAC)	• 24x7 access to software updates • Web access to technical repositories • Telephone support through the Cisco utilizing Cisco expertise and	• Enables proactive or expedited issue resolution **(OS)—available** • Lowers cost of ownership by **Cisco** knowledge
Packaged SMARTnet— available through resellers	• Advance replacement of hardware parts	• Minimizes network downtime

Ordering Information

Model numbers	Configuration
WS-C2950G-48-EI	• 48 10/100 ports + 2 1000BaseX ports • Enhanced Software Image (EI) installed
WS-C2950G-24-EI	• 24 10/100 ports + 2 1000BaseX ports • EI installed
WS-C2950G-24-EI-DC	• 24 10/100 ports + 2 1000BaseX ports, DC power • EI installed
WS-C2950G-12-EI	• 12 10/100 ports + 2 1000BaseX ports • EI installed
WS-C2950T-24	• 24 10/100 ports + 2 1000BaseT ports • EI installed
WS-C2950C-24	• 24 10/100 ports + 2 100BaseFX ports • EI installed
WS-C2950ST-24-LRE	• 24 LRE ports + 2 10BaseT/100BaseTX/1000BasetT Ethernet ports + 2 Small Form Factor Pluggable (SFP) Transceivers (two of four uplink ports active at one time • EI Installed
WS-C2950ST-8-LRE	• 8 LRE ports + 2 10BaseT/100BaseTX/1000BasetT Ethernet ports + 2 Small Form Factor Pluggable (SFP) Transceivers (two of four uplink ports active at one time • EI Installed

For More Information on Cisco Products, Contact:

- United States and Canada: 800 553-NETS (6387)
- Europe: 32 2 778 4242
- Australia: 612 9935 4107
- Other: 408 526-7209
- World Wide Web URL: http://www.cisco.com

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada• Chile • China PRC • Colombia • Costa Rica • Croatia Czech Republic • Denmark• Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary• India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg• Malaysia • Mexico • The Netherlands• New Zealand• Norway• Peru • Philippines • Poland Portugal • Puerto Rico • Romania• Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

LW3663 0902

3. Cisco 1900

(CISCO SYSTEMS, s.f.) ofrece la siguiente reseña básica del enrutador *CATALYST* 1900, enrutador perteneciente, al igual que el 2900, a la serie *Integrated Services Routers*.

16. Provee un punto de entrada altamente seguro a la red WAN.
17. Ofrece virtualización de servicios.
18. Es ideal para aquellas pequeñas oficinas que requieren flexibilidad modular, así como movilidad altamente segura.
19. Ofrece velocidades de transmisión por circuitos de hasta 25 Mbps.
20. Provee un punto de acceso IEEE 802.11n de fábrica (en aquellos modelos en los cuales esta función está disponible).

En la próxima página se presenta el *datasheet* del enrutador *CATALYST 1900*.

Cisco 1941 Series Integrated Services Routers

Product Names: CISCO1941/K9, CISCO1941W-A/K9, CISCO1941W-E/K9, CISCO1941W-P/K9, CISCO1941W-N/K9, CISCO1941W-C/K9

Cisco® 1900 Series Integrated Services Routers build on 25 years of Cisco innovation and product leadership. The new platforms are architected to enable the next phase of branch-office evolution, providing rich media collaboration and virtualization to the branch while maximizing operational cost savings The Integrated Services Routers Generation 2 platforms are future-enabled with multi-core CPUs, Gigabit Ethernet switching with enhanced POE, and new energy monitoring and control capabilities while enhancing overall system performance.
Additionally, a new Cisco IOS® Software Universal image and Services Ready Engine module enable you to decouple the deployment of hardware and software, providing a stable technology foundation which can quickly adapt to evolving network requirements. Overall, the Cisco 1900 Series offer unparalleled total cost of ownership savings and network agility through the intelligent integration of market leading security, unified communications, wireless, and application services.

Product Overview

Cisco® 1941 builds on the best-in-class offering of the existing Cisco 1841 Integrated Services Routers by offering 2 models - Cisco 1941 and Cisco 1941W. In addition to the support of a wide range of wireless and wired connectivity options supported on Cisco 1941 Series, Cisco 1941W offers integration of IEEE 802.11n access point which is backwards compatible with IEEE 802.11a/b/g access points.

All Cisco 1900 Series Integrated Services Routers offer embedded hardware encryption acceleration, optional firewall, intrusion prevention, and application services. In addition, the platforms support the industries widest range of wired and wireless connectivity options such as T1/E1, xDSL, 3G, and GE.

Figure 1. Cisco 1941 Integrated Services Router

Key Business Benefits

The Integrated Services Routers Generation 2 (ISR G2) provide superior services integration and agility. Designed for scalability, the modular architecture of these platforms enables you to grow and adapt with your business needs Table 1 lists the business benefits of the Cisco. 1900.

Table 1. Key Features and Benefits of the Cisco 1941 Integrated Services Router Series

Benefits	Description
Service Integration	• The Cisco 1941 Series offer increased levels of services integration with data, security, wireless and mobility services enabling greater efficiencies cost savings.
Services on Demand	• A single Cisco IOS® Software Universal image is installed on each ISR G2. The Universal image contains all of the Cisco IOS technology sets which can be activated with a software license. This allows your business to quickly deploy advanced features without downloading a new IOS image. Additionally, larger default memory is included to support the new capabilities. • The Cisco Services Ready Engine (SRE) enables a new operational model which allows you to reduce capital expenditures (CapEx) and deploy a variety of application services as needed on a single integrated compute services module.
High Performance with Integrated Services	• The Cisco 1900 Series enables deployment in high speed WAN environments with concurrent services enabled up to 25 Mbps. • Multi-Gigabit Fabric enables high bandwidth module to module communication without compromising routing performance.
Network Agility	• Designed to address customer business requirements, Cisco 1941 Series with the modular architecture, offers performance range of modular interfaces and services as your network needs grow. • Modular interfaces offer increased bandwidth, a diversity of connection options, and network resiliency.
Energy Efficiency	• The Cisco 1941 Series architecture provides energy savings features that include the following: ◦ The Cisco 1900 Series offers intelligent power management and allows the customer to control power to the modules based on the time of day. Cisco EnergyWise technology will be supported in the future. ◦ Services integration and modularity on a single platform performing multiple functions, optimizes raw materials consumption and energy usage. ◦ Platform flexibility and ongoing development of both hardware and software capabilities lead to a longer product lifecycle, lowering all aspects of the total cost of ownership, including materials and energy use. ◦ High efficiency power supplies are provided with each platform.
Investment Protection	• The Cisco 1941 Series maximizes investment protection by supporting: ◦ Reuse of a broad array of existing modules supported on the original Integrated Services Routers provides a lower cost of ownership. ◦ Rich set of Cisco IOS Software features carried forward from the original Integrated Services Routers and delivered in the universal image. ◦ Flexibility to grow as your business needs evolve.

Architecture & Modularity

The Cisco 1941 Series is architected to meet the application demands of today's branch offices with design flexibility for future applications. The modular architecture is designed to support expanding customer requirements, increased bandwidth, and fully integrated power distribution to modules supporting 802.3af Power over Ethernet (PoE) and Cisco Enhanced PoE (ePoE). Table 2 lists the architectural features and benefits of the Cisco 1941 Series.

Table 2. Architectural Features and Benefits

Architectural Feature	Benefits
Modular Platform	• The Cisco 1941 Series ISR are highly modular platforms with multiple module slots to provide connectivity and services for varied branch network requirements. • The ISRs offer an industry-leading breadth of LAN and WAN connectivity options through modules to accommodate field upgrades to future technologies without requiring replacement of the platform.
Processors	• The Cisco 1941 Series is powered by high-performance multi-core processors that support growing demands of branch office networks by supporting high throughput WAN requirements.
MultiGigabit Fabric	• The Cisco 1941 introduces an innovative MultiGigabit Fabric (MGF) which allows for efficient module to module communication, enabling direct services interactions across modules while reducing the overhead on the router processor.
Embedded IPSec VPN Hardware Acceleration	• Embedded hardware encryption acceleration is enhanced to provide higher scalability, which, combined with an optional Cisco IOS Security license, enables WAN link security and VPN services (IPSec acceleration). • The onboard encryption hardware out-performs the Advanced Integration Modules of previous generations.

Architectural Feature	Benefits
Integrated Gigabit Ethernet Ports	• All onboard WAN ports are 10/100/1000 Gigabit Ethernet WAN routed ports.
Innovative universal-serial-bus (USB)-based console access	• A new, innovative, mini-B USB console port supports management connectivity when traditional serial ports are not available. • The traditional console and auxiliary ports are also available. Either the USB-based console or the RJ-45-based console port can be used to configure the router.
Optional Integrated Power Supply for Distribution of Power Over Ethernet (PoE)	• An optional upgrade to the internal power supply provides in-line power (802.3af-compliant Power-over-Ethernet [PoE] and Cisco standard inline power) to optional integrated switch modules.
Integrated Wireless LAN	• The Cisco 1941 offers a secure integrated access point in a single device. • Integrated access point is based on the IEEE 802.11n draft 2.0 standard that uses MIMO (Multi-Input, Multiple-output) to improve coverage for existing 802.11a/b/g clients and new 802.11n clients. • The Cisco 1941 supports dual radios - 802.11 b/g/n and 802.11a/n and is capable of operating in both autonomous and unified modes.

Modularity Features and Benefits

The Cisco 1941 provides significantly enhanced modular capabilities (refer to Table 2) offering investment protection for customers. Most of the modules available on previous generations of Cisco routers, such as the Cisco 1841 ISR, are supported on the Cisco 1941. Additionally, modules used on the Cisco 1941 can easily be interchanged with other Cisco routers to provide maximum investment protection. Taking advantage of common interface cards across a network greatly reduces the complexity of managing inventory requirements, implementing large network rollouts, and maintaining configurations across a variety of branch-office sizes.

A complete list of supported modules is available at http://www.cisco.com/go/1941.

Table 3. Modularity - Features and Benefits

Feature	Benefits
Cisco Enhanced High Speed WAN Interface Card (EHWIC) 	• The EHWIC slot replaces the high-speed WAN interface card (HWIC) slot and can natively support HWICs, WAN interface cards (WICs), voice interface cards (VICs), and voice/WAN interface cards (VWICs). • Two integrated EHWIC slots are available on the Cisco 1941 for flexible configurations for support of two modules: One double wide HWIC-D or single wide EHWIC/HWIC module and a second single wide E-HIC/HWIC module are supported. • Each HWIC Slot offers high data throughput capability. ◦ Up to 1.6 Gbps aggregate towards the router processor. ◦ Up to 2 Gbps aggregate to other module slots over MultiGigabit Fabric (MGF).
Cisco Internal Services Module (ISM)	• A single ISM Slot provides flexibility to integrate intelligent services modules that do not require interface ports. • ISM replaces the Advanced Integration Module (AIM) slot, existing AIM modules are not supported in the ISM slot. • Each ISM Slot offers high data throughput capability. ◦ Up to 4 Gbps aggregate towards the router processor. ◦ Up to 2 Gbps aggregate to other module slots over MultiGigabit Fabric (MGF). • Power to ISM slots can be managed by extensions similar to the Cisco EnergyWise framework, allowing organizations to reduce energy consumption in their network infrastructure. Full EnergyWise support will be available in future software releases. **Note:** The Cisco 1941 cannot have ISM and WLAN on the same chassis. Please refer to ordering information for WLAN SKUs.
Compact Flash Slots	• Two external Compact Flash slots are available on the Cisco 1941. Each slot can support high-speed storage densities upgradeable to 4GB in density.
USB 2.0 Ports	• Two high-speed USB 2.0 ports are supported. The USB ports enable another mechanism secure token capabilities and storage.

Cisco IOS Software

The Cisco 1941 Series Integrated Services Routers deliver innovative technologies running on industry-leading Cisco IOS Software. Developed for wide deployment in the world's most demanding enterprise, access, and service provider networks, Cisco IOS Software Release 15 M & T provides support for a comprehensive portfolio of Cisco technologies, including new functionality and features delivered in Releases 12.4 and 12.4T, and new innovations that span multiple technology areas, including security, voice, high availability, IP Routing and Multicast, quality of service (QoS), IP Mobility, Multiprotocol Label Switching (MPLS), VPNs, and embedded management.

Cisco IOS Software Licensing and Packaging

A single Cisco IOS Universal image encompassing all functions is delivered with the platforms. You can enable advanced features by activating a software license on the Universal image. In previous generations of access routers, these feature sets required you to download a new software image. Technology packages and feature licenses, enabled through the Cisco software licensing infrastructure, simplify software delivery and decrease the operational costs of deploying new features.

Four major technology licenses are available on the Cisco 1941 Series Integrated Services Routers; you can activate the licenses through the Cisco software activation process identified at http://www.cisco.com/go/sa.

- IP Base: This technology package is available as default
- Data
- Security (SEC) or Security with No Payload Encryption (SEC-NPE)

For additional information and details about Cisco IOS Software licensing and packaging on Cisco 1941 Series Integrated Services Routers, please visit http://www.cisco.com/go/g2licensing.

Key Branch Office Services

The Cisco Integrated Services Routers are industry-leading routers that offer unprecedented levels of services integration. Designed to meet the requirements of the branch office, these platforms provide a complete solution with voice, security, mobility and data services. Businesses enjoy the benefit by deploying a single device that meets all their needs and save on capital and operational expenses.

Integrated Network Security for Data and Mobility

Security is essential to protect a business' intellectual property while also ensuring business continuity and providing the ability to extend the corporate workplace to employees who need anytime, anywhere access to company resources. As part of the Cisco' SAFE architectural framework that allows organizations to identify, prevent, and adapt to network security threats - the Cisco 1900 Series Integrated Services Routers facilitate secure business transactions and collaboration.

The Cisco IOS Software Security technology package license for the Cisco 1900 Series offers a wide array of common security features such as advanced application inspection and control, threat protection, and encryption architectures for enabling more scalable and manageable VPN networks in one solution set. The Cisco 1941 Series offers native hardware-based encryption acceleration to provide greater IPSec throughput with less overhead for the router processor when compared with software-based encryption solutions. Cisco Integrated Services Routers offer a comprehensive and adaptable security solution for branch-office routers that include features such as:

- **Secure connectivity:** Secure collaborative communications with Group Encrypted Transport VPN (GETVPN), Dynamic Multipoint VPN (DMVPN), or Enhanced Easy VPN.
- **Integrated threat control:** Respond to sophisticated network attacks and threats using Cisco IOS Firewall, Cisco IOS Zone-Based Firewall, IOS IPS, IOS Content Filtering and Flexible Packet Matching (FPM).
- **Identity Management:** Intelligently protecting endpoints using technologies such as authentication, authorization, and accounting (AAA) and public key infrastructure (PKI).

Detailed information on the security features and solutions supported on the Cisco 1900 Series routers can be found at http://www.cisco.com/go/routersecurity.

Wireless and Mobility Services

Wireless LAN

The Cisco Integrated Services Routers supporting the Cisco Unified Wireless Network enable deployment of secure, manageable WLANs optimized for remote sites and branch offices, including fast secure mobility, survivable authentication, and simplified management. The Cisco Unified Wireless Network addresses critical points of potential failure and helps enable resiliency and survivability for WLANs at remote locations and branch offices. This solution protects the WLAN by providing fast recovery from a variety of faults that may occur. With Cisco's high availability for remote WLANs, hardware and software work together to enable rapid recovery from disruptions and help ensure fault transparency to users and network applications.

The new Cisco 1941W with IEEE 802.11n integrated access point support both unified and autonomous deployments. This integrated Wi-Fi access point offers IEEE 802.11n draft 2.0 standard support for mobile access to high-bandwidth data, voice, and video applications through the use of multiple-input, multiple-output (MIMO) technology that provides increased throughput, reliability, and predictability. IEEE 802.11n wireless networks create a cohesive working environment by combining the mobility of wireless with the performance of wired networks. Cisco has innovative, next-generation wireless solutions that offer greater performance and extended reach for pervasive wireless connectivity. IEEE 802.11n technology delivers outstanding reliability and up to nine times the throughput of current IEEE 802.11 a/b/g networks. It makes wireless networks an integral part of every type of organization by offering the following benefits:

- Data rates of up to 600 Mbps support more users, devices, and mission-critical, bandwidth-intensive applications.
- New MIMO technology provides predictable WLAN coverage and reliable connectivity.
- Next-generation wireless technology provides superior investment protection to support emerging mobile applications.

These routers help extend corporate networks to secure remote sites while giving users access to the same applications found in corporate offices for both data and voice applications. When users require WLAN access, visibility and control of network security are even more critical at the remote site. The new fixed Cisco Integrated Services Routers meet this need with a single device that combines integrated IEEE 802.11a/b/g/n capabilities with security features such as Wi-Fi Protected Access (WPA), including authentication with IEEE 802.1X with the Cisco Light Extensible Authentication Protocol (LEAP) and Protected EAP (PEAP) and encryption with the WPA Temporal Key Integrity Protocol (TKIP).

Wireless WAN

Cisco third-generation (3G) wireless WAN (WWAN) modules combine traditional enterprise router functions, such as remote management, advanced IP services such as voice over IP (VoIP), and security, with mobility capabilities of 3G WAN access. Using high-speed 3G wireless networks, routers can replace or complement existing landline infrastructure, such as dialup, Frame Relay, and ISDN. Cisco 3G solutions support 3G standards High-Speed Packet Access (HSPA) and Evolution Data Only/Evolution Data Optimized (EVDO) providing you with a true multipath WAN backup and the ability to rapidly deploy primary WAN connectivity. For more information about 3G solutions on Cisco Integrated Services Routers, please refer to http://www.cisco.com/go/3g.

Integrated LAN Switching

The Cisco 1941 Integrated Services Router Series will support the EHWIC LAN modules when they become available in future. The Cisco 1941 Series support the existing single wide EtherSwitch HWIC and the double wide HWIC-D modules, which greatly expand the router's capabilities by integrating industry leading Layer 2 or Layer 3 switching.

Application Services

As organizations continue to centralize and consolidate their branch IT infrastructure in an effort to reduce cost and complexity in the branch office, they are challenged to provide adequate user experience, ensure continuous service availability, and deliver business-relevant applications when and where they are needed. To address these challenges, the Cisco 1941 Series provides the ability to host Cisco, 3rd party, and custom applications on Cisco Services Ready Engine (SRE) module that seamlessly integrate into the router. The module has its own processor, network interface, and memory that operate independently of the host router resources, helping to ensure maximum concurrent routing and application performance while reducing physical space requirements, lowering power consumption, and consolidating management.

Cisco Services Ready Engine

The Cisco Services Ready Engine solution is available in a Internal Service Module (ISM) form-factor. The Internal Service Module hardware offers up to a seven times performance improvement over the previous-generation Advanced Integration Modules and provides a x86 processor. The Cisco SRE module enables on-demand provisioning of branch-office applications on the Cisco 1900 Series platforms so that you can deploy the right application, at the right time, in the right place. The hardware and software decoupling provided by the service- ready deployment model enables applications to be provisioned on the module at the time of its installation or remotely anytime thereafter. Supported solutions include Cisco Application Extension Platform (AXP), Cisco Wireless LAN Controller (WLC), and other applications under development. The Service Ready Engine enables organizations of various sizes to future-proof their network by allowing them to quickly deploy new branch-office applications without deploying new hardware, reducing the cost of rolling out branch-office services.

WAAS Express

Organizations today face several unique wide area network (WAN) challenges: the need to provide employees with constant access to centrally located information, the requirement to continuously back up and replicate mission-critical data to centrally managed data centers, the desire to provide satisfactory experience for IP phone and video communication, and the mandate to control bandwidth costs without sacrificing application availability and performance.

Cisco WAAS Express is designed to help organizations address these challenges. Cisco WAAS Express extends the Cisco WAAS product portfolio, with a small-footprint, cost-effective IOS-based software solution integrated into the ISR G2 to offer bandwidth optimization and application acceleration capabilities. Cisco WAAS Express increases remote user productivity, reduces WAN bandwidth costs, and offers investment protection by interoperating with existing Cisco WAAS infrastructure. Cisco WAAS Express is unique in providing network transparency, improving deployment flexibility with on-demand service enablement, and integrating with native IOS-based services such as security, Netflow, and QoS.

Cisco WAAS Express is fully interoperable with WAAS on SM-SRE modules, WAAS appliances and can be managed by a common WAAS Central Manager.

Cisco WAAS Express is available in IOS from version 15.1(2)T1.

Further information on Cisco WAAS Express can be found at http://wwwin.cisco.com/artg/products/waas/.

Managing Your Integrated Services Routers

Network Management applications are instrumental in lowering Operating Expenditures (OPEX) while improving network availability by simplifying and automating many of the day-to-day tasks associated with managing an end-to-end network. "Day-one-device-support" provides immediate manageability support for the Integrated Services Router enabling quick and easy deployment, monitoring and troubleshooting from Cisco and third party applications.

Organizations rely on Cisco, third-party and in-house developed network management applications to achieve their Opex and productivity goals. Underpinning those applications are the embedded management features available in every ISR. The new ISRs continue a tradition of broad and deep manageability features within the devices. Features such as IPSLA, EEM, Netflow, allow you to know what's going on in your network at all times. These features along with SNMP and SYSLOG support enable your organization's management applications.

Refer to Tables 4, 5 and 6 for details on IOS, Network Management and Manageability support on Cisco 1941 Series Integrated Services Routers.

Table 4. Cisco 1941 with Cisco IOS Software Feature and Protocol High-Level Support

Protocols	IPv4, IPv6, static routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN.
Encapsulations	Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), Point-to-Point Protocol over Ethernet (PPPoE), and ATM.
Traffic management	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), and Network-Based Advanced Routing (NBAR).

Note: For a more comprehensive list of features supported in Cisco IOS software refer to the Feature Navigator tool at: http://www.cisco.com/go/fn.

Table 5 highlights several integrated services router management capabilities that are available within Cisco IOS Software:

Table 5. Cisco IOS Software Management Capabilities

Feature	Description of Feature Supported by Cisco Integrated Services Routers
WSMA	The Web Services Management Agent (WSMA) defines a mechanism through which you can manage a network device, retrieve configuration data information, and upload and manipulate new configuration data. WSMA uses XML- based data encoding that is transported by the Simple Object Access Protocol (SOAP) for the configuration data and protocol messages.
EEM	Cisco IOS Embedded Event Manager (EEM) is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS Software device. It offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached.
IPSLA	Cisco IOS IP Service-Level Agreements (SLAs) enable you to assure new business-critical IP applications, as well as IP services that use data, voice, and video, in an IP network.
SNMP, RMON, Syslog, NetFlow, TR-069	Cisco 1900 Series Integrated Services Routers also support SNMP, Remote Monitoring (RMON), syslog, NetFlow, and TR-069 in addition to the embedded management features previously mentioned.

Cisco Network Management Applications

The applications listed in Table 6 are standalone products that you can purchase or download to manage your Cisco network devices. The applications are built for the different operational phases; you can select the ones that best fit your needs.

Table 6. Network Management Solutions

Operational Phase	Application	Description
Device staging and configuration	Cisco Configuration Professional	• Cisco Configuration Professional is a GUI device-management tool for Cisco IOS Software-based access routers. This tool simplifies routing, firewall, IPS, VPN, unified communications, and WAN and LAN configuration through GUI-based easy-to-use wizards.
Networkwide deployment, configuration, monitoring, and troubleshooting	CiscoWorks LMS	• CiscoWorks LAN Management Solution (LMS) is a suite of integrated applications for simplifying day-to-day management of a Cisco end-to-end network, lowering OpEx while increasing network availability. CiscoWorks LMS offers network managers an easy-to-use web-based interface for configuring, administering, and troubleshooting the Cisco integrated services routers, using new instrumentation such as Cisco IOS EEM. • In addition to supporting basic platform services of the integrated services router, CiscoWorks also provides added-value support for the Cisco Service Ready Engine, enabling the management and distribution of software images to the SRE, thereby reducing the time and complexities associated with image management.
Networkwide staging, configuration, and compliance	CiscoWorks NCM	• CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure. It provides superior visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology requirements.
Security staging, configuration, and monitoring	Cisco Security Manager	• Cisco Security Manager is a leading enterprise-class application for managing security. It delivers provisioning of firewall, VPN, and intrusion-prevention-system (IPS) services across Cisco routers, security appliances, and switch service modules. The suite also includes the Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) for monitoring and mitigation.
Configuration and provisioning	Cisco Unified Provisioning Manager	• Cisco Unified Provisioning Manager provides a reliable and scalable web-based solution for managing a company's crucial next-generation communications services. It manages unified communications services in an integrated IP telephony, voicemail, and messaging environment.
Staging, deployment, and changes of licenses	Cisco License Manager	• Easily manage Cisco IOS Software activation and license management for a wide range of Cisco platforms running Cisco IOS Software as well as other operating systems with the secure client-server application Cisco License Manager
Staging, deployment, and changes to configuration and image files	Cisco Configuration Engine	• Cisco Configuration Engine is a secure network management product that provides zero-touch image and configuration distribution through centralized, template-based management.

Summary and Conclusion

As businesses strive to lower the total cost of ownership in running their network and increase their overall employee productivity with more centralize and collaborative network applications, more intelligent branch office solutions are required. The Cisco 1941 Series offers these solutions by providing enhanced performance and increased modular density to support multiple services. The Cisco 1941 Series is designed to consolidate the functions of separate devices into a single, compact system that can be remotely managed.

Product Specifications

Table 7. Product Specifications of Cisco 1941 Integrated Services Router

	Cisco1941, Cisco1941W
Services and Slot Density	
Embedded hardware-based crypto acceleration (IPSec)	Yes
Total Onboard LAN 10/100/1000	2
RJ-45-Based Ports	2
SFP-Based Ports	0
SM Slots	0
Double-Wide SM Slots	0
EHWIC Slots	2
Double-Wide EHWIC slots (use of a double-wide EHWIC slot will consume two EHWIC slots)	1
ISM Slots	1 (0 on the Cisco 1941W)
Memory (DDR2 Error Correction Code [ECC] ECC DRAM) - Default	512 MB
Memory (DDR2 ECC DRAM) - Maximum	2.0 GB
Compact Flash (external) - Default	slot 0: 256 MB slot 1: none
Compact Flash (external) - Maximum	slot 0: 4 GB slot 1: 4 GB
External USB flash memory slots (Type A)	2
USB Console Port (Type B) (up to 115.2 kbps)	1
Serial Console Port (up to 115.2 kbps)	1
Serial Auxiliary Port (up to 115.2 kbps	1
Power Supply Options	AC, POE
Redundant Power Supply Support	No
Power Specifications	
AC Input Voltage	100-240 V ~
AC Input Frequency	47-63 Hz
AC Input Current range AC Power Supply (Max) (Amps)	1.5-0.6
AC Input Surge Current	<50 A
Typical Power (No Modules)	35 W
Maximum Power capacity with AC power supply	110 W
Maximum Power capacity with PoE power supply (platform only)	110 W
Maximum PoE device power capacity with PoE power supply	80 W

	Cisco1941, Cisco1941W
Physical Specifications	
Dimensions (H x W x D)	3.5 in x 13.5 in x 11.5 in
Rack Height	2 RU
Rack-mount 19in. (48.3 cm) EIA	Included
Wall-mount (refer to installation guide for approved orientation)	Yes
Weight - with AC power supply (no modules)	12 lbs
Weight - with POE power supply (no modules)	12.8 lbs
Maximum Weight - Fully Configured	14 lbs
Airflow	Front to Side
Environmental Specifications	
Operating Condition	
Temperature - 5906 feet (1800 m) max. altitude	0-40°C (32-104°F)
Temperature - 9843 feet (3000 m) max. altitude	0-25°C (32-77°F)
Altitude	3000 m (10000 ft)
Humidity	10 to 85% RH
Acoustic: Sound Pressure (Typ/Max)	26/46 dBA
Acoustic: Sound Power (Typ/Max)	36/55 dBA
Transporation/Storage Condition	
Temperature	-40-70°C (-40-158°F)
Humidity	5 to 95%RH
Altitude	4570m (15000 ft)
Regulatory Compliance	
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Part 15 ICES-003 Class A EN55022 Class A CISPR22 Class A AS/NZS 3548 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 EN50082-1
Telecom	TIA/EIA/IS-968 CS-03 ANSI T1.101 ITU-T G.823, G.824 IEEE 802.3 RTTE Directive

WLAN Specifications

Table 8. WLAN specifications of the Cisco 1941W

Feature	Description
WLAN hardware	• IEEE 802.11n draft 2.0 standards-based access point with 802.11a/b/g compatibility • Automatic rate selection for 802.11g/n • Dual Radios for 802.11b/g/n and 802.11a/n modes. • RP-TNC connectors for field-replaceable external antennas • 2-dBi default antenna gain • 2 x 3 multiple input, multiple output (MIMO) radio operation • Wi-Fi 802.11n Draft v2.0 certified
WLAN software features	• Autonomous or unified access point • Cisco WCS support for monitoring of autonomous-mode access points • Option to maximize throughput or maximize range • Software-configurable transmit power • Radio roles, including access point, root bridge, non-root bridge, and workgroup bridge • Wi-Fi Multimedia (WMM) certification • Traffic specifications (TSPEC) Call Admission Control (CAC) to ensure voice quality is maintained • Unscheduled Automatic Power Save Delivery (UPSD) to reduce latency
Unified WLAN management	• Unified access point features: • Supported by wireless LAN controller and Cisco WCS • Configurable local or central switching for HREAP mode • Radio management through Cisco WCS • Transparent roaming with mobility groups
WLAN security features	• Standard 802.11i • Wi-Fi Protected Access (WPA) and AES (WPA2) • EAP authentication: Cisco LEAP, PEAP, Extensible Authentication Protocol Transport Layer Security (EAP TLS), Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Subscriber Information Module (EAP-SIM), Extensible Authentication Protocol- Message Digest Algorithm 5 (EAP-MD5), and Extensible Authentication Protocol-Tunneled TLS (EAP-TTLS) • Static and dynamic Wired Equivalent Privacy (WEP) • Temporal Key Integrity Protocol/Simple Security Network (TKIP/SSN) encryption • MAC authentication and filter • User database for survivable local authentication using LEAP and EAP-FAST • Configurable limit to the number of wireless clients • Configurable RADIUS accounting for wireless clients • Pre-Shared Keys (PSKs) (WPA-small office or home office [WPA-SOHO])
Certifications	abg WiFi n DRAFT CERTIFIED®
Service Set Identifiers (SSIDs)	16
Wireless VLANs	16
Encrypted wireless VLANs	16
Multiple Broadcast Service Set Identifiers (MBSSIDs)	16

Supported Modules

Cisco 1941 Series support a wide range of modules that span industry leading breadth of services at the branch. Please refer to the link below for the list of modules supported on the Cisco 1900. http://www.cisco.com/en/US/products/ps10538/products_relevant_interfaces_and_modules.html.

Ordering Information

The Cisco 1941 is orderable at the Cisco Ordering Home Page.

For more information about the Cisco 1900 Series, visit http://www.cisco.com/go/1900

Table 9 gives ordering information for the Cisco 1941 Router. For information about how to order the Cisco 1900 Series, please visit the Cisco 1900 Series Ordering Guide. To place an order, visit the Cisco Ordering Home Page and refer to Table 9, which provides basic ordering information. For additional product numbers, including the Cisco 1900 Series bundle offerings, please check the Cisco 1900 Series Integrated Services Router Price List or contact your local Cisco account representative.

Table 9. Cisco 1941 Series Basic Ordering Information

Product Number	Product Description
Cisco 1941/K9	Cisco 1941 with 2 onboard GE, 2 EHWIC slots, 1 ISM slot, 256MB CF default, 512MB DRAM default, IP Base.
Cisco1941W-A/K9	Cisco 1941 Router w/802.11 a/b/g/n FCC Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base.
Cisco1941W-E/K9	Cisco 1941 Router w/802.11 a/b/g/n ETSI Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base.
Cisco1941W-P/K9	Cisco 1941 Router w/802.11 a/b/g/n Japan Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base.
Cisco1941W-N/K9	Cisco 1941 Router w/802.11 a/b/g/n Aus and NZ Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base.
Cisco1941W-C/K9	Cisco 1941 Router w/802.11 a/b/g/n China Compliant, 2 onboard GE, 2 EHWIC slots, 256MB CF default, 512MB DRAM default, IP Base.

To download the Cisco ISR 1941 Cisco IOS Software release go to Download Software, click "Router Software," and go to Cisco ISR 1941 Integrated Services Router.

ISR Migration Options

Cisco ISR 1900 Series Routers are included in the standard Cisco Technology Migration Program (TMP). Refer to http://www.cisco.com/go/tmp and contact your local Cisco account representative for program details.

Warranty Information

The Cisco 1900 Series Integrated Services Router have a 1 year limited liability warranty.

For More Information

For more information about the Cisco ISR 1900 Series, visit http://www.cisco.com/go/1900 or contact your local Cisco account representative.

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies. For more information, please visit http://www.cisco.com/go/services.

Cisco SMARTnet® technical support for the Cisco 1900 Series is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates in protocol, security, bandwidth, and feature improvements
- Full access rights to Cisco.com technical libraries for technical assistance, electronic commerce, and product information
- 24-hour access to the industry's largest dedicated technical support staff

For More Information

For more information about the Cisco 1900 Series, visit http://www cisco.com/go/1900 or contact your local Cisco account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA
556319-07 04/13

C78-

ANEXO II. COMANDOS DE NETFLOW

En el anexo se presenta una guía de configuración de *Netflow*. S utilizarán para ellos tablas provenientes de (Cisco Systems, 2008) en las cuales se desarrolla la explicación para cada comando aplicado. Dichas tablas están escritas en idioma inglés, al igual que los *datasheets* del 0 debido a que éste es el idioma utilizado por CISCO en todas sus publicaciones y documentos.

Aunque el protocolo puede ser configurado en todas las tecnologías y protocolos de red incluidos en los dispositivos CISCO, sólo serán mostrados los comandos necesarios para el funcionamiento de *Netflow* en sesiones PPP y en sesiones IP debido a que los otros protocolos requieren configuraciones adicionales que no son objeto del Trabajo de Grado. Entre esos protocolos están MPLS y BGP, muy utilizados para el transporte metropolitano de redes.

Todos los comandos y procedimientos explicadosen el anexo fueron obtenidos de (Cisco Systems, 2008).

1. Configuración en sesiones IP

Tabla I. Configuración en sesiones IP

PASO	COMANDO	DESCRIPCIÓN
1	enable Example: Router> enable	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
2	configure terminal Example: Router# configure terminal	(Required) Enters global configuration mode.

PASO	COMANDO	DESCRIPCIÓN
3	ip flow-export destination {{ip-address | hostname} udp-port} Example: Router(config)# ip flow-export destination 172.16.10.2 99	(Optional) IP address or hostname of the workstation to which you want to send the NetFlow information and the number of the UDP port on which the workstation is listening for this input. Note The workstation is running an application such as NetFlow Collection Engine (NFC) that is used to analyze the exported data.
4	Repeat Step 3 once to configure a second NetFlow export destination.	(Optional) You can configure a maximum of two export destinations for NetFlow.
5	ip flow-export version 9 Example: Router(config)# ip flow-export version 9	(Optional) Enables the export of information in NetFlow cache entries. • The version 9 keyword specifies that the export packet uses the Version 9 format.
6	interface interface-type interface-number Example: Router(config)# interface ethernet 0/0	(Required) Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.

PASO	COMANDO	DESCRIPCIÓN
7	ip flow {ingress | egress} Example: Router(config-if)# ip flow ingress or Example: Router(config-if)# ip flow egress	(Required) Enables NetFlow on the interface. • ingress—captures traffic that is being received by the interface • egress—captures traffic that is being transmitted by the interface.
8	exit Example: Router(config-if)# exit	(Optional) Exits interface configuration mode and returns to global configuration mode. Note You only need to use this command if you want to enable NetFlow on another interface.

2. Configuración en sesiones PPP

Según se puede leer en (Cisco Systems, 2008), para que *Netflow* funcione de forma adecuada en presencia de sesiones del protocolo PPP, es necesario configurarlo en la interfaces virtuales creadas para el procesamiento y transmisión de las VLAN, en lugar de hacerlo en las interfaces físicas del enrutador, tal como se hace en sesiones IP.

Mediante la ejecución de los siguientes comandos se realiza la habilitación de *Netflow* en presencia de ambientes PPP:

```
Router>configure terminal
Router(config)# interface Virtual-Template 1
Router(config-if)# ip unnumbered ethernet 0
Router(config-if)# encapsulation ppp
```

```
Router(config-if)# ip flow egress
```

3. Personalización de la exportación de data de *Netflow*

En cada enrutador, de acuerdo a lo expresado en (Cisco Systems, 2008), se puede exportar la data creada por *Netflow* a destinos remotos, tales como un servidor de monitoreo de la red. Se explica que en cada en enrutador pueden configurarse hasta dos destinos de exportación aplicando los siguientes comandos:

Ip flow-export destination {{*ip-address* | *hostname*} *udp-port*}

ip flow-export source *interface-type interface-number*

ip flow-export version 9

ip flow-export interface-names

ip flow-export template refresh-rate

ip flow-export template timeout-rate

ip flow-export template options export-stats

ip flow-export template options refresh-rate packets

ip flow-export template options timeout-rate minutes

El segundo comando, ip flow-export source *interface-type interface-number*, especifica cuál será el origen del paquete IP creado durante la exportación de la data capturada por *Netflow*. Es la dirección que aparecerá en los encabezados de los paquetes IP.

El cuarto comando, ip flow-export interface-names, permite que *Netflow* incluya los nombres de las interfaces en las cuales se originan los flujos capturados por la herramienta.

El próximo comando, ip flow-export template refresh-rate, comando opcional, permite determinar el número de paquetes que serán recolectados por Netflow antes de que se realice a exportación de los mismos hacia la irección o *host* especificados previamente. La tasa de refrescamiento puede

ser configurada entre 1 y 600, aunque el valor predeterminado es de 20 paquetes.

El próximo comando, ip flow-export template timeout-rate minutes, especifica el tiempo que el protocolo *Netflow* debe esperar antes de reenviar un flujo de exportación hacia su destino. Se puede variar este tiempo entre 1 y 3600 minutos. Su valor predeterminado es de 30 minutos.

El comando ip flow-export template options export-stats especifica que en la exportación de la data se incluyen todos los flujos y paquetes capturados por *Netflow* de acuerdo a los parámetros configurados en el Capítulo IV.

BIBLIOGRAFÍA

Baeiros, M., & Lundqvist, P. (2011). *QoS - Enabled Networks - Tools and Foundations.* West Susex, Reino Unido: Wiley.

Barry, P. (2002). *Cisco ISP Esentials.* Cisco Press.

Case, J.; M, Fedor; M, Schoffstall;. (1990). *A simple network management protocol.* IETF, Network Working Group.

Cisco. (2012). *Annual report 2012.* Cisco Press.

Cisco Systems. (s.f.). Recuperado el 2012 de Septiembre de 2012, de www.cisco.com

Cisco Systems. (2001). *Configuring NetFlow.* San José, California, Estados Unidos: Cisco Systems.

Cisco Systems. (2007). *Netflow Performance Analysis.* San José.

Cisco Systems. (2007). *Netflow version 9.* San José.

Cisco Systems. (2008). CCNA Exploration v 4.0: Conmutación y Conexión Inalámbrica de LAN. San José, California, Estados Unidos.

Cisco Systems. (2008). *Cisco IOS Netflow Configuration Guide.* San Jose, California, Estados Unidos: Cisco Systems, Inc.

Cisco Systems. (Mayo 2012). *Introduction to Cisco IOS Netflow.* San José.

Colegio de Ingenieros de Venezuela. (2012). *Código de Ética.* Caracas, Venezuela.

Ferrer, G. G. (2012). *Investigación comercial* (Tercera ed.). Madrid, España: Universidad Rey Juan Carlos.

Flannagan, M. (2001). *Administering Cisco QoS in IP Networks.* Rockland: Syngress Publishing, Inc.

Gerencia de Tráfico - CANTV. (2010). *Datatrafic.* Caracas, Venezuela: CANTV.

Hewlett Packaard. (25 de Agosto de 2004). Recuperado el 27 de Septiembre de 2012, de www.hp.com

Landaeta, J. M. (s.f.). *Fundamentos de investigación de operaciones para administración.* Universitaria Potosina.

Landeau, R. (2007). *Elaboración de trabajos de investigación* (Primera ed.). Caracas: Editorial Alfa.

Lerma, H. (2007). *Metodología de la investigación: Propuesta, anteproyecto y proyecto* (Segunda ed.). Bogotá, Colombia: Ediciones Ecoe.

Muñoz, C. (1998). *Cómo Elaborar y Asesorar una Investigación de Tesis.* Pearson Educación.

Murray, P., & Stalvig, P. (2008). *SNMP: Simplified.* Seattle: F5 Networks, Inc.

Naghi, M. (2005). *Metodología de la investigación.* México: Limusa.

Paessler. (s.f.). Recuperado el 27 de Septiembre de 2012, de http://www.paessler.com/prtg/?source=adwords&campaign=prtg_Latin_Searc

h_English&adgroup=prtg_traffic_grapher&adnum=003&gclid=CK2A0cqG1rICFWlnOgodKl4Asg

Rodríguez, E. (2005). *Metodología de la investigación.* Tabasco, México: Univ. J. Autónoma de Tabasco.

Sampieri, R. H., Collado, C. F., & Lucio, P. B. (2010). *Metodología de la investigación.* Mc Graw Hill.

Schmidt, D. R. (2005). *Escential SNMP* (Segunda ed.). Sebastopol, Estados Unidos: O´Reilly.

Solie, K. (2003). *CCIE Practical Studies* (Vol. 2). Cisco Press.

Suck, A. T., & Rivas-Torres, R. (2007). *Manual de investigación documental* (Primera ed.). Editores Plaza y Valdés.

Taha, H. (2004). *Inestigación de operaciones* (Séptima ed.). México: Pearson Educación.

Universidad Católica Andrés Bello. (2007). *Revista sobre Relaciones Industriales y Laborales.* Departamento de Investigaciones sobre Relaciones Industriales y Laborales.

Wireshark. (18 de Julio de 2012). Recuperado el 27 de Septiembre de 2012, de www.wireshark.org