Planificación y Gestión de Red

Unidad I. INTRODUCCIÓN A LA GESTIÓN DE REDES

Documento base para los temas:

1. Apreciaciones Conceptuales de los Sistemas y la Contabilidad
2. Relación entre los Sistemas y la Contabilidad
3. Importancia de los Sistemas y Consideraciones
4. Clasificación de los Sistemas en una Empresa

1ra. Edición

Contenido >> M.Sc. Luis Molero

Diseño Instruccional >> Michell Villaruel

Diseño Gráfico >> Erwin Aguirre

Diagramación >> Alvaro Martínez

Maracaibo, Venezuela, 2010.

CONTENIDO

INTRODUCCIÓN

Toda organización en la actualidad debe precisar de elementos a través de los cuales sea posible medir, mantener y mejorar los procesos informáticos lo que se llama con frecuencia "**Calidad de servicio**" (QoS) término utilizado para garantizar los servicios ofrecidos en todas y cada una de las áreas funcionales dentro de la organización, ya que se espera que se ejecuten de forma óptima y garanticen las operaciones de los usuarios con la red de datos.

Cada área funcional dentro de la empresa, representa diferentes retos tanto comunicacionales como de almacenamiento y/o seguridad, por lo tanto, todo esto debe ponerse de manifiesto a la hora de configurar y mantener el equipamiento informático que lleva la carga de todas estas operaciones.

En este sentido, es preciso abordar la gestión de red por ser el protagonista de todos estos controles que deben llevarse permanentemente para poder ofrecer lo que al principio se conoció como calidad en el servicio.

OBJETIVO

Analizar la gestión de redes en entornos compartidos, a través, de mecanismos de monitorización y control, empleando diferentes modelos de información de gestión.

TEMA 1. ASPECTOS BASICOS DE LA GESTION DE REDES

Las redes, desde sus inicios han sembrado en sus usuarios una serie de necesidades que hasta la fecha han resultado en incrementos notables de anchos de banda debido a los evolucionados e incontables servicios que presta. Es así como los servicios de voz, datos e Internet, proporcionan a cada uno de ellos múltiples aplicaciones que van desde video conferencia, aplicaciones remotas y hasta compras a través de medios electrónicos.

Por consiguiente, la constante evolución de todos y cada uno de estos servicios ha involucrado de forma paralela la ejecución de estrategias y métodos para el control de esta información al tiempo de proveer de mecanismos de seguridad para proteger la integridad de los datos que se ofrecen en la red.

1.1. Evolución de la gestión de red

Desde sus inicios, las redes de datos han venido creando la necesidad sobre sus usuarios de proporcionar una diversa y gran variedad de servicios, integrándolos a sus plataformas computacionales, es por ello que cada día, las redes evolucionan para poder satisfacer todas y cada una de las expectativas planteadas de funcionamiento.

Bajo estos preceptos y paralelamente a estos hechos, un punto álgido en este creciente desarrollo de servicios ha sido la necesidad de mantener y controlar el buen funcionamiento de estos servicios de forma tal, que los usuarios de los sistemas, puedan satisfacer sus necesidades de forma permanente y sin ninguna interrupción.

En ese sentido, la gestión de redes da un paso adelante sobre todos y cada uno de estos aspectos, los cuales han venido evolucionando a la par con cada uno de los diferentes servicios que proporcionan las redes de datos.

La gestión de red, en sus primeros pasos, estableció como norte la monitorización del tráfico de red y el establecimiento de lo que se conoce como Calidad de Servicio (QoS), al tiempo de poder ofrecer la detección de los errores que se pudiesen producir en la red y el cómo identificarlos y solventarlos.

Siguiendo con la misma idea, la gestión de red fue conocida como gestión integrada, ya que ofrecían una gestión de red Autónoma, la cual establecía las habilidades de cada administrador de red sobre cada uno de los nodos en la red en función de que cada uno poseía su propio sistema de gestión local. Asimismo, evolucionó hacia los sistemas heterogéneos, donde esta evolución trajo consigo la necesidad de sistemas de gestión de red de diversas naturalezas.

En tal sentido, la gestión de red heterogénea, ha planteado y desarrollado desde su evolución diversos modelos a explicar a lo largo de este tema, donde se reseñan los más importantes que son: la Gestión de Red OSI y la Gestión Internet, este último ampliamente utilizado en la actualidad.

Finalmente, y como es visto en la actualidad, existen una gran diversidad de sistemas heterogéneos por lo cual se exige que haya un marco de elementos (protocolos, estándares, entre otros) que permitan un control permanente de la red, motivo por el cual, se desarrollo el protocolo SNMP que junto con otros protocolos de TCP/IP permite una gestión de red consolidada y marcada hasta la fecha el punto final en materia de protocolos de gestión.

1.2. Gestión de red

Martí (1999) expresa que la gestión de red extiende sus bases sobre la planificación, organización y el control de los elementos comunicacionales que garanticen una adecuada calidad de servicio sobre un determinado costo; éste busca mejorar la disponibilidad, rendimiento y efectividad de los sistemas.

De lo anterior se desprende, que a través de la gestión de red se establecen una serie de parámetros de calidad y control sobre todos y cada uno de los servicios que una red de comunicaciones ofrece a sus usuarios para garantizar un óptimo nivel de operatividad y acceso.

1.3. Elementos de la gestión de red

Entre los elementos de la gestión de red se encuentran**: los agentes, gestores y un dispositivo administrativo**; los cuales se visualizan en el siguiente gráfico.

Gráfico I.1. Elementos de la gestión de red.

Partiendo del gráfico anterior, se describen los elementos de la gestión de red mencionados en el mismo.

1.3.1. Agentes

Los agentes son un software de administración de red que se encuentra en un nodo administrado. Este posee una base de datos local de información de administración, denominada **MIB** por sus siglas en ingles, la cual es traducida a un formato compatible de acuerdo al protocolo de administración que rige en el sistema y es organizada en jerarquías.

Ejemplo I. 1 Agentes

En redes basadas en Windows, las estaciones de trabajo (Workstations) tienen instalado versiones cliente del servicio SNMP (SNMP Client), también conocido como Protocolo de Administración Sencilla de Red Cliente, a fin, de gestionar y auditar todos los servicios provistos por la estación de trabajo a través de un software de gestión local.

1.3.2. Gestores

Los gestores también pueden ser conocidos como Sistema de Gestión de redes **NMS**, Este ejecuta aplicaciones que supervisan y controlan permanentemente todos los dispositivos administrados. Los NMS proporcionan un conjunto de recursos de procesamiento y memoria requeridos para la administración de toda la red. Uno o más gestores deben existir en cualquier red administrada.

Ejemplo I.2 Gestores

Aplicaciones de consola que para la administración de SNMP, permitiendo establecer vistas y control remoto de dispositivos como router, switch e incluso impresoras.

1.3.3. Dispositivo administrativo

El dispositivo administrativo es cualquier nodo en la red que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de **control** y **monitoreo**, la cual es puesta a disposición de los gestores usando protocolos de administración de red.

Ejemplo I.3 Dispositivos Administrativos

Routers, servidores de acceso, switches, bridges, hubs, computadores o impresoras.

Es preciso destacar, que bajo el paradigma gestor-agente los elementos descritos con anterioridad son de vital importancia a la hora de enfatizar un modelo de gestión basado en un diseño distribuido donde la información de monitoreo y control no solo es recopilada y administrada por un solo regente (Gestor), sino también, a través de un agente local quien inicialmente captura y modela esos datos para servir como información de gestión.

1.4. Procesos de la gestión de red

La información generada por los elementos y/o aplicaciones de la red pretende establecer dos (2) procesos clave: **monitoreo y control**, ambos procesos se retroalimentan entre sí.

Por ende, la arquitectura de monitoreo y control establece una serie de bloques que comprenden actividades relacionadas con el control de todos los **nodos** dispuestos sobre la red.

En el siguiente gráfico se visualizan los procesos de la gestión de red.

Gráfico I. 2. Procesos de la gestión de red.

Partiendo del gráfico anterior, se describen los procesos de la gestión de red mencionados en el mismo.

1.4.1. Proceso de monitoreo

El monitoreo es un proceso permanente que busca mantener información del comportamiento de todos los entornos dispuestos sobre la red, a fin de establecer posibles controles y mejoras en el funcionamiento de los mismos para garantizar calidad en los servicios que esta fluyendo sobre la red.

La monitorización establece las **funciones de lectura** las cuales observan y analizan el estado y el comportamiento de las configuraciones de red y sus componentes.

Ejemplo I.4. Proceso de monitoreo.

WebNMS, es una aplicación de desarrollo y monitoreo que permite conocer en tiempo real el comportamiento de todos los objetos en la red, tales como router, switch e impresoras por citar algunos. Esta API audita permanentemente estos servicios de manera tal que cualquier error que ocurra disparará un mensaje como señal de problema permitiéndole al administrador poner en práctica sus habilidades y destrezas para solventar cualquier situación y/o comportamiento del dispositivo.

1.4.2. Proceso de control

Al igual que el proceso de monitoreo, el control es un proceso permanente que busca mejorar el desempeño de los servicios que se dan lugar en una red, el monitoreo es el paso inicial donde se capturan los datos de los diferentes entornos que operan de forma simultánea, y seguidamente, el control evalúa tales comportamientos y establece las directrices optimas de operatividad.

Por otra parte el control, establece las **funciones de escritura** que mantiene un registro de los parámetros (configuraciones) de los componentes de la red.

Es importante precisar, que en el proceso de gestión de red es necesario implementar políticas de calidad de servicio, término este, que obliga a mantener equilibrada y en optimas condiciones de funcionamiento a todos los servicios que la red ofrece, en donde los términos de monitoreo y control abordados en los preceptos anteriores tanto el monitoreo como el control sirven de base para la implementación de óptimos cánones de calidad de servicio.

Ejemplo I.5. Proceso de control.

HP provee un software llamado JetAdmin que permite afinar y optimizar las colas de impresión de sus servidores de impresión en virtud del escenario que se presente, ofreciendo por ende, un óptimo rendimiento y desempeño de operación.

TEMA 2. ÁREAS FUNCIONALES DE GESTIÓN DE RED

Martí (1999) manifiesta que todo flujo de información de gestión viene dado por un esquema de funcionamiento de gestión, que consiste en una serie de agentes contenidos en los diferentes recursos (nodos ó elementos) de la red, los cuales constantemente generan mediciones que son enviadas a los sistemas gestores para su posterior control. Éste control por su parte, está determinado por los diferentes mensajes que los sistemas gestores envían a estos nodos en la red provistos en algunos casos, con información de configuración que tienen como función principal de mejorar sus parámetros de funcionamiento para un óptimo desempeño.

En tal sentido, en la gestión de redes se involucran diversas áreas de aplicabilidad, en términos de la materia conocidas por Stalling (2000) como áreas de gestión de red ó áreas funcionales.

Dentro de las áreas de gestión de red o áreas funcionales se encuentran: **gestión de configuración**, **de prestaciones, de fallos, de seguridad y de costos**; los cuales se visualizan en el siguiente gráfico.

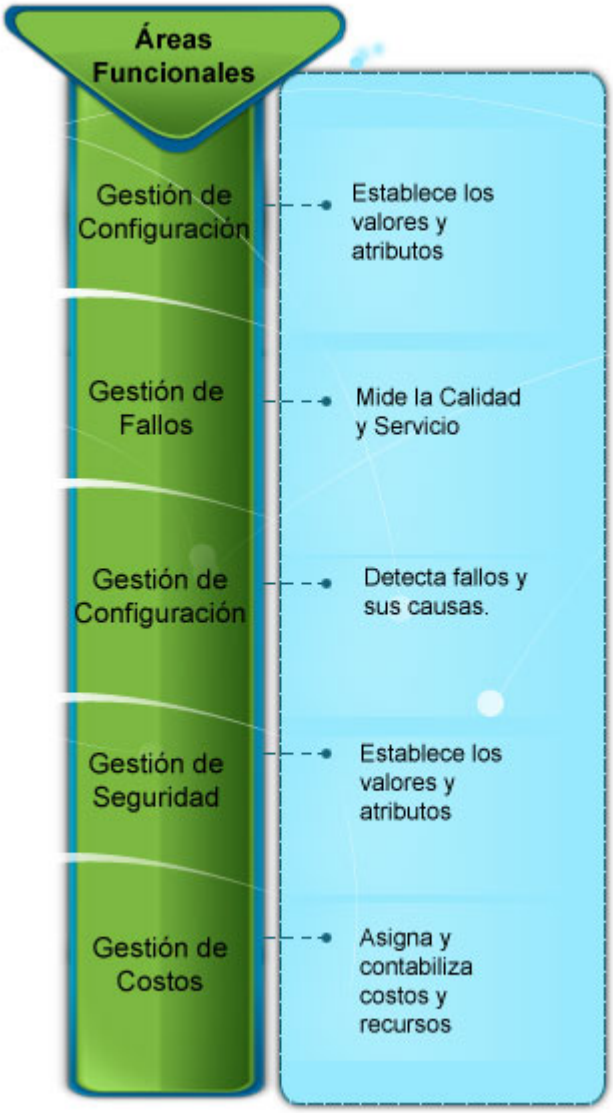

Gráfico I.3. Áreas de gestión de red o áreas funcionales.

A continuación, se describen las áreas de gestión de red o áreas funcionales mencionadas en el gráfico anterior.

2.1. Gestión de configuración

La gestión de configuración maneja el conjunto de recursos y procesos de red que operan entre sí de forma apropiada. Asimismo, se ocupa de la inicialización, mantenimiento y finalización de componentes individuales y subsistemas lógicos de la red.

En tal sentido, la gestión de configuración puede indicar el proceso de inicialización, identificando y especificando las características de los componentes y recursos que constituyen. También, se especifican valores iníciales o por defecto para los diferentes atributos, de forma que los recursos gestionados comiencen a operar en los estados deseados, teniendo los valores de atributos deseados y las relaciones adecuadas con otros componentes de la red.

2.1.1. Funciones de gestión de configuración

Durante el funcionamiento de la red, la gestión de configuración es responsable de realizar cambios en respuesta a comandos del usuario o en respuesta a otras funciones de gestión de red. Algunas de sus funciones y tareas consisten en:

- Definir la información de configuración.
- Establecer y modificar los valores de atributos.
- Establecer y modificar las relaciones.
- Operación de inicialización y apagado de la red.
- Distribución de software.
- Examinar los valores y relaciones.
- Informar sobre el estado de la configuración.

2.2. Gestión de prestaciones

La gestión de prestaciones asegura el correcto funcionamiento del entorno de red empleando para ello criterios de grado y calidad de servicio. Asimismo, mantiene un permanente monitoreo de la red para evitar embotellamientos, determina los parámetros de calidad de servicio y recoge y procesa los datos medidos tales como tráfico para generar los informes correspondientes.

En esta gestión, se establecen los indicadores apropiados para monitorizar adecuadamente las prestaciones de la red, entre ellos se encuentran: **medidas orientadas a servicios y orientadas a eficiencia**; los cuales se describen a continuación.

2.2.1. Medidas orientadas a servicios

Son las medidas que permiten mantener los niveles de determinados servicios a satisfacción de los usuarios. En tal sentido, se encuentran los siguientes aspectos:

- **Disponibilidad:** es el porcentaje de tiempo que una red, un dispositivo o una aplicación está disponible para el usuario.
- **Tiempo de respuesta:** cuánto tarda en aparecer la respuesta en el terminal del usuario cuando éste realiza una acción.
- **Fiabilidad:** porcentaje de tiempo en el que no ocurren errores en la transmisión y entrega de información.

Ejemplo I.6. Medidas orientadas a servicios.

En una red de datos, es de gran utilidad un servicio de impresión que permita a los usuarios descargar en físico la documentación organizacional, sin embargo, se hace necesario que este servicio esté disponible en horario de labores y que maneje un sistema de cola de impresión que no descarte ninguna documentación a imprimir por falta de recurso, es

decir, por falta de memoria para impresión, velocidad del equipo, entre otros.

2.2.2. Medidas orientadas a eficiencia

Son las medidas que permiten mantener los niveles de satisfacción anteriores al mínimo costo posible.

- **Prestaciones** *(througtput):* es la tasa a la que ocurren eventos en la capa de aplicación. Como puede ser el número de sesiones para una aplicación determinada durante un cierto período de tiempo. Sin embargo, es útil hacer un seguimiento de estas medidas en el tiempo para conseguir una visión aproximada de la diferencia entre las demandas reales de la red y las previstas y detectar puntos probables de problemas de prestaciones.

- **Utilización:** es el porcentaje de la capacidad teórica de un recurso que se está utilizando y es empleado para ubicar posibles áreas de congestión en la red, tales como concentradores y *switch*.

Ejemplo I.7. Medidas orientadas a eficiencia.

Si se maneja un servicio de impresión es preciso monitorear el rendimiento del equipo de impresión y establecer los niveles óptimos operativos en función del número de usuarios que hace uso de este recurso, de manera tal que, de haber un incremento en el número de usuarios que hacen uso de este servicio, se puedan mejorar sus parámetros de funcionamiento para compensar tal crecimiento y seguir ofreciendo un tiempo de respuesta optimo.

2.2.2.1. Funciones de gestión de prestaciones

Algunas de las funciones o tareas de la gestión de prestaciones son las siguientes:

- Capturar los datos ó variables indicadoras de rendimiento, tales como: la tasa de datos efectiva de la red, los tiempos de respuesta a los usuarios, entre otros.
- Analizar los datos para determinar los niveles normales de rendimiento.
- Establecer indicadores de problemas en el rendimiento de la red, en caso de quebrantarse.
- Determinar un sistema de procesamiento periódico de datos de desempeño acerca de los distintos equipos en la red para su estudio permanente.

2.3. Gestión de fallos

La gestión de fallos se encarga de detectar los fallos en la red lo más rápido posible, así como también, identificar sus causas para corregirlos con el fin de mantener la red disponible ante cualquier situación. Estas actividades se logran a través del monitoreo de la red y estado del sistema (Enable, Unable, Disable: Activado, desactivado temporalmente o desactivado), la recepción y procesamiento de alarmas, el diagnóstico permanente de los elementos de red y las medidas de recuperación ante errores.

A continuación, se describen elementos importantes tales como: **los archivos históricos**, conocidos también como **archivos logs, y administrador de red;** que son piezas importantes dentro de las actividades descritas con anterioridad en función de la gestión de fallos.

2.3.1. Archivos históricos (logs)

Están referidos a los archivos históricos (logs) de errores significativos de la red que debe llevar la gestión de fallos, por las siguientes razones:

- Manejar los criterios para evitar la sobrecarga de información.
- Obtener información concreta acerca de los fallos sucedidos.

Además, debe definir mecanismos para anticiparse a posibles errores estableciendo límites de disparo para determinados valores monitorizados en la red.

2.3.2. Administrador de red

Esta gestión debe asistir al administrador de red en el diagnóstico y encapsulamiento de fallos en la red proporcionando herramientas tales como (*Testers*, aplicaciones de escucha de paquetes en la red (*Sniffers*), entre otros) para realizar pruebas de conectividad, de integridad de datos, de integridad de protocolos y tiempos de respuesta entre otros.

Asimismo, debe proporcionar una interfaz de usuario efectiva debido a que es el área de gestión donde es más importante localizar, aislar y diagnosticar fallos lo más pronto posible.

2.3.3. Funciones de gestión de fallos

La gestión de fallos, plantea la detección y corrección de los fallos producidos en la red. Sus principales funciones son:

- Determinar los síntomas del problema.
- Aislar el fallo.
- Resolver el fallo.

- Comprobar la validez de la solución en todos los subsistemas importantes de la red.
- Almacenar la detección y resolución del problema.

2.4. Gestión de seguridad

La gestión de seguridad se encarga de proteger el activo más importante de la organización que corresponde a la información que se genera diariamente. Adicional a ello, se encarga de proteger los equipos de comunicación, servidores y estaciones de trabajo de posibles ataques proveniente de terceros para mantener la integridad del sistema.

2.4.1. Funciones de gestión de seguridad

Algunas de las funciones y tareas de la gestión de seguridad son:

- Monitorear la red o el sistema frente ataques.
- Encriptado de la información.
- Establecimiento de procedimientos de autentificación.
- Implementación de medidas de seguridad.
- Mantenimiento de la información de seguridad.
- Control de acceso a los recursos.

2.4.2. Ataques en la gestión de seguridad

Algunos de los ataques que pueden ser perpetrados hacia el software y el hardware durante la gestión de seguridad son: **interrupción, intercepción y modificación**; los cuales se describen en el siguiente cuadro.

Cuadro I.1. Ataques en la gestión de seguridad.

Ataques	Descripción	Ejemplos
Interrupción	La interrupción de un recurso de software ó hardware, tal es el caso de un equipo de comunicaciones o un servidor de archivos.	**Ejemplo I.8. Interrupción** Existen técnicas de *Haking* que son utilizadas por usuarios malintencionados para apagar servidores de datos de manera tal, que sea inaccesible la información que contienen.
Intercepción	Intercepción de un usuario no autorizado que logra entrar a través de una computadora a la red para violar la integridad de los datos.	**Ejemplo I.9. Intercepción** Existen usuarios que se introducen a las redes pinchando cables de red o suplantando identidades de red y luego de ellos perpetran actos lascivos contra el equipamiento y/o el software.
Modificación	Cuando un usuario no autorizado, luego de tener acceso a los datos de la red los modifica.	**Ejemplo I.10. Modificación** En ocasiones, luego de romper las barreras de seguridad implementadas por los administradores de red, los usuarios malintencionados modifican datos estratégicos de la organización ocasionando daños por decenas de millones de bolívares.

2.5. Gestión de costos

La gestión de costos conocida también como gestión de contabilidad, se basa en el registro del uso de los recursos y servicios proporcionados por la red a los usuarios estudiando para ello su distribución en relación con las políticas de tráfico todo esto, de acuerdo con las necesidades de la organización. En esta gestión se hacen mención de: **funciones, recursos y datos obtenidos**; los cuales se describen a continuación.

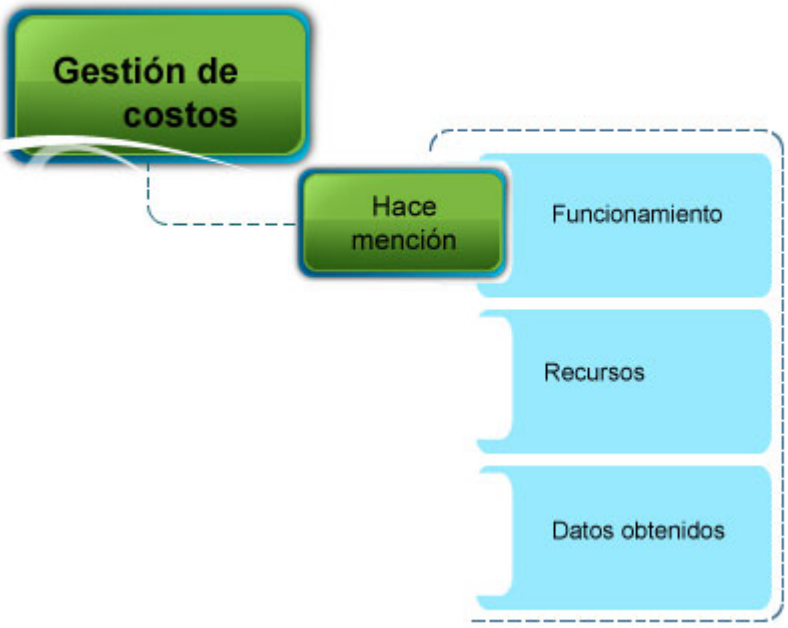

Gráfico I.4. Gestión de costos.

A continuación, se describe los aspectos de la gestión de costos mencionados en el gráfico anterior.

2.5.1. Funciones de gestión de costos

Algunas de las funciones y tareas que están relacionadas con dicha gestión son:

- Tomar y almacenar los datos del uso de los recursos.
- Mantenimiento del registro de cuentas de usuario.
- Asignación de costos.
- Asignación y monitorización de cuotas de uso.
- Mantenimiento de estadísticas de uso.

2.5.2. Recursos gestionados de costos

Algunos de los recursos gestionados en esta área son: **recursos de comunicación, hardware de computación, software y servicios**; los cuales se describen en el siguiente cuadro.

Cuadro I.2. Recursos gestionados de costos.

Recursos	Descripción
Recursos de comunicación	Estos recursos están referidos a redes LAN, WAN, líneas dedicadas de datos, entre otros.
Hardware de computación	Están referidos a servidores, estaciones de trabajo.
Software	Son los software de servidores, aplicaciones de datos, entre otros.
Servicios	Son todos los servicios de información y servicios de comunicaciones comerciales disponibles.

2.5.3. Datos obtenidos de la red

Algunos datos obtenidos de la red, que son contabilizados por esta gestión son: **identificación de usuario, receptor, número de paquetes, nivel de seguridad y recursos utilizados**; los cuales se describen a continuación.

Cuadro I. 3. Datos obtenidos de la red.

Datos	Descripción
Identificación de usuario	Proporcionada por el generador de una transacción o petición de servicio.
Receptor	Identifica el recurso de red utilizado.
Número de paquetes	Cantidad de datos transmitidos.
Nivel de seguridad	Identificación de las prioridades de la transmisión y el procesamiento.
Recursos utilizados	Recursos involucrados en una transacción o evento de servicio.

TEMA 3. MODELO DE GESTIÓN DE REDES OSI

Según Martí (1999) el modelo de gestión OSI comprende la administración de sistemas que delimita la operación de cualquiera de las siete (7) capas del modelo OSI (capa n) y la administración de los objetos gestionados (**MO**s), en los cuales se plantea el modelo de información, organización, comunicación y función, considerados sub-modelos del modelo OSI.

A continuación, se expone en el siguiente gráfico el modelo de gestión OSI.

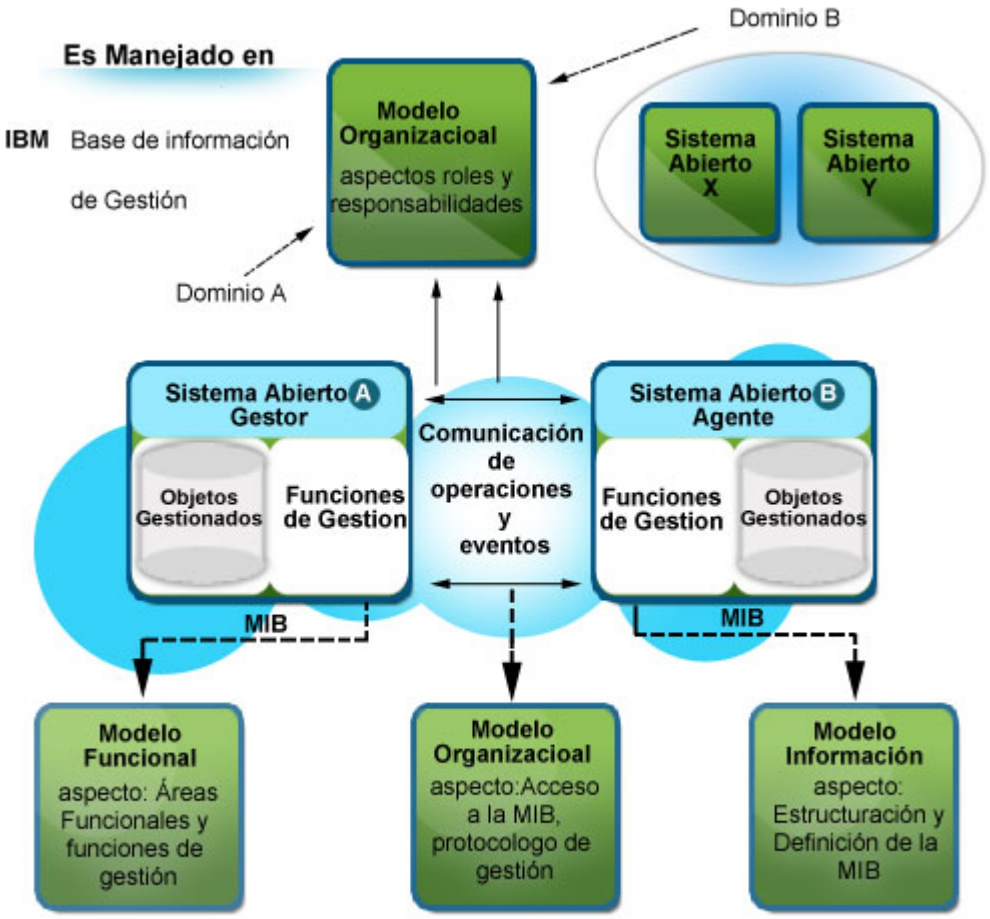

Gráfico I.5. Modelo de gestión OSI según Martí (1999)

En el gráfico anterior se presenta la arquitectura del modelo de gestión OSI y como actúa cada uno de sus componentes (modelos) con los elementos de gestión como son: el agente, el gestor y le dispositivo administrado.

3.1. Arquitectura de gestión OSI

De acuerdo con Martí (1999), la arquitectura de gestión OSI surge como un modelo que involucra tanto al computador como a la red, donde los elementos previos a su desarrollo vienen dado sobre arquitecturas aisladas, con poca coordinación e integración entre sí.

En tal sentido, existieron otras situaciones que aumentaban la necesidad de coordinación sobre la arquitectura de red, esta se sustentaba en el hecho de que en el mercado no todos los diseños de redes manejaban los mismos requerimientos, por tanto, cada diseño de red exigía retos diferentes en cuanto a su implementación, situación propia de los ambientes heterogéneos.

Por ende, los ambientes heterogéneos ameritaron el desarrollo de un modelo de gestión que proporcionará integración (siendo este desarrollo parte de la evolución de sistemas de gestión) apoyándose así sobre un mismo bloque de normas y estándares de diseño de redes, es por ello, que fue diseñada la arquitectura de gestión OSI.

3.2. Capas del modelo OSI

Cabe destacar que el modelo OSI está compuesta por siete (7) capas: aplicación, presentación, sesión, transporte, red, enlace de datos y física, con la finalidad de ofrecer coordinación e integración entre los diferentes fabricantes. En tal sentido, las capas antes mencionadas se describen en el siguiente cuadro.

Cuadro I.3. Capas del modelo OSI.

Capas	Descripción
Aplicación	Responsable inicial de la creación de datos en la red.
Presentación	Encargada de la codificación, formato y compresión de datos.
Sesión	Inicia, mantiene y finaliza una conversación entre dos nodos en la red.
Transporte	Maneja varios esquemas de transmisión de paquetes y encargada del proceso de control de flujo.

Capas	Descripción
Red	Encargada del direccionamiento IP y enrutamiento de paquetes.
Enlace de datos	Constituye el direccionamiento MAC, el control de flujo, la detección de errores, el entramado y la gestión de comunicación.
Física	Constituye las normas eléctricas, de propagación de señales, conectorización de los diferentes medios para redes de datos y especificaciones de frecuencia.

3.3. Modelo de información OSI

El modelo de información, modela y describe previamente los objetos gestionados (**MO**s) en una red, para poder ser operados y administrados en un entorno de recursos compartidos, explícitamente heterogéneo.

La norma **ISO/IEC 10165-1** (1993) define que este modelo de información administra los objetos y sus propiedades que corresponde a los aspectos de información de los modelos de administración de sistemas.

Este modelo establece lo siguiente:

- Los principios de nomenclatura de los objetos gestionados y sus atributos.
- Define la estructura lógica de los sistemas de administración de la información.
- Define los conceptos de la administración de los objetos en el modelo de información.
- Describe el concepto de la administración de clases de objetos y las relaciones en la que los objetos gestionados pueden entrar en las clases de objetos.

Además, el modelo de información está fundamentado en las normas ISO/IEC 10165-1, 10165-2, 10165-3, 10165-4, 10165-5, 10165-6, 10165-7, 10165-8, 10165-9.

3.3.1. Objetos gestionados (MO)

Martí (1999) expresa que un objeto gestionado es conocido por sus siglas MO (*Managed Object*) ya que es una abstracción de un recurso que representa sus propiedades para el propósito de su gestión, es decir, es un compendio de elementos llamados propiedades ó atributos que definen a un elemento en la red, tal es el caso de una conexión de red, un tipo de impresora, una interfaz de un router, entre otros.

Cuando se habla de objeto gestionado se hace mención de las **propiedades y de las operaciones**; las cuales se describen en el siguiente cuadro.

Cuadro I.4. Objetos gestionados.

Objetos	Descripción
Las propiedades	Son atributos que pueden cambiarse y/o modificarse.
Las operaciones y las acciones	Se pueden aplicar sobre un **MO**. Asimismo, un **MO** puede enviar notificaciones (mensajes no solicitados) acerca de algún evento ocurrido que contiene detalles del porqué y donde ocurrió, entre otros.

A continuación, en el siguiente gráfico se visualiza la estructura de los objetos gestionados con las siglas **MOC**, y **MO.**

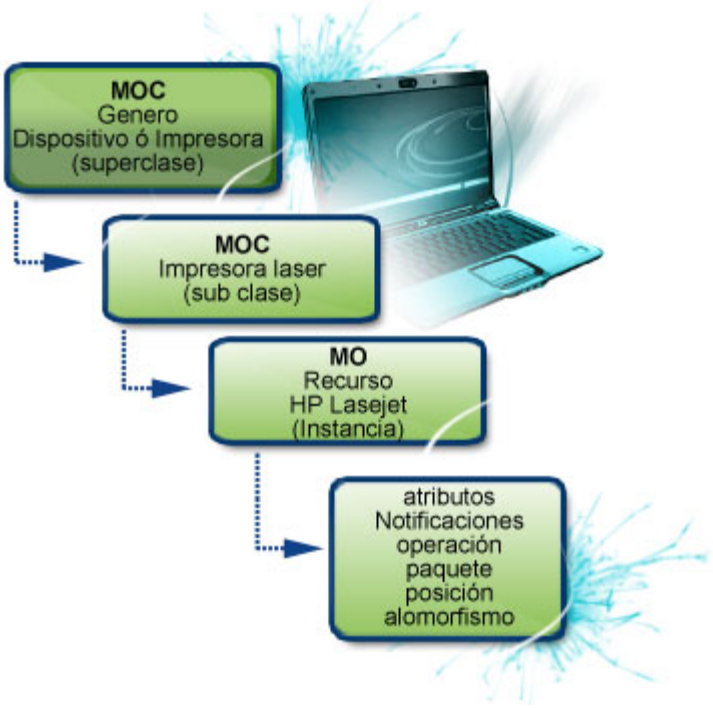

Gráfico I.6. Estructura de los objetos gestionados.

La administración de los **MO**s dentro de la administración de capa *n*, está delimitada en cada capa en particular, mientras que las operaciones de capa *n*, está delimitada al monitoreo y control de una sola instancia (recurso) de comunicación de la información de administración dentro de cada una de las capas.

A continuación, en el siguiente cuadro se describen la estructura de los objetos gestionados mencionados en el gráfico anterior.

Cuadro I.5. Estructura de los objetos gestionados.

Estructuras	Descripción
MOC	Es una serie de paquetes que pueden ser obligatorios y/o condicionados agrupados de acuerdo a sus características similares, de forma tal, que el administrador y los agentes conozcan los detalles de los recursos y puedan controlar las actividades de cada uno de ellos. En ese sentido, son las propiedades visibles que están descritas en el Límite de objetos gestionados (**MOB**) de cada clase que incluye los atributos, las operaciones definidas, notificaciones y descripciones del comportamiento de cada clase (genero).
MO	Son instancias (recursos) de las clases objetos gestionados (MOC).

3.3.1.1. Componentes de los objetos gestionados

Según Martí (1999) los objetos gestionados dentro de la **SMI** están compuestos por los siguientes componentes: **atributos, comportamiento, acciones, notificaciones, paquetes condicionales y jerarquía o posición**; los cuales se describen en el siguiente cuadro.

Cuadro I.6. Componentes de los objetos gestionados.

Componentes	Descripción
Atributos	Propiedades, que pueden ser obligatorios, condicionales ó de grupo.
Comportamiento	Semántica del atributo, notificaciones y operaciones permitidas sobre el **MO**.

Componentes	Descripción
Acciones	Operaciones complejas que afectan a todo el MO, tales como *Reset*, *Create* ó *Delete* **MO**.
Notificaciones	Eventos y/o comportamientos ocurridos del **MO**.
Paquetes Condicionales	Agrupación de **MO** de acuerdo a sus características.
Jerarquía ó Posición	Ubicación del **MO** en su jerarquía.
Alomorfismo	Capacidad de una instancia de una subclase de simular el comportamiento de su superclase.

3.3.2. Estructura de administración de información (SMI o MIB)

El modelo de información maneja un enfoque orientado a objeto que construye una base de datos conceptual llamada **Estructura de administración de información** (**SMI**) (en otras referencias se le conoce como **MIB** – Base de Información de Gestión) para almacenar los detalles de los objetos gestionados. Este **modelo conceptual**, no tiene relación en la forma de cómo los datos se encuentran, física o lógicamente, formateados y almacenados, y es descrito en la norma ISO/IEC 10165-9 (2000) sobre sistemas de administración de la capa de aplicación de objetos gestionados.

Por consiguiente, el modelo conceptual orientado a objetos de acuerdo a lo descrito en la norma ISO/IEC 10165-9 acerca de la **Estructura de administración de información** (**SMI**), se desprende los siguientes conceptos.

- **Encapsulamiento:** relación de inclusión entre un objeto y sus atributos, que asegura su integridad.
- **Clases:** género ó agrupación de objetos que comparten los mismos atributos.
- **Ejemplares:** recursos ó instancias de una clase.
- **Clases de objetos:** nueva subclase que aparece como extensión de una superclase existente añadiendo nuevas propiedades, donde se introduce una relación de herencia.

Cabe destacar que los conceptos antes descritos representan los objetos gestionados dentro de la estructura SMI, tomando en cuenta, que la SMI es una base de datos de todos los objetos gestionados en una red de datos.

3.4. Modelo de organización OSI

Martí (1999), expresa que el modelo de organización es una estructura dividida en dominio de red el cual comprende su operabilidad y ofrece el soporte a los aspectos de gestión del mismo. Por su parte, este modelo establece los diferentes papeles tales como dominios y sub-dominios.

Por otra parte, el sistema de gestión define los conceptos tanto para una gestión cooperativa entre iguales (concepto simétrico - Dominios), como para una gestión basada en una estructura jerarquizada (concepto asimétrico – Dominios y Sub-dominios), según su distribución espacial. La gestión de los dominios define la división del entorno teniendo en cuenta dos (2) motivos principales: **políticas funcionales y otras políticas**; las cuales se describen a continuación.

- **Políticas funcionales:** se consideran a aquellos dominios con las mismas políticas de seguridad, contabilidad entre otros.
- **Otras políticas:** en este ámbito hace referencia a los dominios geográficos y tecnológicos entre otros.

3.4.1. Funciones del modelo de organización OSI

Algunas funciones del modelo de organización OSI son las siguientes:

- Estructurar la red en dominios administrativos.
- Establecer un mantener, las actividades propias de cada dominio.
- Permitir la reasignación dinámica de los gestores y loa agentes.
- Mantener un protocolo de transporte para la gestión de dominios.

3.5. Modelo de comunicación OSI

El modelo de comunicaciones, detalla el protocolo de gestión del modelo OSI conocido como CMIP, asimismo, especifica cuáles son los servicios que proporciona este protocolo para operar sobre la red de datos.

3.5.1. Funciones del modelo de comunicación OSI

En la norma ISO/IEC 9595:1998 tiene como la función del modelo de comunicación, ya que precisa el Servicio de Información de Gestión Común por sus siglas en ingles (CMISE - *Common Management Information Service*). Este servicio puede ser empleado por los elementos de la red para la gestión de red y define la interfaz de servicio, que es ejecutado por el Protocolo Común de Gestión de Información (CMIP).

En el modelo de información de gestión de Internet también se pueden definir objetos afines dentro de grupos de objetos (object group), los cuales se ven como una unidad de implementación, y un programador puede codificar cero o más objetos de los contenidos en el grupo.

3.5.2. Protocolo CMIP

El CMIP, es un protocolo de gestión red orientado a conexión definido por el Servicio de Información de Gestión Común por sus siglas en ingles **CMISE**. Este protocolo CMIP administra información y permite las acciones de ejecución y modificación en relación a

los objetos gestionados (**MO**). Asimismo, el CMIP permite comunicaciones entre aplicaciones de gestión de red y sus agentes de administración, conocidos comúnmente como servicios CMIS individuales, es decir; que dicho protocolo CMIP proporciona el servicio CMIS, ambos están definidos en la capa de aplicación del modelo OSI.

3.5.2.1. Características del protocolo CMIP

De acuerdo con Martí (1999), el CMIP presenta las siguientes características:

- Requiere gran cantidad de memoria y capacidad de procesamiento
- Genera largas cabeceras en los mensajes.
- Comunicación con los agentes orientada a conexión.
- Estructura de funcionamiento distribuida.
- Permite jerarquía de sistemas de operación.
- Asegura que los mensajes llegan a su destino.
- Orientado a gestión por eventos.

3.5.2.2. Gestión del protocolo CMIP

El Protocolo Común de Gestión de Información (CMIP) opera con el servicio de aplicación de elemento ACSE y los protocolos de servicio de operaciones remotas ROSE, ambos son protocolos OSI de capa de aplicación 7. En tal sentido, ACSE se utiliza para gestionar las asociaciones entre las aplicaciones de gestión (es decir, gestionar las conexiones entre los agentes CMIP) mientras que ROSE, se emplea para todas las interacciones de intercambio de datos. Además, de la presencia de estos protocolos capa 7, CMIP asume la presencia de todas las capas del modelo OSI en los niveles inferiores, pero no se especifica explícitamente lo que estos deberían ser.

Por otra parte, el protocolo de gestión de red CMIP hace uso de un metalenguaje de plantillas simple distinguido como GDMO soportados por la norma ISO 10165-4 basado en la Notación de Sintaxis Abstracta (ASN.1) descrito en la norma ISO 8824 que será descrito más adelante en esta unidad. Este metalenguaje, especifica el formato y los

lineamientos para las definiciones de las clases de objetos (MOC) modelo de información OSI ya descrito.

3.5.2.3. Soportes de seguridad CMIP

Este protocolo de gestión, ofrece soporte en términos de seguridad tales como se pueden apreciar a continuación.

- Control de acceso.
- Soporte para autorizaciones.
- Archivos de registros de seguridad (Logs).
- Reportes de condiciones de red inusuales.

3.6. Modelo funcional OSI

La norma ISO/IEC 7498-1 al **7498-4**, expresa que las funciones de gestión de red son muy amplias y se detallan a un nivel descriptivo, donde cada una las áreas de funcionamiento de gestión de red (SMFA´s) supone el uso de funciones específicas (SMF's), y hay un considerable solapamiento entre las funciones de soporte, es decir, no solo se conocen las SMF's como funciones especificas sino también, que son funciones de soporte de cada SMFA. Las funciones de soporte/especificas son genéricas, es decir, que la SMFA **x** puede utilizar una o varias SMF's y la SMFA **y** también puede utilizar una o las mismas que la SMFA **x.**

3.6.1. Áreas funciones de gestión específica (SMFA)

Las áreas funcionales de gestión específicas, estandarizan un conjunto de sub-funciones específicas de la red de datos, éstas por su parte, son llamadas funciones de gestión del sistema conocidas por sus siglas en ingles **SMF** (*System Management Functions*). Cada estándar de SMF define la funcionalidad para soportar los requisitos de las **SMFAs**. Una SMF determinada puede dar soporte a varias SMFAs y cada SMFA requiere varias SMFs. Asimismo, cada estándar de SMF define su funcionalidad y proporciona una

correspondencia entre los servicios de la SMF y de la CMISE. En tal sentido, cada SMF puede utilizar los servicios de otras SMFs y de la CMISE. A continuación, se exponen las áreas funcionales de la gestión de servicio (**SMFAs**) en el siguiente gráfico, donde se muestran los componentes y estándares con los que lleva a cabo la gestión de red.

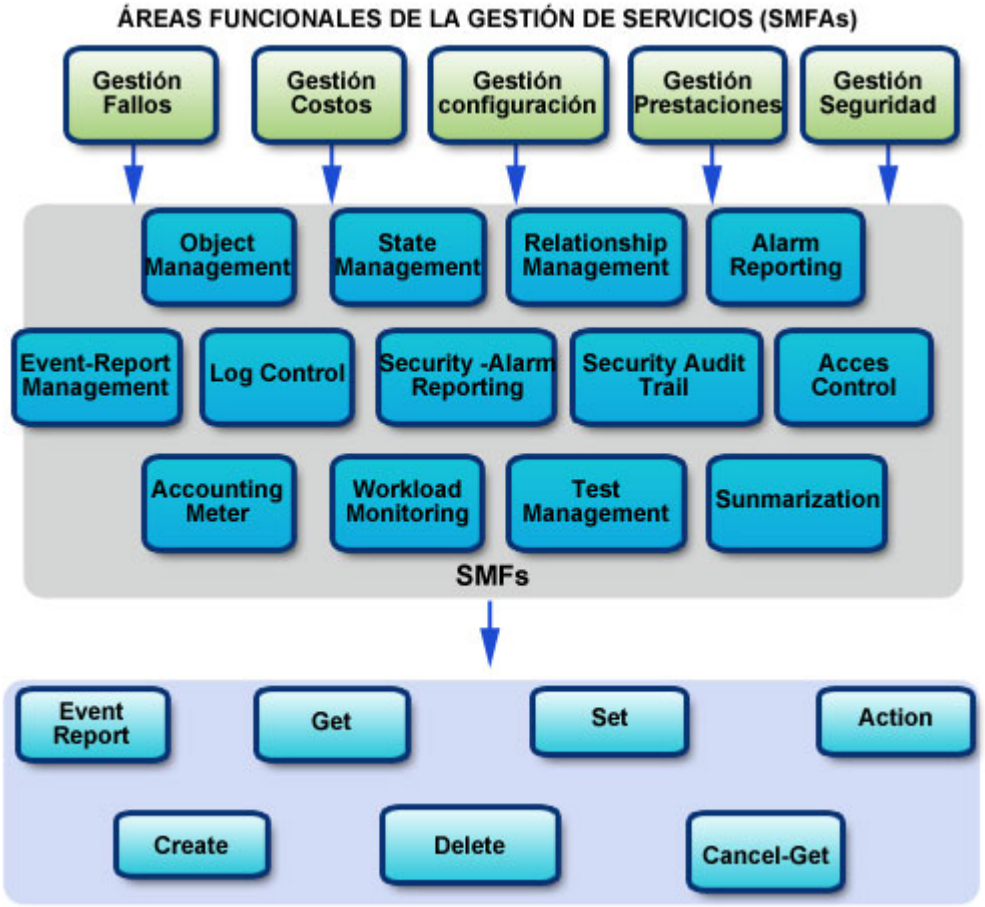

Gráfico I. 7. Áreas funcionales específicas (SMFAs).

3.6.1.1. Estándares de los servicios SMFs

Son trece (13) estándares que definen a las funciones de gestión de servicios *SMFs,* ellas son: **Gestión de objeto, de estado, de relación, reporte de alarma, de reporte de eventos, control de históricos, reporte de alarmas de seguridad, rastreo de seguridad y auditoria, control de acceso, cuentas, monitoreo de atributos, gestión de prueba y estadísticas**; los cuales se describen en el siguiente cuadro.

Cuadro I.7. Estándares de los Servicios SMFs.

Estándares Gestionados	Descripción
Gestión de Objeto (*Object management***)**	Soporta la creación y borrado de objetos gestionados (MO) y la lectura y cambio de atributos de objetos. También especifica las notificaciones que se deben enviar cuando cambia el valor de un atributo.
Gestión de Estado (*State management***)**	Especifica el modelo de representación del estado de gestión de un objeto. Proporciona servicios para soportar ese modelo.
Gestión de Relación (*Relationship Management***)**	Especifica el modelo de representación y gestión de relaciones entre objetos. Proporciona servicios para soportar ese modelo.
Reporte de Alarma (*Alarm reporting***)**	Soporta la definición de alarmas de fallos y las notificaciones utilizadas para comunicarlas.
Gestión de Reporte de Eventos (*Event-report Management***)**	Soporta el control de informe de eventos (notificaciones), incluyendo la especificación de los receptores de la notificación, la definición de notificaciones, y la especificación de criterios para generar y distribuir notificaciones.
Control de Históricos (*Log control***)**	Soporta la creación de históricos, la creación y almacenamiento de registros en históricos, y la especificación de criterios para realizar históricos.
Reporte de Alarmas de Seguridad (*Security-alarm reporting***)**	Soporta la definición de alarmas de seguridad y las notificaciones utilizadas para comunicarlas.
Rastreo de Seguridad y Auditoria (*Security-audit trail***)**	Especifica los tipos de informe de eventos que debería contener un histórico utilizado para evaluación de seguridad.
Control de Acceso (*Access control***)**	Soporta el control de acceso a la información y operaciones de gestión.
Cuentas (*Accounting meter***)**	Proporciona informes de la utilización de los recursos del sistema y un mecanismo para poner límites.
Monitoreo de Atributos (*Workload monitoring***)**	Soporta la monitorización de atributos de los objetos relacionados con las prestaciones del recurso.

Estándares Gestionados	Descripción
Gestión de Prueba (*Test Management*)	Soporta la gestión de procedimientos de prueba y diagnóstico.
Estadísticas (*Summarization*)	Soporta la definición de medidas estadísticas para los atributos y la comunicación de la información resumida.

TEMA 4. NOTACIÓN SINTÁCTICA ABSTRACTA UNO (ASN.1, ISO 8824)

El protocolo de gestión de red CMIP, administra información y permite las acciones de ejecución y modificación en relación a los objetos gestionados (MO). Asimismo, permite comunicaciones entre aplicaciones de gestión de red y sus agentes de administración, es por ello, que CMIP hace uso de la notación sintáctica abstracta uno como modelo estándar que especifica el formato y los lineamientos para las definiciones de las clases de objetos (MOC) y los objetos gestionados (MO). Por otra parte, ASN.1 está dividido en dos (2) elementos:

- La primera parte corresponde a las **reglas de sintaxis** para describir el contenido de un mensaje en términos de tipo de datos y la secuencia de contenido ó su estructura.
- La segunda, es la de **codificar** cada elemento de datos en un mensaje.

Otro aspecto importante en ASN.1 es la heterogeneidad de entornos donde puede funcionar. Esta característica hace que esta notación ofrezca versatilidad debido a que puede actuar en diferentes tipos de redes de forma simultánea, por ende, se hace necesario que se codifique la información abstracta en un flujo de bits único, estrategia que se consigue a través del uso de las reglas de codificación básicas (BER) para que la información pueda ser interpretada en cualquier nodo de la red de la misma manera.

4.1. Definición de ASN

Stalling (1999) define la notación sintáctica abstracta uno, como un metalenguaje que especifica el formato y los lineamientos para las definiciones de las clases de objetos utilizado ampliamente en el desarrollo de normalizaciones relacionadas con los modelo OSI y TCP/IP. Asimismo, se utiliza para definir el formato de las unidades de datos de protocolo (PDU), la representación de la información distribuida y las operaciones realizadas con los datos transmitidos.

Siguiendo con la idea anterior, se entiende que ASN proporciona diferentes componentes que no solo se encargan de elaborar una dato de protocolo (PDU) sino también, la forma de cómo este será representado a través de una sintaxis para poder de esta forma viajar por un medio tangible o intangible y llegar al nodo destino.

Por otra parte, Larmouth (1999) expresa que esta sintaxis trata de un estándar internacional, independiente del proveedor, independiente de la plataforma e independiente de los idiomas de notación para especificar estructuras de datos a un alto nivel de abstracción. De lo anterior se desprende que ASN.1, se apoya en normas que determinan los patrones precisos de bits para representar los valores de estas estructuras de datos cuando tienen que ser transferidos a través de una red de computadoras, utilizando la codificación.

4.1.1. Tipos de componentes de ASN.1

Existen dos (2) tipos de componentes de ASN.1 tales como: el **componente de aplicación y de transferencia**; los cuales se describen a continuación.

4.1.1.1. Componente de aplicación

Es la forma de cómo el usuario ve los datos a través de las aplicaciones, que no es más que un conjunto estructurado de información.

Ejemplo I.11. Componente de aplicación.

Un archivo, un texto en un documento, una base de datos, entre otros. El usuario en este caso, está relacionado con la semántica (representación) de los datos.

En tal sentido, el componente de aplicación es quien debe proporcionar una representación de estos datos que se puedan convertir en bits, que esté relacionado con la sintaxis de los datos. Asimismo, para el componente de aplicación, la información se

representa en una sintaxis abstracta que trata con tipos de datos y los valores de esos datos para intercambiar información entre componentes de aplicación en sistemas diferentes (heterogéneos), de esta forma, es como los protocolos de la capa de aplicación describen sus **PDU** en términos de esta sintaxis.

4.1.1.2. Componente de transferencia

Los datos recibidos de una aplicación se muestran como una secuencia de octetos binario (10001110 = A, 00110101 = s), donde estos se pueden ensamblar directamente en Unidades de Datos de Servicio (**SDU**) para ser transferidos entre capas (Aplicación, Presentación) y en Unidades de Datos de Protocolo (**PDU**) para ser transferidos entre entidades de una misma capa.

Ejemplo I.12. Componente de transferencia.

Un archivo, un texto en un documento, una base de datos, entre otros. El usuario en este caso, está relacionado con la semántica (representación) de los datos.

Para el componente de trasferencia, la sintaxis de transferencia especifica la representación de los datos que se van a intercambiar entre los componentes de transferencia de datos. La traducción de ambas sintaxis la abstracta y la de transferencia se realiza por medio de reglas que especifican la representación de cada valor de los datos de cada tipo de datos.

4.2. Tipos de datos

Según Stalling (1999) ASN.1 es una notación para tipos de datos abstractos y sus valores. Un tipo (elemento), se puede ver como una colección de valores (atributos), que puede ser infinito. Los tipos se dividen en cuatro (4) categorías: **primitivos, estructurado, definidos y etiquetados**; los cuales se describen en el siguiente cuadro.

Cuadro I. 8. Tipos de datos.

Tipos	Descripción
Primitivos	Son tipos autónomos sin componentes que incluyen a los *INTEGER, OCTET, STRING, OBJECT IDENTIFIER y NULL*.
Estructurado	Los tipos de datos estructurados SEQUENCE y SEQUENCE OF, definen tablas y filas (entradas) dentro de dichas tablas. Por convención, los nombres para los objetos tabla terminan con el sufijo *Table*, y los nombres para las filas terminan con el sufijo *Entry*.
Definidos	Los tipos de datos definidos incluyen *NetworkAddress, IpAddress, Counter, Gauge, TimeTicks, y Opaque.*
Etiquetados	Son empleadas generalmente para activar el sistema de recepción para decodificar correctamente los valores de varios tipos de datos, que determina un protocolo que se puede transmitir en cualquier momento dado. La etiqueta no tiene notación de valor propio, su tipo de notación se compone de tres (3) elementos: una etiqueta definida por el usuario, posiblemente seguida por una implícita ó explícita, y por último, seguido por la notación del tipo valor que se ha marcado. Asimismo, existen las clases de etiquetados o etiquetas corresponden a un tipo de valor definido previamente como base para ser utilizado por las etiquetas. ASN.1 define cuatro (4) tipos de etiquetas: • **Universal:** para tipos de datos generales, como "*Boolean", "Integer*" y "Real". • **Aplicación:** definidos para la aplicación específica. • **Especifico al contexto:** definidos para el contexto local en que se usan estos tipos. • **Privado:** definidos por el usuario.

4.3. Reglas de codificación BER

Es uno de los formatos de codificación definidos como parte del estándar ASN.1. Asimismo, son las reglas definidas originalmente en el estándar ASN.1 para codificar información de abstracción en un conjunto de bits único para que pueda ser interpretado en cualquier equipo de igual forma. Las reglas, denominadas sintaxis de transferencia en el contexto de ASN.1, especifican las secuencias de octetos exactas para codificar un elemento de datos dado.

Dichos elementos definidos por esta sintaxis son los que se presentan a continuación.

- Estructura de la longitud de información.
- Representaciones para tipos de datos básicos.
- Medios para definir tipos complejos ó compuestos basados en más tipos primitivos.

4.4. Formato BER

Un formato BER detalla un formato auto-descriptivo y auto-delimitativo para codificar las estructuras de datos ASN.1, donde cada elemento de datos está codificado por un identificador de tipos, una descripción longitud, los elementos de datos actuales, donde sea necesario y un marcador de fin-de-contenido.

Según lo antes expuesto, estos tipos de codificaciones son llamados comúnmente TLV (Tipo-Longitud-Valor). Este formato permite a un equipo receptor decodificar la información ASN.1 desde una corriente incompleta de bits, sin necesitar conocimiento previo del tamaño, contenido, o significado semántico de los datos. Existen tres (3) campos del formato BER, tales como: **campo TYPE, longitud y valor**; los cuales se describen a continuación.

4.5.1. Campo TYPE del formato BER

El campo Tipo contiene una identificación para la estructura codificada, además, codifica la etiqueta de ASN.1 (tanto la clase como el número) para el tipo de dato contenido en el campo Valor. Los posibles valores en bits que puede tener el campo TYPE se muestran a continuación, haciéndose visible los dos (2) primeros bits que indican la clase de datos.

- Universal: 00
- Propio de la aplicación: 01
- Específico del contexto: 10
- Privado: 11

Siguiendo con la idea anterior, un bit indica si el dato es primitivo (0) o construido (1). Los cinco (5) bits restantes indican un número de etiqueta, que identifica al tipo de dato en sí. Si el número de etiqueta vale 31 significa que el campo tipo ocupa más de un byte.

Ejemplo I.13. Campo tipo.

Es cuando el tipo INTEGER es UNIVERSAL, primitivo (simple) y su número de etiqueta es 2, luego se codifica: 00 0 00010.

4.5.2. Campo longitud

Este campo indica cuantos bytes ocupa el valor, si el primer bit vale cero, el campo longitud ocupa un byte. En caso de que el primer bit valga 1, los 7 bits restantes indican la longitud del propio campo longitud.

Ejemplo I.14. Campo longitud.

La longitud 4 se codifica 0 0000100 y una longitud de mil bytes se codifica 10000010 00000011 11101000. Existe un valor especial de longitud (10000000) para representar una longitud indefinida. El campo valor acaba con un byte especial denominado "Fin de contenido" ("End Of Content" o EOC).

4.5.3. Campo valor

En este campo se introduce el valor concreto del objeto al que se refiere el punto anterior. El campo valor puede contener cero o más octetos, los cuales trasportan los valores de los datos.

Ejemplo I.15. Campo valor.

Un número entero o un carácter ASCII.

SINOPSIS

En esta unidad, se abordaron diversos puntos a estudiar, como la gestión de red y los elementos que involucra, con la finalidad de hacer más pertinente este importante bloque dentro de la administración de redes de datos. Asimismo, establece a través de normas de diferentes organismos internacionales tales como la ITU-T, ISO y la IETF/RFC los diferentes niveles de gestión tanto de monitoreo como de control para garantizar elevados niveles de Calidad de Servicio, este último muy en boga debido a la gran proporción de servicios que actualmente pueden viajar por la red empresarial.

Finalmente, se estudia el esquema de codificación ASN.1 que se implementa sobre cualquier plataforma de redes sirviendo como un módulo de abstracción para identificar y monitorear a través de las MIB a cualquier nodo en la red.

REFERENCIA BIBLIOGRAFICA

Barba Martí, A. (1999). "Gestión de Red". Edición UPC.

Stallings, W. (1999) "SNMP, SNMPv2, SNMPv3, and RMON 1 and2". 3ªEdición, AddisonWesley.

Larmouth, J. (1999) "ASN.1 Complete"

VÍNCULOS RECOMENDADOS

http://www.rfc-es.org/ Sobre documentos RFC "Request for commend"

http://www.avellanadigital.com/es/gestion-dominios.php sobre gestión de dominios