UNIVERSIDAD POLITÉCNICA SALESIANA

FACULTAD DE INGENIERÍAS

SEDE QUITO-CAMPUS SUR

CARRERA DE INGENIERÍA ELECTRÓNICA

MENCIÓN (TELECOMUNICACIONES)

“Identificación y levantamiento de las plataformas de gestión y monitoreo para la elaboración de un manual de usuario que será utilizado en la aplicación y ejecución de procesos en la red Backbone IP/MPLS de la Corporación Nacional de Telecomunicaciones”

TESIS PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERO ELECTRÓNICO

AUTORES:

GINA ALEJANDRA OJEDA OJEDA

DIANA ALEXANDRA VALDIVIESO CARRIÓN

DIRECTOR: ING. VERÓNICA SORIA

QUITO, NOVIEMBRE 2011

DECLARACIÓN

Nosotras, Gina Alejandra Ojeda Ojeda y Diana Alexandra Valdivieso Carrión, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normativa institucional vigente.

Gina Alejandra Ojeda	Diana Alexandra Valdivieso

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Gina Alejandra Ojeda Ojeda y Diana Alexandra Valdivieso Carrión, bajo mi dirección.

_____

Verónica Soria

DIRECTORA DE TESIS

AGRADECIMIENTO

Mi más amplio agradecimiento a Dios, por regalarme la vida, para cumplir cada una de mis metas.

Gracias a mis padres por el amor y apoyo brindado a lo largo de mi vida universitaria.

Un agradecimiento especial para la Ingeniera Verónica Soria, directora de esta tesis por su valiosa orientación y colaboración para la conclusión del mismo.

DIANA VALDIVIESO

DEDICATORIA

A mis padres Marcelo y Lucita a quienes amo por el sacrificio y apoyo incondicional durante toda mi vida.

A mi hermana Vanessa que siempre ha visto en mí un ejemplo a seguir.

A mis amigas con las que he compartido muchos momentos de alegría.

DIANA VALDIVIESO

AGRADECIMIENTO

Quiero agradecer de todo corazón a Dios por permitirme cumplir mis metas.

A mis padres por creer en mí y apoyarme en todo momento.

A la Ingeniera Verónica Soria, gracias por todo su apoyo y por colaborar con sus conocimientos para finalizar nuestra tesis con éxito.

Al Ingeniero Germán Arévalo por siempre darnos su apoyo y confiar en nosotras.

GINA OJEDA

DEDICATORIA

A mis padres Georgina y Jaime que han sido incondicionales conmigo, gracias papi y mami por darme una carrera para mi futuro y por brindarme ánimo y fuerza, ustedes son el motor de mi vida y un gran ejemplo de amor y superación.

A mi grande amor, gracias por estar a mi lado apoyándome en todo momento, gracias por todo.

A mi hermana, por compartir muchos momentos a lo largo de mi vida universitaria.

A mi sobrina por llegar a mi vida y darme tanta felicidad.

A mis amigas las quiero y las extrañaré siempre.

GINA OJEDA

CONTENIDO

ÍNDICE DE FIGURAS

CAPITULO 1

CAPITULO 2

CAPITULO 3

CAPITULO 4

CAPITULO 5

ÍNDICE DE TABLAS

CAPITULO 1

CAPITULO 3

CAPITULO 5

ACRÓNIMOS

AAA: Autenticación, Autorización y Administración

ATM: Asynchronous Transfer Mode

BGP: Border Gateway Protocol

CE: Customer Equipment

CMDB: Base de Datos para la Gestión de la Configuración

CMIP: Common Management Information protocol

CR-LDP: Constraint-Based Routing Ldp

CSV: Comma-Separated Values

DSL: Digital Subscriber Line

EAP: Extensible Authentication Protocol

FEC: Forwarding Equivalence Class

FIB: Forwarding Information Base

FR: Frame Relay

FTP: File Transferer Protocol

GPL: General Public License

HTTP: HyperText Transfer Protocol

ICMP: Internet Control Message Protocol

IETF: Internet Engineering Task Force

IP: Internet Protocol

IPX: Internetwork Packet Exchange

IS-IS: Intermediate System to Intermediate System

ISP: Internet Service Provider

ITIL: Information Technology Infraestructure Library

LAN: Local Area Network

LER: Label Edge Router

LFIB: Label Forwarding Information Base

LIB: Label Information Base

LSP: Label Switched Path

LSR: Label Switching Router

MIB: Management Information Base

MPLS: Multi -Protocol Label Switchin

MRTG: Multi Router Traphic Grapher

MySQL: My Structured Query Language

NM: Managed Nodes

NMS: Network Management Station

NOC: Network Operation Center

OSPF: Open Shortest Path First

PDU: Packet Data Unit

PE: Provider Equipment

PING: Packet INternet Groper

POP3: Post Office Protocol 3

RFC: Request For Comments

RRD: Round Robin Database

RSVP: Resource Reservation Protocol

RSVP-TE RSVP: Resource Reservation Protocol Traffic Engineering

SMS: Short Message Service

SNMP: Simple Network Management Protocol

SSH: Secure Shell

SSL: Secure Sockets Layer

TCP: Transmission Control Protocol

VLAN: Virtual Local Area Networks

VPN: Virtual Private Networks

RESUMEN

En el presente trabajo se muestra detalladamente los principales pasos para la correcta administración de las plataformas de gestión y monitoreo utilizados en la Corporación Nacional de Telecomunicaciones.

El manual creado consta con procesos del manejo de las plataformas de gestión y monitoreo como son: ANA, WHAT`S UP, CACTI, NAGIOS, IP SOLUTION CENTER, ACS, cada una de éstas plataformas están mostradas con su respectivo manual de usuario los mismos que serán de gran utilidad para los administradores de red.

La configuración y administración de las Plataformas de Gestión y Monitoreo cumplen un papel muy importante en aquellas organizaciones que poseen una estructura de red bien definida y que comprenden varias sedes de trabajo para la comunicación entre los diferentes usuarios ya que por medio de ésta utilidad el administrador de red podrá tener un control sobre todos los dispositivos y servicios que la integran; estar informado por medio de notificaciones de diversos sucesos o eventos que se ejecuten dentro de la red así como la falla de algún componente de hardware o el estado de los mismos.

La implementación y configuración de un Servicio de Gestión y Monitoreo dentro de una infraestructura de red de una determinada empresa requiere de diversos parámetros y protocolos de servicios que organicen y fomenten el desarrollo y funcionamiento en su totalidad con el fin de emplear de forma rápido y ágil todos los recursos que serán destinados a cada uno de los usuarios que los requieran y sea factible la realización de un inventario general y explícito de los mismos con el fin de tener un control sobre la infraestructura de red en la cual se está trabajando.

CAPÍTULO 1

SITUACIÓN ACTUAL

1.1 ANTECEDENTES [1]

La Corporación Nacional de Telecomunicaciones CNT.S.A nace el 30 de octubre del 2008 debido a la fusión de las extintas Andinatel S.A. y Pacifictel S.A., sin embargo, luego de aproximadamente más de un año, el día 4 de febrero del 2010, la CNT S.A., pasa a ser desde ese momento LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT EP, empresa líder en el mercado de las telecomunicaciones del Ecuador cuyo propósito es promover y fomentar el acceso a las tecnologías de la información y brindar diferentes servicios de telecomunicaciones a la población ecuatoriana.

La Corporación Nacional de Telecomunicaciones desde marzo de 2010 oficialmente se fusionó con la empresa de telefonía móvil ALEGRO, con el fin de fortalecer la cartera de productos enfocando los esfuerzos empresariales en el empaquetamiento de servicios y en convergencia de tecnologías, en beneficio de la comunidad.

Dentro de las áreas de la CNT que se encuentran en continuo mejoramiento se tiene al departamento de Backbone ATM/IP-MPLS cuyas funciones fueron segmentadas en distintas áreas debido a la integración de la telefónica móvil ALEGRO; dichas áreas son INGENIERIA, O&M, GESTIÓN Y NOC.

El área Backbone ha traspasado una serie de funciones a las nuevas áreas creadas para el desarrollo, administración, gestión y monitoreo de la red.

1.2 ESTRUCTURA GENERAL DE LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES

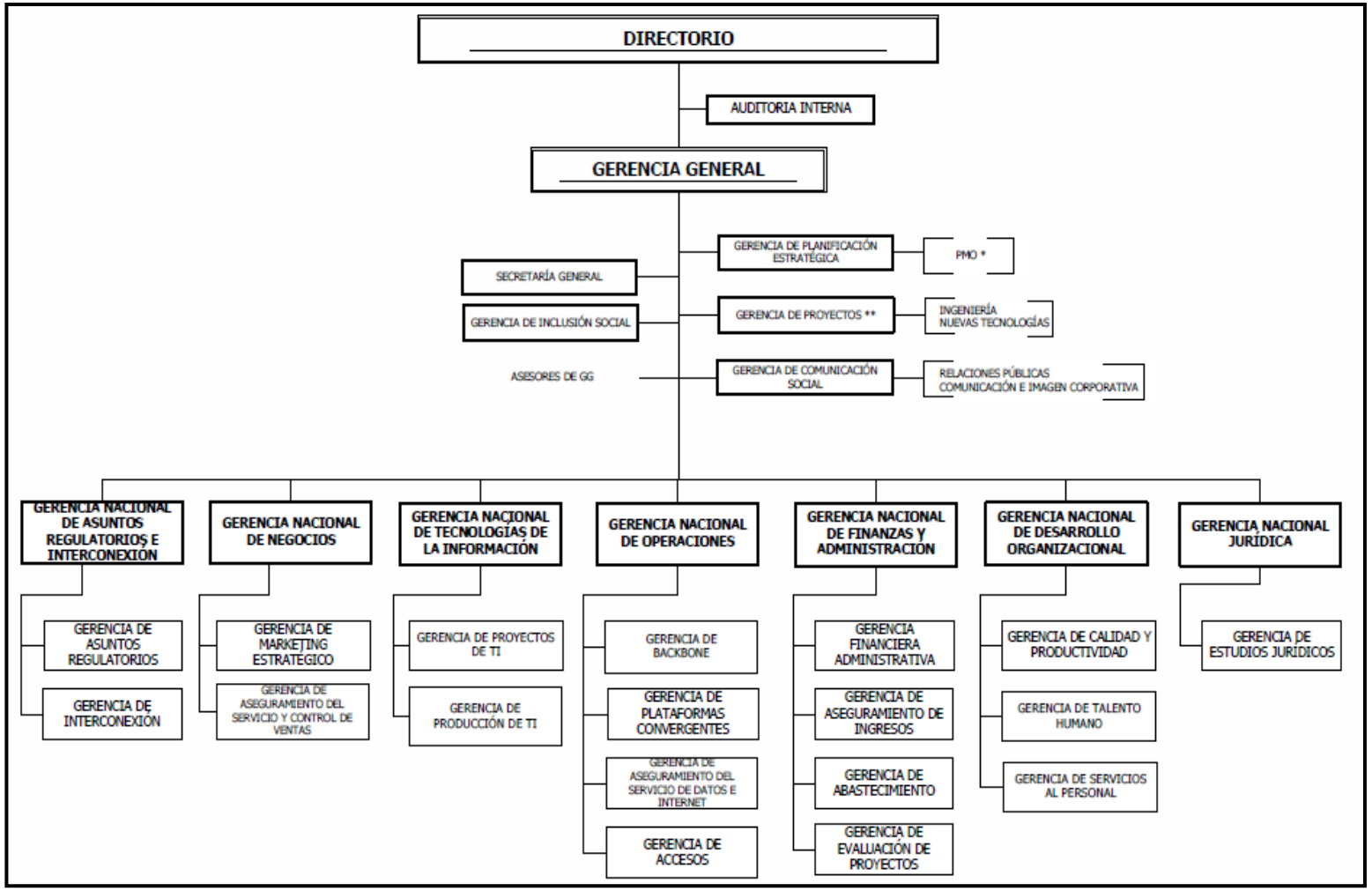


Figura 1.1: Estructura General de CNT [1]

1.3 ESTRUCTURA ANTERIOR DEL ÁREA IP/MPLS

A continuación se muestra en la figura Figura1.2 la estructura anterior del área IP/MPLS de la Corporación Nacional de Telecomunicaciones.

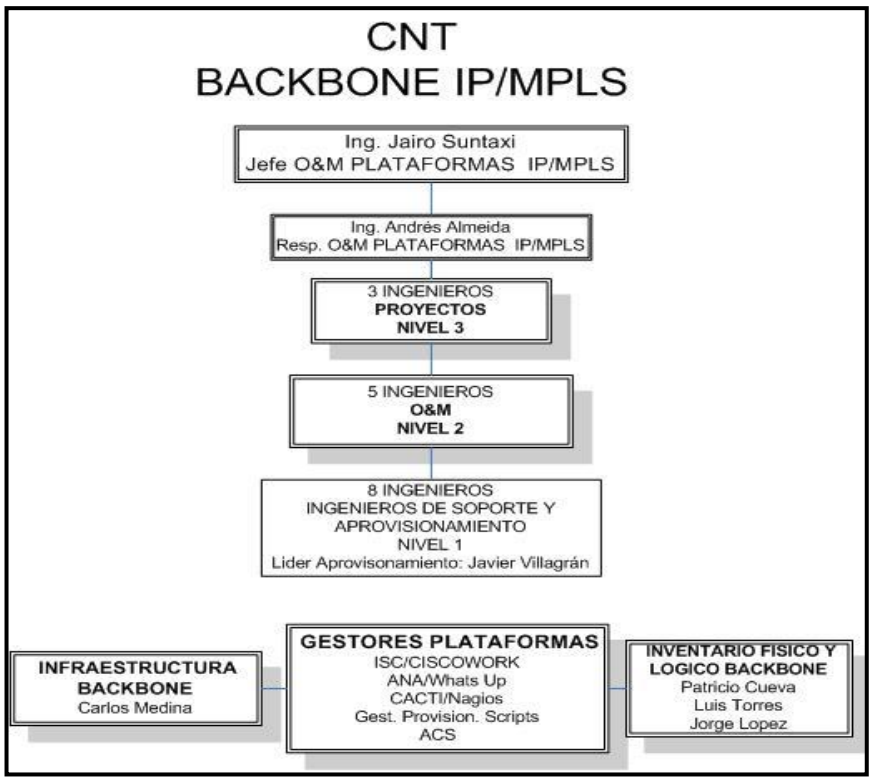


Figura 1.2: Estructura del área IP/MPLS anterior[2]

1.4 NUEVA ESTRUCTURA DEL ÁREA O&M IP/MPLS

A continuación se muestra en la figura Figura1.3 la nueva estructura del área ahora con el nombre de Operación y Mantenimiento de la Corporación Nacional de Telecomunicaciones.

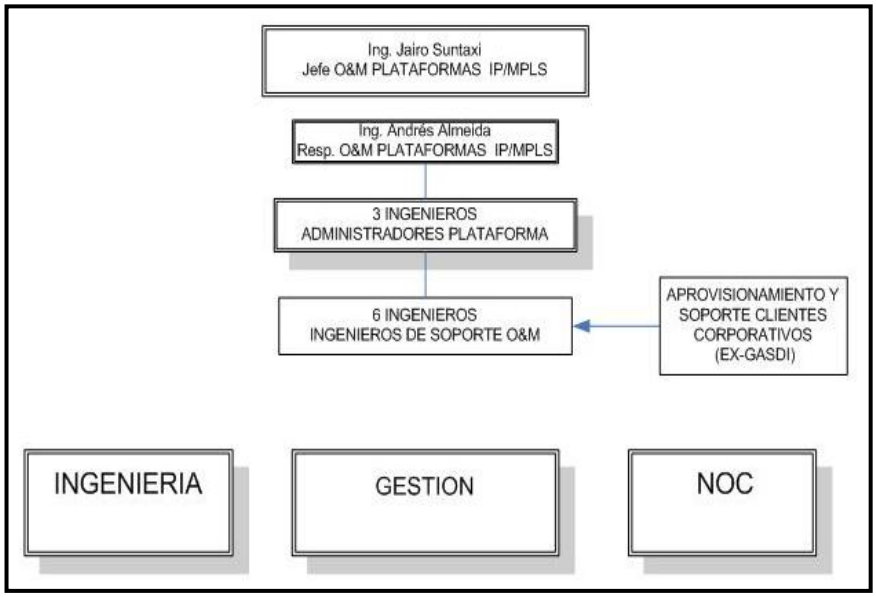


Figura 1.3: Nueva Estructura del área O&M de la CNT[2]

1.5 IDENTIFICACIÓN DE FUNCIONES DE LAS NUEVAS ÁREAS

En las nuevas áreas creadas se asignaron funciones específicas las mismas que se detallan a continuación.

1.5.1 ÁREA DE OPERACIÓN Y MANTENIMIENTO

Las funciones a realizarse en ésta área son las siguientes:

- Aprovisionamiento de clientes corporativos de datos e internet.
- Soporte en problemas de datos e internet clientes corporativos.
  - ✓ Problemas de lentitud en enlaces de internet.
  - ✓ Problemas de navegación, páginas que no se tiene acceso.

- ✓ Problemas de intermitencias en enlaces de internet.
- ✓ Problemas de lentitud en enlaces de datos.
- ✓ Problemas de intermitencias entre la matriz y sucursales de clientes.

- Mantenimientos coordinados con los ingenieros de soporte para clientes corporativos.
  - ✓ Implementación y pruebas de redundancia.
  - ✓ Implementación de sesiones BGP[1].
  - ✓ Cambios de instalaciones de los clientes luego del mantenimiento.
- Instalación de nuevos nodos.
- Verificación de transmisión para ingreso de un nuevo cliente.
- Coordinación con personal de DSLAM[2] para instalación de equipos.
  - ✓ Asignación de puertos.
  - ✓ Pruebas de conectividad.
- Factibilidad de transmisión hacia nodos para instalación de clientes.
  - ✓ Verificación de transmisión disponible para ingreso de un nuevo cliente.
- Procedimiento para el aprovisionamiento de clientes corporativos.
- Documentación con los datos de los equipos que se interconectan con otros proveedores.

1.5.2 ÁREA DE INGENIERÍA

Las funciones a realizarse en ésta área son las siguientes:

- Contacto con proveedores.
- Coordinación con negocios para nuevos servicios.

[1] Véase Acrónimos.
[2] DSLAM (**Digital Subscriber Line Access Multiplexer**): es un multiplexor localizado en la central telefónica que proporciona a los usuarios servicios de banda ancha sobre cable de par trenzado de cobre estos separa la voz y datos de la línea de los abonados.

- Generación de catálogos de servicios.
- Planificación y reuniones de futuros y actuales servicios.
- Entrega formal de nuevos servicios.
- Cambios de sistemas operativos (IOS, PTR, VRP)
- Definición de servicios.
- Guías de ingeniería
- Soporte en trabajos nivel 2.

1.5.3 ÁREA DE GESTIÓN

Las funciones a realizarse en ésta área son las siguientes:

- Actualización de archivos de gestión.
- Procesos de administración de inventario físico de la red.
- Reporte general de incidentes.
- Disponibilidad de las plataformas (Internet, Mpls, L2, BRAS, enlaces internacionales).
- Reportes Suptel, Fiscalía tanto masivos como corporativos.
- Ocupación troncales ATM/IP/MPLS/BRAS
- Estadísticas de servicios configurados en la red por mes y/o servicio.
- Informes de requerimientos de salidas internacional hacia interconexión.
- Informes de eventos operativos hacia negocios.
- Informes fallas de la red.
- **Uso de herramientas de administración para monitoreo del estatus de la red**.[3]

[3] La tesis está enfocada a las áreas de Gestión y Noc que se encargan del manejo de herramientas de monitoreo y gestión de la red como se puede verificar en las letras resaltadas en negrilla en los puntos 1.5.3, 1.5.4.

1.5.4 ÁREA DEL NOC[4]

Las funciones a realizarse en ésta área son las siguientes:

- Identificación de incidentes en la red y aplicación de procedimientos.
- Administración de incidentes utilizando herramientas básicas y documentación de los mismos.
- **Uso de herramientas de administración para monitoreo del estatus de la red.**
- **Interpretación y verificación de alarmas, ocupaciones y determinación de su severidad para inicio de troubleshooting en un primer nivel.**
- **Monitoreo de plataformas operativas mediante herramientas tales como ANA, Whats up, CACTI, Nagios.**
- Atención de llamadas y soporte al call center de clientes corporativos (INGENIERO DE SOPORTE).
- Diagnóstico de primer nivel de falla de clientes corporativos y masivos para correcto direccionamiento hacia áreas de OPERACIÓN Y MANTENIMIENTO(O&M).
- Atención Casos Remedy de call center.
- Soporte nivel uno problemas de intermitencias entre la matriz y sucursales de clientes.
- Corte y reconexiones suspensiones a nivel de clientes corporativos de plataformas datos, internet e tv.
- Generación de tickets de eventos en las salidas de internet con proveedores internacionales.
- Informes de eventos operativos y fallas masivas hacia GESTIÓN.

[4] NOC(Network Operation Center): Es un centro donde se reciben fallas de todas las plataformas de CNT

1.6 POLÍTICAS

1.6.1 ESCALAMIENTO INTERNO BACKBONE

La Corporación Nacional de Telecomunicaciones cuenta con un Centro de Operación de Red con cobertura nacional denominado NOC (Network Operation Center).

En el NOC se reciben los reportes de fallas de las diferentes plataformas de red de CNT. Se verifican los datos del cliente, se obtienen indicaciones de la falla, se realizan pruebas de primer nivel y luego se realiza la verificación de extremo a extremo de la red. El NOC funciona las veinticuatro (24) horas, todos los días de la semana, los trescientos sesenta y cinco (365) días del año.

El NOC es el encargado de asignar el problema al área correspondiente.

Escalamiento al área O&M PLATAFORMA MPLS:

Una vez que el NOC ha realizado todas las verificaciones correspondientes del incidente presentado en la red y haber agotado los recursos para identificar el problema, se procede a completar el formato establecido de check list generado por el área O&M para escalar a dicha área, el mismo que será enviado mediante correo electrónico, para facilitar la solución del inconveniente en el menor tiempo posible.

Para el escalamiento de problemas realizar el siguiente procedimiento:

- Si es un problema de clientes masivos enviar correo a **OPE GESTIÓN ATM**
- Si es un problema de clientes corporativos enviar un correo a **OPE BACKBONE ATM IP**.

En el caso de existir casos de daños masivos, el Ing. Administrador de la Plataforma debe emitir un informe técnico del daño tiene un tiempo estimado de entrega de 24 a

48 horas laborables si se cuenta con toda la información del caso, si se requiere información de otro país o Carrier hay que incluir el tiempo que estos se tomen para responder.

Cuando estos trabajos tomen lugar de manera programada y afecten los servicios del cliente, se debe informar a GESTIÓN DE TRANSMISIÓN la ejecución del mismo con por lo menos catorce (14) días de anticipación.

Se aclara que para hacer uso de un nivel de escalamiento superior, es necesario haber agotado los tiempos expuestos.

1.6.2 TIEMPOS DE RESPUESTA

El tiempo promedio para solucionar una incidencia de la red es de una hora para soporte masivo y 45 minutos para soporte corporativo.

El tiempo máximo es de 10 a 15 minutos para realizar la verificación del checklist, que es un manual de revisiones con sus respectivas redes y escalamientos, al alcance de todos sus colaboradores.

1.7 INDICADORES DE GESTIÓN

Para efectuar los indicadores de gestión se presenta la siguiente tabla con los respetivos tiempos de respuesta de cada uno de los problemas que se presentan en la red de CNT.

PROBLEMA	TIEMPO PARA DAR SOLUCION AL PROBLEMA	INCIDENCIAS TOTALES MES	INCIDENCIAS ATENDIDAS	INCIDENCIAS SOLUCIONADAS	TOLERANCIA
Fallo de equipos de acceso	2 días	10	9	7	10%
Conectividad limitada o nula	30 min	30	30	25	5%
Problemas de configuración en plataformas	30 min	15	14	12	7%
Pérdidas de paquetes por intermitencias del enlace	30 min	40	38	34	12.5%

Tabla 1.1- Incidencias

- **FALLO DE EQUIPOS DE ACCESO**

  - ✓ **INDICADOR DE EFICIENCIA**

Fallos de equipo atendidos/ fallos totales=9/10=0.9

Se atendió el 90% de los fallos, el 10% restante no fue atendido debido a la falta de información para poder dar solución inmediata al problema.

  - ✓ **INDICADOR DE EFICACIA**

Fallos solucionados/ Fallos atendidos=7/9=0.7

Se tiene un 78% de respuesta, el porcentaje restante no puede ser solucionado debido a la falta de conocimiento del manejo de equipos y configuraciones incorrectas en los mismos.

  - ✓ **INDICADOR DE EFECTIVIDAD**

Fallos solucionados / Total de fallos presentados=7/10=0.7

Se tiene un 70% de efectividad el porcentaje restante no obtuvo una respuesta debido a las causas anteriormente mencionadas.

- **CONECTIVIDAD LIMITADA O NULA**

  - ✓ **INDICADOR DE EFICIENCIA**

Fallos de equipo atendidos/ fallos totales=30/30=1

Se atendió el 100% de los fallos presentados.

  - ✓ **INDICADOR DE EFICACIA**

Fallos solucionados/ fallos atendidos=25/30=0.83

Se tiene un 83% de respuesta.

  - ✓ **INDICADOR DE EFECTIVIDAD**

Fallos solucionados / total de fallos presentados=25/30=0.83

Se tiene un 83% de efectividad el porcentaje restante no pudo ser solucionado debido a configuraciones incorrectas en los equipos MPLS.

- **PROBLEMAS DE CONFIGURACIÓN EN PLATAFORMAS**

  - ✓ **INDICADOR DE EFICIENCIA**

Fallos de equipo atendidos/ fallos totales=14/15=0.93

Se atendió el 93% de los fallos.

  - ✓ **INDICADOR DE EFICACIA**

Fallos solucionados/ fallos atendidos=12/14=0.86

Se tiene un 86% de respuesta.

- ✓ **INDICADOR DE EFECTIVIDAD**

Fallos solucionados / total de fallos presentados=12/15=0.8

Se tiene un 80% de efectividad el porcentaje restante no pudo ser solucionado debido a configuraciones incorrectas en los equipos y a problemas de transmisión cuyo proceso debe ser atendido o escalado a otra área.

- ➢ **PÉRDIDAS DE PAQUETES POR INTERMITENCIAS DEL ENLACE**

- ✓ **INDICADOR DE EFICIENCIA**

Fallos de equipo atendidos/ fallos totales=38/40=0.95

Se atendió el 95% de los fallos.

- ✓ **INDICADOR DE EFICACIA**

Fallos solucionados/ fallos atendidos=34/38=0.89

Se tiene un 89% de respuesta.

- ✓ **INDICADOR DE EFECTIVIDAD**

Fallos solucionados / total de fallos presentados=34/40=0.85

Se tiene un 85% efectividad el porcentaje restante no pudo ser solucionado debido a configuraciones incorrectas en los equipos, a problemas de transmisión cuyo proceso debe ser atendido o escalado a otra área y a problemas físicos en los equipos para lo cual los administradores deben movilizarse al equipo correspondiente para verificar conexiones lo cual requiere de un tiempo determinado.

1.7.1 BENEFICIOS DE LOS INDICADORES DE GESTIÓN

La implementación de los indicadores de gestión proporciona los siguientes beneficios:

1.7.1.1 SATISFACCIÓN DEL CLIENTE

La satisfacción del cliente es una prioridad por lo tanto la empresa buscara las estrategias con los indicadores de gestión para que todo el personal logre los resultados deseados.

1.7.1.2 MONITOREO DEL PROCESO

El seguimiento continuo de cada uno de los procesos permitirá el mejoramiento en el manejo de las herramientas básicas para detectar fallas, solucionarlas y encontrar oportunidades para implementar nuevas acciones de perfeccionamiento.

1.7.1.3 GERENCIA DEL CAMBIO

Un sistema de medición permitirá al personal de las distintas áreas conocer sus falencias, sus aportes para solucionar problemas, además de descubrir los resultados que se generan cuando el trabajo se ha realizado correctamente.

1.8 CONOCIMIENTO TÉCNICO DEL PERSONAL

En la actualidad el área de Operación y Mantenimiento de la Corporación Nacional de Telecomunicaciones se encuentra conformado por 14 ingenieros los cuales tienen sus funciones divididas de acuerdo a las necesidades que se presenten para la resolución de incidencias de la red.

De acuerdo a un sondeo realizado al personal del área O&M acerca del manejo y utilización de las plataformas de gestión y monitoreo se obtuvo los siguientes resultados.

PLATAFORMA	PORCENTAJE DE UTILIZACIÓN (%)	DESCRIPCIÓN
CACTI	50	Manejo básico de las herramientas de administración de la plataforma. Desconocimiento de las nuevas aplicaciones de monitoreo.
NAGIOS	45	Configuraciones Básicas de los equipos y envío de alarmas.
IP SOLUTION CENTER	65	No todos los recursos de administración de la plataforma son aprovechados.
WHATSUP UP	30	Usado únicamente para la visualización de la red y alerta de incidencias.
ACS	20	Falta de conocimiento de las herramientas de la plataforma. Escaso manejo de la nueva versión implementada.
ANA	20	Los recursos que presenta esta herramienta no son usados en su totalidad.

Tabla 1.2- Conocimiento Técnico del Personal[2]

Como se muestra en la tabla 1.1 una parte de las causas del insuficiente manejo de las plataformas de gestión y monitoreo dentro del área es por la falta de

conocimiento por ello nació la necesidad de generar un manual de usuario que contenga la información de todos los procesos de administración de estas herramientas con el fin de facilitar su uso, aprovechar todos los recursos posibles y dar solución a problemas existentes en la red.

Cabe mencionar que anteriormente en el área Backbone IP/MPLS se ha realizado el levantamiento de información de ciertos procesos de forma esporádica, según las necesidades que se han presentado durante los dos años desde que el área se conformó. Dichos procesos cubrían necesidades temporales puesto que la información no se encontraba completa y detallada.

El manual de usuario es una solución viable para capacitar al personal de las nuevas áreas creadas que carecen de información acerca de los sistemas de monitoreo de la red.

CAPÍTULO 2

ARQUITECTURA MPLS Y MODELOS DE SISTEMAS DE GESTIÓN

2.1 INTRODUCCIÓN

El crecimiento del internet ha producido la innovación de una serie de tecnologías y sofisticados servicios. MPLS (Multi-Prototocol Label Switching) es una nueva arquitectura de red de reciente aparición que permitirá soportar las futuras aplicaciones multimedia y proporcionan una eficaz alternativa al ATM[5] para multiplexar diversos servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de routers con funciones especializadas en el transporte de paquetes en el núcleo de las redes.

Actualmente existen varios servicios de telecomunicaciones basados en la transmisión sobre fibra óptica tales como DWDM (Dense Wavelength Division Multiplexing) que ofrece capacidad, flexibilidad y optimización del uso del ancho de banda.

La convergencia de voz, datos y video son servicios cuya transmisión garantizan algunos parámetros de calidad de servicio (QoS) como por ejemplo el retardo máximo, y el número de paquetes que puedan ser descartados.

MPLS es un nuevo avance en las tecnologías de enrutamiento y envío en redes IP, que implica una mejor visión al momento de construir y gestionar redes. Presenta un sin número de ventajas son indudables en relación a: Calidad de Servicio (Qos), Ingeniería de Tráfico, Redes Privadas Virtuales (VPNs) sobre una topología inteligente, muy superior en prestaciones a las soluciones tradicionales de túneles y circuitos virtuales, además de soportar múltiples protocolos.

[5] **ATM(Asynchronous Transfer Mode):** Es un modo de transferencia asíncrono para trasmisiones a alta velocidad de voz, video y datos a través de redes públicas o privadas.

2.2 MPLS (MULTIPROTOCOL LABEL SWITCHING) [1], [2]

MPLS es un protocolo de transporte de datos estándar creado por IETF[6] y definido en la RFC[7]. 3031, para soluciones de conmutación multinivel. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

2.2.1 ELEMENTOS DE MPLS [2], [4]

Los elementos de MPLS permiten a la red funcionar más efectivamente que otras tecnologías. Entre los elementos que constituyen una red MPLS es importante mencionar a los LSPs (*Label Switching Path)* que son una ruta de tráfico específico en la red. Una red MPLS está compuesta por dos tipos de routers o nodos: LER (*Label Edge Router*) y LSR (*Label Switching Router*).

2.2.1.1 DOMINIO MPLS

Conjunto de nodos con funcionalidad MPLS y que pertenecen a un mismo dominio de encaminamiento IP. Nodos adyacentes.

2.2.1.2 LER (LABEL EDGE ROUTER)

Los LERs o routers de etiqueta de borde, son nodos situados en la periferia que clasifican el tráfico que ingresa al dominio MPLS, son capaces de conectar un dominio MPLS con nodos externos al dominio; éstos son los responsables de asignar y retirar las etiquetas, a la entrada o salida de la red MPLS. Su conmutación se basa en FECs (*Forwarding Equivalence Classes*).

---

[6] **IETF (Internet Engineering Task Force)**: Tiene como principal función la investigación y desarrollo de nuevas tecnologías, junto con el análisis de nuevas propuestas y la regulación de los estándares, publicados bajo la forma de RFC.

[7] **RFC** (**Request For Comments**): Es en un documento que contiene una propuesta para una nueva tecnología a cerca de su uso, recursos y mejoras.

2.2.1.3 LSR (LABEL SWITCHING ROUTER)

Los LSRs o routers de conmutación de etiquetas, son nodos internos de un dominio MPLS que conmutan los paquetes en función de la etiqueta. Su conmutación es directa.

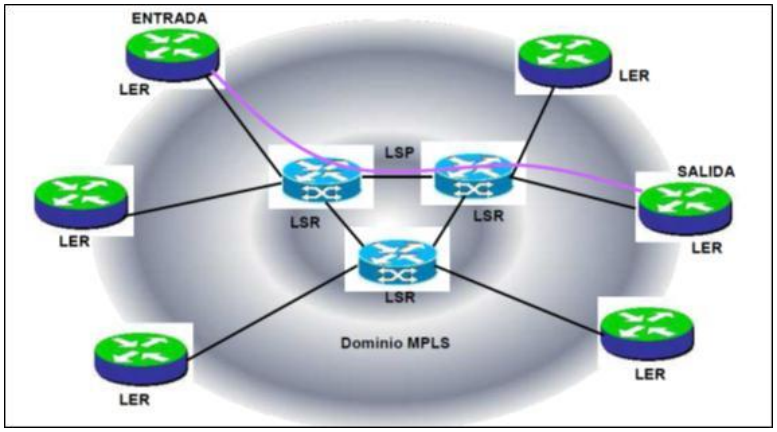


Figura 2.1: Dominio MPLS, LER, LSR [1]

2.2.1.4 FEC (FORWARDING EQUIVALENCE CLASS) [4]

La Clase Equivalente de Envío es el conjunto de paquetes que pueden ser tratados de la misma manera por un router. Una FEC está constituida por todos los paquetes a los que se pueden aplicar una etiqueta específica. La escalabilidad de MPLS está garantizada por los FECs.

Cada FEC tiene un camino específico a través de los LSR de la red, razón por la cual MPLS es orientada a conexión y además contiene una serie de valores que definen los requerimientos de QoS del flujo.

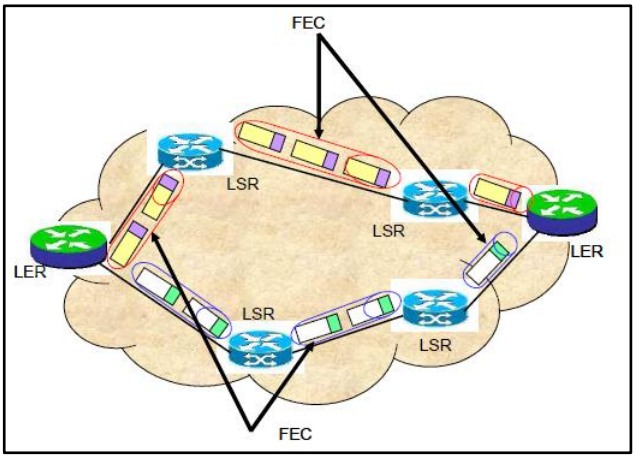


Figura 2.2: FEC [1]

2.2.1.5 LSP (LABEL SWITCHED PATH) [5]

El LSP es la ruta unidireccional construida para concatenar uno o más LSRs dentro de un nivel jerárquico por el que un paquete etiquetado y perteneciente a una determinada clase puede circular.

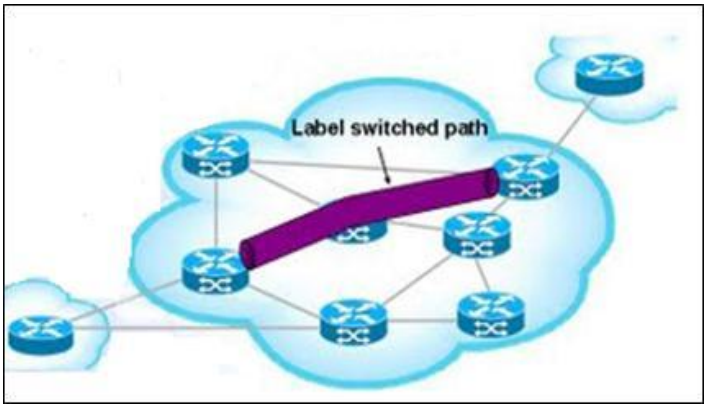


Figura 2.3: LSP [6]

Los LSPs sirven como túneles de transporte a lo largo de la red MPLS; incluyen los parámetros QoS que determinan la cantidad de recurso a reservar al LSP, así como la fila de procesos en cada LSR.

MPLS maneja dos tipos de técnicas de selección de una ruta o LSP dentro de un FEC específico: enrutamiento *hop by hop* y enrutamiento explícito. [2]

2.2.1.5.1 Enrutamiento hop by hop [1]

Este tipo de enrutamiento se caracteriza porque cada uno de los LSR's selecciona de forma independiente el siguiente hop para una FEC determinada.

2.2.1.5.2 Enrutamiento explícito (ER-LSP) [1]

Este tipo de ruteo es definido desde la fuente por el propio operador de la red. Sin embargo, la ruta específica puede ser no óptima, por eso es necesario que a lo largo de la trayectoria, los recursos deban ser reservados para asegurar una calidad de servicio para el tráfico de datos.

Las rutas explicitas se las selecciona por configuración o dinámicamente; para tener un enrutamiento explícito dinámico, el LER debe tener información de la topología de la red y de los requisitos de calidad de servicio en el dominio MPLS con lo cual se mejora la ingeniería de tráfico.

2.3 TUNELIZACIÓN EN MPLS [1], [2], [4]

MPLS crea túneles a través de los routers intermedios para controlar la ruta de un paquete sin especificar los routers intermedios. Un LSP puede ser un túnel, si utiliza una conmutación de etiquetas.

Un túnel LSP se define como LSP <R1, R2,…..Rn>, donde R1 es el punto de trasmisión del túnel, Rn el de recepción. El punto de transmisión ubica un paquete en el túnel y añade una etiqueta para el túnel en la pila, el punto de recepción extrae la etiqueta de la pila.

2.4 ETIQUETA [1], [2]

Una etiqueta es un identificador pequeño de longitud fija, que es usado para identificar un FEC. Las etiquetas sólo tienen significado local en cada interfaz.

Las operaciones que se realizan con una etiqueta son:

Label swap.- Es el cambio del valor de la etiqueta que se realiza en cada nodo.

Label merging.- Es el cambio de varias etiquetas a una única, que identifica al mismo FEC.

2.4.1 Asignación y distribución de etiquetas

Se define los modos de distribución y retención de etiquetas dentro del funcionamiento de MPLS los cuales son: LSR *upstream* (Ru) que es el encaminador que envía los paquetes y LSR (Rd) *downstream* que recibe los paquetes.

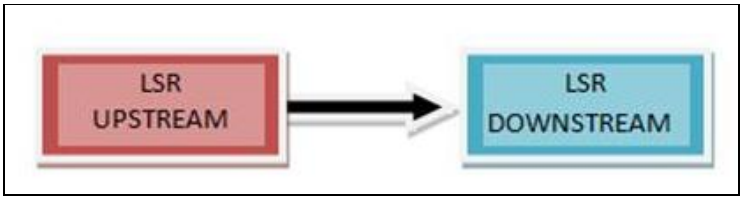


Figura 2.4: Upstream, Downstream

2.4.1.1 Asignación de etiquetas Downstream

La asignación *Downstream*, es local y se usa como etiqueta de entrada, el LSR que es *downstream* crea la asociación entre una etiqueta y un FEC particular.

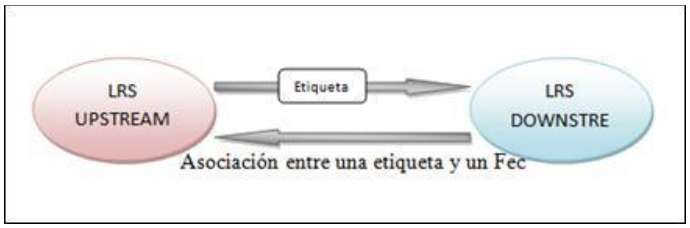


Figura 2.5: Asignación de etiquetas Downstream.

2.4.1.1.1 Downstream on Demand

Permite que un LSR *upstream* haga una petición explícita de una etiqueta para un determinado FEC al LSR *downstream* que es el próximo salto del camino.

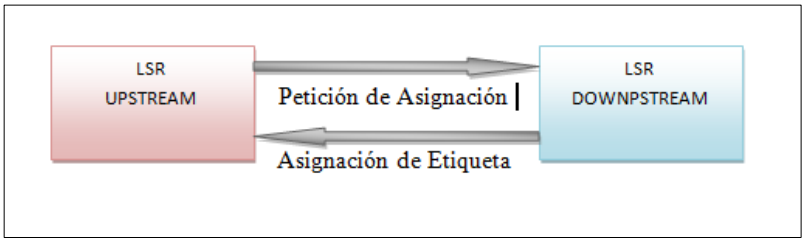


Figura 2.6: Downstream on Demand

2.4.1.1.2 Unsolicited Downstream

Permite que un LSR *downstream* asigne una etiqueta sin que haya recibido una petición explícita.

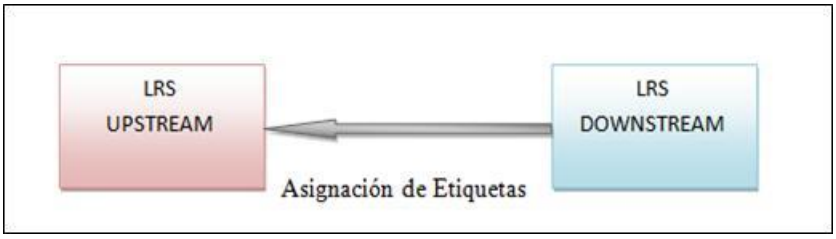


Figura 2.7: Unsolicited Downstream

2.4.1.2 Asignación de etiquetas Upstream

La asignación de etiquetas *Upstream*, se usa como etiquetas de entrada si la asignación es remota; y, se utiliza como etiqueta de salida si la asignación es local.

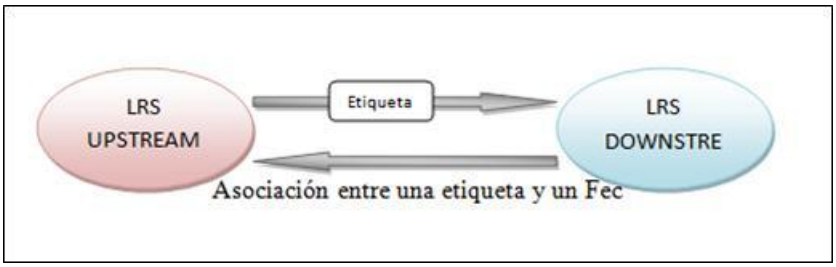


Figura 2.8: Asignación Upstream

2.4.2 FORMATO DE LA CABECERA MPLS [1], [2]

La etiqueta MPLS genérica está conformada por 32 bits, divididos en cuatro campos que son los siguientes:

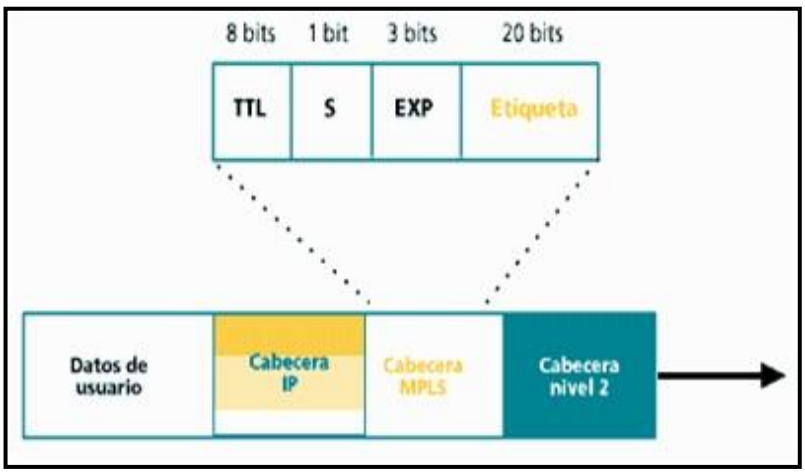


Figura 2.9: Cabecera MPLS [9]

EXP.- Es el campo reservado para uso experimental, indica la clase de servicio (*CoS*), consta de 3 bits; el valor de este campo afecta a los algoritmos de planificación y/o descarte que se aplican al paquete a medida que se transmite a través de la red.

S (*Stack*).- Consta de 1 bit, es el campo de posición de la pila. Si tiene el valor de 1 indica que es la última etiqueta añadida al paquete IP, si es un 0 indica que hay más etiquetas añadidas al paquete.

Etiqueta.- Este campo contiene el valor de la etiqueta y está conformado por 20 bits, proporciona la información sobre el protocolo de nivel de red así como información adicional necesaria para reenviar el paquete.

TTL (*Time To Live*).- Campo de 8 bits, se utilizan para codificar el valor de conteo de saltos (IPv6) o de tiempo de vida (IPv4). Para procesar el paquete TTL se debe considerar:

- ✓ Cuando un paquete IP llega al router de entrada en un dominio MPLS, se añade una etiqueta de entrada a la pila. Cuando el paquete MPLS llega a los LSRs del núcleo de la red el valor TTL es disminuido. El paquete es excluido si llega a cero para evitar lazos o que el paquete permanezca demasiado tiempo en la red debido a un enrutamiento defectuoso. Si el valor es positivo se añade una nueva etiqueta y es reenviado al próximo salto.

- ✓ Cuando un paquete MPLS llega a un LSR de salida, el valor TTL es disminuido para posteriormente quitar la etiqueta de la pila, entonces la pila queda vacía.

2.4.3 Pila de etiquetas (*Label Stack*) [7]

La pila de etiquetas es una característica importante de MPLS. Un paquete puede apilar varias etiquetas según la filosofía LIFO "último en entrar, primero en salir". La cima de la pila aparece al principio del paquete y el fondo aparece después; si la pila de etiquetas de un paquete tiene profundidad m, la etiqueta de nivel 1 es la que está en el fondo y la de la cima se considera de nivel m.

El proceso de etiquetado no sigue un nivel jerárquico aunque MPLS soporta jerarquía. En cualquier LSR se puede realizar dos operaciones en la pila de etiquetas: en la operación *push* la etiqueta puede añadirse a la pila y en la operación *pop* la etiqueta puede quitarse de la pila. El apilamiento de etiquetas permite crear un túnel, es decir agrupar varios LSPs en uno solo.

2.5 DISTRIBUCIÓN DE LA CAPA DE RED EN PLANOS [8]

La arquitectura MPLS está formada por dos planos:

2.5.1 Plano de Control

El componte de control es la que se encarga de crear y mantener la información de etiquetas asignadas entre un grupo de LSR interconectados, por esto cada nodo de MPLS utiliza los protocolos de encaminamiento como lo son: OSPF, IS-IS y BGP-4[8], realizando un intercambio de información con los enrutadores para la construcción y mantenimiento de las tablas de encaminamiento.

2.5.1.1 Tabla de Enrutamiento [1], [2]

Las tablas de enrutamiento se construyen usando los algoritmos implementados en el sistema, ya sean interiores como OSPF, IS-IS y exteriores como los BGP actualización del EGP que intercambiarán información con los enrutadores vecinos que estén conectados a la misma red o por un enlace punto a punto y con los vecinos exteriores que serán los conectados a sistemas independientes diferentes.

En MPLS, la tabla de enrutamiento puede ser:

- LFIB (Label Forwarding Information Base)
- FIB (Forwarding Information Base)

LFIB (*Label Forwarding Information Base*): En donde se almacenan las entradas que el LSR solicita; contiene información de las etiquetas entrantes y salientes, del FEC, de las interfaces y la dirección del siguiente salto. Esta tabla se construye con la información de enrutamiento que provee el plano de control.

[8] Véase Acrónimos

FIB (*Forwarding Information Base*): En donde se almacenan todas las entradas, incluyendo las de la LFIB que los demás LSRs comparten.

LIB (*Label Information Base*): LIB es una tabla que mantiene todas las etiquetas asignadas por un LSR y las asociaciones recibidas de los demás routers, para informar de la asociación entre la etiqueta y el FEC se necesitan protocolos de distribución de etiquetas.

2.5.2 Plano de Datos

Lleva a cabo tareas relacionadas con el forwarding o envío de paquetes. Esos paquetes pueden ser ya sea paquetes IP o paquetes IP etiquetado. La información en el plano de datos, tal como el valor que llevan las etiquetas, se obtienen el plano de control.

Figura 2.10: Planos MPLS [8]

2.6 FUNCIONAMIENTO DE MPLS [1], [2], [7], [8]

Un dominio MPLS está formado por un conjunto de nodos que pueden ser: LERs denominados también routers de acceso y LSRs denominados también routers de tránsito, estos routers son capaces de conmutar y enviar los paquetes en base a la etiqueta añadida a cada paquete.

Las etiquetas determinan un flujo de paquetes entre dos puntos terminales; este flujo se denomina FEC, el mismo que crea un camino particular llamado LSP y contiene los requisitos de calidad de servicio.

A continuación se describe los pasos que sigue el flujo de paquetes MPLS:

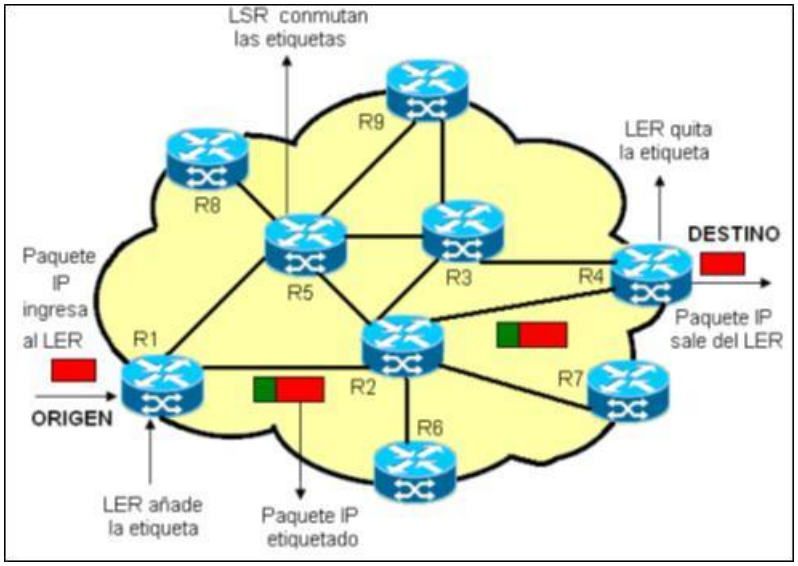


Figura 2.11: Funcionamiento MPLS [2]

1. Antes de enviar la información se debe determinar un LSP y establecer los parámetros de calidad de servicio para dicho camino. Los parámetros de QoS sirven para comprobar:

   - ✓ La cantidad de recursos a reservar al LSP.
   - ✓ Las políticas de descarte de paquetes y prioridades en colas en cada LSR.

Para lograr lo mencionado anteriormente se utilizan dos protocolos para el intercambio de información entre los routers:

- ✓ El protocolo OSPF es utilizado para intercambiar información sobre la topología, y el enrutamiento en sí.
- ✓ Para determinar los LSPs y establecer las etiquetas entre los siguientes LSRs se puede utilizar el protocolo LDP (*Label*

Distribution Protocol) o el protocolo RSVP-TE (*Resource Reservation Protocol Traffic Engineering*), también se lo puede realizar manualmente.

2. Un paquete ingresa al dominio MPLS a través de un router de acceso (LER), este router determina los parámetros de QoS, le asigna un FEC específico al paquete el cual determina un LSP, se etiqueta y se envía el paquete. Si no existe un LSP para este FEC, el LER junto con los otros routers definen un nuevo LSP.

3. El paquete enviado por el LER es recibido por un router de tránsito (LSR), en este momento el paquete se encuentra dentro del dominio MPLS.

El LSR realiza las siguientes funciones:

- ✓ Desecha la etiqueta del paquete entrante y añade una nueva etiqueta al paquete saliente.
- ✓ Envía el paquete al próximo LSR dentro del LSP.

4. El LER de salida desecha la etiqueta, lee la cabecera del paquete IP y envía el paquete a su destino final.

2.7 PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS [1], [2], [8], [7], [4]

Los protocolos de distribución de etiquetas se crean con el propósito de mantener informados a los LSR de las asignaciones de etiquetas a FEC's. Estos protocolos son los responsables de la creación de las tablas de enrutamiento.

Los protocolos de distribución de etiquetas se pueden clasificar de la siguiente manera:

Protocolos de enrutamiento implícitos.- Permiten el establecimiento de LSPs pero no ofrecen características de ingeniería de tráfico. Éstos son:

- ✓ LDP (Label Distribution Protocol)
- ✓ BGP (Border Gateway Protocol)

Protocolos de enrutamiento explícitos.- Son recomendables para ofrecer ingeniería de tráfico y para la creación de túneles. Éstos son:

- ✓ CR-LDP (Constraint Protocol LDP)
- ✓ RSVP-TE (Resource reservation Protocol Traffic Engineering)

2.7.1 PROTOCOLO LDP (LABEL DISTRIBUTION PROTOCOL)

El protocolo LDP, ha sido creado específicamente para la asignación de etiquetas a FEC, dentro de una red MPLS, y asegura la fiabilidad en el envió de mensajes. LDP tiene la función de mapear las FECs a etiquetas, las cuales al ser mapeadas indican la ruta que deben seguir para llegar a su destino final armando así los LSP.

Las sesiones de LDP se establecen entre LSR vecinos en la red MPLS (no necesariamente adyacentes) los cuales intercambian los distintos tipos de mensajes y se realiza mediante el envió de PDU's de LDP.

2.7.2 PROTOCOLO BGP (BORDER GATEWAY PROTOCOL)

BGP es un protocolo vector distancia, que asigna a cada ruta a un valor de prioridad y selecciona la ruta que tenga mayor valor. La forma de configurar y definir la información que contiene e intercambia el protocolo BGP es creando un Sistema

Autónomo2. Cada sistema autónomo (AS)[9] tendrá sesiones internas "iBGP" y además sesiones externas "eBGP".

2.7.3 PROTOCOLO CR-LDP (CONSTRAINT-BASED ROUTING LDP)

El protocolo CR-LDP, es un protocolo de encaminamiento basado en restricciones donde las rutas que siguen los paquetes pueden ser restringidas por ancho de banda, retardo (delay), variación de retardo (jitter), conteo de saltos (hop's), QoS (Calidad de Servicio) entre otras.

CR-LDP es una extensión del protocolo LDP, soporta el encaminamiento basado en restricciones (CR) y se ha creado para tolerar el establecimiento y mantenimiento de LSPs encaminados de forma explícita pero no incluye los algoritmos necesarios para calcular los trayectos según los criterios del operador de la red.

2.7.3.1 CR-LSP

Un CR-LSP se calcula en el LSR origen basado en criterios de calidad de servicio y de información de enrutamiento, es bidireccional entre dos LSRs pero con flujo separado.

Se pueden utilizar los CR-LSPs para:

- ✓ Realizar balance de carga en una red IP, es decir el tráfico se lo distribuye uniformemente en sus enlaces.
- ✓ Crear túneles MPLS.
- ✓ Realizar rutas basadas en calidad de servicio.

[9] AS (Sistema Autónomo): Conjunto de routers con la misma administración y políticas de ruteo.

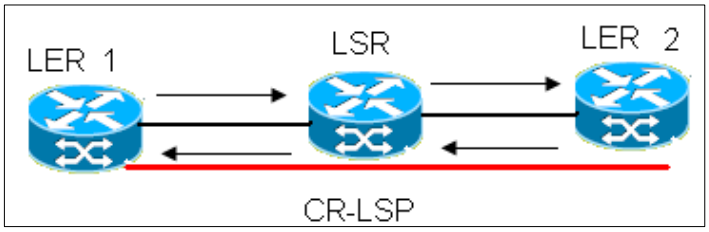


Figura 2.12: CR-LSP [10]

2.7.4 PROTOCOLO RSVP-TE (RSVP - TRAFFIC EXTENSION)

RSVP es un protocolo de señalización para identificar la disponibilidad y reserva de recursos a lo largo de una ruta de un origen a un destino específico. Este protocolo permite crear túneles LSP, para el establecimiento de los túneles LSP el protocolo de señalización utiliza el modelo *downstream* bajo demanda.

Para la asignación de etiquetas en MPLS a este protocolo se aplican nuevos elementos como los son objetos, formatos de paquetes y procedimientos para establecer túneles LSP, los cuales permiten el transporte de flujo de datos por debajo de los procedimientos básicos de enrutamiento IP.

2.7.4.1 RSVP-TE

El protocolo RSVP-TE es una extensión del protocolo RSVP original, el mismo que soporta la creación de rutas explícitas con o sin reserva de recursos. Una de las características adicionales más importantes de este protocolo es que permite el re-enrutamiento de los túneles LSP, con el fin de dar una solución ante caídas de red, congestión y cuellos de botella.

2.8 APLICACIONES DE MPLS [1], [2], [4], [8], [7]

MPLS ofrece las siguientes aplicaciones:

- ✓ Ingeniería de tráfico
- ✓ Calidad de Servicio (QoS)

- ✓ Redes privadas virtuales (VPN)

2.8.1 INGENIERÍA DE TRÁFICO

La ingeniería de tráfico es el proceso de controlar y rutear el flujo de datos a través de la red con el fin de optimizar los recursos disponibles y prestaciones de la red. MPLS facilita la asignación de recursos en las redes para equilibrar la carga dependiendo de las demandas de tráfico de los usuarios.

MPLS emplea la ruta más corta que cumpla con los requisitos del flujo de tráfico, que incluye: ancho de banda, de medios y de prioridades sobre otros flujos. La ingeniería de tráfico MPLS se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costos de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

2.8.2 CALIDAD DE SERVICIO (QoS) [8]

QoS es la habilidad para diferenciar diversas clases de tráfico y asignarles prioridades sobre cada router en la red. El tráfico puede ser clasificado basado en el tipo (voz, aplicaciones, datos, etc.) y sobre las propiedades de los patrones de tráfico.

Una vez realizado este proceso se identifica las operaciones que se van a realizar en dichos routers, además de aplicar las Políticas de Servicio (Service Policy) y finalmente después de que estas son definidas se las aplica sobre la interfaz del dispositivo.

QoS permite a los administradores de redes el uso eficiente de los recursos de sus redes con la ventaja de garantizar que se asignaran más recursos a aplicaciones que así lo necesiten, sin arriesgar el desempeño de las demás aplicaciones. En otras palabras el uso de QoS le da al administrador un mayor control sobre su red, lo que significa menores costos y mayor satisfacción al cliente final.

QoS otorga mayor control a los administradores sobre sus redes, mejora la interacción del usuario con el sistema y reduce costos al asignar recursos con mayor eficiencia (bandwith). Mejora el control sobre la latencia (Latency y Jitter) para asegurar la capacidad de transmisión de voz sin interrupciones y por ultimo disminuye el porcentaje de paquetes desechados por los enrutadores: confiabilidad.

2.8.3 SOPORTE DE REDES VIRTUALES PRIVADAS [7]

MPLS provee un mecanismo eficiente para el manejo de redes privadas virtuales, para que el tráfico atraviese al internet de manera eficaz y de manera transparente para el usuario, protegiendo la información. Las VPNs creadas con tecnología MPLS tienen mayor capacidad de expansión y son más flexibles en cualquier red principalmente en la IP.

Los componentes básicos de una VPN son: Customer Edge Routers, Provider Edge Routers y los Provider Routers.

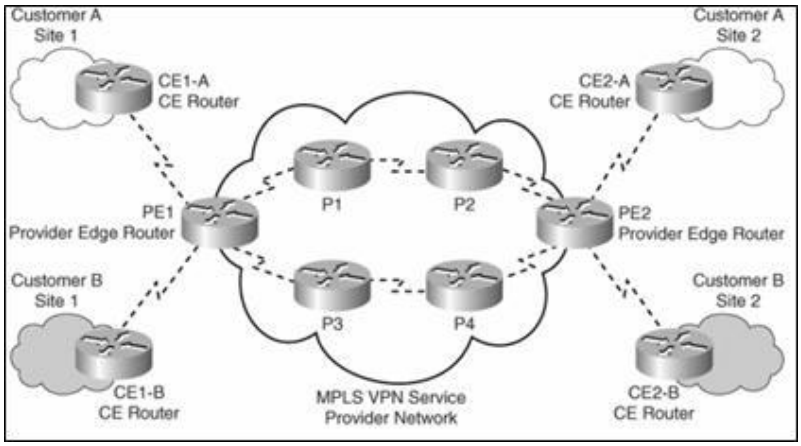


Figura 2.13: Componentes de una VPN [7]

- ✓ **Customer Edge (CE) Routers:** Son los routers localizados en la frontera de la red del cliente que solicita el servicio.

- ✓ **Provider Edge (PE) Routers:** Son los routers localizados en el borde del proveedor, estos routers actúan como los LERs.

- ✓ **Provider (P) Routers:** Son los routers en el *backbone* del proveedor, estos routers conmutan los paquetes MPLS sobre LSPs determinados.

2.8.3.1 Funcionamiento de una VPN [7]

Cada VPN está asociada con una o más instancias de Ruteo/Reenvío Virtual llamadas (*VRF*). Una VRF determina la membrecía que tiene el cliente conectado al router PE de la compañía proveedora del servicio. Cada VRF está compuesta por una tabla de ruteo IP, una tabla de Reenvío Express de Cisco (*CEF*)[10], un grupo de interfaces que utilizan dicha tabla y un conjunto de reglas y parámetros del protocolo de ruteo que controlan la información que se incluye en la tabla de ruteo. Las VRF contienen las rutas disponibles en la VPN que pueden ser accesadas por los sitios de los clientes, cada sitio puede estar suscrito a varias VPN, pero solo a un VRF. Para prevenir que no salga ni entre tráfico fuera de la VPN, cada VRF tiene guardada información de reenvío de paquetes en las tablas IP y CEF.

2.8.3.2 Modelo de enrutamiento VPN en MPLS

Desde la perspectiva de un router cliente CE, los datos son enviados al router PE. Los routers CE no requieren de una configuración específica para ser parte de un dominio VPN MPLS. El único requerimiento de un router cliente CE es un protocolo de enrutamiento que permita el intercambio de información de una ruta con el router PE del proveedor.

En la implementación de MPLS VPN, el router PE lleva a cabo multiples tareas. En primer lugar debe ser capaz de aislar el tráfico de usuario, si más de un cliente está conectado al router PE. Cada cliente por lo tanto tiene asignado una tabla de enrutamiento independiente. El enrutamiento a través de la red del proveedor es llevado a cabo usando un proceso de ruta en la tabla de enrutamiento global. Los routers P, permiten la comnutación de etiquetas entre los routers extremo del

[10] CEF (Cisco Express Forwarding): se utiliza principalmente para aumentar la conmutación de paquetes de velocidad mediante la reducción de retardos introducidos por las técnicas de enrutamiento.

proveedor. Los routers en la red del cliente no están concientes acerca del router P y por lo tanto la topología de red del proveedor es transparente al cliente.

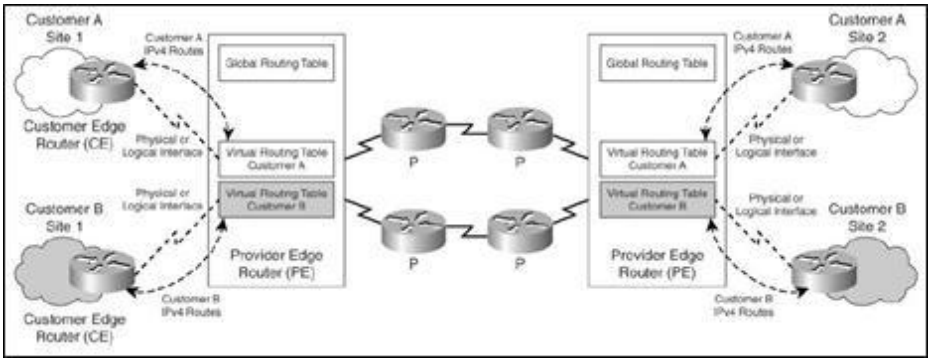


Figura 2.14: Arquitectura MPLS VPN [7]

2.8.3.3 Redes privadas virtuales MPLS

Las VPNs con MPLS solo se aplican al *backbone* del proveedor garantizando escalabilidad y seguridad. En VPN / MPLS los clientes pueden crear libremente sus propias tablas de direcciones.

Existen dos tipos de Redes Privadas Virtuales que pueden ser soportadas por MPLS: VPNs MPLS de Capa 3 y VPNs MPLS de Capa 2.

2.8.3.3.1 VPNs MPLS de Capa 3 (VPNs BGP / MPLS)

La implementación de las VPNs BGP / MPLS se usa para distribuir la información de enrutamiento de la VPN a través del *backbone* del proveedor y MPLS para enviar el tráfico de un lugar a otro de la VPN. Se pueden proveer diferentes servicios a determinados usuarios dentro de la red. Las VPNs BGP / MPLS son IP / VPNs basadas en dispositivos *Provider Edge*, para intercambiar información utiliza el modelo *Peer to Peer*[11] y realizan el enrutamiento VPN mediante el protocolo BGP.

[11]**Modelo Peer to Peer:** El proveedor de servicio y el cliente intercambian información de enrutamiento de capa 3, es utilizado para implantar VPNs / MPLS.

2.8.3.3.2 VPNs MPLS de Capa 2

Las VPNs MPLS proveen independencia de la capa 3 ya que el proveedor de servicios genera conectividad de capa 2, pero el cliente puede utilizar cualquier protocolo de capa 3. Las VPNs MPLS de capa 2 no están estandarizadas, pero existen 2 *drafts* [12]y son: Martini y Kompella.

Martini L2 VPN.- Los *drafts* de Martini establecen la creación de túneles punto a punto sobre una red MPLS. Para establecer los túneles LSPs se debe utilizar el protocolo LDP, las VPNs utilizan el modelo *overlay*[13]

Existen dos *drafts* de Martini: El primero de ellos especifica cómo debe realizarse la encapsulación sobre circuitos virtuales para tecnologías como ATM, Ethernet, HDLC y PPP. El segundo borrador de Martini define los procedimientos para la distribución de etiquetas, lo que permite el transporte de PDUs a través de una red MPLS.

Kompella L2 VPN.- Los *drafts* de Kompella especifican el uso del protocolo BGP para la distribución de etiquetas. Se permite circuitos punto a punto y punto a multipunto, las VPNs utilizan el modelo *overlay*.

2.9 VENTAJAS MPLS [1], [11]

- Mejora desempeño de re-envío de paquetes en la red.
- Soporta QoS y CoS (clases de servicio) para diferencias servicios.
- Soporta escalabilidad de la red es decir permite expandir la red para incrementar el número de abonados.
- Integra IP, ATM Frame, Relay y Ethernet en la red.
- Construye redes inter-operables.

[12] **Drafts:** Son los proyectos en estudio, no estandarizados por la IETF.
[13]**Modelo Overlay:** El proveedor de servicio y el cliente no intercambian información de enrutamiento de capa 3, puede implementarse con varias arquitecturas como: X.25, Frame Relay, ATM, etc.

- Soporta cualquier tipo de tráfico en una red IP sin depender de los protocolos de enrutamiento, de la capa transporte y de los esquemas de direccionamiento.
- Permite realizar "*tunneling*" de manera más eficiente que IP.
- Soporta eficientemente la creación de VPNs.

2.10 MODELOS DE SISTEMAS DE GESTIÓN

2.10.1 GESTIÓN DE REDES

"La gestión de redes incluye el despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable"[14]

2.10.2 ELEMENTOS DE GESTIÓN DE REDES [12]

A continuación se describen los elementos de gestión de redes:

- **GESTORES:** Estaciones Gestoras (NMS, Network Management Station), nodo en el que se ejecuta la aplicación gestora. Es la parte de la aplicación que emite las directivas de operaciones de gestión y recibe notificaciones y respuestas.

- **AGENTES:** Nodos gestionados (NM, Managed Nodes), elementos de red como host, router, gateway, etc. En estos reside el agente gestor encargado de llevar a cabo las funciones de gestión requerida por la "Estación Gestora", actúan como servidores suministrando información al gestor.

[14] T.Saydam and T. Magedanz, "From Networks and Network Management into Service and Service Management", *Journal of Networks and Systems Management*, Vol 4, No. 4 (Dic 1996).

- **MIB:** es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos (información sobre variables/valores que se pueden adoptar), con identificadores exclusivos para cada objeto.

- **Protocolo de Gestión de Red:** Define la comunicación entre los nodos gestionados y las estaciones gestoras. El protocolo depende del modelo de gestión usado.

  En la actualidad SNMP (Simple Network Management Protocol), forma parte del modelo de gestión de internet, y CMIP (Common Management Information protocol), es parte del modelo de gestión OSI son los protocolos predominantes.

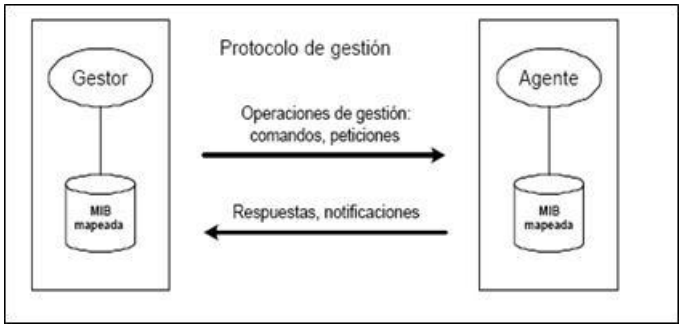


Figura 2.15: Elementos de Gestión de red [12]

2.10.3 MODELO DE GESTIÓN OSI [13], [14], [15]

Arquitectura definida por ISO, utiliza CMIS/CMIP (Common Management Information Services Element/Common Management Information Protocol). Constituye un estándar concebido para operar sobre protocolos OSI. Puede operar a nivel de aplicación sobre otros protocolos sea el caso de TCP/IP, para cuyo caso se denomina CMOT (Common Management Over TCP/IP).

ISO generó un modelo para administración de red el cual se divide en cuatro partes:

- **ORGANIZACIÓN:** Describe los componentes de la administración de red (administrador, agente, etc.) y sus relaciones.

- **INFORMACIÓN:** Se encarga de la estructura y el almacenamiento de la información de administración de los objetos de la red. Esta información se guarda en una base de datos llamada MIB (Base de Información de Administración, Management Information Base). El estándar de la industria se centra en la SMI (Estructura de la información de administración, Structure of Management Information) para definir las sintaxis y semánticas de la información de administración que se almacena en la MIB.

- **COMUNICACIÓN:** Indica la forma en que se comunica los datos de administración entre el agente y el proceso administrador. Tiene en cuenta los protocolos de transporte y aplicación y los comandos y respuestas entre iguales.

- **FUNCIONALIDAD:** Direcciona las aplicaciones de administración de red que residen en el NMS (Sistema de administración de la red, Network Management System).

ISO ha definido cinco áreas funcionales dentro de la gestión de red cada una con sus normas específicas.

- **GESTIÓN DE FALLO:** Comprende las tareas de detección, diagnóstico, asilamiento, reparación e información de las averías en los recursos y fallos de servicios de la red.

- **GESTIÓN DE CONFIGURACIÓN:** Facilita la optimización en el uso de los recursos manteniendo un inventario de los mismos (hardware y software), y estableciendo los cambios necesarios en los mismos para adaptarlos a las necesidades de los servicios.

- **GESTIÓN DE CONTABILIDAD:** Permite distribuir el coste de los recursos entre los usuarios y facilita información a los mismos sobre las tarifas aplicadas.

- **GESTIÓN DE RENDIMIENTO:** Efectúa la evaluación del comportamiento y eficacia de los recursos en relación con la prestación de los servicios a los usuarios, mediante el registro y análisis de los datos correspondientes a los parámetros de la red (demanda de tráfico, número de usuarios, rutas utilizadas, etc.).

- **GESTIÓN DE SEGURIDAD:** Se refiere a la protección contra el acceso no autorizado o accidental a las funciones de control de la red, a la red misma y a la información que circula por ella.

2.10.4 MODELO DE GESTIÓN INTERNET [15]

Este modelo utiliza SNMP (Simple Network Management Protocol), estándar del facto que opera sobre el protocolo TCP/IP. SNMP es un protocolo de aplicación que fue diseñado para facilitar el intercambio de información entre los dispositivos de una red.

El modelo de administración de las redes basadas en SNMP está compuesto por las ya mencionadas NMS que incluye una colección de software, llamado aplicación de administración de red, que incorpora una GUI para permitir a los administradores autorizados controlar la red.

Las MIB que contienen formato SMI (Structrure of Management Information) que permite definir entradas en las MIB. SMI presenta una estructura en forma de árbol global para la información de administración, convenciones, sintaxis y las reglas para la construcción de MIBs.

Los Agentes son plataformas equipados con SNMP para que puedan ser administrados y responden a peticiones de información y demanda acciones desde el NMS. Un agente puede controlar lo siguiente:

- ✓ Número y estado de sus circuitos virtuales
- ✓ Número de ciertos tipos de mensajes de error recibidos
- ✓ Número de bytes y paquetes entrantes y salientes del dispositivo
- ✓ Longitud máxima de cola de salida (para routers y otros dispositivos de red)
- ✓ Mensaje de difusión enviados y recibidos
- ✓ Interfaces de red que han caído y los que se ha activado

El NMS lleva a cabo la monitorización recuperando los valores desde la MIB y puede hacer que se lleve a cabo una acción en un agente o cambiar la configuración de otro. Un protocolo de administración de la capa de red es el encargado de efectuar la comunicación entre el administrado y el agente.

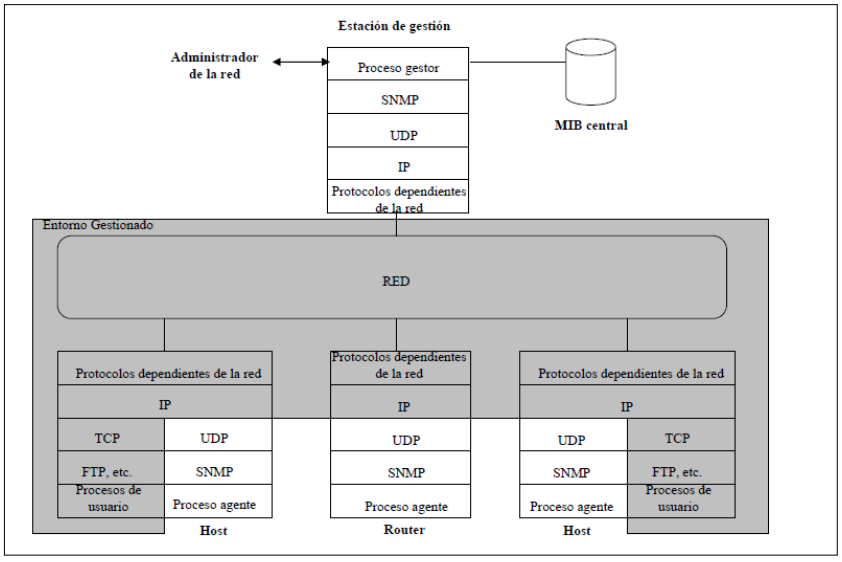


Figura 2.16: Entorno de Gestión [15]

El protocolo SNMP opera sobre el UDP usando los puertos 151/152 y está basado en un intercambio de tres tipos de mensajes.

- ✓ **Get:** Habilita a la estación de administración a recuperar el valor de los objetos MIB desde el agente.
- ✓ **Set:** Habilita a la estación de administración a establecer el valor de los objetos MIB en el agente.
- ✓ **Trap:** Habilita el agente a notificar los eventos significativos a la estación de administración.

Proceso de envío de un mensaje SNMP:

TRANSMISIÓN

- ✓ Se construye PDU
- ✓ Se invoca al servicio de autenticación, con la dirección de transporte y el community
- ✓ Se construye el mensaje SNMP
- ✓ Se codifica

RECEPCIÓN

- ✓ Comprobación sintáctica (eventual descarte)
- ✓ Verificación de la versión utilizada
- ✓ Autenticación: Si falla, trap de autenticación

Todos los objetos administrados en el entorno SNMP están ordenados en una estructura jerárquica o en árbol. Los objetos hoja del árbol son los objetos administrados, cada uno de los cuales representa el mismo recurso, actividad o información relacionada.

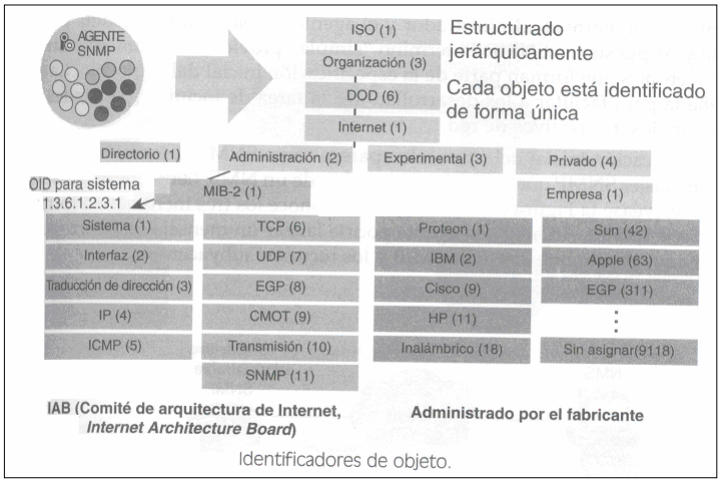


Figura 2.17: Estructura jerárquica de los objetos administrados por SNMP [12]

2.10.4.1 VERSIONES SNMP

A continuación se describen las diferentes versiones de SNMP:

Versión 1:

SNMPv1, maneja tres tipos de mensajes SNMP que se envían en nombre de un NMS: GetRequest, GetNextRequest y SetRequest. El agente reconoce los tres mensajes en forma de otro mensaje GetResponse. Además, un agente podría lanzar un mensaje de interrupción como respuesta a un evento que afecte a las MIB y los recursos subyacentes.

Versión 2:

El avance más importante de SNMPv1, fue la introducción del tipo de mensaje GetBulkRequest y la incorporación de los contadores de 64 bits para reducir la carga de tráfico adicional para la monitorización y solucionar los problemas de monitorización remota o distribuida (con las RMON), ha dado paso a una nueva versión v2. Las versiones de SNMP son compatibles, en el sentido que SNMPv2 puede leer SNMPv1.

Versión 3:

Gracias al desarrollo de SNMP v3, las funciones de administración del modelo de gestión de internet se ha extendido de tal modo que se ha agregado la funcionalidad de seguridad de red.

2.10.5 MODELO DE GESTIÓN INTERNET TMN [14], [16]

Este modelo fue definido por la ITU-T, se basa en los modelos anteriores e incluye el acceso a los recursos de telecomunicaciones, se refiere a la utilidad para los grandes operadores de telecomunicaciones.

En este modelo se definen los objetos que serán gestionados en cada nivel, es decir, las funcionalidades que caracterizan a cada tecnología.

2.10.5.1 MODELO DE CAPAS TMN

El modelo de capas presenta la siguiente estructura:

- Elementos de red
- Gestión de elementos de red
- Gestión de red
- Gestión de servicios
- Gestión empresarial (negocio, comercio)

2.10.5.1.1 ELEMENTOS DE RED

En el nivel Elemento de Red se sitúa todo el equipamiento que forma parte de la red: conmutadores, routers, multiplexores, infraestructura SDH, etc.

2.10.5.1.2 GESTIÓN DE ELEMENTOS DE RED

El nivel de gestión de elementos tiene como responsabilidad.

- Control y Coordinación de un subconjunto de elementos de red.
- Mantenimiento de datos estadísticos, registros y otros datos acerca de un conjunto de elementos de red.
- Tareas de configuración, gestión de alarmas, registros de actividad, para ello, empleará el protocolo de gestión CMIP del ISO. Por otra parte, ha de ser capaz de comunicar con el nivel superior mediante el empleo de un interfaz estandarizado, siendo este Q3.

2.10.5.1.3 GESTIÓN DE RED

Desde este nivel se tiene una visión de parte de la red que comparte la misma tecnología. En este nivel, además de las habituales tareas de mantenimiento, se desarrollan los servicios que serán ofrecidos a la capa superior. Comunica con los niveles superior e inferior mediante Q3.

2.10.5.1.4 GESTIÓN DE SERVICIOS

Es responsabilidad de este nivel:

- La prestación de servicios a clientes, es por ello necesario tener una visión global de los recursos disponibles en la red.
- Interacción con proveedores de servicio
- Mantenimiento de datos estadísticos (ejemplo: QoS)
- Interacción entre servicios
- Desarrolla la contratación, facturación, informes de calidad de servicio y todas aquellas tareas orientadas al cliente.

2.10.5.1.5 GESTIÓN EMPRESARIAL

Es responsabilidad de este nivel:

- Soporte para proceso de toma de decisiones de inversión y utilización óptima.
- Soporte de gestión de presupuesto de telecomunicaciones.
- Soporte de suministro y demanda de mano de obra.

2.10.5.2 CONJUNTOS DE FUNCIONES DE GESTIÓN TMN

- Tareas necesarias para proporcionar un servicio de gestión
- Servicio de monitorización de prestaciones
  - ✓ Establecimiento de objetivo de prestaciones de QoS
  - ✓ Comprobación de prestaciones de QoS
  - ✓ Establecimiento de objetivos de prestaciones de red
  - ✓ Comprobación de prestaciones de red
  - ✓ Criterios de calidad de servicio del cliente
  - ✓ Comprobación de prestaciones de Elementos de Red
  - ✓ Comprobación de Integridad de Datos

2.10.5.3 INTERFAZ Q3

- Garantiza la interoperabilidad entre los sistemas de operación y los elementos de red.
- Está compuesto por:
  - ✓ Protocolo de comunicaciones : CMIP
  - ✓ Conocimiento de Gestión Compartida (SMK) entre los extremos del interfaz: MIBs GDMO.

CAPITULO 3

PLATAFORMAS DE GESTIÓN Y MONITOREO DE UN BACKBONE: ANA, WHAT`S UP, CACTI, NAGIOS, IP SOLUTION CENTER, ACS.

3.1 INTRODUCCIÓN [1]

La configuración y administración de las Plataformas de Gestión y Monitoreo cumplen un papel muy importante en aquellas organizaciones que poseen una estructura de red bien definida y que comprenden varias sedes de trabajo para la comunicación entre los diferentes usuarios ya que por medio de ésta utilidad el administrador de red podrá tener un control sobre todos los dispositivos y servicios que la integran; estar informado por medio de notificaciones de diversos sucesos o eventos que se ejecuten dentro de la red así como la falla de algún componente de hardware o el estado de los mismos.

La implementación y configuración de un Servicio de Gestión y Monitoreo dentro de una infraestructura de red de una determinada empresa requiere de diversos parámetros y protocolos de servicios que organicen y fomenten el desarrollo y funcionamiento en su totalidad con el fin de emplear de forma rápido y ágil todos los recursos que serán destinados a cada uno de los usuarios que los requieran y sea factible la realización de un inventario general y explícito de los mismos con el fin de tener un control sobre la infraestructura de red en la cual se está trabajando.

3.2 ANA (ACTIVE NETWORK ABSTRACTION) [9], [10], [11]

Cisco es propietario de la plataforma ANA, dicha herramienta es un proveedor flexible y un eficaz sistema de administración de dispositivos que sirve como una plataforma que permite a la red usar diversas aplicaciones para la gestión de servicios en múltiples tecnologías y un ambiente de red multiservicio.

Ana es un modelo inteligente de información en tiempo real que posee conocimiento de los dispositivos y los servicios de red.

3.2.1 COMPATIBILIDAD QUE PRESENTA ANA

ANA es compatible con todas las implementaciones IP-NGN[15], particularmente con lo siguiente:

- ✓ IP / MPLS [16]y redes básicas de servicios de borde.
- ✓ Transporte Móvil por paquetes

ANA es una herramienta de gestión que se encuentra entre los elementos de red y las aplicaciones de software libre de gestión.

3.2.2 CARACTERÍSTICAS DE ANA

ANA posee las siguientes características:

- ✓ Información completa, consistente y extensible sobre los inventarios de elementos de red física y lógica.
- ✓ Multi-tecnología de cobertura (IP, ATM, FR, MPLS, VPN, Spanning Tree, VLAN, y más).[17]
- ✓ Posee elementos básicos y personalizables de gestión, incluyendo el descubrimiento de fallas y aislamiento de los mismos mediante el análisis de la causa.
- ✓ Conjunto de aplicaciones y herramientas que ofrecen una interfaz sencilla e intuitiva para visualizar la red, servicios de red, inventario de elementos de red y estado de fallos.

[15] NGN (Next Generation Network): Redes de nueva generación o redes de siguiente generación.
[16] Véase Acrónimos
[17] Véase Acrónimos

3.2.3 NIVELES FUNCIONALES DE ANA

ANA construye y mantiene diariamente un modelo virtual de la red con conocimiento de los servicios de extremo a extremo a través de varias tecnologías, lo cual permite tener una correcta gestión de red y de servicios

ANA mantiene las siguientes funcionalidades:

- ✓ Gestión de elementos.
- ✓ Red y monitorización de servicios
- ✓ Servicio de activación

3.2.3.1 GESTIÓN DE ELEMENTOS

ANA proporciona soporte de gestión a más de 50 familias de elementos en la red de Cisco. Presenta las siguientes características:

- **INVENTARIO Y GESTIÓN DE TOPOLOGÍA**
  - ✓ El descubrimiento de la red, el modelado físico y lógico del dispositivo y la representación física de la topología.
  - ✓ Los datos obtenidos pueden incluir alarmas de aviso cuando se produzca fallos en el servicio.
- **GESTIÓN DE FALLOS**
  - ✓ Detección de fallas
  - ✓ Análisis de la causa principal de la falla
  - ✓ Servicio de notificación de eventos a través de SNMP Trap[18]

[18] **SNMP Trap** (Simple Network Management Protocol Trap): Son notificaciones o mensajes enviados por un dispositivo de red a un sistema de gestión o monitorización.

- **ADMINISTRACIÓN DE CONFIGURACIÓN**
  - ✓ Ejecución de comandos, con acceso completo al modelo de información
  - ✓ Auditoría de todas las acciones de aprovisionamiento.

- **SEGURIDAD**
  - ✓ Gestión de usuarios nuevos
  - ✓ Ámbitos y roles
  - ✓ Autenticaciones locales y externas (LDAP[19])

- **PERSONALIZACIÓN**
  - ✓ Propiedades para extender el modelo de información.
  - ✓ Comando *Builder* para crear y ejecutar secuencias de comandos.
  - ✓ Editor de flujo de trabajo para organizar una serie de secuencias de comandos.
  - ✓ ANA Configuration se puede configurar para personalizar un comportamiento específico.

[19] **LDAP** (Lightweight Directory Access Protocol): Hace referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

3.2.3.2 RED Y MONITORIZACIÓN DE SERVICIOS

Presenta las siguientes características:

- **SERVICIOS Y TECNOLOGÍAS**
  - ✓ Descubrimiento y puntos de vista topológicos de los enlaces.
  - ✓ Análisis del nivel de fallas de la red y análisis de causa principal de dicha falla.

- **SERVICIO DE MAPAS**
  - ✓ Topología estructurada y mapas de servicios para una mejor configuración de dispositivos.

- **TRAYECTORIA**
  - ✓ Seguimiento del servicio o la red de conectividad entre dos puntos cualesquiera de la red.
  - ✓ Todos los caminos posibles descubiertos.
  - ✓ Información asociada para cada tramo de la ruta.

3.2.3.3 SERVICIO DE ACTIVACIÓN

- **ACTIVACIÓN**
  - ✓ Incorpora la comprobación de errores semánticos y sintácticos y su restauración
  - ✓ Marco extensible para la definición de los tipos de nuevos servicios y atributos

3.2.4 BENEFICIOS DE ANA

Ana presenta los siguientes beneficios:

- ✓ Aplicación de gestión para una red convergente
- ✓ Reducción de los gastos de funcionamiento de las incidencias
- ✓ Flexible y de fácil adaptación en distintos escenarios de implementación

3.3 WHATS UP [9]

3.3.1 WHATS UP

WhatsUp es una aplicación de red que muestra notificaciones del estado de los dispositivos, esto ayuda a mantener a la red en funcionamiento.

Con Whats Up se puede crear rápidamente un mapa de una red, iniciar el monitoreo y obtener retroalimentación sobre el desempeño de la red.

3.3.2 FUNCIONALIDADES DE WHATS UP

Se tiene las siguientes funcionalidades

Mapa de la red: Proceder a seleccionar varios comandos según se requiera para crear un mapa de los dispositivos (por ejemplo: routers, switches, servidores, estaciones de trabajo) en la red.

Monitoreo de dispositivos y servicios: El uso de protocolos estándar (TCP / IP, SNMP, NetBIOS[20] e IPX) [21]para localizar y controlar la red.

[20] **NetBIOS** (Network Basic Input/Output System): Es una especificación de interfaz para acceso a servicios de red.
[21] Véase Acrónimos

WhatsUp sondea continuamente los dispositivos asignados (y servicios en los dispositivos).

Existe una alarma visible y audible que se activa cuando los dispositivos de control y los servicios del sistema tienen problemas o están en un estado down.

Escuchar los eventos: Whats Up puede informar cuando se producen acontecimientos específicos. Por ejemplo, cuando se recibe una captura de SNMP[22].

Los eventos pueden ocurrir en cualquier momento, se puede ser notificado tan pronto como el evento (s) se produce, independientemente del ciclo de sondeo del mapa.

Recibe notificación de problemas: Cuando Whats Up detecta un problema, se puede recibir una notificación instantánea por beeper, e-mail, mensaje de voz, entre otros. Genera informes para ayudarle al administrador a analizar el funcionamiento de la red y los dispositivos.

Permite visualizar los mapas creados desde un navegador en un equipo remoto. Además, es fácil de configurado y administrar.

3.3.3 DESCRIPCIÓN DE LAS FUNCIONES BÁSICAS

WhatsUp presenta diversas funciones básicas entre las principales se mencionan las siguientes:

- ✓ Crear mapas
- ✓ Monitoreo conjunto y opciones de notificación
- ✓ Generación de informes

[22] Véase Acrónimos

3.4 CACTI [6],[7],[8]

3.4.1 CACTI

Es una completa herramienta de graficado en red, diseñada para aprovechar el poder de almacenamiento y la funcionalidad de graficar que poseen las RRDtool. Esta herramienta, desarrollada en PHP, provee un pooler ágil, plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios. Tiene una interfaz de usuario fácil de usar.

3.4.2 RRDTOOL

Es el acrónimo de Round Robin Database tool, o sea que se trata de una herramienta que trabaja con una BD (Base de datos) que maneja Planificación Round-Robin. Esta técnica trabaja con una cantidad fija de datos y un puntero al elemento actual. El modo en que trabaja una base de datos utilizando Round Robin es el siguiente; se trata la BD como si fuera un círculo, sobrescribiendo los datos almacenados, una vez alcanzada la capacidad de la BD. La capacidad de la BD depende de la cantidad de información como historial que se quiera conservar.

3.4.3 PHP

PHP Hypertext Pre-processor, diseñado originalmente para la creación de páginas web dinámicas.

3.4.4 BASE DE DATOS

Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

3.4.5 VENTAJAS

- **Gráficos**
  - ✓ Permite utilizar todas las funciones de *rrgraph* para definir los gráficos y automatiza algunas de ellas.
  - ✓ Permite organizar la información en árboles jerárquicos.

- **Fuentes de datos**
  - ✓ Permite utilizar todas las funciones de *rrcreate* y *rrdupdate*, incluyendo la definición de varias fuentes de datos por archivo RRD[23].

- **Colección de datos**
  - ✓ Las fuentes datos pueden ser actualizadas vía SNMP o mediante la definición de scripts.
  - ✓ Soporte SNMP incluido utilizando *php-snmp* o *net-snmp.*
  - ✓ Un componente opcional, *cactid*, implementa las rutinas SNMP en lenguaje C con multithreading[24].
  - ✓ Muy importante para grandes números de dispositivos.

- **Plantillas**
  - ✓ Permite crear plantillas para reutilizar las definiciones de gráficos, fuentes de datos y dispositivos.

[23] Véase Acrónimos
[24] **Multithreading:** Es la tarea de crear un nuevo hilo de ejecución dentro de un proceso existente en lugar de comenzar un nuevo proceso para comenzar una función.

- **Gestión de usuarios**
  - ✓ Permite definir autenticación (local o LDAP) y distintos niveles de autorización para usuarios.

3.4.6 MONITOREO DE UN EQUIPO CON CACTI [6], [7], [8]

Debido a que CACTI es un desarrollo libre (GPL[25]), requiere de un trabajo dedicado para lograr una buena gráfica de monitoreo. Para esto, es necesario, crear plantillas de Gráficas, plantillas de Equipos y plantillas de Datos, las cuales son en formato XML[26].

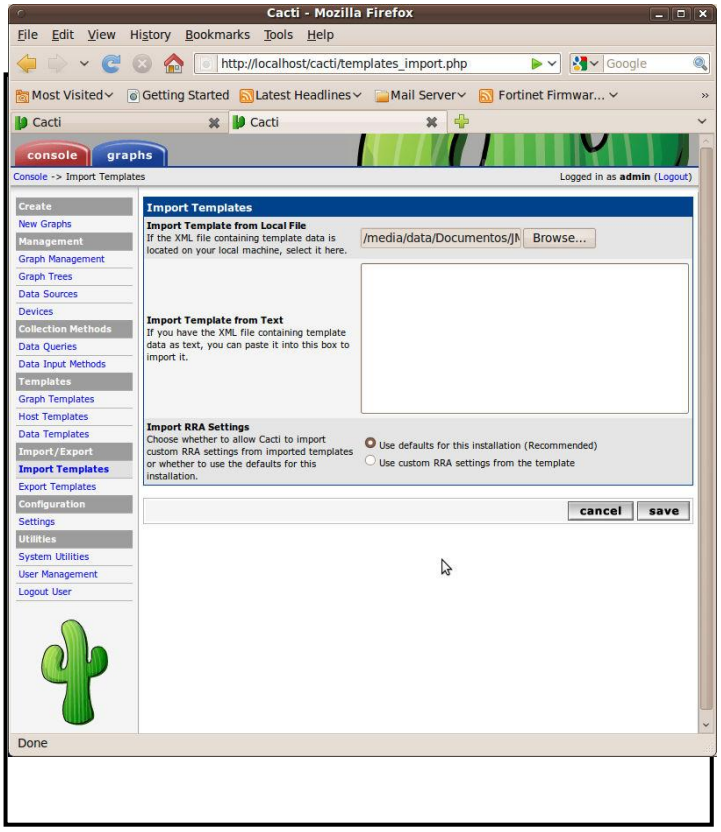


Figura 3.1: Monitoreo de un equipo

[25] Véase Acrónimos
[26] Véase Acrónimos

3.5 NAGIOS [2], [3]

Nagios es un sistema de monitorización de equipos y servicios de red, basada en software libre ampliamente utilizado que ayuda a los administradores a tener siempre el control de qué está pasando en la red y conocer los problemas que ocurren en la infraestructura que administran antes de que los usuarios de la misma los perciban, vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Nagios es fácil de usar posee gran versatilidad y es potente, debido a esto es muy modular y capaz de adaptarse a cualquier escenario.

Es un sistema completo en cuanto a sus características se refiere, además hace uso en algunos casos de diversos sistemas como por ejemplo sistemas gestores de bases de datos, servidores web, etcétera. Es relativamente complejo de instalar y configurar.

3.5.1 CARACTERÍSTICAS PRINCIPALES [2], [3], [4]

Entre sus características principales figuran la monitorización de servicios de red mediante protocolos como: (SMTP, POP3, HTTP, PING, Syslog[27] y Agentes Externos).[28]

- ✓ La monitorización de los recursos de sistemas hardware.
- ✓ Independencia de sistemas operativos.
- ✓ Posibilidad de monitorización remota mediante túneles SSL[29] cifrados o SSH[30].
- ✓ Posibilidad de programar plugins específicos para nuevos sistemas.

[27] **Syslog:** Es un estándar para el envío de mensajes de registro en una red informática IP.
[28] Véase Acrónimos
[29] Véase Acrónimos
[30] Véase Acrónimos

- ✓ Posibilidad de monitorear servidores Windows y Linux mediante agentes externos y las cargas de performance de los servidores con el protocolo SNMP.
- ✓ Nagios permite monitorear cualquier objeto que este en contacto con la red como por ejemplo servidores, teléfonos IP, Switch, Router, Computadoras e impresoras.

Nagios se basa en una interfaz web donde se muestra información de los equipos que están siendo monitoreados además se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante correo electrónico, mensajes SMS[31] y sonidos.

Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix.

Nagios está licenciado bajo la GNU General Public License Version 2 publicada por la Free Software Fundation.

3.5.2 DESCRIPCIÓN DEL SERVIDOR NAGIOS

- ✓ Monitorización de servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP)[32].
- ✓ Monitorización de los recursos de equipos hardware en varios sistemas operativos.
- ✓ Monitorización remota, a través de túneles SSL cifrados o SSH.
- ✓ Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades.

[31] Véase Acrónimos
[32] Véase Acrónimos

- ✓ Chequeo de servicios paralizados.
- ✓ Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- ✓ Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos.
- ✓ Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.
- ✓ Rotación automática del archivo de registro.
- ✓ Soporte para implementar hosts de monitores redundantes.
- ✓ Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros.

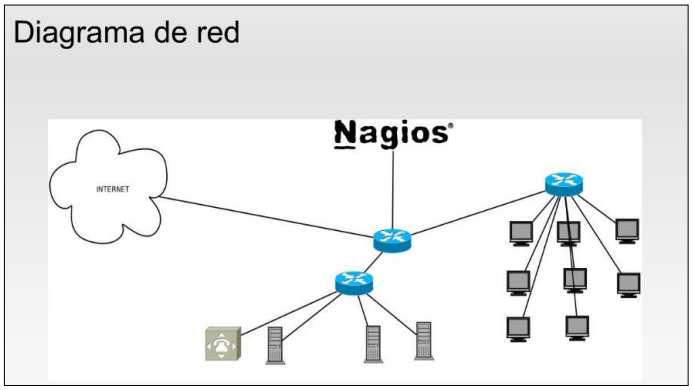


Figura 3.2: Diagrama de red Nagios [2]

3.6 IP SOLUTION CENTER [12]

IP Solution Center (ISC) es una familia de aplicaciones inteligentes de gestión de red que ayudan a reducir la administración general y los costos de gestión, proporcionando una rápida gestión de recursos y planificación.

Cisco IP Solution Center también ayuda a reducir los costos operacionales, proporcionando flujo de trabajo automatizado basado en la solución de problemas y capacidades de diagnóstico para redes VPN MPLS. Las aplicaciones pueden funcionar como aplicaciones independientes o como un conjunto, las funciones incluyen el aprovisionamiento y el diagnóstico automático de MPLS VPN, ATM, Frame Relay y Ethernet sobre MPLS VPN, ATM y Frame Relay[33].

3.6.1 APLICACIONES

Cisco IP Solution Center presenta aplicaciones de gestión de red las mismas que se muestran a continuación:

- ✓ MPLS VPN de gestión
- ✓ Diagnóstico MPLS VPN de Nivel 2
- ✓ Gestión de VPN,
- ✓ Gestión de Ingeniería de Tráfico.
- ✓ Estas aplicaciones pueden funcionar por sí solos o en conjunto como una suite.

[33] Frame Relay: Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o *frame* para datos, perfecto para la transmisión de grandes cantidades de datos.

- **IP SOLUTION CENTER - MPLS VPN DE GESTIÓN**

Presenta las siguientes funcionalidades:

- ✓ IP Solution Center MPLS VPN de gestión ayuda a las empresas y proveedores de servicios a asegurar la exactitud de la implementación de servicios a través del servicio de auditorías de configuración y funcional.
- ✓ El uso de perfiles de servicio predefinido, permitiendo la activación de servicio rápido y fiable.

- **CISCO IP SOLUTION CENTER- MPLS VPN DE DIAGNÓSTICO**

- ✓ Es un sistema automatizado, es un flujo de trabajo basado en productos de gestión de red que soluciona problemas y diagnósticos de MPLS VPNs.

- **CISCO IP SOLUTION CENTER DE GESTIÓN CAPA 2 VPN**

- ✓ IP Solution Center de gestión capa 2 VPN proporciona a las empresas y prestadores de servicios de aprovisionamiento de VPNs de Capa 2 y Metro Ethernet a través de la automatización de estas funciones, protege la inversión en el software Cisco IOS y actualizaciones de tarjeta de línea en la red, y ayuda a asegurar la exactitud de implantación de servicios a través de la configuración del servicio y las auditorías funcionales para Metro Ethernet VPN y cualquier medio de transporte sobre MPLS VPN.

- **IP SOLUTION CENTER DE GESTIÓN- INGENIERÍA DE TRÁFICO**

  - ✓ El Cisco IP Solution Center de ingeniería de tráfico simplifica la visualización, la configuración y gestión de túneles MPLS Ingeniería de Tráfico en la red. Se integra la configuración de Cisco cuenta con ingeniería de tráfico MPLS en una única herramienta de gestión.

3.6.2 CARACTERÍSTICAS Y VENTAJAS

IP Solution Center proporciona las características necesarias para la activación y la seguridad de capa 3 y VPNs de Capa 2, cualquier medio de transporte sobre MPLS y los servicios Metro Ethernet.

La Tabla 1 proporciona detalles sobre las características que presenta IP Solution Center.

Característica	Descripción	Beneficio
Seguimiento de los recursos de capa 3 y capa 2	Administra los recursos, tales como Border Gateway Protocol (BGP) sistema autónomo(AS), regiones, clientes, sitios de clientes, dominios de acceso, los dominios de los proveedores de servicios administrativos, VRF's, direcciones IP, VLAN ID, ID pseudowire[34] y circuitos virtuales.	La automatización de la gestión de recursos reduce el costo de las tareas y ayuda a asegurar la exactitud.

[34] **Pseudowire:** Es un servicio punto a punto de nivel 2 en el que se emula un "hilo" en un túnel.

Perfiles de aprovisionamiento	Permite a los operadores de servicios definir las capas 3 y 2 VPN de aprovisionamiento en los parámetros de una política de servicio, carga la configuración de elementos de red para calcular el cambio en la configuración necesaria para la activación del servicio con éxito.	Al subir la configuración antes de aplicarla, IPS ayuda a asegurar que la configuración de activación del servicio se aplica con éxito y rapidez y no chocará con la configuración existente.
Reconocimiento de la configuración del servicio incorrecto	Proporciona aprovisionamiento de servicios con el fin de determinar si la capa 3 y VPNs de Capa 2 están activos y funcionales.	Reduce el tiempo necesario para solucionar interrupciones en la red debido a la configuración incorrecta de servicios.

Tabla 3.1- Características y beneficios de Cisco IP Solution Center

3.7 ACS (ACCESS CONTROL SERVER) [13]

Cisco Secure Access Control Server (ACS) es una política de acceso a la plataforma de control que le ayude a cumplir con los crecientes requisitos regulatorios y corporativos. ACS mediante la integración con otros sistemas de control de acceso ayuda a mejorar la productividad y contener los costos. Es compatible con múltiples escenarios simultáneamente, incluyendo:

Administración de dispositivos: Autentica los administradores, autoriza a los comandos, y proporciona una pista de auditoría

Acceso remoto: Funciona con VPN y otros dispositivos de acceso remoto de la red para hacer cumplir las políticas de acceso

Conexión inalámbrica: Autentica y autoriza a los usuarios inalámbricos y los host y hace cumplir las políticas específicas inalámbricas.

Control de admisión de red: Se comunica con los servidores de auditoría para cumplir las políticas de control de admisión

Cisco Secure ACS permite gestionar de forma centralizada el acceso a recursos de red para una creciente variedad de tipos de acceso, dispositivos y grupos de usuarios.

3.7.1 CARACTERÍSTICAS

ACS presenta las siguientes características:

- ✓ Soporte para una amplia gama de protocolos, incluyendo protocolo de autenticación extensible (EAP) [35]y los protocolos no-EAP, proporciona la flexibilidad para satisfacer todas sus necesidades de autenticación.
- ✓ Se integra con los productos de Cisco para el control de acceso a los dispositivos de administración y permite un control centralizado y la auditoría de los actos administrativos

3.7.2 FUNCIONALIDAD DE ACS

ACS es altamente escalable y de alto rendimiento para el control de acceso que funciona como un servidor RADIUS[36] o TACACS[37] y los controles de autenticación, autorización y contabilidad (AAA[38]) de los usuarios que acceden a los recursos corporativos a través de una red.

---

[35] Véase Acrónimos

[36]**RADIUS (**Remote Authentication Dial-In User **S**erver): Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red.

[37] **TACACS** (Terminal Access Controller Access Control System): Es un protocolo de autenticación remota que se usa para gestionar el acceso.

[38] Véase Acrónimos

Cisco Secure ACS le permite controlar el acceso del usuario a la red, autorizar los diferentes tipos de servicios de red para los usuarios o grupos de usuarios, y llevar un registro de todas las acciones de la red del usuario.

Cisco Secure ACS apoya el control de acceso y la contabilidad de los servidores de acceso telefónico, cable y soluciones de banda ancha DSL[39], firewalls, VPNs, Voz sobre IP (VoIP), el almacenamiento y conmutación LAN[40] y WLAN[41].

3.7.3 ¿POR QUÉ ES NECESARIO USAR ACS?

Los cambios dinámicos de la red y el aumento de las amenazas de seguridad han creado nuevas demandas en la gestión de control de acceso. ACS amplía la seguridad de acceso mediante la combinación de autenticación de acceso, usuario y administrador, y el control de la política de una solución de identidad de red centralizada. Esto permite una mayor flexibilidad y movilidad, una mayor seguridad, y las ganancias de la productividad del usuario.

3.7.4 NUEVAS CARACTERÍSTICAS

Añade las siguientes características:

- ✓ Las restricciones administrativas sobre la configuración del registro
- ✓ Administrador forzado es decir cambio de contraseña al iniciar sesión
- ✓ Administrador de la directiva de contraseñas
- ✓ Administrador de autenticación a través de una base de datos externa
- ✓ Historial de contraseñas para los administradores

[39] Véase Acrónimos
[40] Véase Acrónimos
[41] Véase Acrónimos

CAPÍTULO 4

ITIL FOUNDATION (INFORMATION TECHNOLOGY INFRAESTRUCTURE LIBRARY

4.1 INTRODUCCIÓN [3]

El uso de los Sistemas de Información (SI) y las Tecnologías de Información (TI), han logrado excelentes mejoras ya que proveen de procesos operativos, proporcionan una completa información para la toma de decisiones y lograr ventajas competitivas.

Las Tecnologías de la Información han sido consideradas como la unificación y convergencia de la computación, las telecomunicaciones, y la técnica del procesamiento de datos, en donde sus principales componentes son: la información, el equipamiento, el factor humano, la infraestructura, el software y los mecanismos de intercambio de información, los elementos de política y regulaciones, además de los recursos financieros.

Estas áreas consideradas de soporte de negocio han descuidado el uso de criterios para medir la rentabilidad, eficacia y calidad de servicios a toda la organización. ITIL se basa en la calidad de servicios y en el desarrollo eficaz y eficiente de todos los procesos que cubren las actividades más importantes tanto del Sistema de Información como el de Tecnologías de Información.

4.2 DESCRIPCIÓN [3]

ITIL, Information Technology Infraestructure Library es un conjunto de documentos donde se describen los procesos requeridos para la gestión efectiva de los Servicios de Tecnologías de Información dentro de una organización. Son un conjunto de mejores prácticas y estándares en procesos para hacer más eficiente el diseño y administración de infraestructuras de datos, garantizando así los niveles de servicio establecidos entre la organización y sus clientes.

Esta metodología está especialmente desarrollada para reducir los costos de provisión y soporte de los servicios IT, al mismo tiempo de garantizar los requerimientos de la información en cuanto a seguridad, mantienen e incrementan sus niveles de fiabilidad, consistencia y calidad.

4.3 OBJETIVOS DE ITIL [3]

- Diseminar las mejores prácticas en la gestión de servicios de Tecnologías de Información de forma sistemática basada en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos.

- Replanteamiento del área tecnológica y la definición de los elementos y procesos críticos dentro de la empresa.

- Los procesos de Administración de Servicios deben ser usados por las personas y herramientas efectivas y económicas para el desarrollo de la alta calidad y la innovación de los servicios de TI alineados con los procesos de negocio.

4.4 ÁREAS ADMINISTRADAS POR ITIL [3]

A continuación en la figura 4.1 se presenta las áreas a las cuales ITIL ofrece procesos de administración TI:

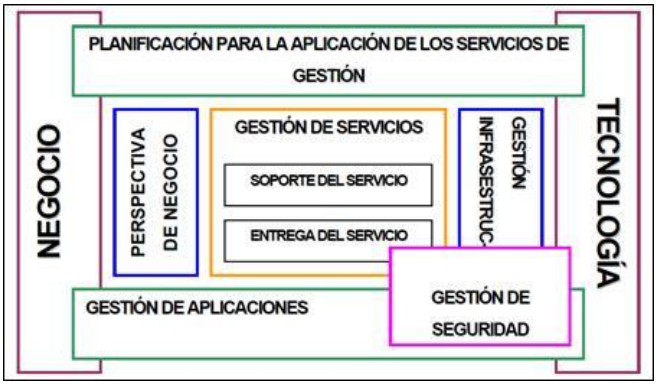


Figura 4.1: Áreas administradas por ITIL [3]

Planificación para la Aplicación de los Servicios de Gestión: Plantea una guía para establecer una metodología de administración orientada a servicios.

Perspectiva de Negocio: Cubre el rango de elementos concernientes al entendimiento y mejora en la provisión de servicios de TI como una parte Integral de los requerimientos generales del negocio.

Gestión de Infraestructuras: Cubre los aspectos relacionados con la administración de los elementos de la Infraestructura.

Servicios de Soporte: Se orienta en asegurar que el usuario tenga acceso a los servicios apropiados para soportar las funciones de negocio.

Provisión de Servicios: Se orienta a detectar el Servicio que la Organización requiere del proveedor de TI a fin de brindar el apoyo adecuado a los clientes del negocio.

Gestión de Aplicaciones: Se encarga del control y manejo de las aplicaciones operativas y en fase de desarrollo.

Gestión de Seguridad: Cubre los aspectos relacionados con la administración del aseguramiento lógico de la información.

4.5 ESTRUCTURA ITIL [1], [2], [3]

La Infraestructura de las Tecnologías de Información (ITIL) es un conjunto de librerías desarrolladas por el ministerio de Comercio del Reino Unido (OCG) en el cual describen cómo los procesos, que han sido identificados, pueden ser optimizados y cómo la coordinación entre ellos puede ser mejorada, además de detallar las mejores prácticas en la Gestión de Servicios de TI.

Estas librerías presentan un marco común para todas las actividades del departamento interno de TI, estas actividades se dividen en procesos, cada uno de

estos cubre una o más tareas tales como el desarrollo del servicio, la administración de infraestructura, provisión y soporte de servicio.

Los libros centrales del ITIL se han agrupado en dos, que se dividen en diez procesos cubriendo las áreas de Servicio de Soporte y Provisión de Servicios.

SOPORTE DE SERVICIOS

- Gestión de incidentes (incident management)
- Gestión de problemas (problem management)
- Gestión del cambio (change management)
- Gestión de la configuración (configuration management)
- Gestión de versiones (version management)

PROVISIÓN DE SERVICIOS

- Gestión del nivel de servicio (service level management)
- Gestión financiera (financial management)
- Gestión de la capacidad (capacity management)
- Gestión de la disponibilidad (availability management)
- Gestión de la continuidad (continuity management)
- Gestión de la seguridad (security management)

4.6 GESTIÓN DE SERVICIO [3]

Gestión de Servicio trata de la entrega y apoyo en TI para cumplir los objetivos de negocios de la organización. Basándose en la implementación de procesos con la orientación de ITIL que proporciona un conjunto completo, consistente y coherente de prácticas óptimas para los procesos, promocionando un enfoque de calidad para alcanzar efectividad y eficacia en el uso de los sistemas.

4.7 SOPORTE DE SERVICIOS [1], [3], [4], [5]

El soporte al servicio se preocupa de todos los aspectos que garanticen la continuidad, disponibilidad y calidad del servicio prestado al usuario. En la figura 4.2 se muestra un resumen de los principales aspectos de la metodología del soporte al servicio según los estándares ITIL:

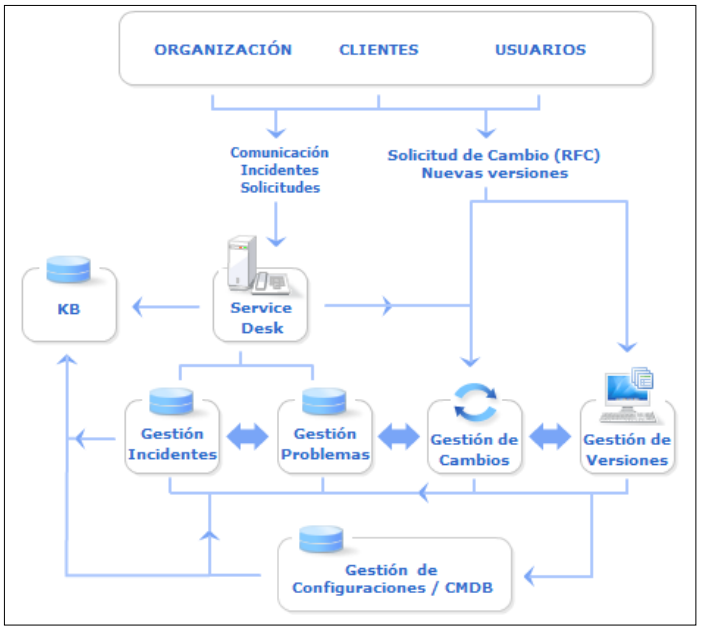


Figura 4.2: Soporte de Servicio [1]

4.7.1 COMPONENTES DE LA METODOLOGÍA DE SOPORTE AL SERVICIO

Organización: la propia organización TI debe considerarse como otro cliente/usuario mas de los servico TI.

Clientes: son los encargados de contratar los servicios TI y a los que hay que rendir cuentas respecto a los Acuerdos de Nivel de Servicio.

Usuarios: son aquellos que utilizan los servicios TI para llevar a cabo sus actividades.

KB(Knowledge Base): La base del conocimiento tiene que recoger toda la información necesaria para:

- ✓ Ofrecer una primera linea de soporte ágil y eficaz sin necesidad de recurrir a escalados.
- ✓ Realizar una tarea comercial y de soporte de negocio

Service Desk: Representa el centro de todos los procesos de soporte al servicio:

- ✓ Registrando y monitorizando incidentes.
- ✓ Aplicando soluciones temporales a errores conocidos en colaboración con la Gestión de Problemas.
- ✓ Colaborando con la Gestión de configuraciones para asegurar la actualización de CMDB[42].
- ✓ Gestionando cambios solicitados vía peticiones de servicio en colaboración con la Gestión de Cambios y Versiones.

4.7.2 GESTIÓN DE INCIDENCIAS

Incidencia es cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar una interrupción, o una reducción de la calidad del mismo.

La Gestión de Incidentes tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible.

El uso de una herramienta de Gestión de Incidencias tiene tres objetivos básicos:

[42] **CMDB (Base de Datos para la Gestión de Configuración**): es una base de datos donde se integran los detalles relevantes de empleados, estaciones de trabajo, empleados de TI, otros dispositivos, incidencias, problemas, cambios y otros elementos relevantes para el negocio.

- ✓ Minimizar los períodos fuera de servicio.
- ✓ Registrar la información relevante de todas las incidencias.
- ✓ Incorporar las mejores prácticas del mercado de forma sistemática.

En la figura 4.3 se muestra las propiedades y funcionalidades de la Gestión de Incidentes:

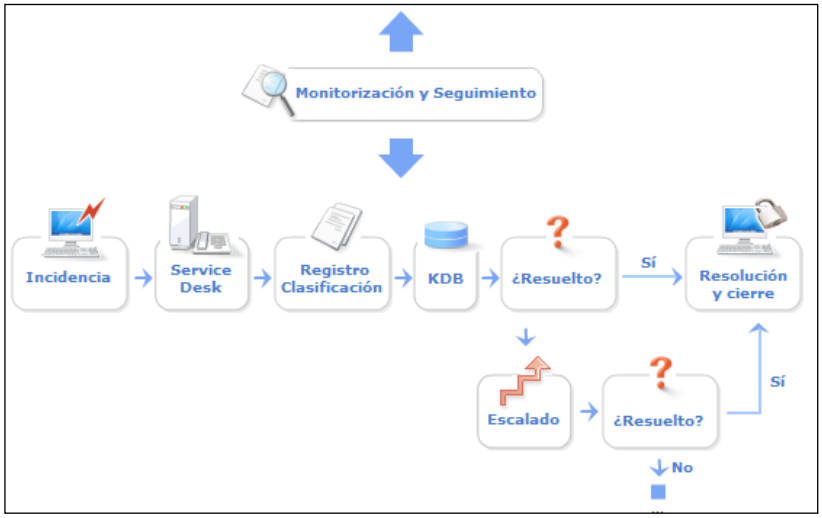


Figura 4.3: Gestión de Incidencias [1]

La Gestión de Incidencias es un instrumento para aquellas organizaciones que quieran incorporar las mejores prácticas en la gestión de incidencias. En la práctica esto puede:

- ✓ Registrar la incidencia: quién informa del problema, síntomas, equipo involucrado, etc.
- ✓ Clasificar la incidencia y asignar el trabajo a realizar a un grupo de soporte o a un técnico.
- ✓ Investigar la causa de la incidencia y compararla con otras incidencias parecidas.
- ✓ Documentar la solución, anexar ficheros con información relacionada y cerrar la incidencia.

- ✓ Comunicar automáticamente al usuario el estado de su solicitud a través del e-mail y/o portal de soporte.
- ✓ Elaborar informes, que ayuden a conocer qué está sucediendo y a mejorar el proceso.

Los beneficios de una gestión eficaz de incidencias son:

- ✓ Reducción del impacto de las incidencias sobre la organización.
- ✓ Uso más eficiente de los recursos de personal.
- ✓ Usuarios más satisfechos.
- ✓ Mayor visibilidad del trabajo realizado.

4.7.3 GESTIÓN DE PROBLEMA

Un problema es el origen de uno o varios incidentes. Los problemas son registrados en la CMDB, separadamente de los incidentes con los cuales ellos son relacionados. Los errores conocidos, ya detectados, también son guardados como registros en el CMDB, vinculados a los problemas que ellos causan.

Las funciones principales de la Gestión de Problemas son:

- ✓ Investigar las causas subyacentes a toda alteración, real o potencial, del servicio TI.
- ✓ Determinar posibles soluciones a las mismas.
- ✓ Proponer las peticiones de cambio (RFC) necesarias para restablecer la calidad del servicio.
- ✓ Realizar Revisiones Post Implementación (PIR) para asegurar que los cambios han surtido los efectos buscados sin crear problemas de carácter secundario.

La Gestión de Problemas puede ser de dos tipos:

Reactiva: Analiza los incidentes ocurridos para descubrir su causa y propone soluciones a los mismos.

Proactiva: Monitoriza la calidad de la infraestructura TI y analiza su configuración con el objetivo de prevenir incidentes incluso antes de que estos ocurran.

En la figura 4.4 se muestra las interacciones y funcionalidades de la Gestión de Problemas.

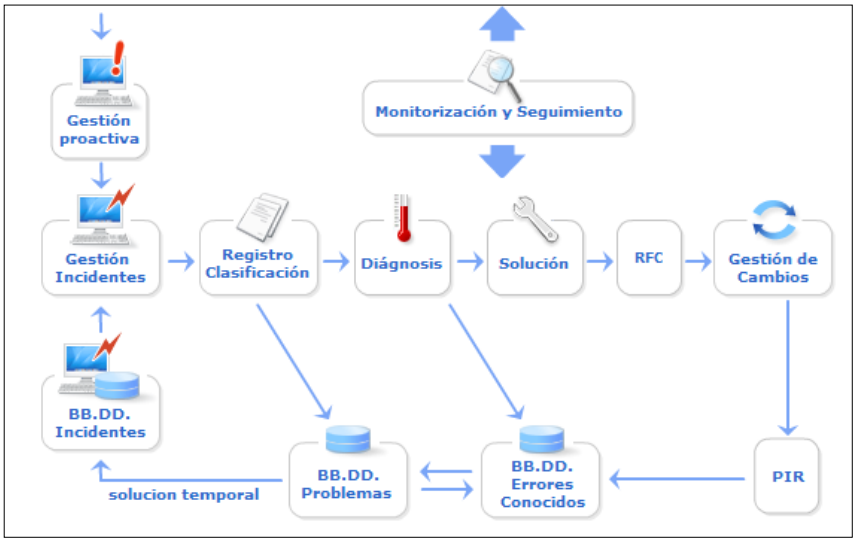


Figura 4.4: Gestión de Problema [1]

Cuando algún tipo de incidente se convierte en recurrente o tiene un fuerte impacto en la infraestructura TI es la función de la **Gestión de Problemas** el determinar sus causas y encontrar posibles soluciones.

4.7.4 GESTIÓN DE CAMBIO

El principal objetivo de la Gestión de Cambios es la evaluación y planificación del proceso de cambio para asegurar que, si éste se lleva a cabo, se haga de la forma más eficiente, siguiendo los procedimientos establecidos y asegurando en todo momento la calidad y continuidad del servicio TI.

Las principales razones para la realización de cambios en la infraestructura TI son:

- ✓ Solución de errores conocidos.
- ✓ Desarrollo de nuevos servicios.
- ✓ Mejora de los servicios existentes.
- ✓ Imperativo legal.

En la figura 4.5 se muestra las interacciones y funcionalidades de la Gestión de Cambios.

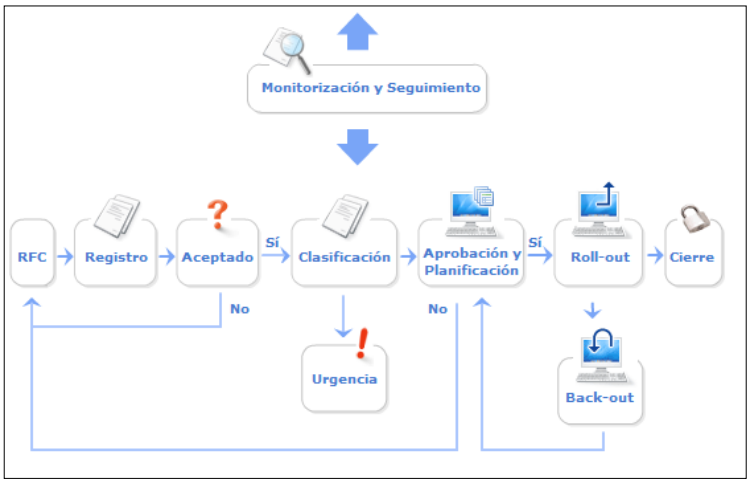


Figura 4.5: Gestión de Cambios [1]

La Gestión de Cambios es el proceso de ITIL que supervisa esta parte de la Gestión del Soporte del Servicio de TI. Cada cambio requiere una Demanda de Cambios (Request for Change, RFC) que también es almacenado en el CMDB.

El proceso de Gestión de Cambios de ITIL mantiene la infraestructura TI en línea con las necesidades del negocio. Este proceso formaliza la aproximación para manejar cualquier cambio para la entrega de servicios (Entrega del Servicio) por un único y centralizado proceso de aprobación, programado y controlado.

Autorización y **Aprobación** son las palabras clave (key words) en este proceso. El Consejo Consultivo de Cambios, o CAB (Change Advisory Board), es un grupo de

personas que investiga y autoriza o niega cualquier cambio propuesto. El CAB debe crear un Agenda de Cambios Avanzada que identifique cualquier cambio futuro las acciones que deben ser tomadas en ellos.

4.7.5 GESTIÓN DE CONFIGURACIONES

Gestión de Configuración es el proceso de identificar y definir los elementos en el sistema, controlando el cambio de estos elementos a lo largo de su ciclo de vida, registrando y reportando el estado de los elementos y las solicitudes de cambio, y verificando que los elementos estén completos y que sean los correctos.

En la figura 4.6 se muestra las interacciones y funcionalidades de la Gestión de Configuraciones.

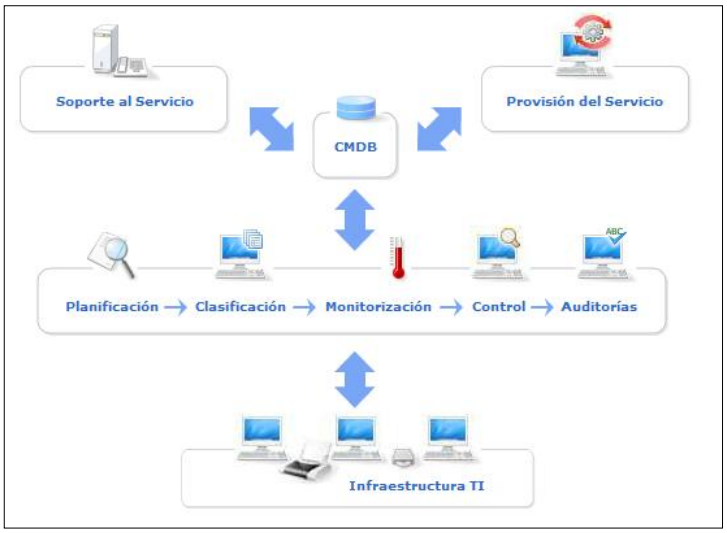


Figura 4.6: Gestión de Configuración [1]

Las principales funciones de Gestión de Configuraciones son las siguientes:

- Llevar el control de todos los elementos de configuración de la infraestructura TI con el adecuado nivel de detalle y gestionar dicha información a través de la Base de Datos de Configuración (CMDB).

- Proporcionar información precisa sobre la configuración TI a todos los diferentes procesos de gestión.

- Interactuar con las **Gestiones de Incidentes, Problemas, Cambios y Versiones** de manera que estas puedan resolver más eficientemente las incidencias, encontrar rápidamente la causa de los problemas, realizar los cambios necesarios para su resolución y mantener actualizada en todo momento la CMDB.

- Monitorizar periódicamente la configuración de los sistemas en el entorno de producción y contrastarla con la almacenada en la CMDB para subsanar discrepancias.

- Provee soporte al servicio, todos los procesos de Soporte al servicio dependen de gran manera de la CMBD:

  - ✓ Se necesita la información de los CLs[43] para analizar incidentes y problemas.
  - ✓ La Gestión de Cambios y Versiones tiene que trabajar en estrecha colaboración con la Gestión de Configuraciones para mantener actualizada la CMBD.

    Los CLs pueden ser:

  - ✓ Dispositivos de hardware como PCs, impresoras, routers, monitores, etc. así como sus componentes: tarjetas de red, teclados, lectores de CDs, etc.
  - ✓ Software: sistemas operativos, aplicaciones, protocolos de red, etc.
  - ✓ Documentación: manuales, acuerdos de niveles de servicio, etc.

[43] **Elementos de configuración (CLs):** todos, tanto los componentes de los servicios TI como los servicios que éstos nos ofrecen, constituyen diferentes elementos de configuración.

4.7.6 GESTIÓN DE VERSIONES

Es el proceso final de ITIL en el enfoque de Soporte del Servicio.La Gestión de Versiones se encarga de la planificación, construcción, pruebas de control de calidad de los elementos de sofware y harware instalados en el entorno de producción.

La Gestión de Versiones debe colaborar estrechamente con la Gestión de Cambios y Configuraciones para asegurar que toda la información de las nuevas versiones se integren en la CMDB para que se encuentre alcualizada.

Una versión es un conjunto de CLs de nueva creación o modificados que han sido validados para su instalación en el entorno de la producción.

Las versiones pueden clasificarse de acuerdo a la Infraestructura TI:

- **Versiones mayores**: que representan importantes despliegues de software y hardware y que introducen modificaciones importantes en la funcionalidad y características técnicas.

- **Versiones menores**: implica la corrección de varios errores conocidos puntuales y que a menudo son modificaciones que vienen a implementar de una manera correctamente documentada soluciones de emergencia.

- **Versiones de emergencia**: modificaciones que reparan de forma rápida un error conocido.

En la figura 4.6 se muestra las interacciones y funcionalidades de la Gestión de Configuraciones.

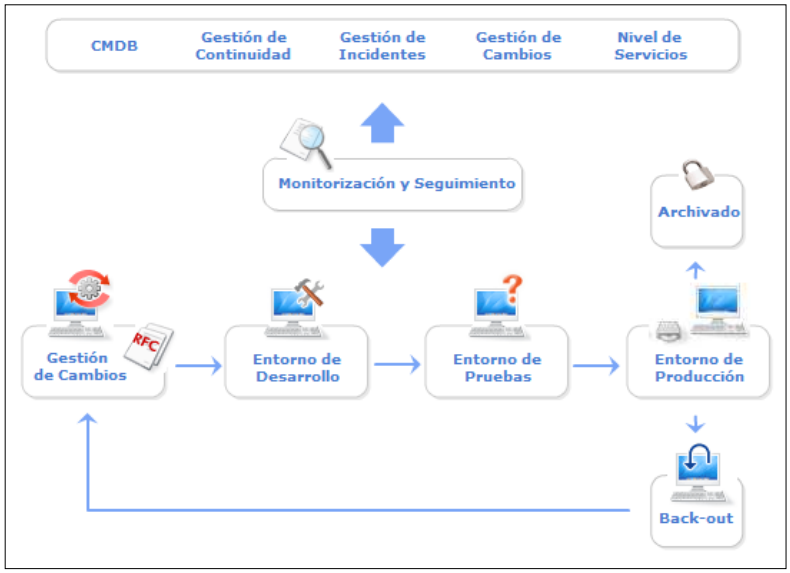


Figura 4.7: Gestión de Versiones [1]

La **Gestión de Versiones** también debe mantener actualizada la Biblioteca de Software Definitivo (**DSL**), donde se guardan copias de todo el software en producción, y el Depósito de Hardware Definitivo (DHS[44]), donde se almacenan piezas de repuesto y documentación para la rápida reparación de problemas de hardware en el entorno de producción.

4.8 PROVISIÓN DE SERVICIOS [1], [3], [4], [5]

La provisión de servicios se ocupa de los servicios ofrecidos en sí mismos. En particular de los Niveles de Servicio, disponibilidad, continuidad, viabilidad financiera, capacidad necesaria de la infraestructura TI y los niveles de gestión requeridos.

[44]**Biblioteca de Software Definitivo (DSL):** Donde se guardan copias de todo el software en producción.
Depósito de Hardware Definitivo (DHS): Donde se almacenan piezas de repuesto y documentación para la rápida reparación de problemas de hardware en el entorno de producción.

Figura 4.8: Provisión de Servicios [1]

4.8.1 GESTIÓN DE NIVELES DE SERVICIOS

El objetivo de la Gestión de Niveles de Servicios es poner la tecnología al servicio del cliente y de esta manera aportar valor a los usuarios. La **Gestión de Niveles de Servicio** debe velar por la calidad de los servicios TI alineando tecnología con procesos de negocio y todo ello a unos costes razonables.

Para cumplir sus objetivos es imprescindible que la **Gestión de Niveles de Servicio**:

- ✓ Conozca las necesidades de sus clientes.
- ✓ Defina correctamente los servicios ofrecidos.
- ✓ Monitoree la calidad del servicio respecto a los objetivos establecidos en los SLAs.

En la figura 4.9 se muestra las interacciones y funcionalidades de la Gestión de Niveles de Servicio:

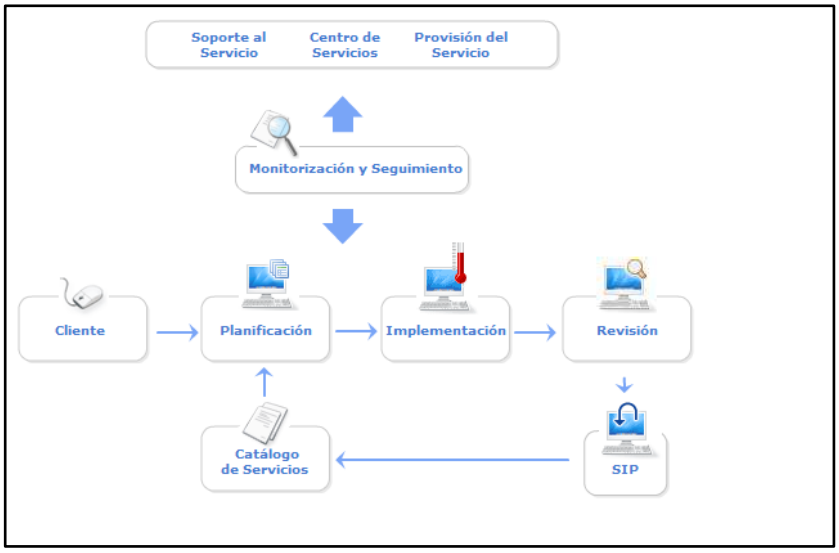


Figura 4.9: Gestión de Niveles de Servicio[1]

La Gestión de Niveles de Servicio es la responsable de:

- ✓ Establecer, en estrecha colaboración con el cliente los Acuerdos de Nivel de Servicio.(SLA)[45]
- ✓ Formalizar los Acuerdos de Nivel de Operación y los Contratos de Soporte con los proveedores externos.(OLAs y UC)[46]
- ✓ Monitorización de la calidad de servicio.

4.8.2 GESTIÓN FINANCIERA DE LOS SERVICIOS TI

Se encarga de la administración de los recursos monetarios de la organización TI para soportar a la empresa en la planificación y ejecución de los planes de negocio. Además se encarga de evaluar y controlar los costos asociados a los servicios TI para ofrecer un servicio de calidad con un uso eficiente de los recursos.

[45] **SLAs (Service Level Agreement):** es un acuerdo de nivel de servicio contiene una descripción del servicio que abarca desde los aspectos más generales hasta los detalles más específicos del servicio.
[46]**OLAs (Acuerdos de Nivel de Operación):** son documentos de carácter interno de la propia organización TI que determinan los procesos y procedimiento necesarios para ofrecer los niveles de servicio acordados con los clientes.
UC (Contratos de Soporte): es un acuerdo con un proveedor externo para la prestación de servicios no cubiertos por la propia organización TI.

En la figura 4.10 se muestra las propiedades y funcionalidades de la Gestión Financiera de los Servicios TI:

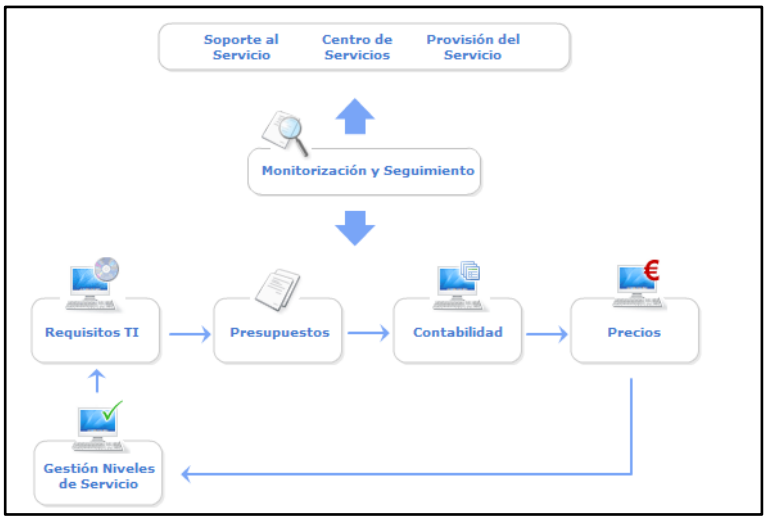


Figura 4.10: Gestión Financiera[1]

Por regla general, a mayor calidad de los servicios mayor es su costo, por lo que es necesario evaluar cuidadosamente las necesidades del cliente para que el balance entre ambos sea óptimo.

Si la organización TI y/o sus clientes no son conscientes de los costes asociados a los servicios no podrán evaluar el retorno a la inversión ni podrán establecer planes consistentes de inversión tecnológica.

4.8.3 GESTIÓN DE CAPACIDAD

La Gestión de Capacidad es la encargada de administrar los recursos de todos los servicios TI y predecir capacidades adicionales por adelantado.

Sin una correcta Gestión de Capacidades los recursos no se aprovechan adecuadamente y se realizan inversiones innecesarias que acarrean gastos adicionales de mantenimiento y administración, o los recursos son insuficientes produciendo una consecuente degradación de la calidad de servicio.

En la figura 4.11 se muestra las propiedades y funcionalidades de la Gestión de Capacidad:

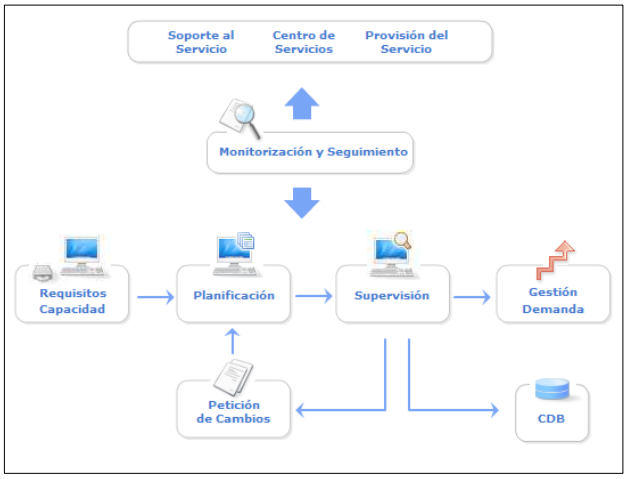


Figura 4.11: Gestión de Capacidad[1]

Para que la Gestión de Capacidad sea exitosa, se debe tomar en cuenta:

- **Predicción y provisión automatizada:** ofrece una serie de herramientas para asegurar la efectividad de todos los aspectos relativos de la capacidad y rendimiento que afectan los servicios del negocio.

- **Capacity Planning:** contribuye a construir un proceso estructurado de la provisión de los recursos TI dependiendo de las necesidades.

- **Informe históricos de uso y tendencia:** proporciona herramientas de análisis que permiten identificar la relación entre el ciclo del negocio y la capacidad de los recursos.

4.8.4 GESTIÓN DE LA CONTINUIDAD DEL SERVICIO

La Gestión de Continuidad se centra en describir las habilidades necesarias de una organización para continuar proporcionando un predeterminado nivel de los servicios TI a continuación de una interrupción o falla en una aplicación del sistema. Además se preocupa de impedir que una imprevista o grave interrupción de los servicios TI,

debido a desastres naturales u otras fuerzas de causa mayor y tenga consecuencias catastróficas en el negocio.

En la figura 4.12 se muestra las propiedades y funcionalidades de la Gestión de Continuidad del Servicio:

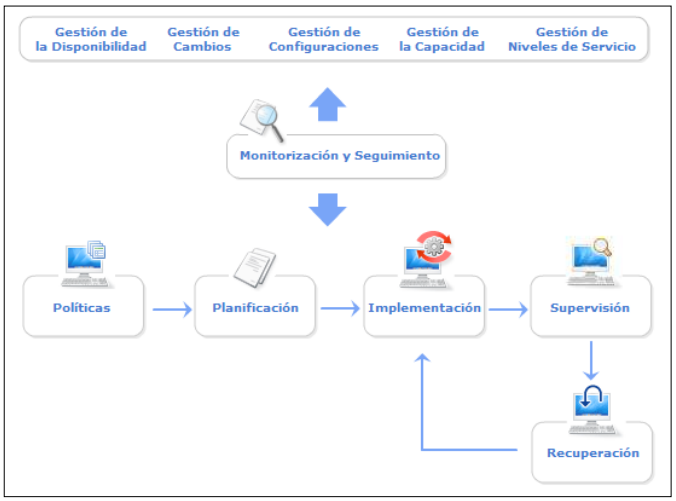


Figura 4.12: Gestión de Continuidad del Servicio[1]

Esta gestión debe combinar equilibradamente los siguientes procedimientos:

- **Proactivos:** buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.

- **Reactivos:** su objetivo es reanudar el servicio tan pronto como sea posible.

Es fundamental establecer una política coherente sobre la continuidad de los servicios TI:

- ✓ En la que se establezca el alcance de la misma.
- ✓ Se asignen los recursos necesarios.
- ✓ Se establezcan las bases para la organización del proceso.

Es importante realizar una evaluación de riesgos y para ello se debe:

- ✓ Conocer en profundidad la infraestructura TI y cuáles son los elementos de configuración involucrados en la prestación de cada servicio.
- ✓ Analizar las posibles amenazas y estimar su probabilidad.
- ✓ Detectar los puntos más vulnerables de la infraestructura TI.

Figura 4.13: Evaluación de Riesgos[1]

Con los resultados del análisis detallado se dispondrá de información necesaria para proponer diferentes medidas de prevención y recuperación que se adapten a las necesidades reales del negocio.

4.8.5 GESTIÓN DE DISPONIBILIDAD

La Gestión de Disponibilidad se encarga de optimizar y monitorizar los servicios TI para que estos funcionen ininterrumpidamente y de manera segura cumpliendo con los SLAs establecidos y todo ellos a un costo razonable. Permite optimizar el uso de los recursos, anticipar y calcular fallas e implementar políticas de seguridad.

La Gestión de Disponibilidad incluye: Seguridad, Servicialidad, Recuperabilidad, Sostenibilidad y Resistencia de los recursos TI, los mismos que se alcanzan determinando los requerimientos de la disponibilidad del negocio nivelando estos con la infraestructura TI y la organización de soporte.

En la figura 4.14 se muestra las propiedades y funcionalidades de la Gestión de Disponibilidad:

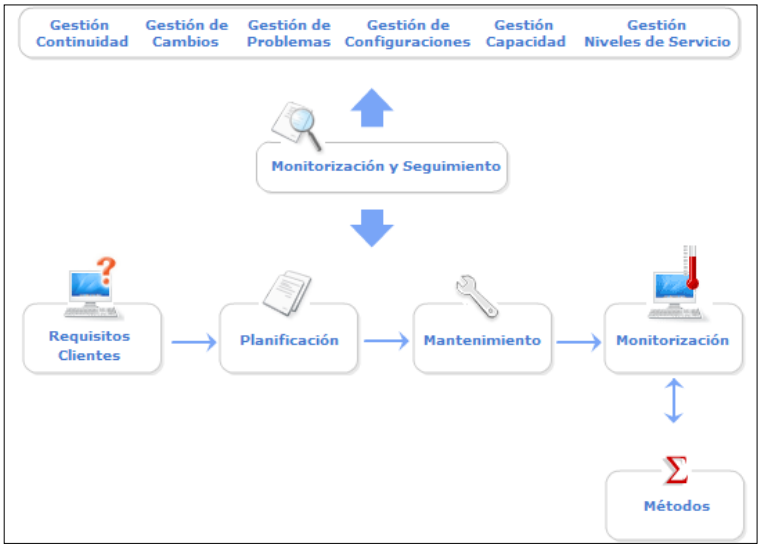


Figura 4.14: Gestión de Disponibilidad[1]

Los indicadores clave sobre los que se sustenta el proceso de **Gestión de la Disponibilidad** se resumen en:

- ✓ **Disponibilidad**: porcentaje de tiempo sobre el total acordado en que los servicios TI han sido accesibles al usuario y han funcionado correctamente.
- ✓ **Fiabilidad**: medida del tiempo durante el cual los servicios han funcionado correctamente de forma ininterrumpida.
- ✓ **Mantenibilidad**: capacidad de mantener el servicio operativo y recuperarlo en caso de interrupción.

La correcta planificación de la disponibilidad permite establecer unos niveles de disponibilidad adecuados tanto en lo que respecta a las necesidades reales del negocio como a las posibilidades de la organización TI.

Algunos de los parámetros que suele utilizar la **Gestión de la Disponibilidad** y que debe poner a disposición del cliente en los informes de disponibilidad correspondientes incluyen:

- ✓ **Tiempo Medio de Parada** (**Downtime**): que es el tiempo promedio de duración de una interrupción de servicio, e incluye el tiempo de detección, respuesta y resolución.
- ✓ **Tiempo Medio entre Fallos** (**Uptime**): es el tiempo medio durante el cual el servicio está disponible sin interrupciones.
- ✓ **Tiempo Medio entre Incidentes**: es el tiempo medio transcurrido entre incidentes que es igual a la suma del Tiempo Medio de Parada y el Tiempo Medio entre Fallos. El Tiempo Medio entre Incidentes es una medida de la fiabilidad del sistema.

4.8.6 GESTIÓN DE LA SEGURIDAD

La Gestión de Seguridad se encarga de la seguridad de la información y para ello debe apoyarse en tres pilares fundamentales:

- ✓ **Confidencialidad**: la información debe ser sólo accesible a sus destinatarios predeterminados.
- ✓ **Integridad**: la información debe ser correcta y completa.
- ✓ **Disponibilidad**: debemos de tener acceso a la información cuando la necesitamos.

La Gestión de la Seguridad debe, por tanto, velar por que la información sea correcta y completa, esté siempre a disposición del negocio y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

En la figura 4.16 se muestra las propiedades y funcionalidades de la Gestión de Seguridad:

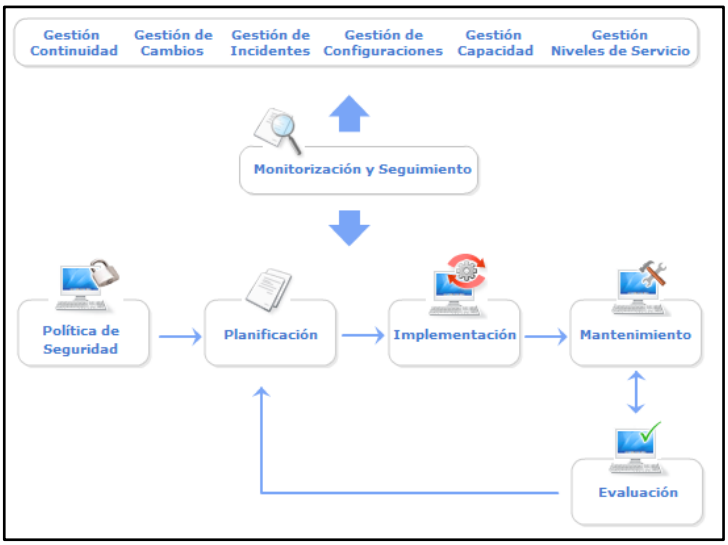


Figura 4.15: Gestión de la Seguridad[1]

El **Plan de Seguridad** debe diseñarse para ofrecer un mejor y más seguro servicio al cliente y nunca como un obstáculo para el desarrollo de sus actividades de negocio. Siempre que sea posible deben definirse métricas e indicadores clave que permitan evaluar los niveles de seguridad acordados.

Se recomienda realizar auditorías de seguridad externas realizadas por el personal independiente de la Gestión de Seguridad.

Es importante que la Gestión de la Seguridad esté al día en lo que respecta a nuevos riesgos y vulnerabilidades frente a virus, ataques de denegación de servicio, etc., y que adopte las medidas necesarias de actualización de equipos de hardware y software, sin olvidar el apartado de formación: el factor humano es normalmente el eslabón más débil de la cadena.

CAPÍTULO 5

LEVANTAMIENTO Y DOCUMENTACIÓN DE PROCESOS NECESARIOS PARA LA ADMINISTRACIÓN DE UNA RED BACKBONE IP/MPLS

5.1 MANUAL CACTI

5.1.1 OBJETIVO

Conocer el funcionamiento y el manejo de las herramientas principales de la plataforma CACTI para el monitoreo y gestión de los equipos y de los servicios de red para lograr una administración potencialmente satisfactoria.

5.1.2 INTRODUCCIÓN

CACTI es una solución completa para la monitorización de redes mediante gráficos y recopilación de datos, todo ello gracias a la potencia de RRDTool‘s, mediante esta herramienta se puede tener información prácticamente a tiempo real sobre diferentes equipos tanto como routers, switches o servidores, tráfico de interfaces, cargas, CPU, temperaturas, etc.

5.1.3 INGRESO AL SISTEMA

Para empezar a utilizar la aplicación, deberá ingresar el nombre de usuario *(Username)* y contraseña *(Password),* presionar ENTER o hacer clic en *Login* como se muestra en la pantalla.

Figura 5.1.1: Ingreso al sistema[1]

La aplicación validará tales datos y por ende aparecerá una pantalla con las opciones disponibles.

5.1.4 PANTALLA INICIAL

La pantalla inicial del sistema es como se muestra en la figura 5.1.2:

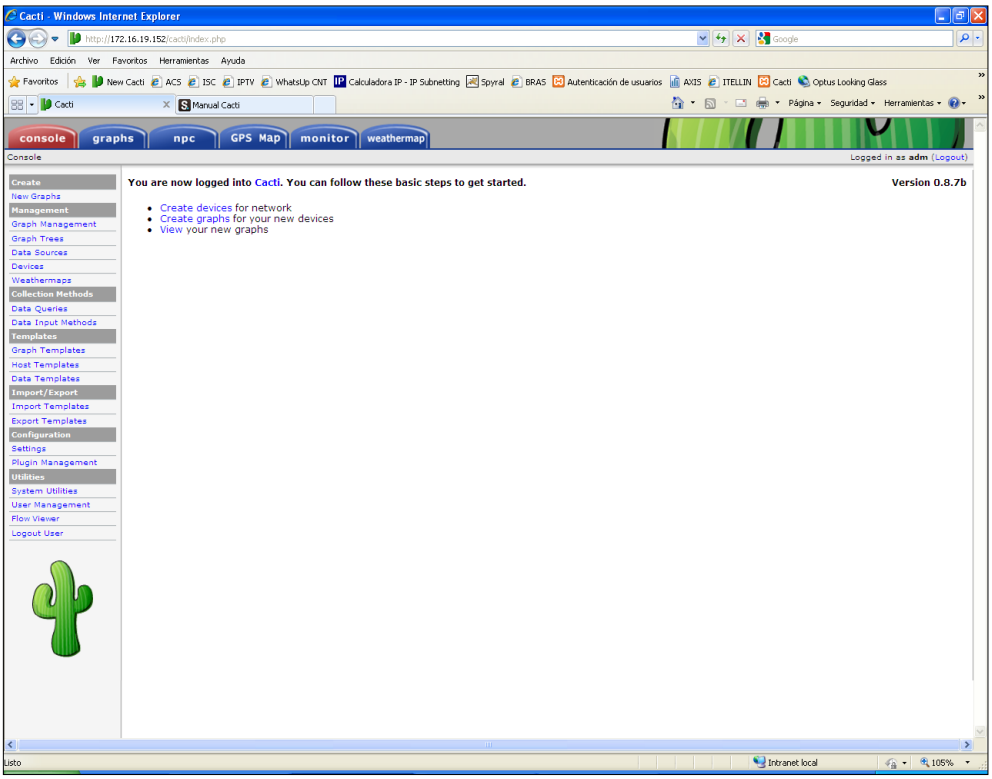


Figura 5.1.2: Pantalla Inicial[1]

5.1.5 TAB CONSOLE

A continuación se muestra la respectiva descripción de cada uno de los componentes del *Tab Console*.

5.1.5.1 DEVICES

Esta opción muestra todos los equipos que han sido configurados previamente en la aplicación la cual permitirá agregar, configurar, modificar y borrar los mismos.

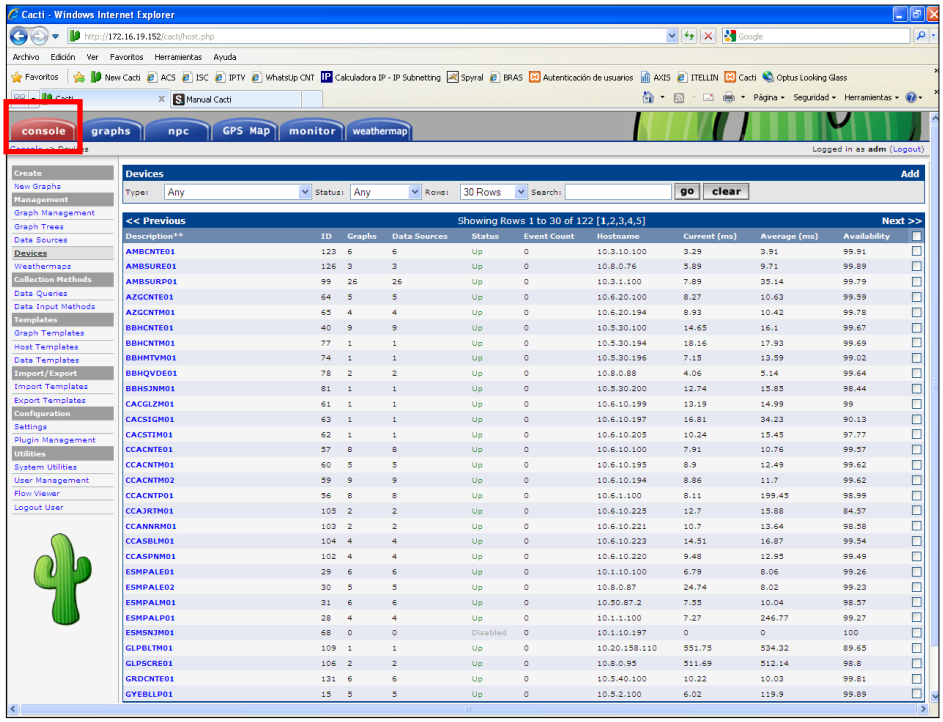


Figura 5.1.3: Devices [1]

5.1.5.2 AÑADIR UN EQUIPO

Para añadir un equipo seguir los pasos que se muestran a continuación:

1. Añadir un equipo mediante el botón *ADD* desde la opción *DEVICES* como se muestra en la figura 5.1.4.

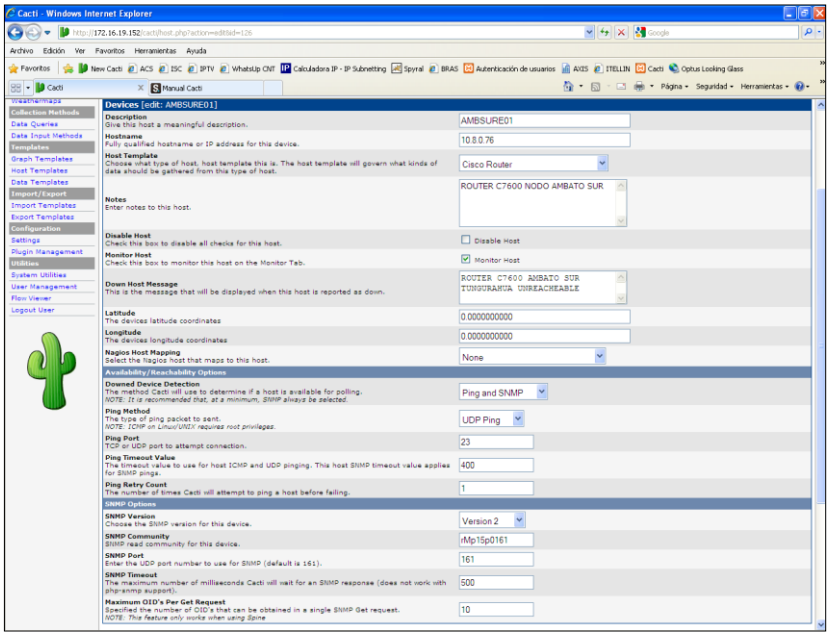


Figura 5.1.4: Añadir un nuevo equipo[1]

2. Colocar los parámetros requeridos en base a los puntos que se muestran a continuación:

➢ **DEVICE**

- ✓ ***Description****:* Nombre asignado para identificar el equipo en la aplicación.
- ✓ ***Hostname:*** Dominio del equipo
- ✓ ***Host Template:*** Configuración pre-establecida para los gráficos de la aplicación por ejemplo la opción *Cisco Router*.
- ✓ ***Notes:*** Identificación del equipo y el nodo al que pertenece.
- ✓ ***Disable Host:*** Estado que desactiva el funcionamiento de la aplicación.
- ✓ ***Monitor Host****:* Marque esta casilla para monitorear el equipo.
    - Colocar un mensaje que aparecerá cuando el Host presente algún tipo de problema.
- ✓ ***Down Host Message:*** Este es el mensaje que se mostrará cuando el equipo se reporta como down.
- ✓ ***Latitude y Longitude:*** Colocamos la latitud y longitud correspondiente a cada uno de los equipos.

- ✓ ***Nagios Host Mapping:*** Seleccionar esta opción si el equipo se encuentra configurado en la plataforma Nagios.

- **SECCIÓN AVAILABILITY/REACHABILITY OPTIONS:**

  - ✓ ***Downed Device Detection:*** Elegir la opción *Ping and SNMP* para los equipos que se requieran monitorear en la red.
  - ✓ ***Ping Method*:** Elegir la opción UDP Ping.
  - ✓ ***Ping Port:*** Colocar el puerto 23 preestablecido.
  - ✓ ***Ping Timeout Value:*** Colocar el valor 400, que es el preestablecido y se refiere al tiempo que SNMP envía las características de tráfico existentes.
  - ✓ ***Ping Retry Count:*** Es el número de veces que CACTI intentará hacer ping a un Host antes de fallar, colocar el número 1 que de la misma manera es un valor preestablecido.

- **SECCIÓN SNMP Options:**

  - ✓ ***SNMP Version:*** Elegir la opción versión 2 que es la versión del servicio SNMP a utilizar en el equipo.
  - ✓ ***SNMP Community:*** Password de lectura del servicio SNMP. Cada equipo tiene una comunidad distinta por esta razón es necesario colocar la comunidad correcta para que los equipos envíen la información de manera satisfactoria.
  - ✓ ***SNMP Port:*** Puerto del servicio SNMP a utilizar en el servidor, en este caso es el 161que es un valor preestablecido.
  - ✓ ***SNMP Timeout:*** Tiempo de respuesta en milisegundos del servicio SNMP a utilizar en el equipo, en este caso colocar el valor 500.
  - ✓ ***Maximum OID's Per Get Request:*** Característica de rendimiento, colocar el valor 10 para todos los equipos, este es un valor preestablecido.

3. Guardar las configuraciones realizadas dando clic en la opción *SAVE.*

5.1.5.3 EDITAR UN EQUIPO

Una vez que se ha creado el equipo en la aplicación y se desee editarlo, presionar el nombre del equipo en la lista que se muestra en la opción *DEVICES* del menú.

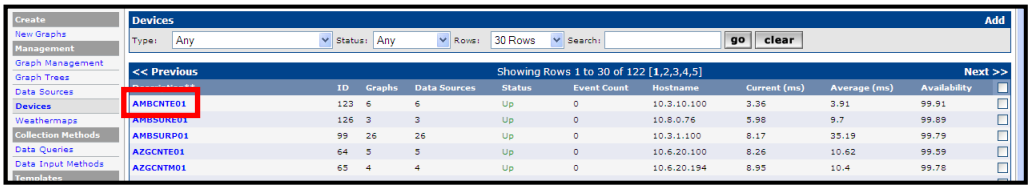


Figura 5.1.5: Menú Devices[1]

Se despliega la misma información que cuando se añade un nuevo equipo *(DEVICES ADD)* como se muestra figura 5.1.6.

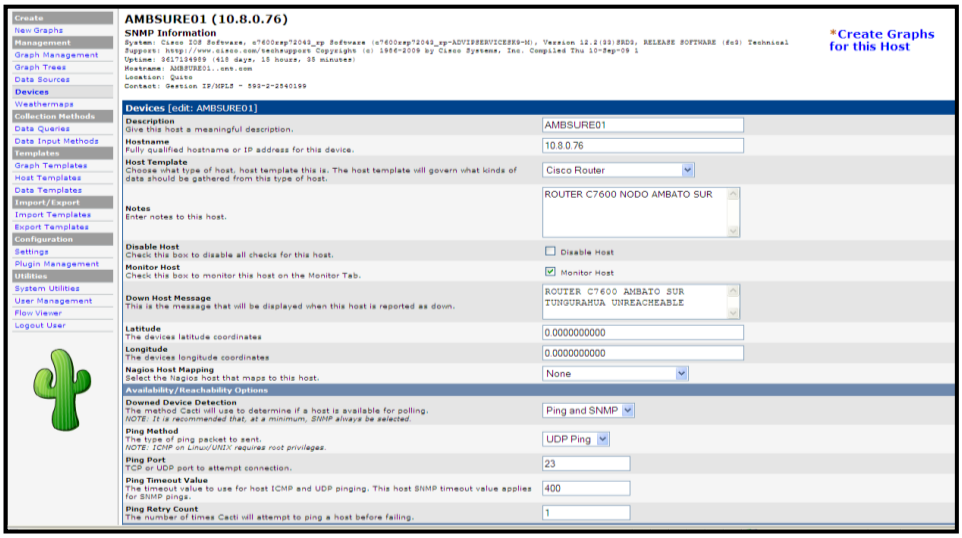


Figura 5.1.6: Edición de un equipo[1]

5.1.5.4 CREACIÓN DE GRÁFICOS

Una vez creados los equipos se procede a realizar los respectivos gráficos del monitoreo de los equipos que se encuentran en la red.

Para la creación de los gráficos seguir los siguientes pasos:

1. Seleccionar en el menú la opción *New Graphs*.

2. En el menú desplegable de la parte superior escoger el equipo donde se va a crear el gráfico como se muestra en la figura 5.1.7:

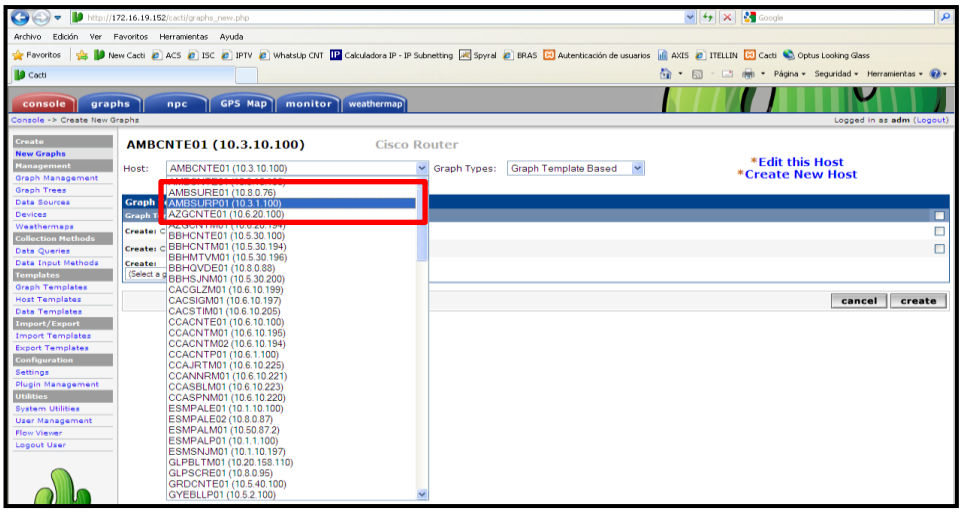


Figura 5.1.7: Creación de gráficos[1]

3. En la opción *Graph Type* seleccionar el tipo de gráfico en la cual se sugiere escoger la opción *SNMP- Interface Statistics* donde aparecerán las interfaces del equipo seleccionado como se muestra en la figura 5.1.8:

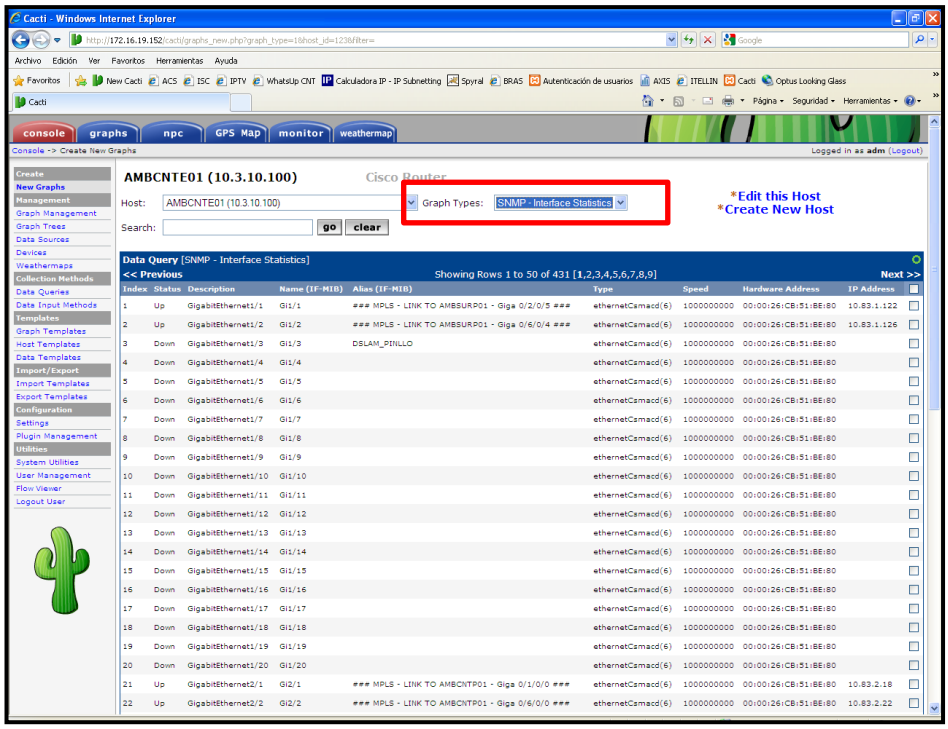


Figura 5.1.8: Opción Graph Type[1]

4. Mediante un filtro se puede realizar la búsqueda de las interfaces del equipo seleccionado como se muestra en la figura 5.1.9:

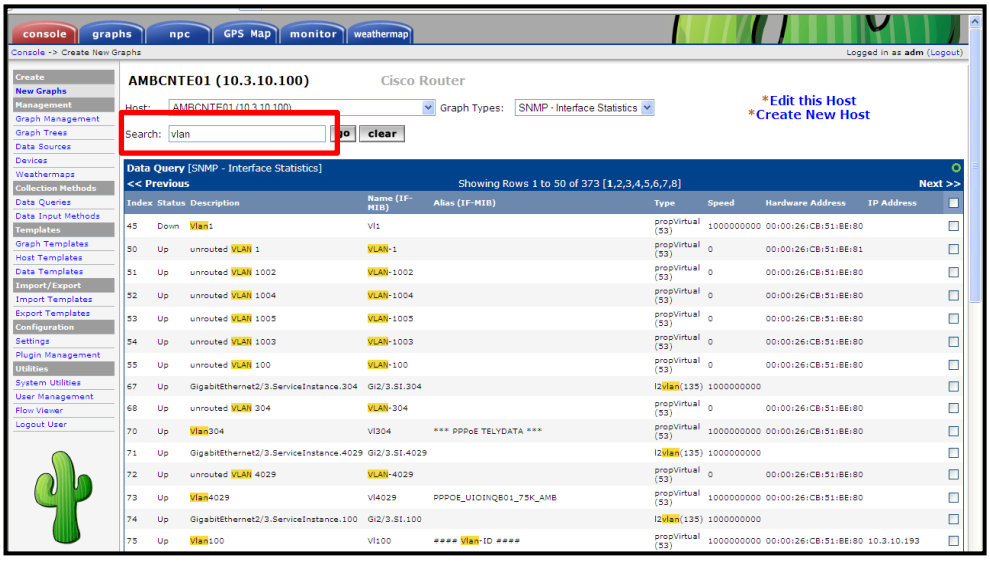


Figura 5.1.9: Filtro para búsqueda de interfaces de un equipo[1]

5. Seleccionar la interfaz a graficar, el tipo de gráfico *(IN/OUT Bits)* y presionar la opción *Create*, como se muestra en la figura 5.1.10:

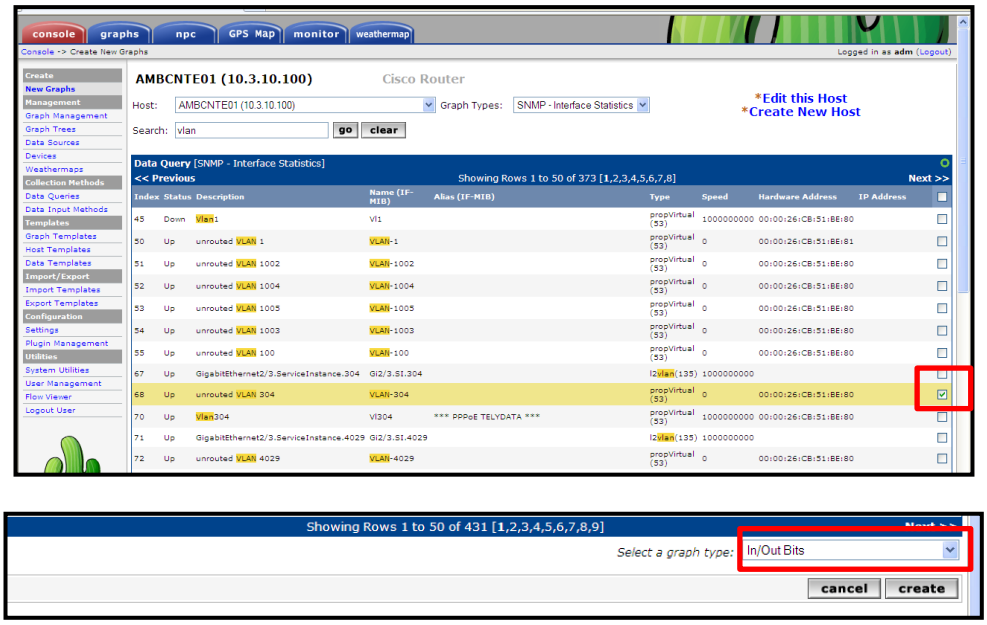


Figura 5.1.10: Selección de Interfaces[1]

6. Si el gráfico se creó correctamente entonces en la parte superior de la pantalla aparecerá un mensaje de éxito como se muestra en la figura 5.1.11:

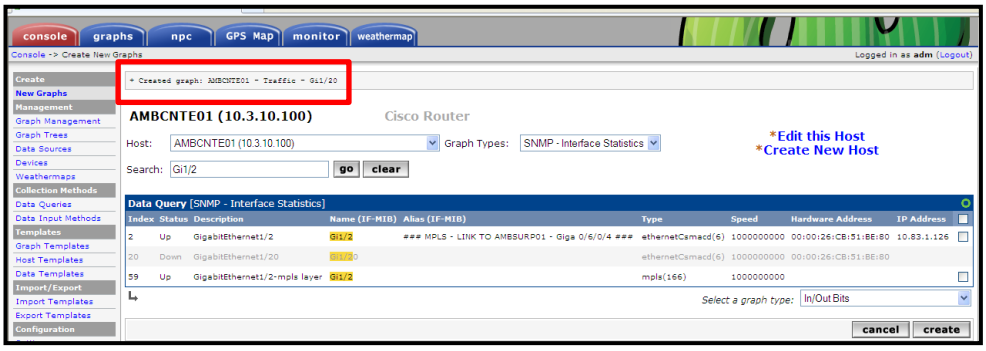


Figura 5.1.11: Mensaje de éxito de la creación del gráfico[1]

5.1.5.5 MANAGEMENT

A continuación se describe los componentes que se encuentran dentro de esta opción.

5.1.5.5.1 GRAPH MANAGEMENT

Para la correcta administración de los gráficos seguir los siguientes pasos:

1. Seleccionar *Graph Management* en la sección *Management* del menú como se muestra en la figura 5.1.12:

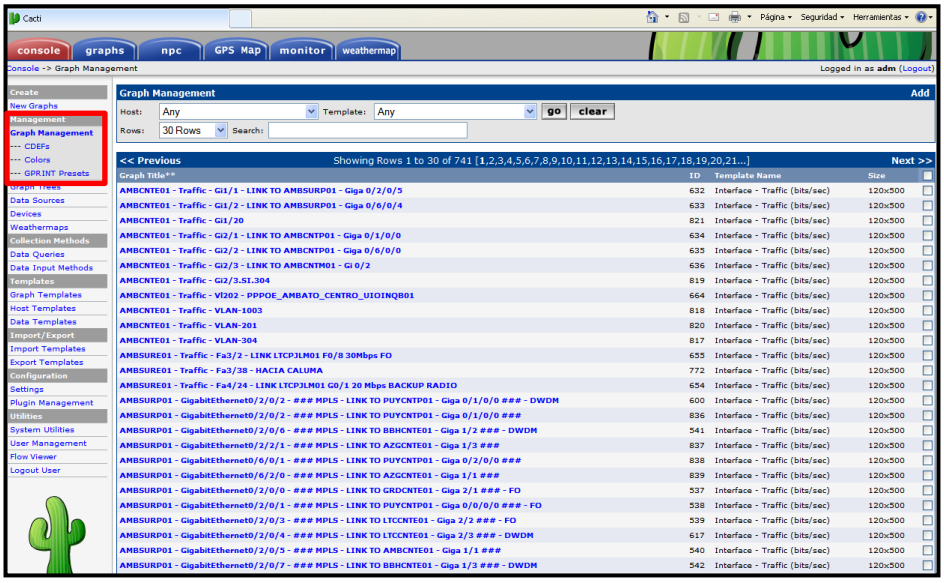


Figura 5.1.12: Opción Graph Management[1]

2. Seleccionar el equipo donde está la interfaz graficada como se muestra en la figura 5.1.13:

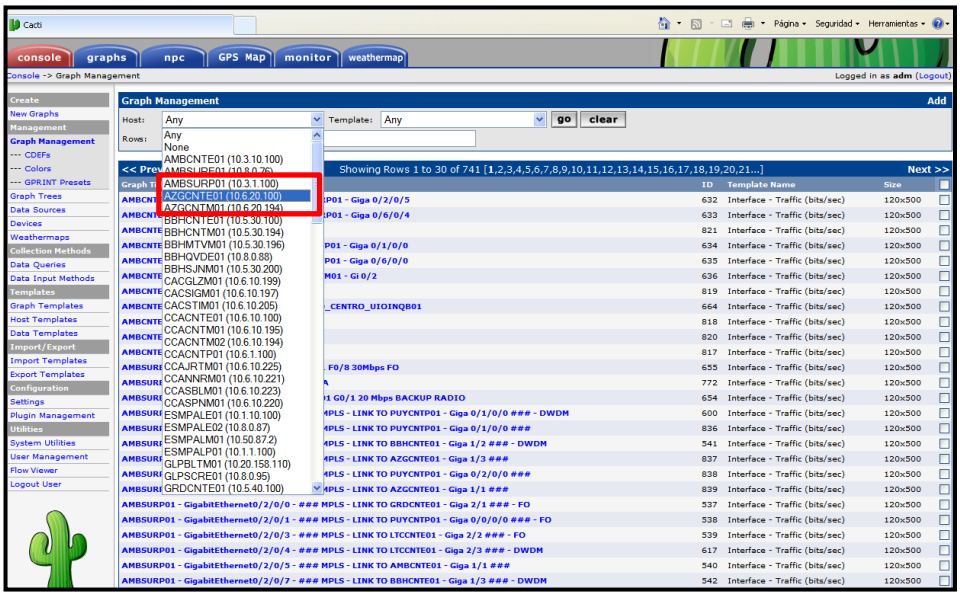


Figura 5.1.13: Selección del equipo en la interfaz[1]

3. Seleccionar el gráfico creado como se muestra en la figura 5.1.14:

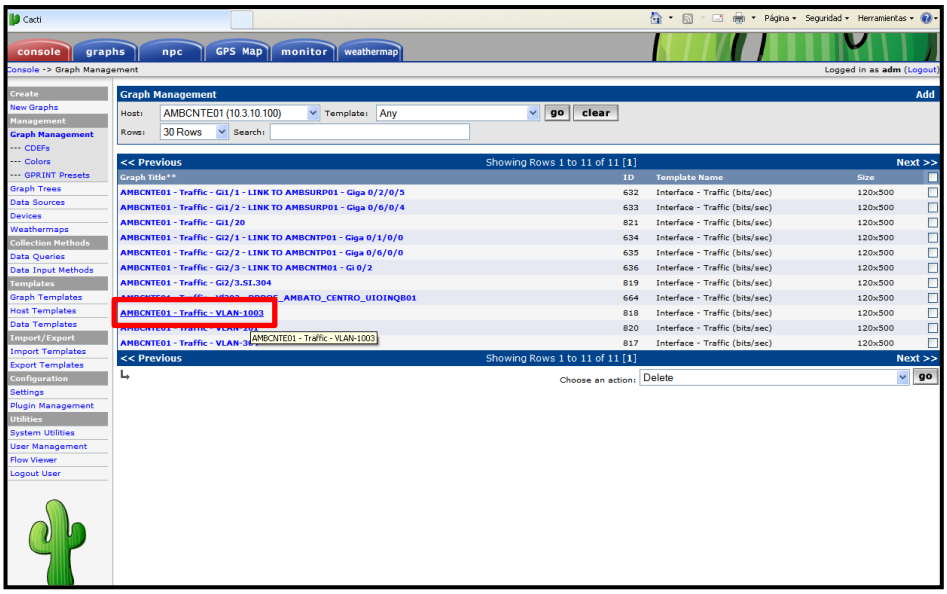


Figura 5.1.14: Selección del gráfico creado[1]

4. En la ventana que aparece existe la opción de editar el titulo de la interfaz se sugiere: *EQUIPO-INTERFAZ-DESCRIPCIÓN* como se muestra en la figura 5.1.15.

5. Guardar los cambios realizados como se muestra en la figura 5.1.15.

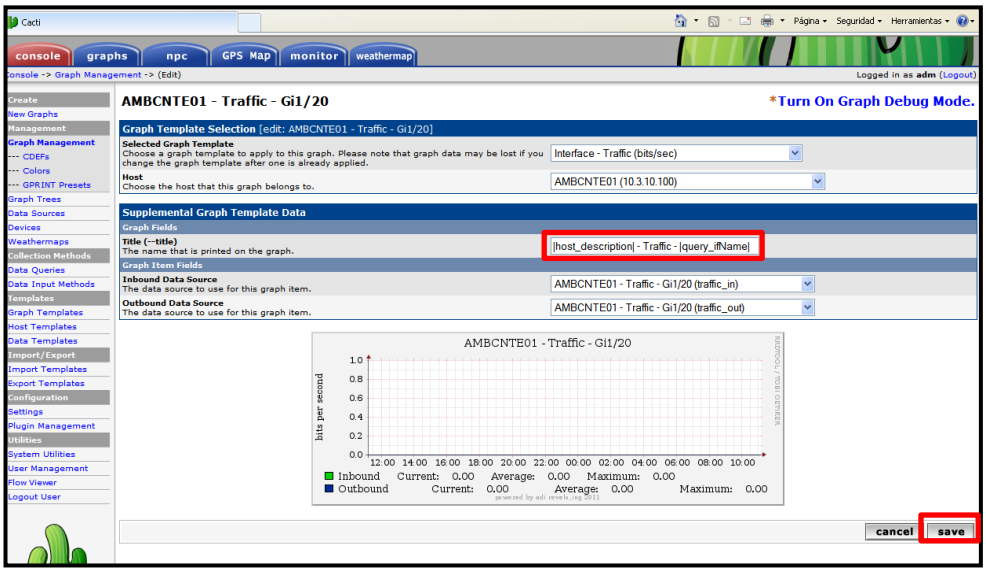


Figura 5.1.15: Edición de una interfaz[1]

6. Se puede ubicar el gráfico dentro de un árbol específico, para ello seleccionar el gráfico y la opción *Place on Tree*, como se muestra en la figura 5.1.16:

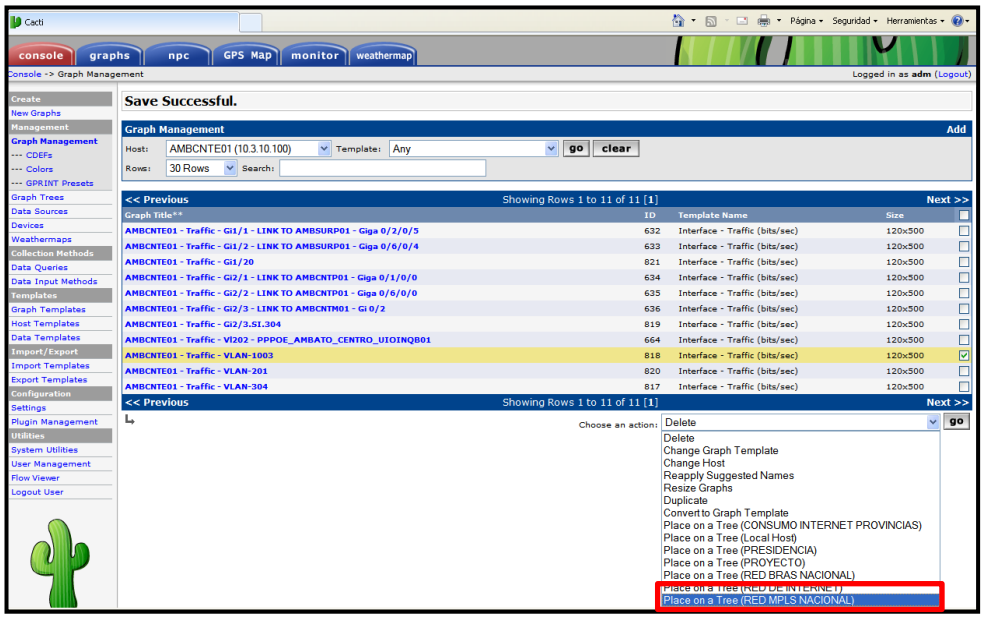


Figura 5.1.16: Ubicación de un gráfico dentro de un árbol[1]

7. En el árbol seleccionado pueden constar más directorios, se escoge específicamente la ubicación del gráfico como se muestra en la figura 5.1.17:

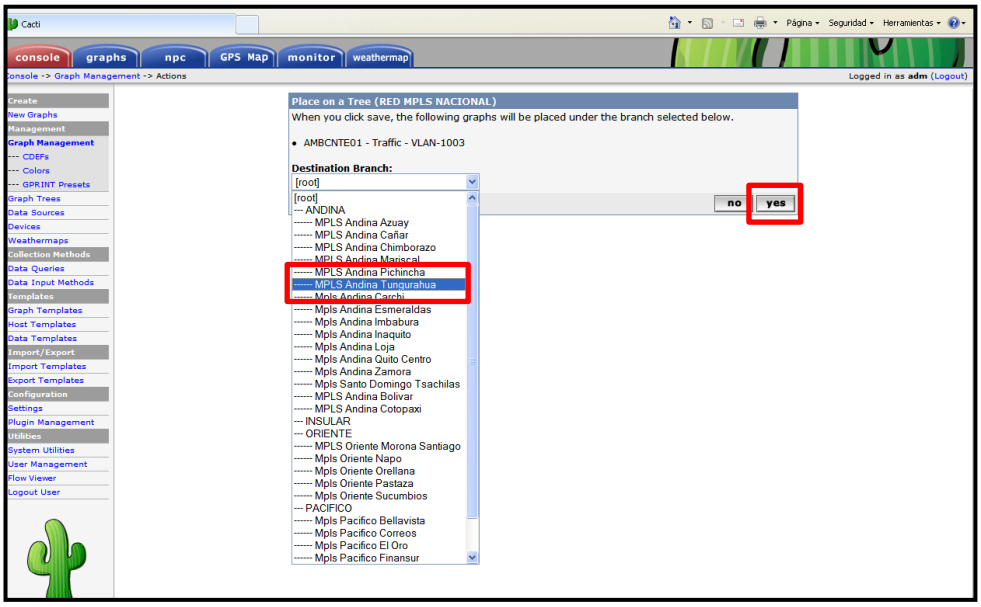


Figura 5.1.17: Elección de la ubicación del gráfico[1]

5.1.5.5.2 CREACIÓN DE UN GRAPH TREE

Los gráficos pueden ser organizados de forma jerárquica.

1. Seleccionar en el menú la opción *Graph Tree*

2. En la parte superior dar clic en *Add* para añadir o crear un nuevo directorio como se muestra en la figura 5.1.18:

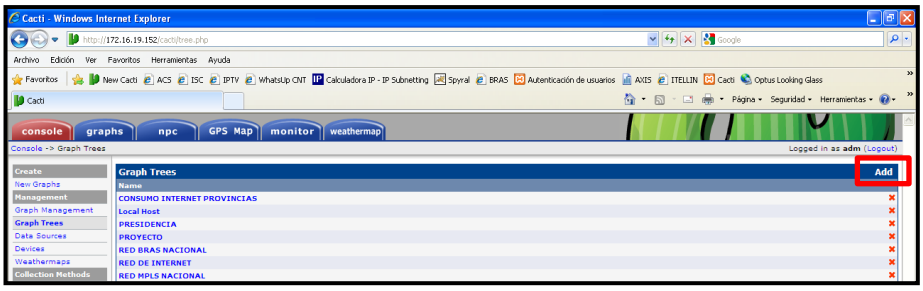


Figura 5.1.18: Adición de un nuevo directorio[1]

3. A continuación aparecerá el cuadro que se muestra en la figura 5.1.19 en el cual se deberá colocar el nombre del directorio que se desee crear, además en la opción *Sorting Type* seleccionar una de las opciones para determinar el orden de los subdirectorios creados en cada uno de los árboles. Se sugiere *Manual Ordering*, en caso necesario se puede usar *Alphabetic Ordering* como se muestra en la figura 5.1.19:

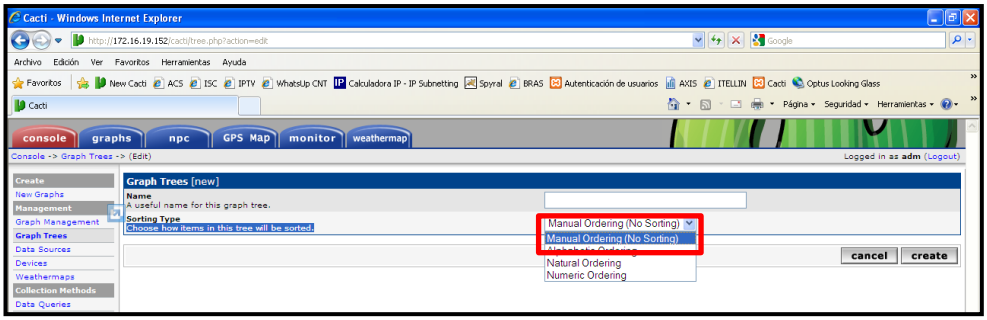


Figura 5.1.19: Parámetros de configuración del equipo[1]

4. En el caso de elegir un directorio, se debe elegir un subdirectorio o crearlo. Ingresar a un directorio creado y en la opción *Tree Items* colocar *add* como se muestra en la figura 5.1.20:

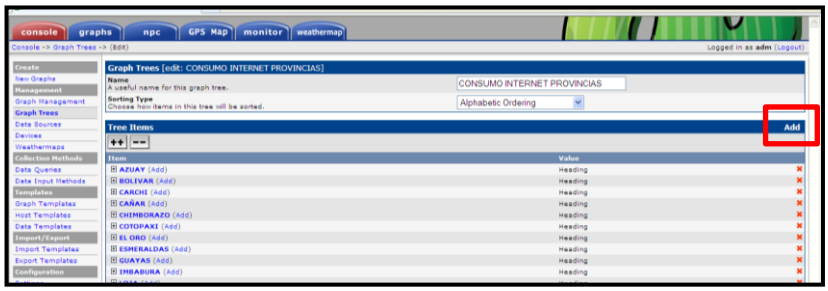


Figura 5.1.20: Creación de subdirectorios[1]

5. En el cuadro que aparece colocar el nombre del subdirectorio, el tipo de item y el titulo como se muestra en la figura 5.1.21:

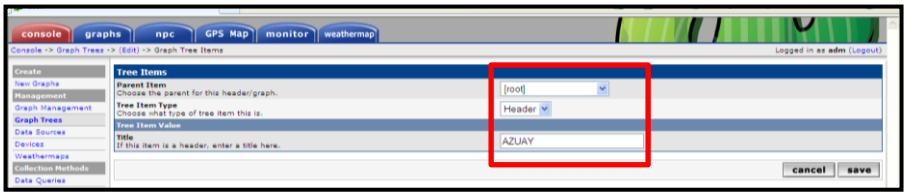


Figura 5.1.21: Parámetros de configuración de un subdirectorio[1]

Nota: Los subdirectorios se deben configurar como *Header*.

6. Insertar gráficas en un subdirectorio, mediante el link *Add* como se muestra en la figura 5.1.22:

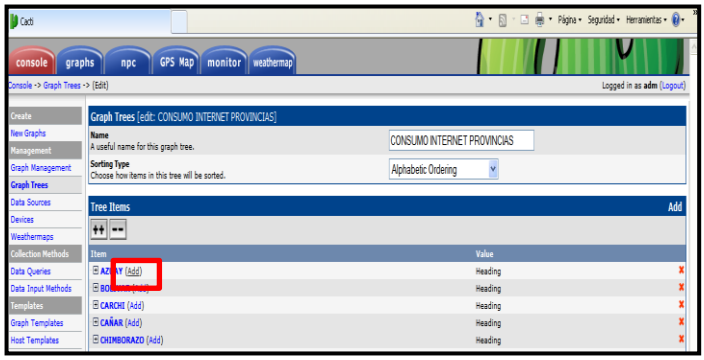


Figura 5.1.22: Inserción de gráficas en un subdirectorio[1]

7. Elegir en *Tree Items Type* la opción *Graph* con la cual se selecciona el gráfico que se desea añadir como se muestra en la figura 5.1.23:

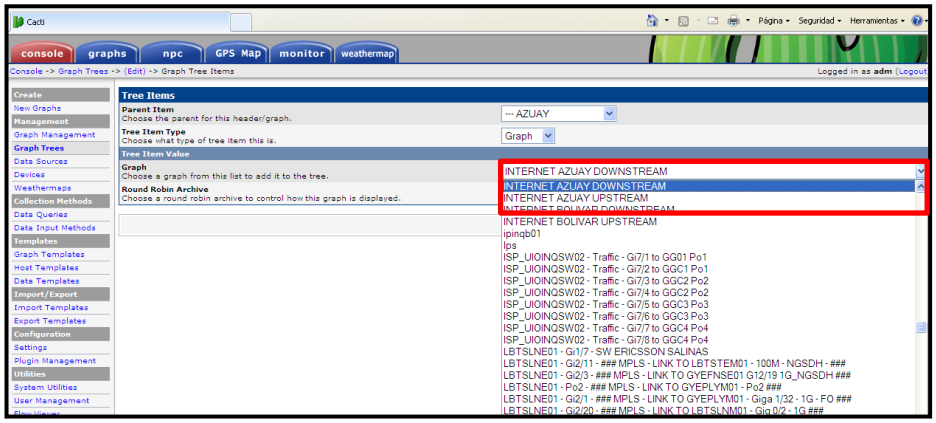


Figura 5.1.23: Selección del gráfico en la opción Graph[1]

8. Configurar las actualizaciones de las gráficas cada 5 minutos como se muestra en la figura 5.1.24:

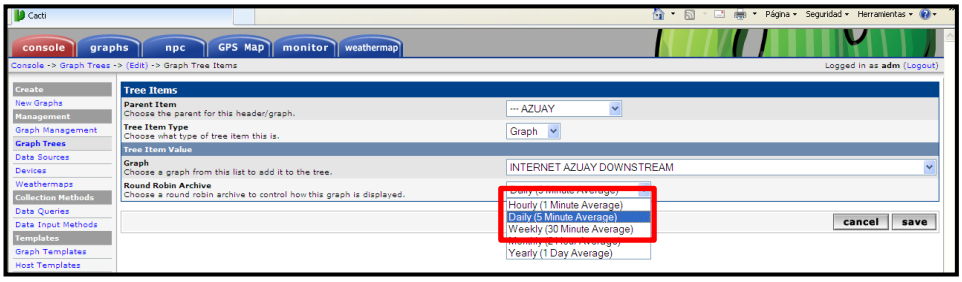


Figura 5.1.24: Actualización de gráficos[1]

5.1.6 TAB GRAPH

A continuación se muestra la respectiva descripción de cada uno de los componentes del *Tab Graph*.

5.1.6.1 VISUALIZACIÓN DE GRÁFICOS

Se observa en la parte izquierda los directorios creados. Para la visualización de gráficos seguir los pasos que se muestran a continuación:

1. Seleccionar previamente uno de los subdirectorios para apreciar los gráficos correspondientes como se muestra en la figura 5.1.25:

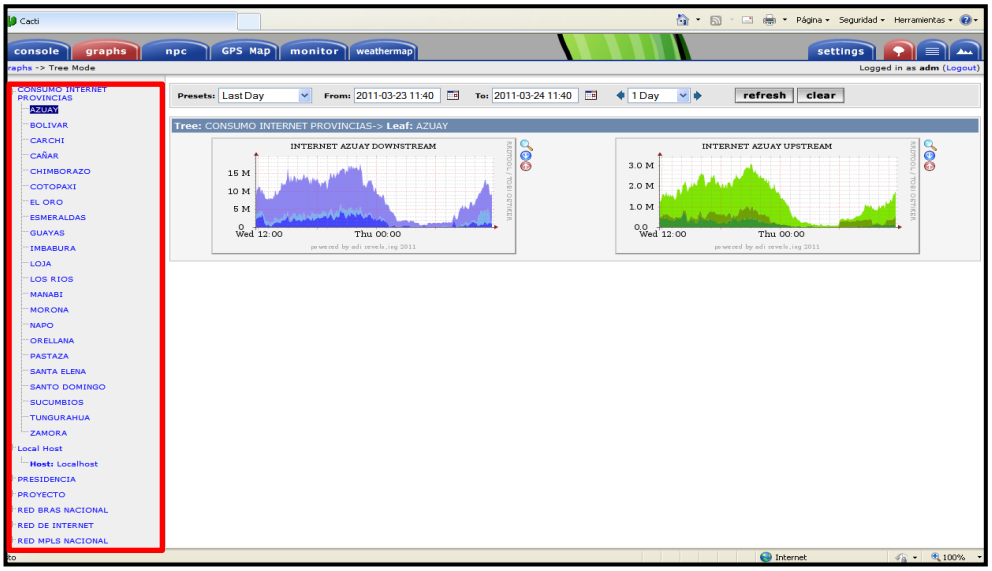


Figura 5.1.25: Visualización de gráficos en directorios y subdirectorios[1]

5.1.6.2 EJEMPLO DE ANÁLISIS DE GRÁFICOS

En los siguientes gráficos 5.1.26 y 5.1.27 se muestra el tráfico en la red MPLS CNT del consumo de internet.

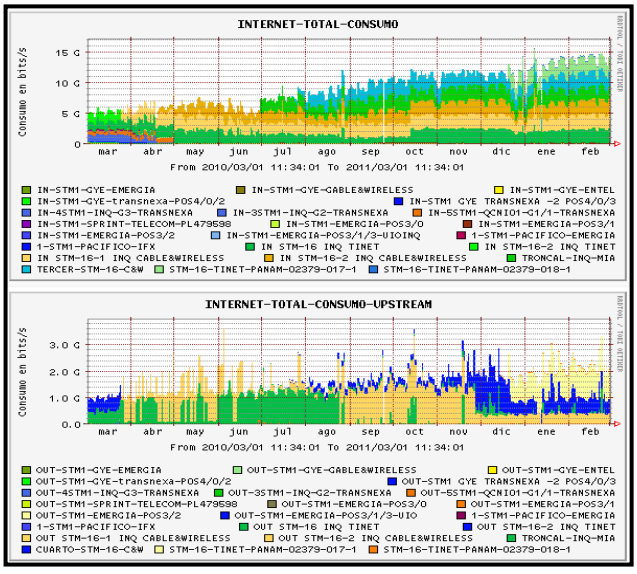


Figura 5.1.26: Tráfico del crecimiento del último año de las salidas internacionales de CNT [1]

En el gráfico se puede observar el consumo de tráfico de las salidas internacionales a internet, este es el consumo total de los clientes de CNT se observa el gran crecimiento que ha tenido en el último año, donde hubo una triplicación en la cantidad de tráfico necesario para satisfacer a los clientes, uno de los aspectos a tomar en cuenta es que los proveedores de los enlaces han cambiado por ese motivo las variaciones en los gráficos donde cada color representa un enlace.

La capacidad inicial de trasmisión de la red fue de 6 Gbps de downstream y 1.5 Gbps de upstream, esta se ha incrementado gradualmente para satisfacer el crecimiento del mercado pues cada vez se tiene un mayor número de clientes que desean internet, cabe recalcar que este incremento ha sido posible gracias a la instalación de equipos de CNT en el NAP de las Américas y a la compra de capacidad de trasmisión en los cables submarinos llegando en la actualidad a tener 16Gpbs de upstream y unos 3.6Gbps de downstream.

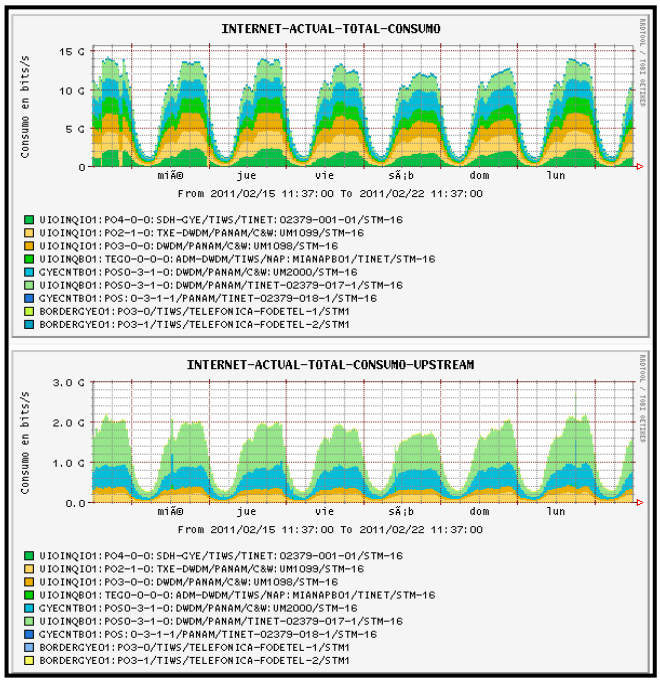


Figura 5.1.27: Consumo semanal de internet[1]

En estos gráficos se observa de manera más detallada el consumo de tráfico de internet de una semana, donde se puede observar que de lunes a jueves el pico de tráfico alcanzado es similar mientras que de viernes a domingo este disminuye, esto se debe al comportamiento de los clientes y a pesar que se puede generar un perfil

puede haber días en los que los picos sean diferentes ya que depende del número de clientes conectados así como del tipo de uso que estos le den.

5.1.7 TAB MONITOR

Muestran un esquema de cada Host activado en la opción *Console* como *Monitor Host* y sus respectivas estadísticas, además incluye una alarma para indicar algún tipo de incidencia como se muestra en la figura 5.1.28:

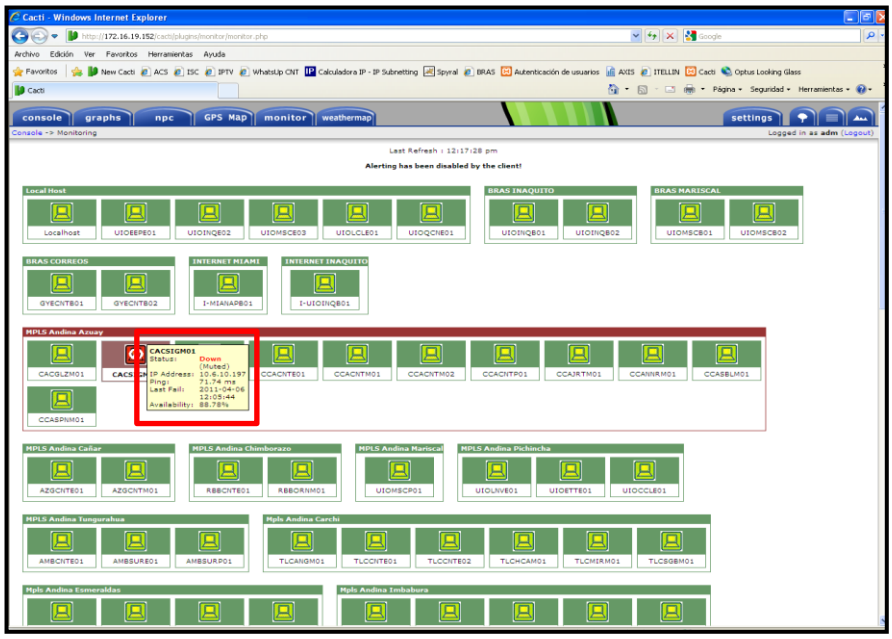


Figura 5.1.28: Monitoreo de equipos[1]

El siguiente cuadro indica el estado de los Host es decir, si está funcionando correctamente se presenta de color verde, si está recuperando la conexión se presenta de color celeste y si tiene algún problema se presentará de color rojo como se muestra en la figura 5.1.29:

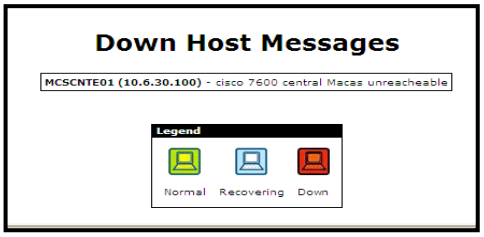


Figura 5.1.29: Estado de los host [1]

Se puede observar el estado del equipo, la dirección IP, y la disponibilidad, además visualizar las gráficas relacionadas con dicho equipo como se muestra en la figura 5.1.30:

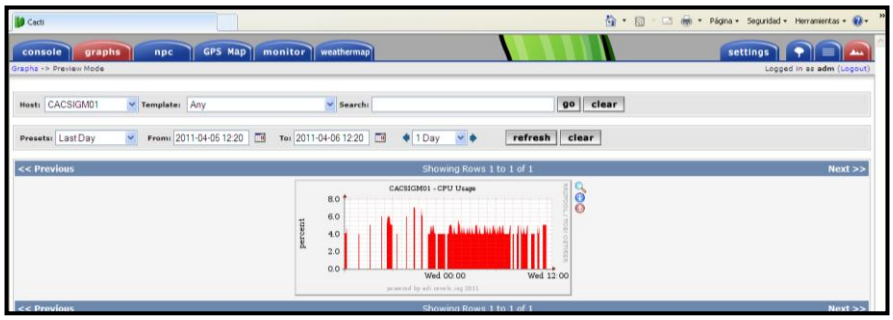


Figura 5.1.30: Visualización de parámetros del equipo[1]

5.1.8 TAB GPS MAP

Esta opción usa *GoogleMaps* y permite identificar claramente en el mapa de Ecuador cada uno de los equipos y nodos situados a lo largo del país.

Presenta tres opciones de visualización que se indican a continuación:

5.1.8.1 MAPA

En la parte izquierda del mapa se muestran dos opciones:

1. La primera opción permite reducir o ampliar el mapa.

2. La segunda opción permite realizar una vista panorámica de los nodos ya sea hacia la derecha, izquierda, arriba y abajo como se muestra en la figura 5.1.31:

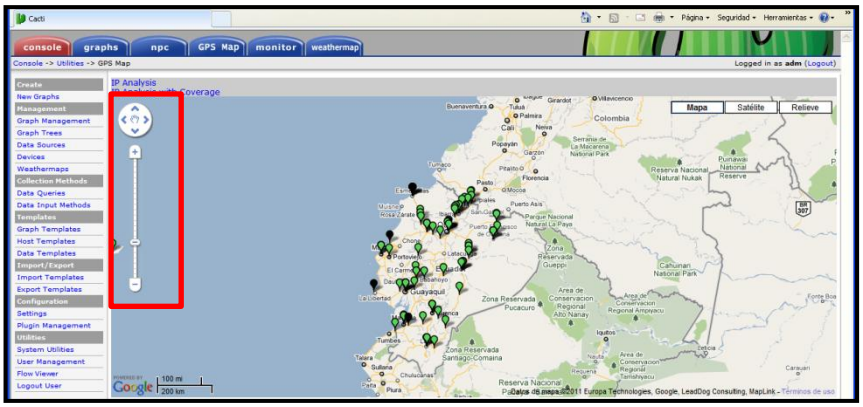


Figura 5.1.31: Opción Mapa[1]

5.1.8.2 SATÉLITE

Esta opción permite una visualización vía satélite como se muestra en la figura 5.1.32:

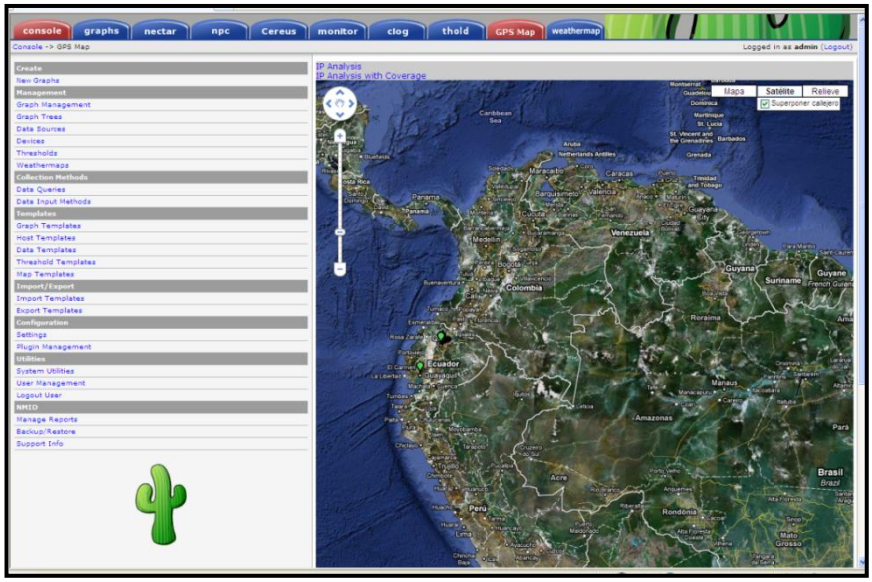


Figura 5.1.32: Opción Satélite[1]

5.1.8.3 RELIEVE

Esta opción permite visualizar el relieve del mapa como se muestra en la figura 5.1.33:

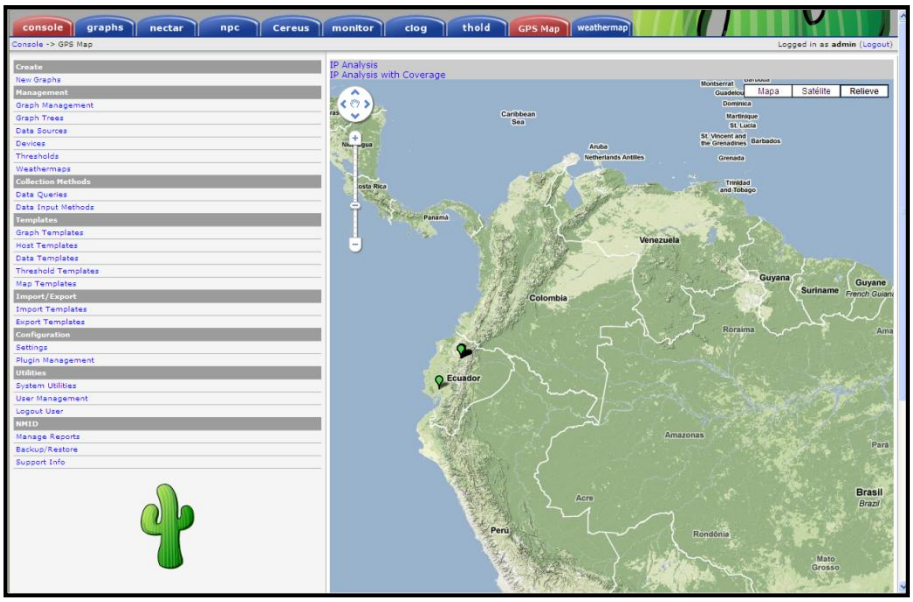


Figura 5.1.33: Opción Relieve[1]

Al colocarse con el puntero sobre algún nodo se despliega cierta información como la dirección IP, disponibilidad, tipo y latencia como se indica en la figura 5.1.34:

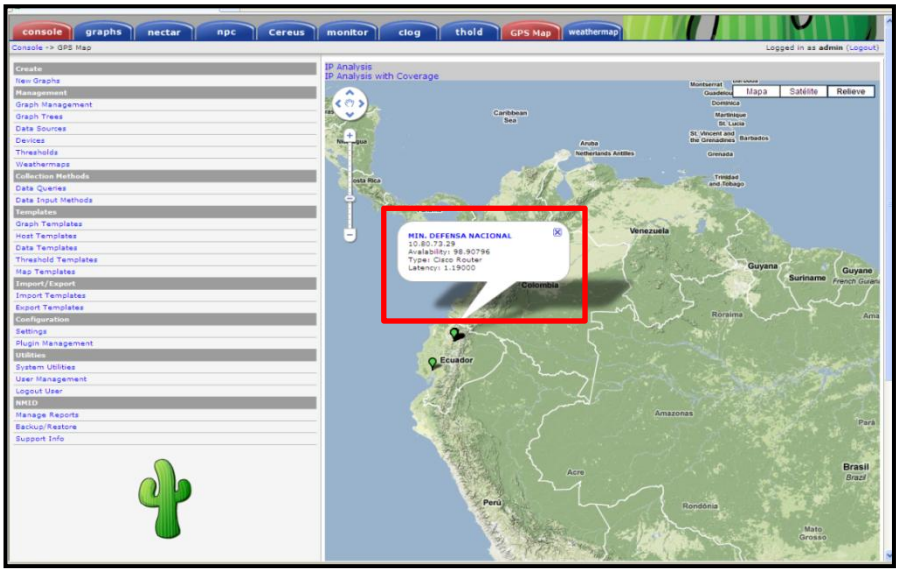


Figura 5.1.34: Visualización de la información básica de un equipo[1]

5.1.9 TAB WEATHERMAP

Permite generar esquemas de red donde se pueden añadir gráficos que CACTI tiene por defecto.

Para crear un nuevo *Weathermap* se debe seguir los pasos descritos a continuación:

1. En la opción de *Weathermap* seleccionar la opción *Editor* como se muestra en la figura 5.1.35:

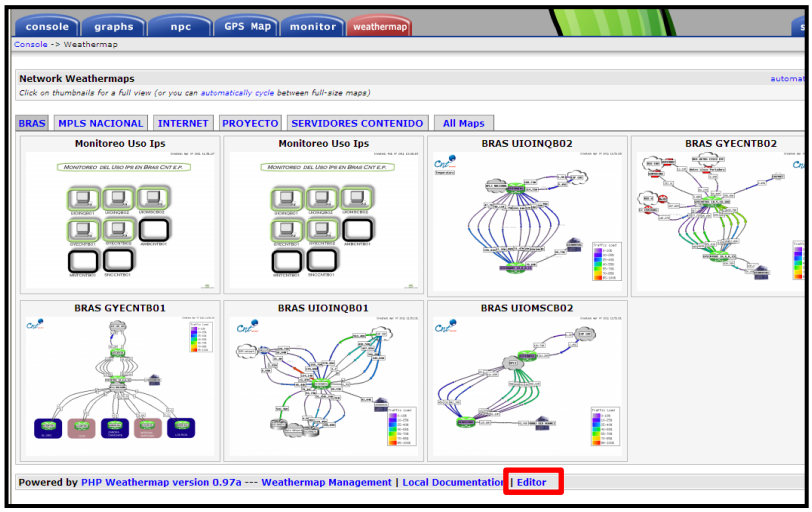


Figura 5.1.35: Opción Editor[1]

2. Colocar el nombre del nuevo mapa que se desea crear. En el caso de que se requiera modificar la configuración de un mapa ya existente seleccionar en la opción *Open An Existing Map* el nombre del mapa como se muestra en la figura 5.1.36:

Figura 5.1.36: Selección del mapa a modificar[1]

3. En la ventana que aparece a continuación se encuentran las siguientes opciones que permitirán administrar los mapas de las redes de mejor manera:

   - ✓ ***Change File:*** Permite escoger el nombre de un equipo para poder ser editado como se muestra en la figura 5.1.37

   - ✓ ***Add node:*** Permite añadir un nodo y colocar los datos correspondientes además incluye la opción para escoger la imagen deseada en la mapa ya sea un router, switch, nube,etc, como se muestra en la figura 5.1.37

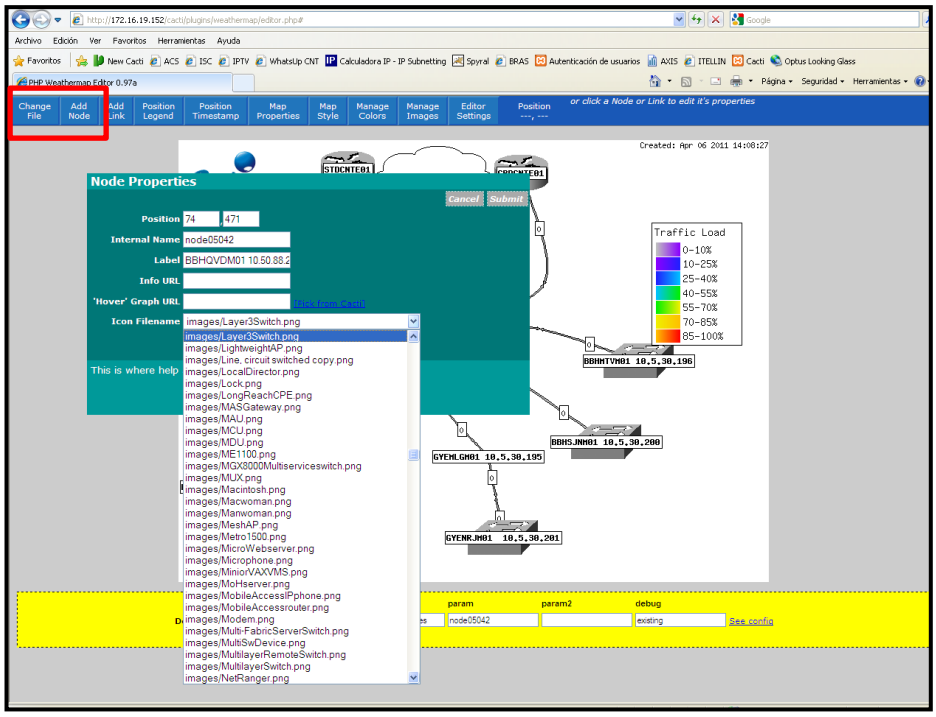


Figura 5.1.37: Administración de mapas[1]

4. En la opción *Pick from*, Cacti permite colocar la interfaz correspondiente a dicho nodo como se muestra en la figura 5.1.38:

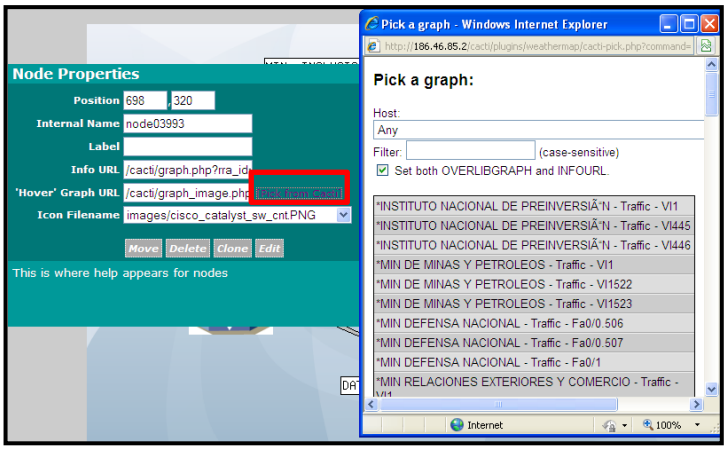


Figura 5.1.38: Opción Pick from[1]

- ✓ ***Add link:*** Permite añadir un enlace y colocar la información necesaria de dicho enlace como se muestra en la figura 5.1.39:

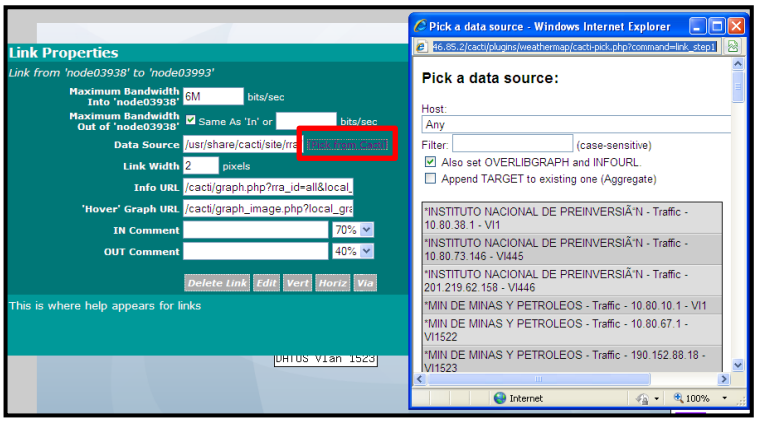


Figura 5.1.39: Opción Add Link[1]

En la opción *Pick from Cacti* se puede buscar la interfaz relacionada con el equipo con su respectivo gráfico.

- ✓ ***Map properties*:** Indica los datos configurados en el mapa como se muestra en la figura 5.1.40:

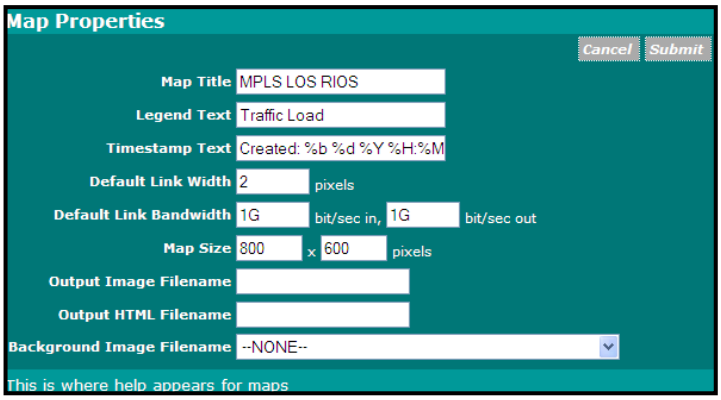


Figura 5.1.40: Opción Map Properties[1]

- ***Map style:*** Permite establecer ciertos parámetros para dar un formato de presentación como se muestra en la figura 5.1.41:

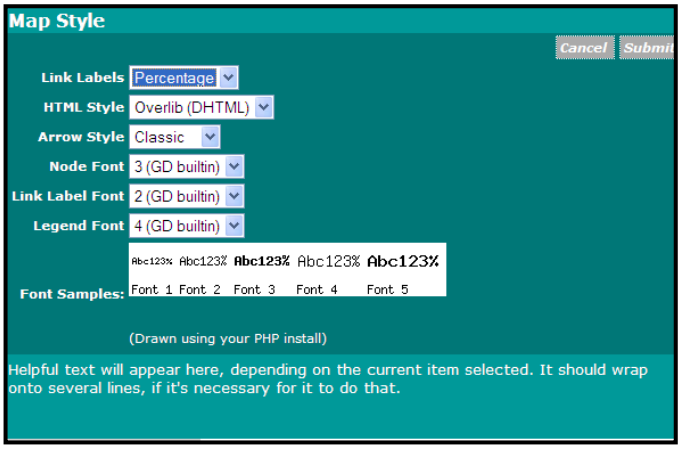


Figura 5.1.41: Opción Map Style[1]

- ***Manage Colors:*** Ésta opción no se encuentra habilitada todavía en la plataforma. Permite administrar los colores de cada uno de elementos insertados en el mapa.

- ***Manage images:*** Esta opción no se encuentra habilitada todavía. Permite administrar las imágenes insertadas en el mapa.

- ***Editor settings:*** Es un editor de configuraciones dependiendo de los requerimientos.

Todas las opciones mencionadas en el punto 5.1.9 se muestran en la figura 5.1.42:

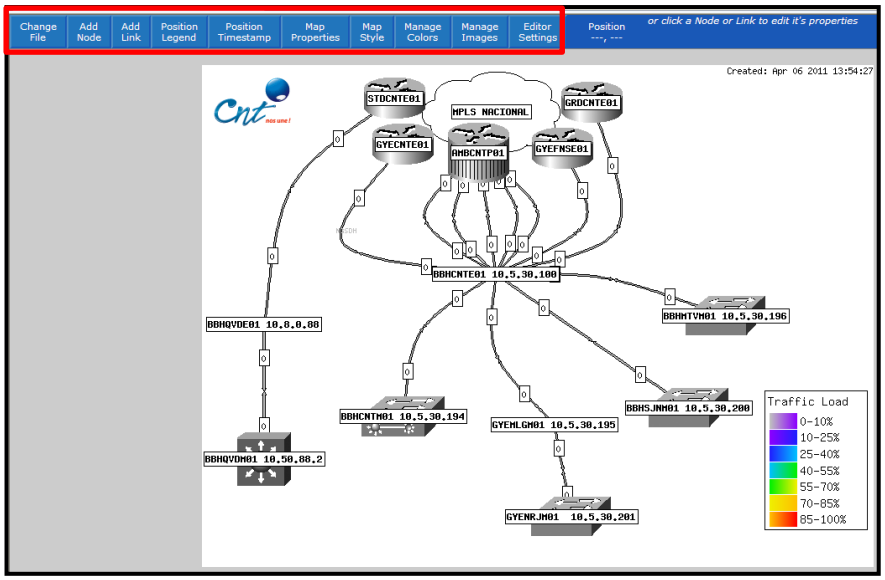


Figura 5.1.42: Opciones del Weathermap[1]

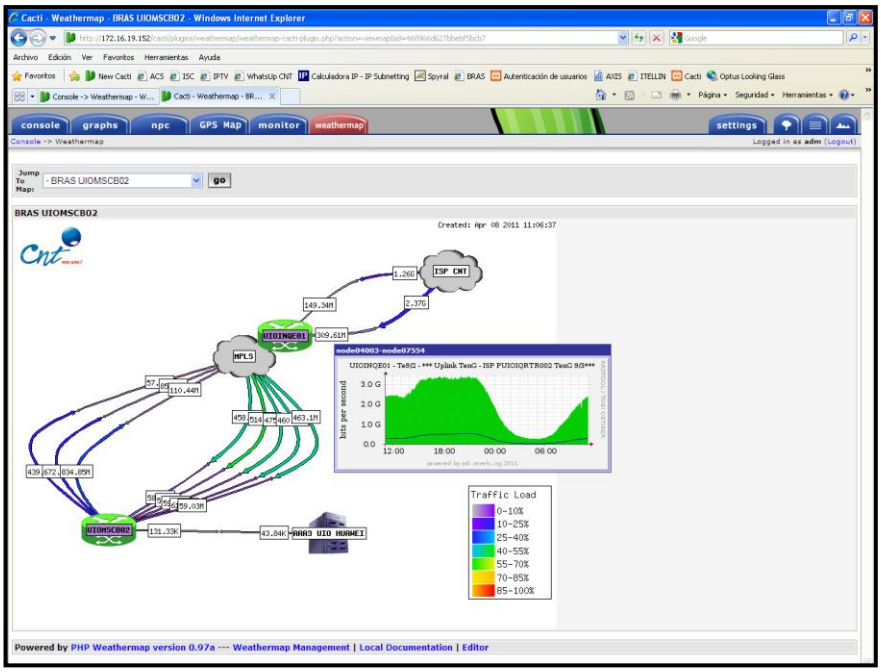


Figura 5.1.43: Ejemplo de un mapa creado[1]

Al colocar con el puntero en uno de los enlaces se despliega el gráfico correspondiente.

5.1.10 TAB NPC

Proporciona una pequeña interfaz hacia otro sistema de monitoreo denominado Nagios, cabe recalcar que CACTI solamente permite la visualización de los equipos configurados en Nagios.

En la parte superior se encuentran tres tablas que permiten monitorear el estado de la plataforma Nagios, de los equipos configurados y de los servicios levantados como se muestra en la figura 5.1.44.

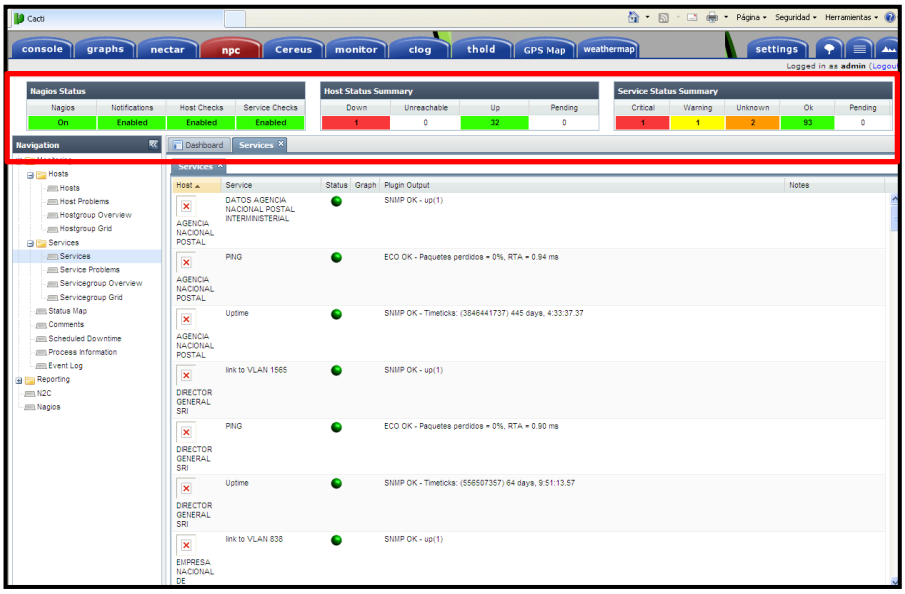


Figura 5.1.44: Monitoreo del estado de la plataforma Nagios[1]

En la parte izquierda se encuentran una serie de opciones que se muestran a continuación:

5.1.10.1 HOSTS

Permite visualizar los equipos configurados en la plataforma Nagios, presentan cuatro pestañas: *Hosts, Hostgroup Problems, Hostgroup Overview, Hostgroup Grid* como se muestra en la figura5.1.45:

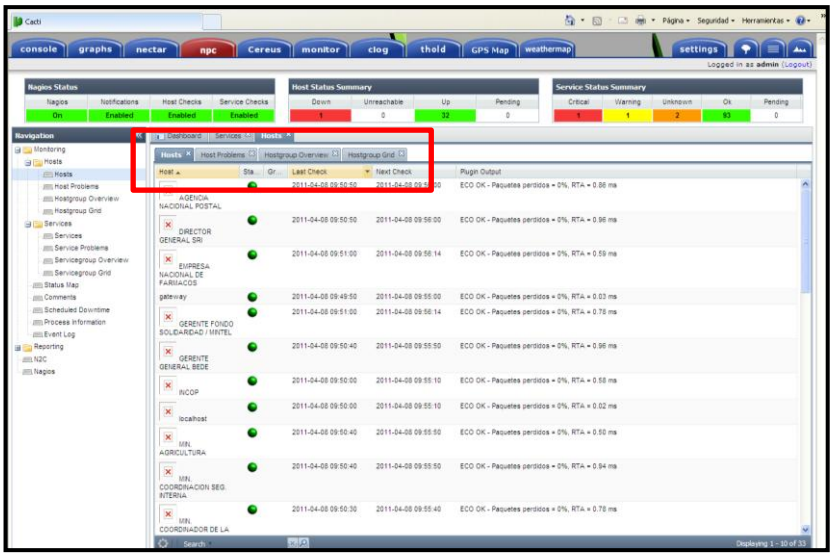


Figura 5.1.45: Opciones Hosts de Nagios[1]

5.1.10.1.1 HOST

Se pueden visualizar, Hosts configurados, su estado, fechas de chequeo e información del ping out como se muestra en la figura 5.1.46:

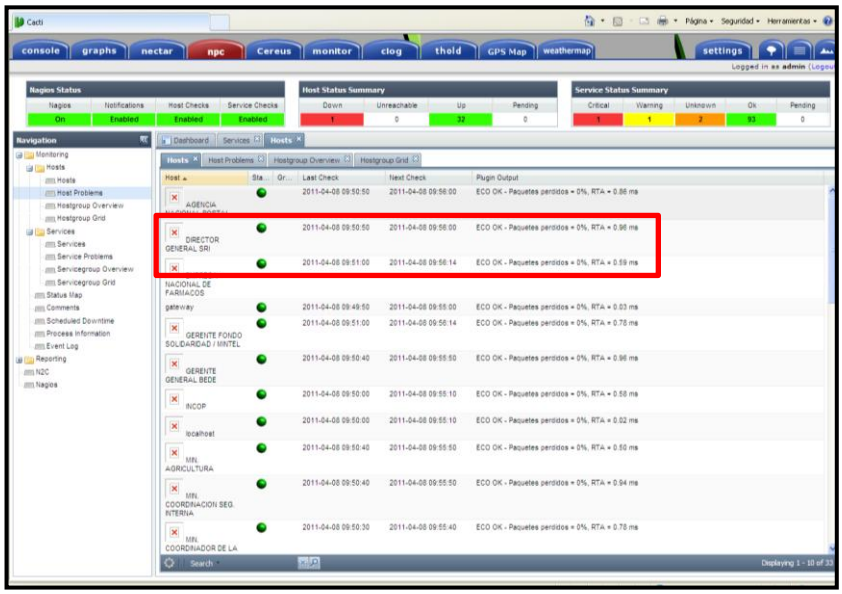


Figura 5.1.46: Visualización del estado del host[1]

5.1.10.1.2 HOSTSGROUP PROBLEMS

Permite visualizar si algún Host presenta problemas como se muestra en la figura 5.1.47:

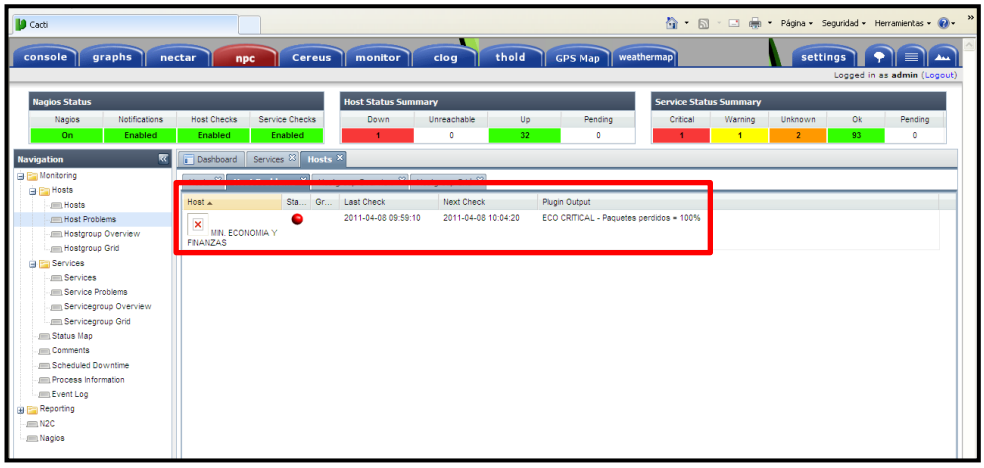


Figura 5.1.47: Visualización de problemas que presenta un host[1]

5.1.10.1.3 HOSTSGROUP OVERVIEW

Se puede visualizar el estado de los equipos ya sea crítico, advertencia y en correcto funcionamiento como se muestra en la figura 5.1.48:

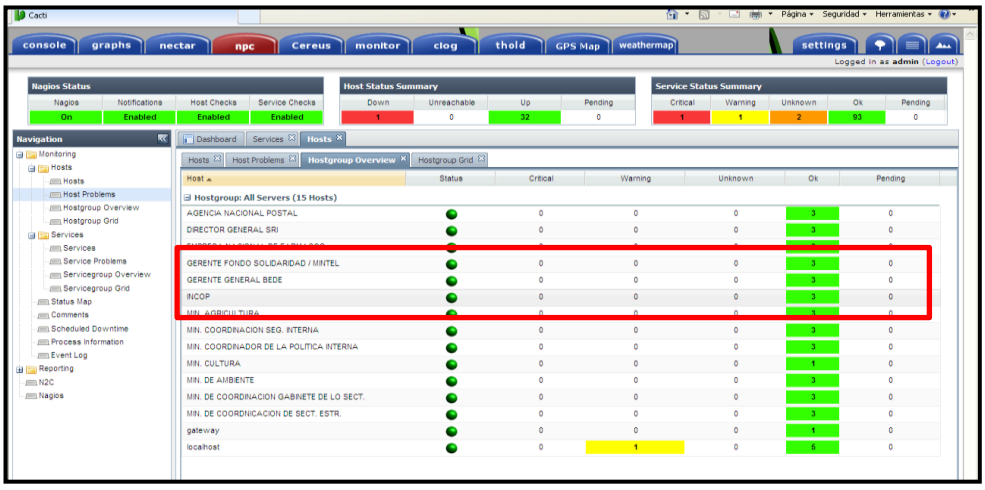


Figura 5.1.48: Visualización de los estados de un equipo[1]

5.1.10.1.4 HOSTSGROUP GRID

Presenta el estado de los equipos configurados, además del porcentaje de paquetes perdidos y el tiempo de respuesta de cada uno como se muestra en la figura 5.1.49:

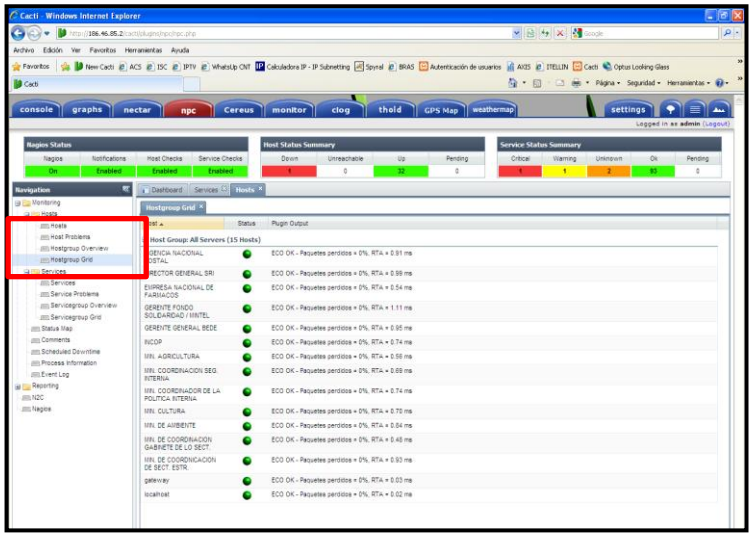


Figura 5.1.49: Visualización del porcentaje de paquetes perdidos y el tiempo de respuesta [1]

5.1.10.2 SERVICES

Permite visualizar los servicios configurados en la plataforma Nagios, presentan tres pestañas: *Services, Servicegroup Overview, Service Problems,* sus respectivas descripciones se muestran a continuación:

5.1.10.2.1 SERVICES

NCP presenta los registros de tres servicios: *Uptime, Ping, Acceso Snmp* como se muestra en la figura 5.1.50:

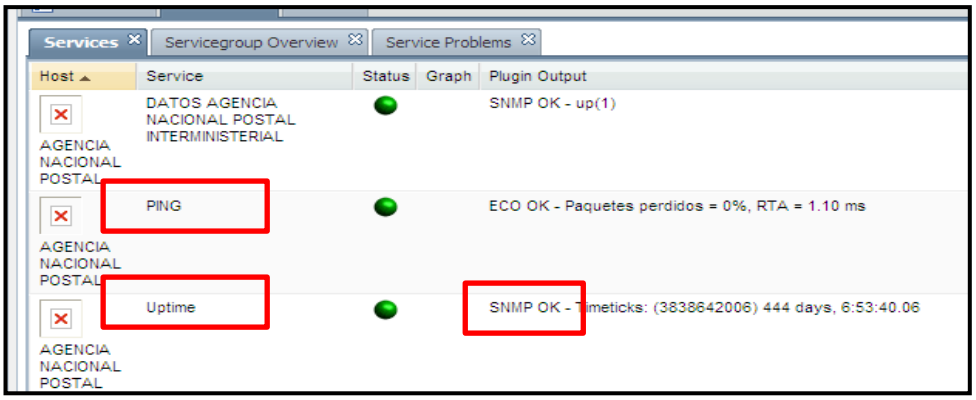


Figura 5.1.50: Servicios activos en Nagios[1]

5.1.10.2.2 SERVICES PROBLEMS

Permite visualizar si algún Host presenta un problema en el servicio como se muestra en la figura 5.1.51:

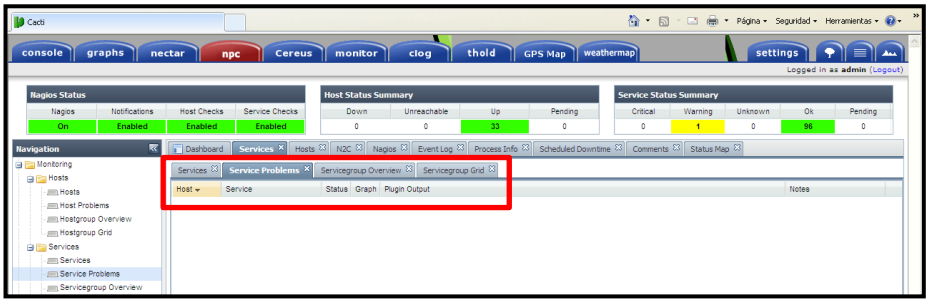


Figura 5.1.51: Visualización de problemas en el servicio[1]

Además presentan opciones como: *servicegroup overview*, *servicegroup grid*, *status map*, *comments*, *Scheduled Downtime*, las mismas que no se encuentran aún habilitados pero permitirán obtener cierta información de los servicios para un mejor monitoreo de los mismos.

5.1.10.3 PROCESS INFORMATION

Permite visualizar la información de los equipos como se muestra en la figura 5.1.52:

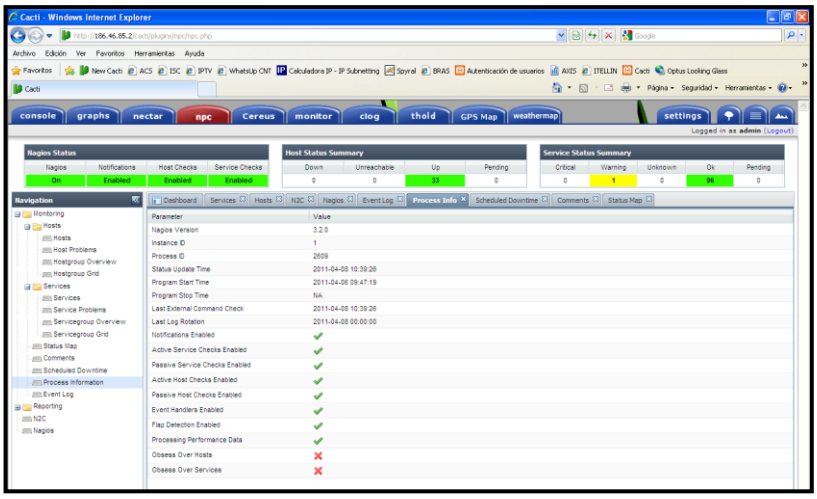


Figura 5.1.52: Visualización de la información del equipo[1]

5.1.10.4 EVENT LOG

Permite obtener información de las incidencias presentadas ya sea en los Host o los servicios como se muestra en la figura 5.1.53:

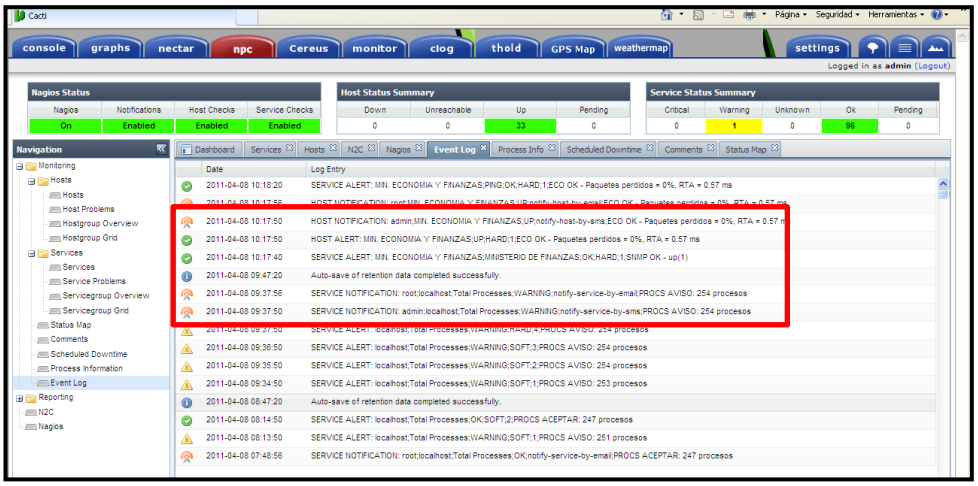


Figura 5.1.53: Visualización de los logs del equipo[1]

5.1.10.5 REPORTING

Presenta las opciones *N2C y Nagios*, las cuales permiten el ingreso a la plataforma Nagios para realizar las configuraciones respectivas como se muestra en la figura 5.1.54:

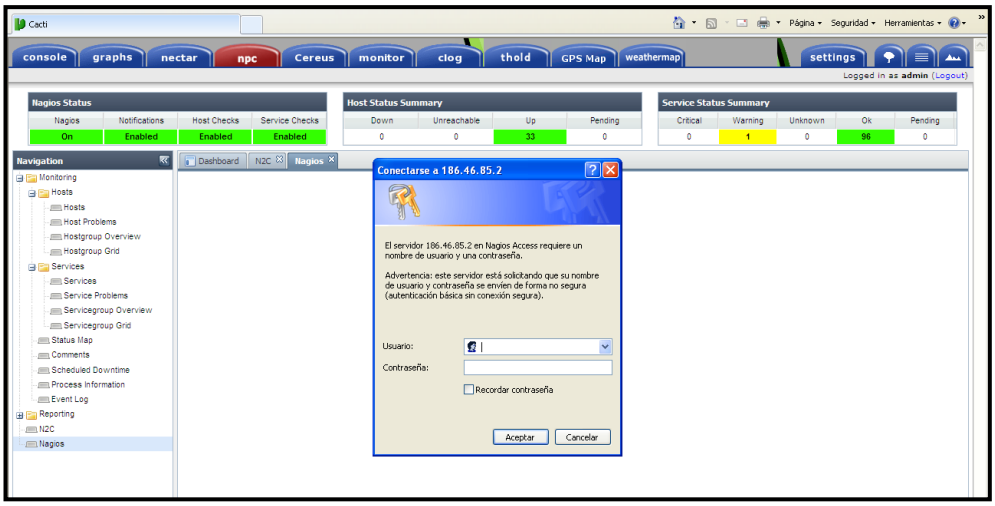


Figura 5.1.54: Ingreso a la plataforma Nagios[1]

Se han implementado nuevos plugins en el CACTI y son los siguientes:

5.1.11 TAB THOLDS

Permite generar alertas basadas en determinados valores, los mismos que pueden ser comparados en tiempos permitiendo realizar estadísticas y mostrar el estado de los equipos, presenta dos pestañas: *Thresholds, Hosts Status.*

5.1.11.1 THRESHOLDS

Permite visualizar el tráfico que pasa por las distintas interfaces configuradas en los equipos y generar una alarma cuando llegue a un tope máximo de 1.5 MHZ, este valor puede ser cambiado dependiendo de los requerimientos de monitoreo como se muestra en la figura 5.1.55:

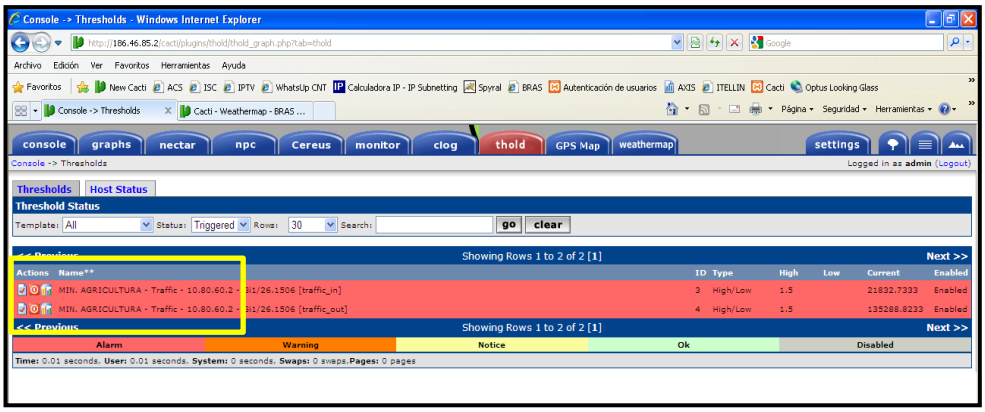


Figura 5.1.55: Visualización del tráfico que pasa por las interfaces configuradas en los equipos [1]

Además presenta la opción de visualización de gráficos de las interfaces y la opción para editar la información con el fin de generar una alarma como se muestra en la figura 5.1.56:

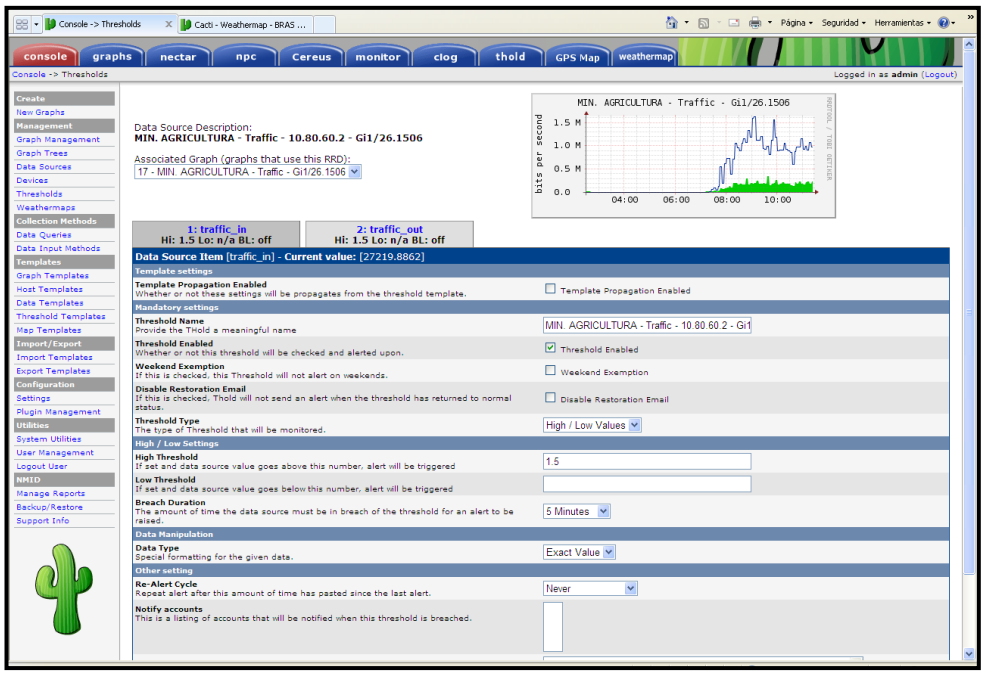


Figura 5.1.56: Visualización de gráficos de las interfaces[1]

5.1.11.2 HOST STATUS

Permite visualizar el estado, disponibilidad en tiempo real y el Hostname de los Host configurados como se muestra en la figura 5.1.57:

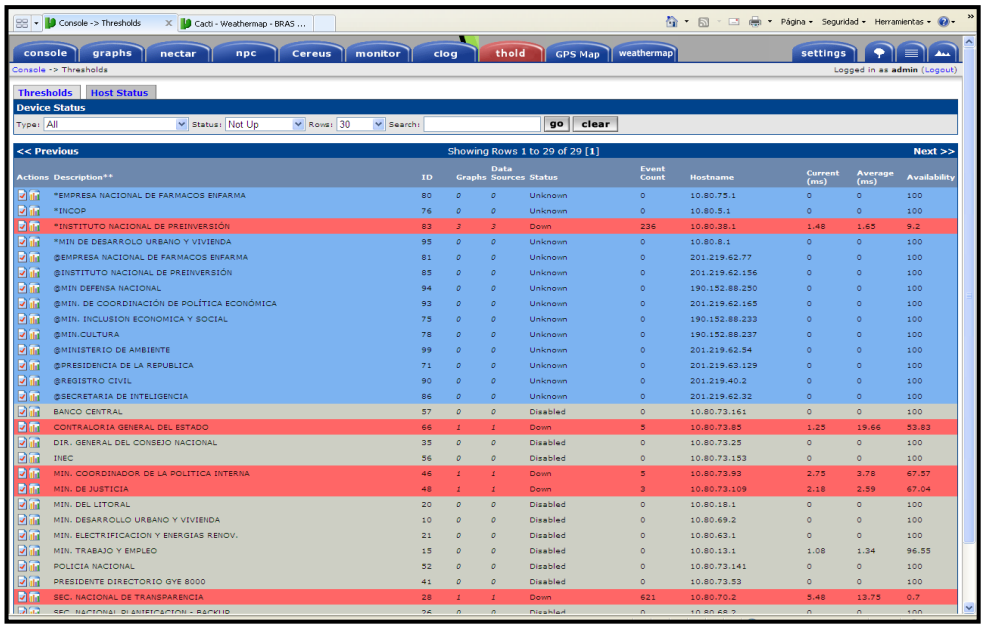


Figura 5.1.57: Visualización de la disponibilidad de los equipos[1]

5.1.12 TAB CLOG

Es un archivo o registro de las incidencias que ocurren en el sistema y permite revisar las actividades que se realizan en el mismo, además se puede verificar los cambios de estado de los host, cabe recalcar que los archivos que se encuentran en color rojo son de gran importancia y requiere mayor atención como se muestra en la figura 5.1.58:

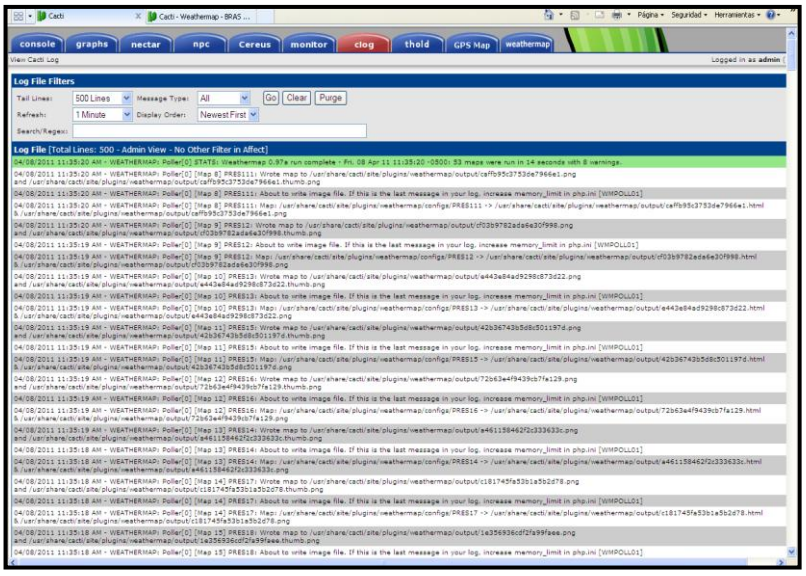


Figura 5.1.58: Visualización del registro de incidencias[1]

5.1.13 TAB CEREOUS

Sirve para la generación de reportes de las gráficas correspondientes a cada uno de los equipos.

Para la creación de estos reportes seguir los siguientes pasos:

1. Ingresar al comando *NMID* que se encuentra en la parte inferior izquierda de la pantalla e ingresar a la opción *Manage Reports* como se indica en la figura 5.1.59:

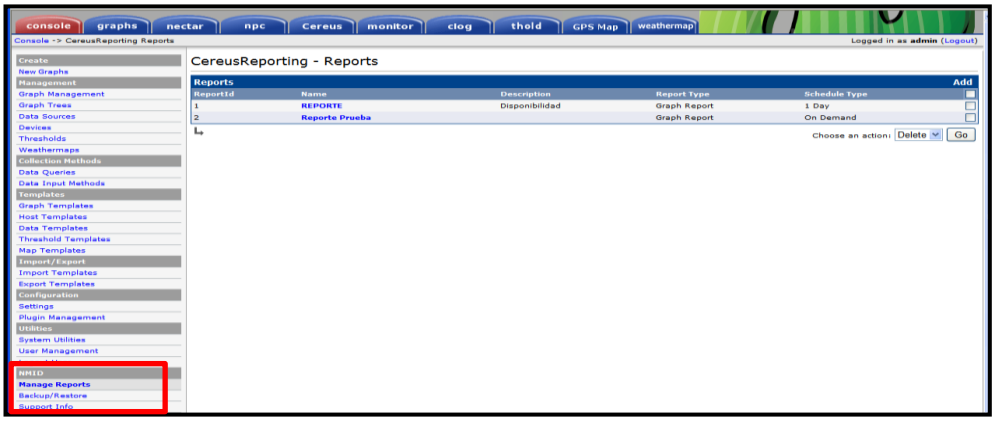


Figura 5.1.59: Ingreso a la opción Manage Report [1]

2. Para añadir un reporte escoger la opción *Add* en la parte superior derecha como se indica en la figura 5.1.60:

Figura 5.1.60: Selección de la opción Add [1]

A continuación establecer los parámetros para el nuevo reporte como por ejemplo:

- ✓ ***Report Name:*** Nombre del nuevo reporte

- ✓ ***Report Description:*** Es una breve descripción del proyecto que aparecerá antes de los gráficos
- ✓ ***Report Type:*** Escoger el tipo de reporte en este caso escoger la opción *Graph Report.*
- ✓ ***Default Report Timespan:*** Esta opción permite escoger el tiempo en el que se desee obtener el reporte ya sea en un mes, un año, una hora, 2 horas etc.

  Con la opción *On Demand* se obtiene reportes continuamente.
- ✓ ***Report Page Size:*** Permite escoger el tamaño de la hoja del reporte se sugiere usar la opción *A4.*
- ✓ ***Report Page Orientation:*** Permite escoger la orientación de la página del reporte se sugiere escoger la opción *Portrait.*
- ✓ ***Report Graph Format:*** Permite establecer el orden de los gráficos ya sea 2 gráficos en columnas o la opción Default que permite colocar un gráfico en una columna.
- ✓ ***Report Output Format:*** Permite establecer el reporte en dos tipos de formato ya sea en PDF o en HTML, se sugiere usar el formato PDF ya que es de fácil manejo para el usuario.

3. Finalmente escoger la opción *Save* para guardar los parámetros creados como se muestra en la figura 5.1.61:

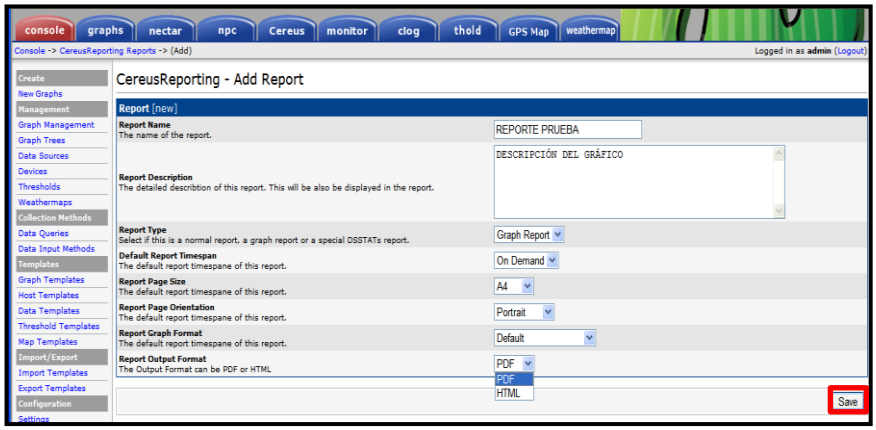


Figura 5.1.61: Guardar configuración mediante la opción Save[1]

4. Posteriormente se podrá observar que el reporte ya se encuentra creado como se indica en la siguiente figura 5.1.62:

Figura 5.1.62: Visualización del reporte creado[1]

5. Para poder añadir gráficos al reporte creado escoger la opción *Graphs* y seleccionar el nombre del reporte como se indica en la figura 5.1.63:

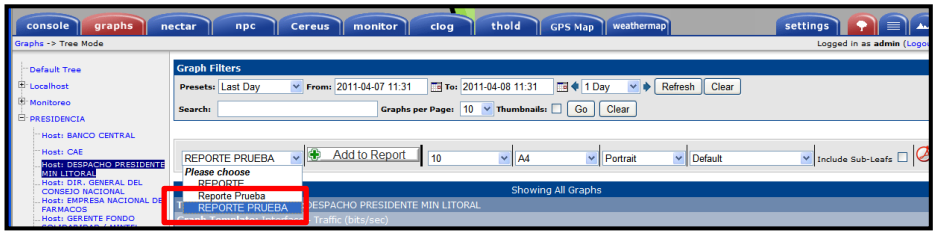


Figura 5.1.63: Selección del nombre del reporte[1]

6. A continuación seleccionar los gráficos que serán incluidos en el reporte, para su respectiva selección dar un clic en un visto que se encuentra junto al gráfico en la parte derecha como se indica en la figura 5.1.6.4:

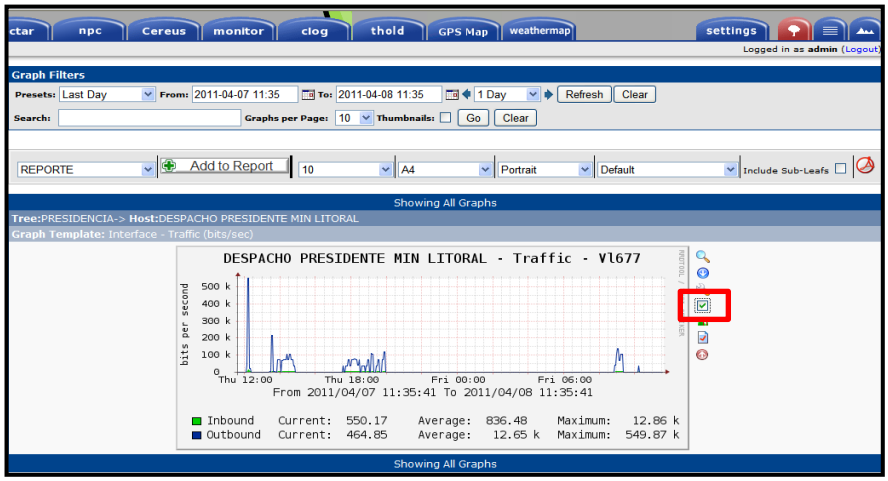


Figura 5.1.64: Selección de gráficos a incluir en el reporte[1]

7. Para la visualización del reporte ingresar a la opción *CEREOUS* y en el nombre del reporte escoger la opción *Generate Report* como se indica en la figura 5.1.65:

Figura 5.1.65: Opción Cereous [1]

8. Posteriormente aparecerá una pantalla que muestra las configuraciones de todos los parámetros previamente establecidos, es necesario mencionar que se debe especificar el tiempo de monitoreo de los gráficos y finalmente escoger la opción *Create* como se muestra en la figura 5.1.66:

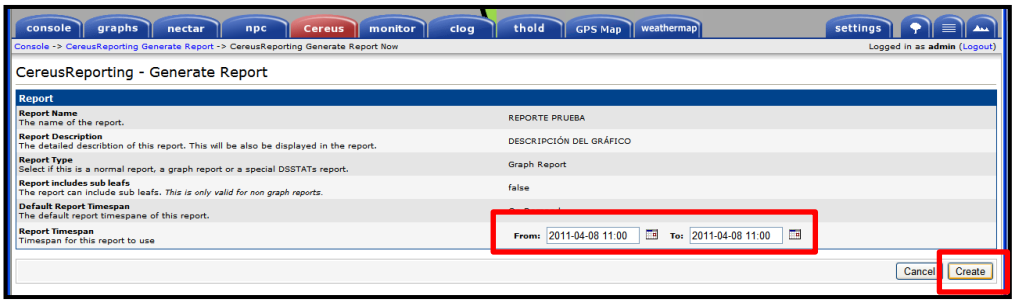


Figura 5.1.66: Parámetros del tiempo de monitoreo[1]

9. Automáticamente aparecerá un cuadro para la descarga del reporte generado en PDF el cual permitirá la visualización del reporte ya creado como se muestra en la figura 5.1.67:

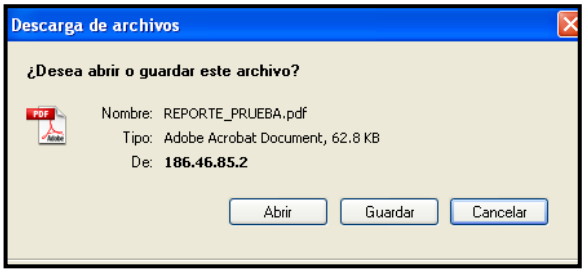


Figura 5.1.67: Descarga del reporte[1]

10. Guardar el reporte en una carpeta para luego poder ejecutarlo como se muestra en la figura 5.1.68:

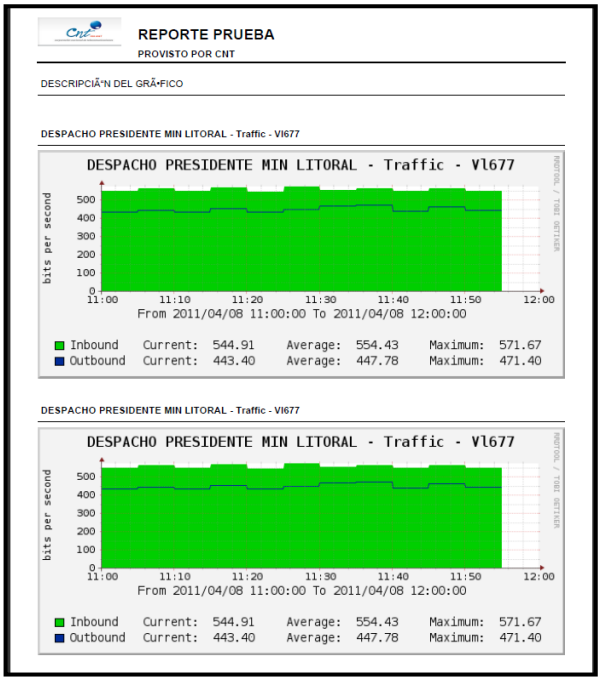


Figura 5.1.68: Visualización del reporte[1]

5.1.14 TAB NECTAR

Nectar es un plugin que permite gestionar el envío de correos programados, estos correos contienen los gráficos que Cacti presenta junto con algunas opciones extras como se muestra en la figura 5.1.69:

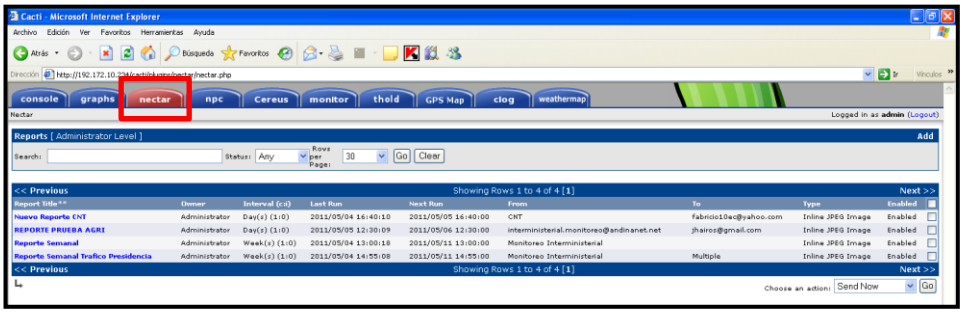


Figura 5.1.69: Selección de la opción Nectar[1]

5.1.14.1 CREACIÒN DE UN REPORTE

Para crear un reporte dar clic en la opción *Add* y posteriormente se desplegará una pantalla en la cual se debe agregar los parámetros del reporte que serán enviados vía correo electrónico como se muestra en la figura 5.1.70:

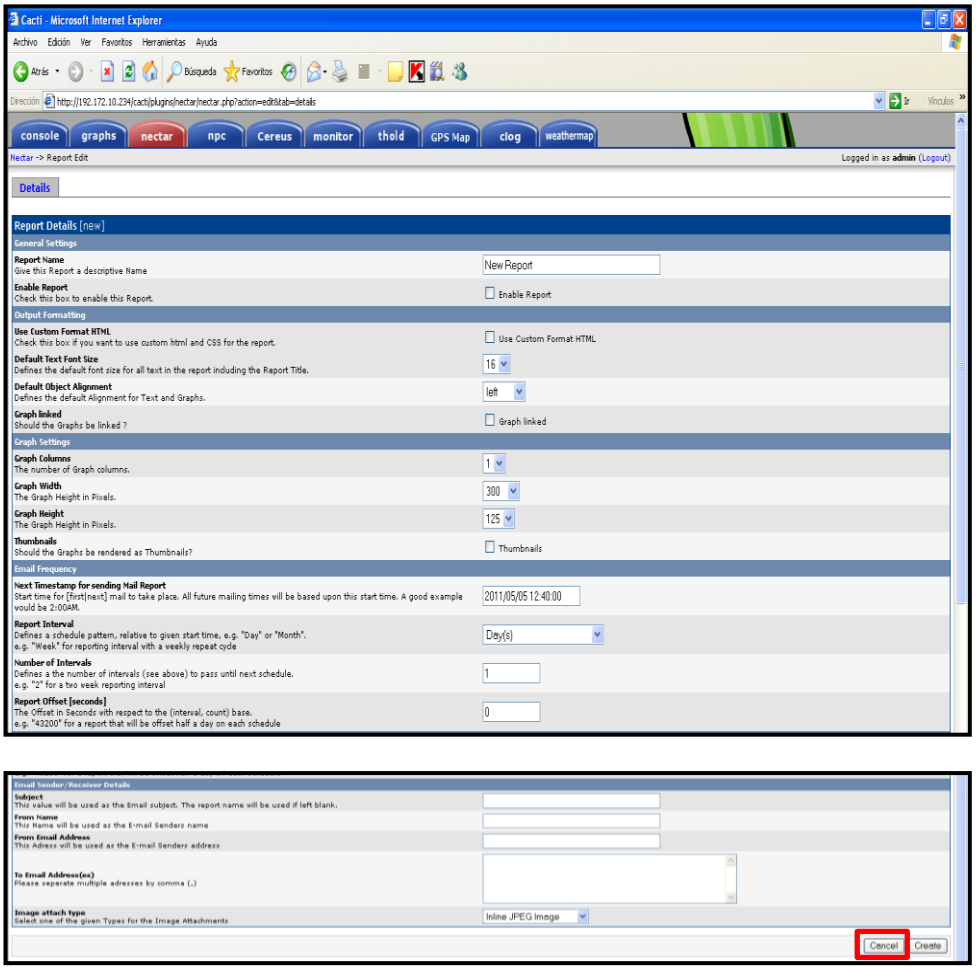


Figura 5.1.70: Creación de reportes[1]

Los parámetros a configurar presentan las siguientes opciones:

- ✓ **Report Name**: Nombre del Reporte
- ✓ **Enable Report**: Seleccionar esta opción para habilitar el reporte

➢ **OUTPUT FORMATTING**

En esta opción se debe colocar los siguientes parámetros:

- ✓ **Use Custom Format HTML**: Marcar esta casilla si desea usar formato HTML para personalizar el reporte.
- ✓ **Default Text Font Size**: Definir el tamaño de fuente para todo el texto del reporte incluyendo el título del mismo.
- ✓ **Default Object Alignment**: Definir la alineación del texto y las gráficas.

- ➢ **GRAPH SETTINGS**

En esta opción se debe colocar los siguientes parámetros:

- ✓ **Graph Columns**: Número de columnas de los gráficos.
- ✓ **Graph Width**: Dimensión del ancho de la gráfica en pixeles
- ✓ **Graph Height**: Dimensión de la altura de la gráfica en pixeles.

- ➢ **EMAIL FREQUENCY**

En esta opción se debe colocar los siguientes parámetros:

- ✓ **Next Timestamp for sending Mail Report**: Fecha y hora de inicio para el envío de los reportes.
- ✓ **Report Interval**: Patrón de horario para la generación del reporte los mismos que pueden ser en días, meses o años.
- ✓ **Number of Intervals**: Número de intervalos.

- ➢ **EMAIL SENDER/RECEIVER DETAILS**

En esta opción se debe colocar los siguientes parámetros:

- ✓ **Subject**: Asunto del envío
- ✓ **From Name**: Nombre de la cuenta de quién envía el mail.
- ✓ **From Email Address**: Dirección de la cuenta de origen.

- ✓ **To Email Address(es)**: Dirección o direcciones de los destinatarios
- ✓ **Image attach type**: Formato de la imagen a enviar.

Dar clic en la opción *Create* y a continuación aparecerán tres nuevas pestañas: *Ítems, Preview, Events.*

5.1.14.1.1 ITEMS

Seguir los siguientes pasos para la creación de un nuevo ítem:

1. Para colocar un nuevo ítem dar clic en la opción *Add* que se encuentra en la parte superior derecha de la pantalla como se muestra en la figura 5.1.71:

Figura 5.1.71: Inserción de un nuevo Item[1]

2. Se despliega una pantalla en la cual se puede agregar al reporte: texto, gráficos, árboles de los gráficos de acuerdo a los requerimientos, como se indica en la figura 5.1.72:

3. Guardar los cambios realizados.

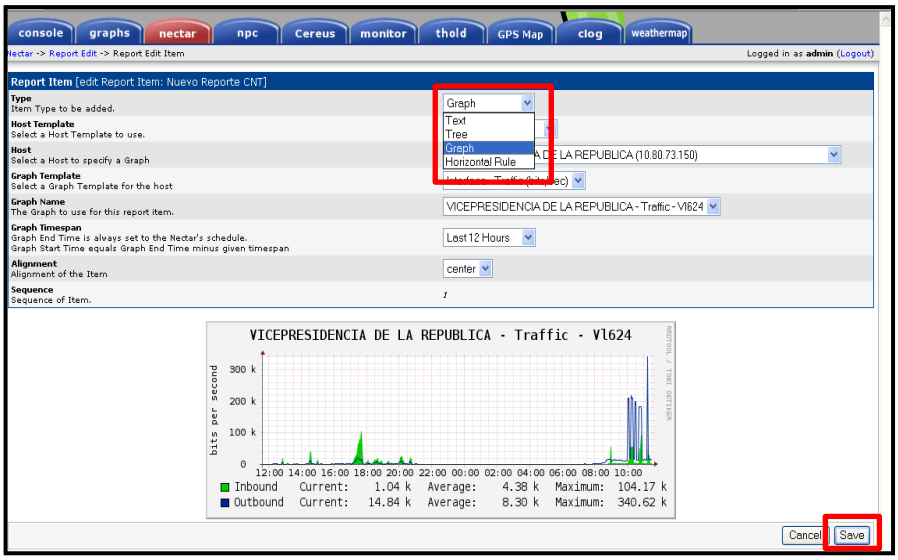


Figura 5.1.72: Guardar parámetro de configuración[1]

5.1.14.1.2 PREVIEW

Muestra el gráfico que se va a enviar en el reporte como se indica en la figura 5.1.73:

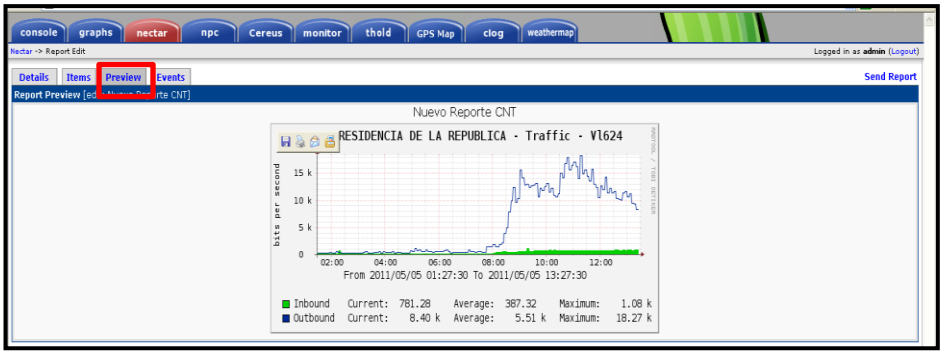


Figura 5.1.73: Visualización previa del reporte[1]

5.1.14.1.3 EVENTS

Muestra un listado organizado del envió de los reportes vía mail por lo general este registro tiene de seis a siete concurrencias, como se indica en la figura 5.1.74:

Figura 5.1.74: Registro de Reportes enviados[1]

5.2 MANUAL DE ADMINISTRACIÓN DE ANA (Active Network Abstraction)

5.2.1 OBJETIVO

Describir las herramientas incluidas en Cisco ANA que permitan la vigilancia, administración y monitoreo de los entornos de red y la integridad de los recursos basados específicamente en las redes IP/MPLS.

5.2.2 INTRODUCCIÓN

Active Network Abstraction es un modelo de plataforma inteligente que provee información en tiempo real de los dispositivos y sus servicios de red los mismos que se encuentran en la base para la gestión de redes de Cisco basado en la red de proveedores de servicios.

ANA permite la gestión de múltiples tecnologías y múltiples capas de redes IP, proporcionando información completa consistente y extensible de elementos de la red realizando inventarios físicos y lógicos.

La arquitectura ANA consiste en dos tipos de servidores:

- ✓ **Cisco ANA Gateway:** Ana Gateway sirve como puerta de entrada a través del cual todos los clientes ANA, incluidas las aplicaciones OSS (Operations Support System) y BSS (Business Support System), pueden acceder al sistema.

  Entre sus funciones principales está el control de acceso y seguridad para todas las conexiones así como la administración de las sesiones de cliente. Además almacena los eventos de configuración de redes y sistemas y alarmas.

- ✓ **Cisco ANA Unit:** El objetivo principal de ANA Units es contener VNEs (Virtual Network Element; es un modelo de elemento de red tanto en lo físico como en lo lógico) y formar con ellas una red para poder interconectarse con

otras independientemente de la unidad en la cual se ejecuten, además permite la distribución óptima de dichas VNEs.

Cada servidor contiene una colección de AVM (Autonomous Virtual Machines) e incluye un registro único de la configuración y comportamiento del servidor y sus componentes.

Los AVMs son procesos java que proporcionan a la plataforma el soporte necesario para la ejecución de diversas tareas de ANA.

Para poder realizar una administración correcta de ANA se debe conocer la información general y las funciones principales que se pueden llevar a cabo en dicho servidor.

5.2.3 ANA MANAGE

- ✓ ANA MANAGE es una aplicación-cliente GUI diseñado para simplificar y facilitar el trabajo diario de los administradores.
- ✓ Los administradores pueden controlar y configurar el comportamiento del sistema.
- ✓ También está relacionada con *Ana Gw* para consultar y modificar la información de configuración.
- ✓ Las múltiples sesiones ANA MANAGE se pueden abrir en cualquier momento dado.

5.2.3.1 FUNCIONES PRINCIPALES

Las funciones principales de administración soportadas por ANA Manage son:

- ➢ Creación y administración de diversos servidores de ANA (ejemplo: AVMs, VNEs).
- ➢ Visualización de los segmentos de la base de datos
- ➢ Gestión de la seguridad, alcances y cuentas de usuarios

- Configuración global y personalizada:
  - ✓ Licencias de cliente
  - ✓ Segmentos DB
  - ✓ Mensaje del día
  - ✓ Grupos de sondeo
  - ✓ Protección de los grupos
  - ✓ Reportes de configuraciones

5.2.3.2 INICIALIZACIÓN DE ANA MANAGE

1. Ejecutar la aplicación.

2. Ingresar la información en el cuadro de diálogo de inicio de sesión:

   - ✓ Nombre de usuario
   - ✓ Contraseña
   - ✓ Host (ANA GW dirección IP del servidor o nombre de host)

Los controles del cliente para una nueva versión se pueden actualizar automáticamente si es necesario.

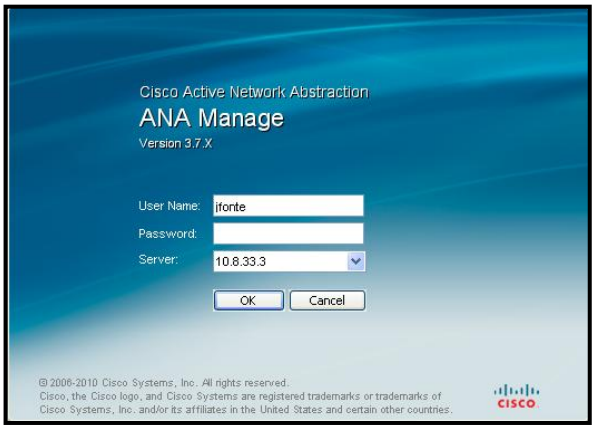


Figura 5.2.1: Inicio de Ana Manage[1]

La ventana principal de ANA Manage está dividida en dos áreas o paneles como se muestra en la figura 5.2.2:

- **Panel de Navegación:** Este panel se encuentra en el lado izquierdo de la pantalla y contiene algunos elementos de ANA (ejemplo: Gateway, Units y AVMs) y funciones administrativas que pueden ser ejecutadas usando ANA Manage.

- **Panel de Visualización:** Este panel se encuentra en el lado derecho de la pantalla y presenta todos los detalles relacionados a la opción que se haya seleccionado en el panel de navegación en la parte izquierda de la pantalla.

ANA Manage además contiene una barra de Menú, barra de herramientas, como se indica en la figura 5.2.2:

Figura 5.2.2: Ventana Principal[1]

5.2.3.3 BARRA DE HERRAMIENTAS

La barra de herramientas contiene siete tareas. La función de las tareas depende de lo que se ha seleccionado en el panel de navegación a continuación se muestran cada una de las opciones en la figura 5.2.3:

Figura 5.2.3: Barra de Herramientas[1]

NEW: Depende del elemento seleccionado.

- ✓ Si se selecciona ANA Servers en el panel de navegación entonces se procede a crear una nueva ANA Unit.
- ✓ Si se selecciona ANA Unit en el panel de navegación entonces se procede a crear un nuevo AVM.
- ✓ Si se selecciona un AVM en el panel de navegación se procede a crear un VNE.
- ✓ Si se selecciona User en el panel de navegación se procede a crear un nuevo usuario.

PROPERTIES: Muestra las propiedades de un elemento seleccionado.

 **DELETE:** Borra un elemento seleccionado.

 **START:** Carga los AVM/VNE seleccionados.

 **STOP:** Descarga los AVM/VNE seleccionados.

 **MAINTENANCE**: Mueve los VNE para su mantenimiento.

 **FIND:** Buscar función- AVM, VNE etc.

Las opciones *Star*, *Stop*, *Maintenance* y *Find* de la barra de herramientas son usadas específicamente para la administración de AVMs y VNEs.

5.2.3.4 ADMINISTRACIÓN DE SERVIDORES ANA

ANA Manage automáticamente lista todos los servidores de ANA que se definen actualmente en el sistema.

Los administradores pueden realizar las siguientes funciones:

- ✓ Agregar, configurar y administrar las unidades activas y respaldo de los servidores ANA.
- ✓ Creación y gestión de los AVMs.
- ✓ Crear, asignar y gestionar VNEs.

5.2.3.4.1 ADMINISTRACIÓN DE ANA UNITS

A continuación se describirá la creación de ANA Unit.

5.2.3.4.1.1 CREACIÓN UN NUEVO UNIT

Para la creación de una ANA Unit seguir los siguientes pasos:

1. Seleccionar ANA Servers en el panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y seleccionar *New ANA Unit* como se muestra en la figura 5.2.4:

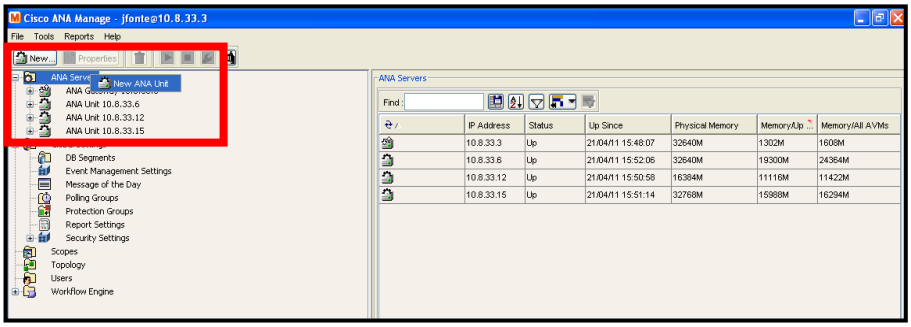


Figura 5.2.4: Nuevo Unit[1]

2. Colocar la IP address del servidor añadido, se recomienda habilitar la opción *Enable Unit Protection* con el fin de dar soporte a la unidad en caso de alguna falla.

Protection Group es un grupo en el cual *Units* y *Stand-by Unit* están relacionados.

Se puede seleccionar la opción *Stand-byUnit* para añadir una unidad en stand-by en el ANA servers.

En caso de que Unit presentara problemas de conmutación el *Standby Unit* puede ser tomado del mismo *Protection Group*.

Protection Group es un grupo de protección que provee alta disponibilidad a los servidores creados.

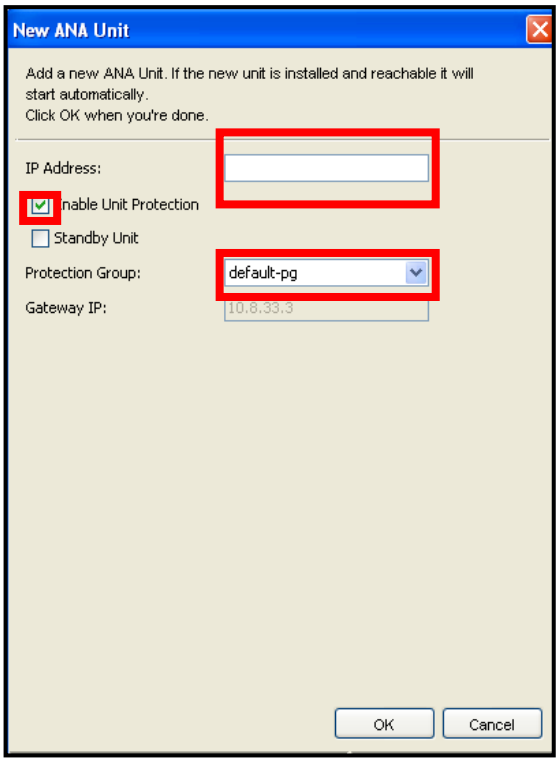


Figura 5.2.5: Nuevo Ana Unit[1]

3. La nueva unidad añadida se muestra en ANA Manage.

Cisco ANA Manage registra automáticamente a ANA Units y crea un enlace de transporte entre Cisco ANA Unit y Cisco ANA Gateway.

Los administradores pueden visualizar las propiedades de ANA Unit dando clic derecho en *Ana Units/ Properties*, se sugiere habilitar la unidad de protección para una alta disponibilidad y seguridad del servidor como se indica en la figura 5.2.6.

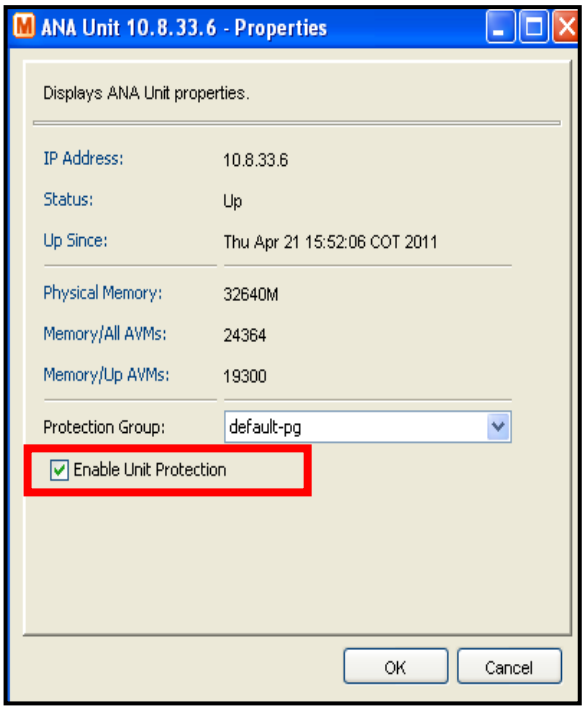


Figura 5.2.6: Propiedades de ANA Unit[1]

5.2.3.4.2 ADMINISTRACIÓN DE LOS AVMs

Los procesos del servidor de Cisco ANA se dividen en AVMs.

Los AVMs son procesos java que proporcionan el soporte necesario de distribución a la plataforma para la ejecución y seguimiento de múltiples VNEs.

VNEs son los elementos de red modelados tanto en lo físico como en lo lógico.

ANA Manage permite a los administradores añadir nuevas AVMs y personalizar los ya existentes en un servidor de la unidad seleccionada.

5.2.3.4.2.1 CREACIÓN DE UNA AVM

Para la creación de un nuevo AVM seguir los siguientes pasos:

1. Seleccionar el elemento de jerarquía de la ANA Units en el panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y seleccionar *New AVM.*

2. Colocar el *Id* del AVM, en la cual se debe ubicar números del 101 hasta el 999 los mismos que son únicos para cada servidor.

3. Colocar una clave significativa que es una cadena que identifica de forma única un AVMs en el sistema, independientemente de su ubicación en la unidad para que un escenario de conmutación por error en el sistema sea transparente.

4. Especificar el tamaño de la memoria

5. Habilitar o deshabilitar la opción *OnCreation*

6. Habilitar o deshabilitar la protección *AVM*.

   Todos estos parámetros se muestran en la figura 5.2.7.

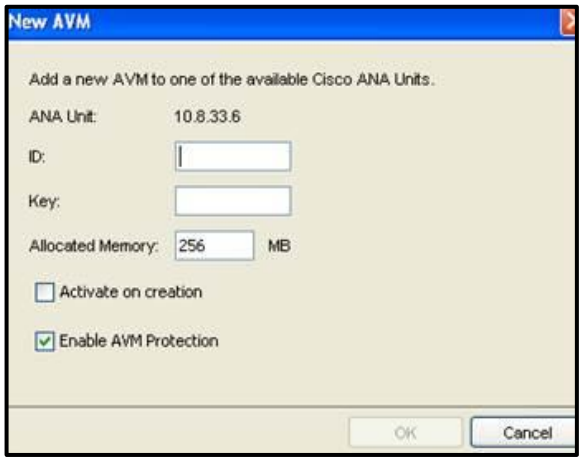


Figura 5.2.7: Nuevo AVM[1]

7. La nueva AVM creada se muestra en ANA Manage.

Las AVMs se encuentran listadas en el panel de navegación; si un servidor es seleccionado en el panel de navegación las propiedades de los AVMs se pueden observar en el panel de visualización.

Una vez creadas las AVMs los administradores pueden realizar las siguientes funciones en los AVMs:

- ✓ Crear una nueva VNE
- ✓ Iniciar o detener
- ✓ Eliminar un AVM
- ✓ Mover un AVM
- ✓ Visualizar las propiedades de los AVMs

Para poder realizar cualquiera de las funciones anteriormente indicadas, se debe llevar a cabo el siguiente proceso:

Seleccionar la AVM deseada y dar clic derecho en dicha AVM como se indica en la figura 5.2.8:

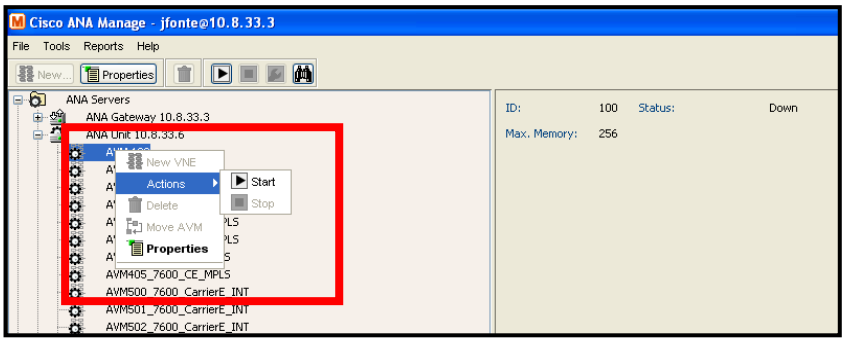


Figura 5.2.8: Funciones en los AVMs[1]

Los administradores pueden visualizar las propiedades de los AVMs dando clic derecho en el AVM requerido y elegir la opción *Properties* como se muestra en la figura 5.2.9:

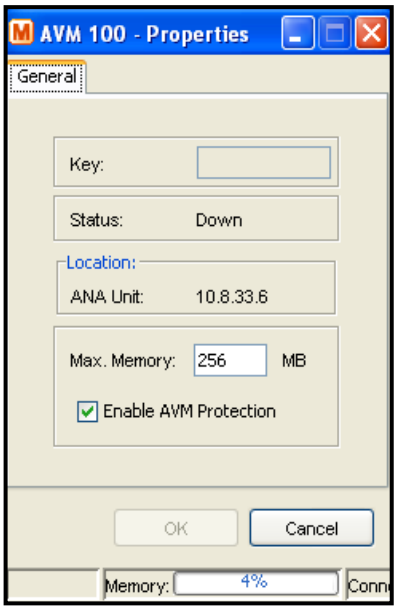


Figura 5.2.9: Propiedades AVMs [1]

5.2.3.4.3 ADMINISTRACIÓN DE VNES

A continuación se describe una serie de tareas para realizar la administración correcta de VNEs.

5.2.3.4.2.2 CREACIÓN DE UNA VNE

Para la creación de una nueva VNE seguir los siguientes pasos:

1. Seleccionar el AVM en el cual se desea añadir la VNE en el panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y seleccionar *New VNE*, como se indica en la figura 5.2.10:

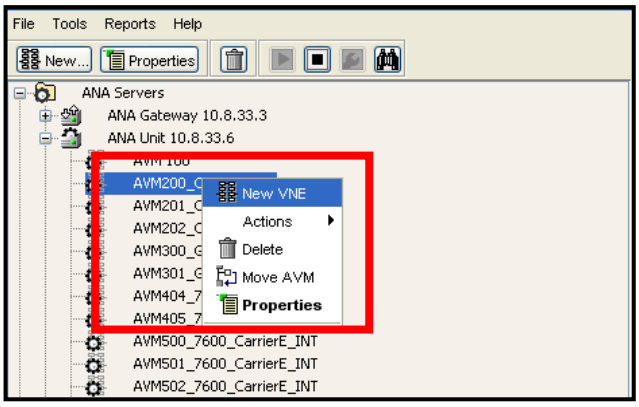


Figura 5.2.10: Nueva VNE[1]

A continuación se despliega el asistente VNE.

El asistente VNE presenta varias pestañas, cada una con opciones diferentes, las mismas se describen a continuación:

- **TAB GENERAL**

1. Colocar el tipo e identificación de la VNE, se sugiere colocar *Auto Detect* para que ANA descubra el tipo de dispositivos y el modelo de acuerdo a sus librerías.

   En la opción *Scheme* se sugiere colocar la opción *Default.*

2. Especificar el estado inicial de la VNE, además se puede observar el número de AVM de la ANA Unit como se indica en la figura 5.2.11:

Figura 5.2.11: Tab General [1]

Un conjunto de etiquetas se suministran cuando se añade un nuevo VNE al sistema de ANA.

- **TAB SNMP**

1. Seleccionar la opción SNMP versión para gestionar la información de acceso SNMP.

2. Seleccionar la versión SNMP soportada por cada elemento de la VNE que está siendo administrada como se indica en la figura 5.2.12.

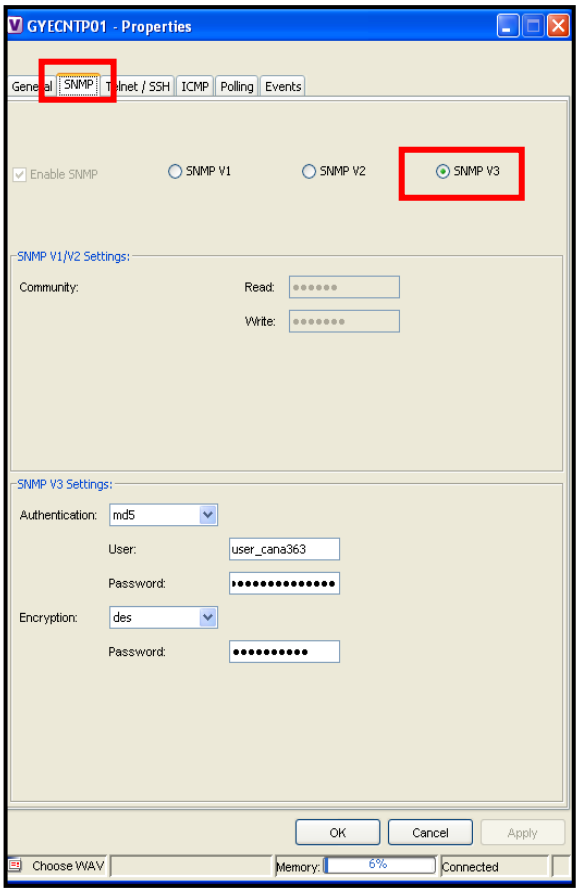


Figura 5.2.12: Tab SNMP[1]

- **TAB TELNET / SSH**

Permite a los VNE almacenar información del elemento de red que no es alcanzable con SNMP usando Telnet. Además contiene las credenciales de acceso de la *CLI* y la secuencia.

1. Seleccionar Telnet, puerto 23 o SSH, puerto 22.

2. Para añadir una nueva secuencia de comandos; colocar el valor del *Prompt/Run* en la tabla, dando clic en el campo *Prompt* y finalmente seleccionar *Add*, como se indica en la figura 5.2.13.

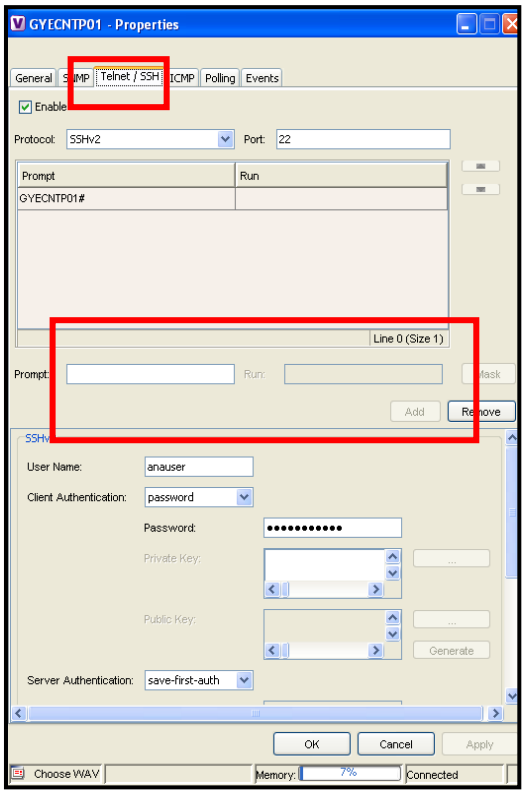


Figura 5.2.13: Tab Telnet/SSH[1]

- **TAB ICMP**

Este tab es opcional para todas las VNEs excepto para el tipo ICMP/VNEs que es usado para verificar que un elemento es accesible como se muestra en la figura 5.2.14.

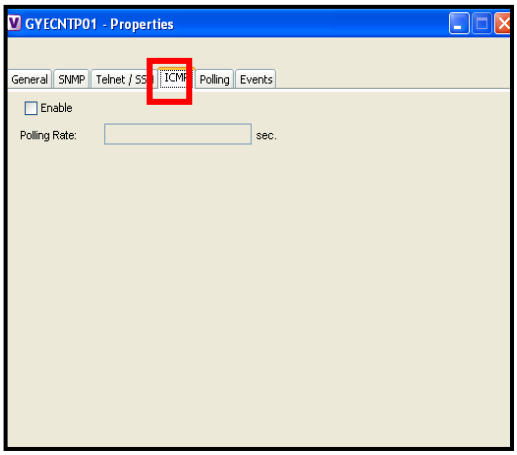


Figura 5.2.14: Tab ICMP[1]

- **TAB POLLING**

Permite a los administradores definir los parámetros de sondeo de una VNE específica.

1. Colocar los intervalos de sondeo para la VNE.

2. Seleccionar la opción *Group* que define un grupo específico de sondeo como se indica la figura 5.2.15:

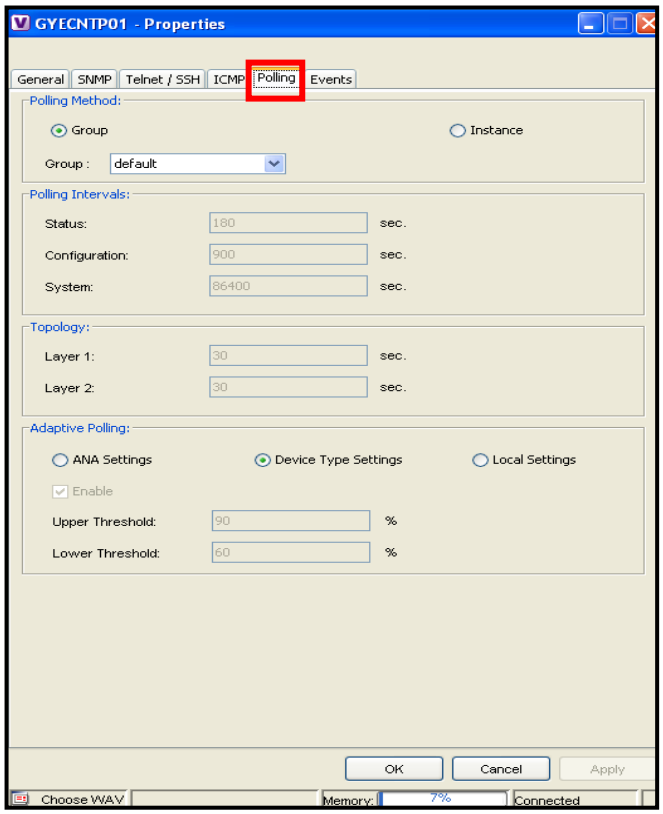


Figura 5.2.15: Tab Polling[1]

Adaptative polling

Además de los intervalos de sondeo definido, se puede aplicar a los VNE sondeos para asegurar que el elemento no tenga sobrecarga.

Cuando un VNE supera el límite máximo del uso de la CPU, una alarma se envía al EventVision, la VNE se sondea con menor regularidad y se produce un retraso entre el envío de comando del elemento de red

Cuando los valores de uso de la CPU se encuentran bajo el nivel mínimo se envía una alarma al *EventVision* y los VNE regresan a su sondeo normal.

- **TAB EVENTS**

Permite configurar una dirección IP alternativa en caso que se desee detectar los eventos de un elemento de red como se indica en la figura 5.2.16:

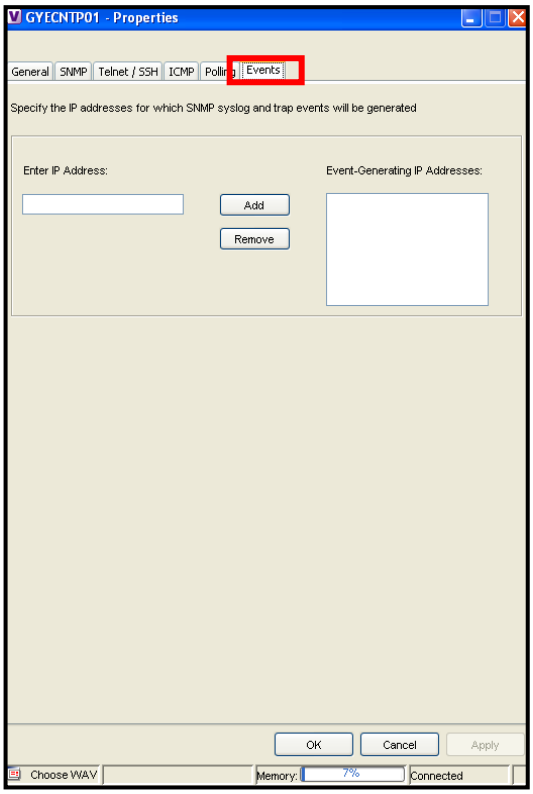


Figura 5.2.16: TabEvent[1]

Una vez creada la VNE los administradores pueden realizar las siguientes funciones en los VNEs:

- ✓ Iniciar o detener
- ✓ Eliminar un VNE
- ✓ Mover un VNE
- ✓ Visualizar las propiedades de los VNEs

Para poder realizar cualquiera de las funciones anteriormente indicadas, se debe llevar a cabo el siguiente proceso:

Seleccionar la VNE deseada y dar clic derecho como se indica en la figura 5.2.17:

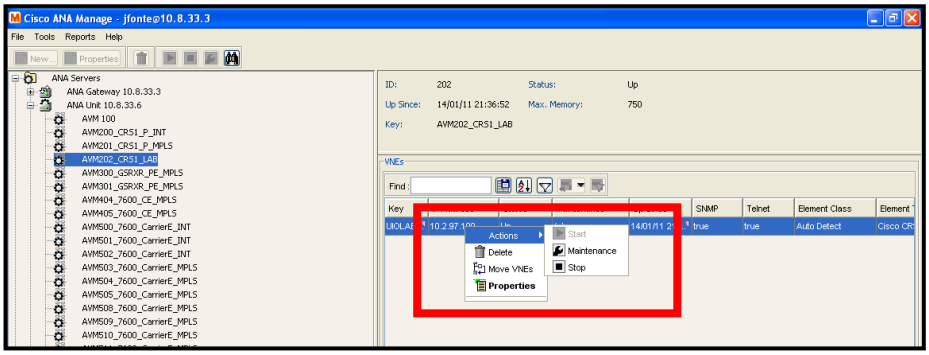


Figura 5.2.17: Funciones en los VNEs[1]

- ➢ **FUNCIONALIDAD FIND**

La función de búsqueda permite a los administradores realizar una búsqueda global para encontrar VNEs y AVMs específicas entre todos los servidores de Cisco ANA.

Para esto en la barra de herramientas seleccionar la opción *Find*, como se indica en la figura 5.2.18:

Figura 5.2.18: Find[1]

5.2.3.5 GLOBAL SETTINGS

Global Settings es una opción que se encuentra en el panel de navegación que describe cómo usar ANA Manage y permite la gestión de configuración de varios componentes globales del sistema, tales como:

- ✓ Segmentos DB
- ✓ Administración de Eventos.
- ✓ Mensaje del día
- ✓ Sondeo grupos
- ✓ Grupos de protección.
- ✓ Administración de reportes
- ✓ Administración de seguridad

Todas estas opciones se muestran en la figura 5.2.19:

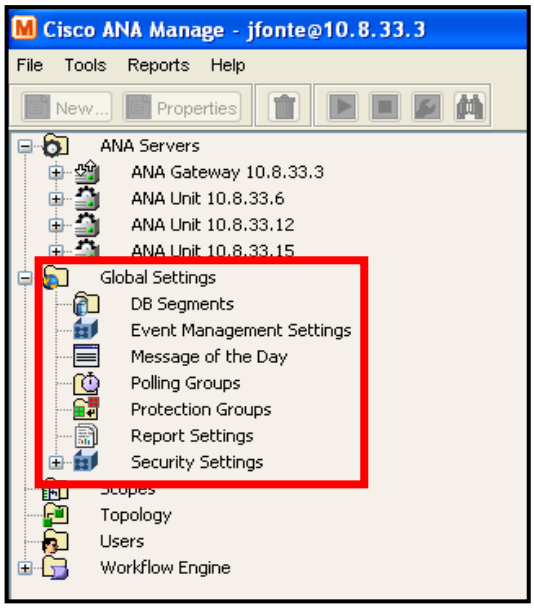


Figura 5.2.19: Global Settings[1]

A continuación se describe cada una de las configuraciones globales que se pueden ejecutar en ANA Manage.

5.2.3.5.1 DATABASE SEGMENTS

Permite a los administradores del sistema ver y controlar la información importante de bases de datos, tales como:

- ✓ Bases de datos de la asignación de segmentos de almacenamiento de información.
- ✓ Bases de datos del uso del disco
- ✓ Base de datos de crecimiento

Cada una de estas bases de datos con su nombre, tipos de segmentos y tamaños como se indica en la figura 5.2.20:

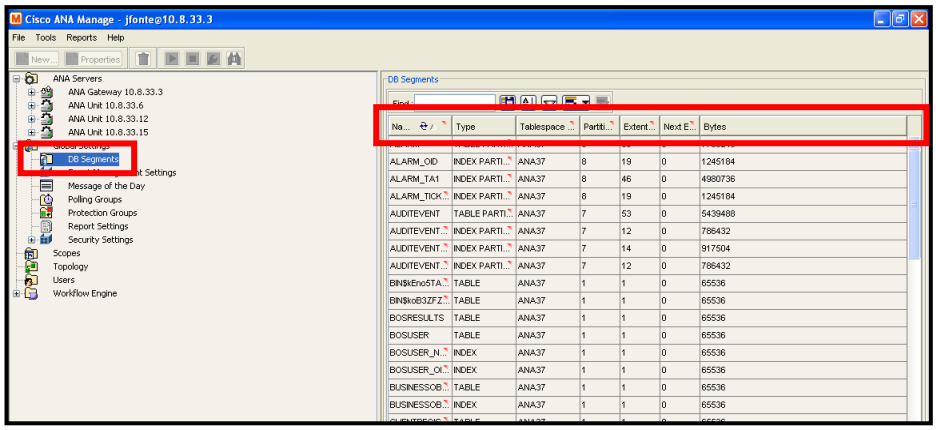


Figura 5.2.20: Database Segments[1]

5.2.3.5.2 EVENT MANAGEMENT SETTINGS

Los administradores pueden especificar el tiempo en el que la información de los eventos se depura de la base de datos, el valor predeterminado es de 14 días.

- ✓ Para cada partición de la base de datos: se debe colocar los días en los que su información va a ser eliminada.

- ✓ Para cada partición: se debe colocar el tamaño (en días) de la partición de la base de datos como se indica en la figura 5.2.21:

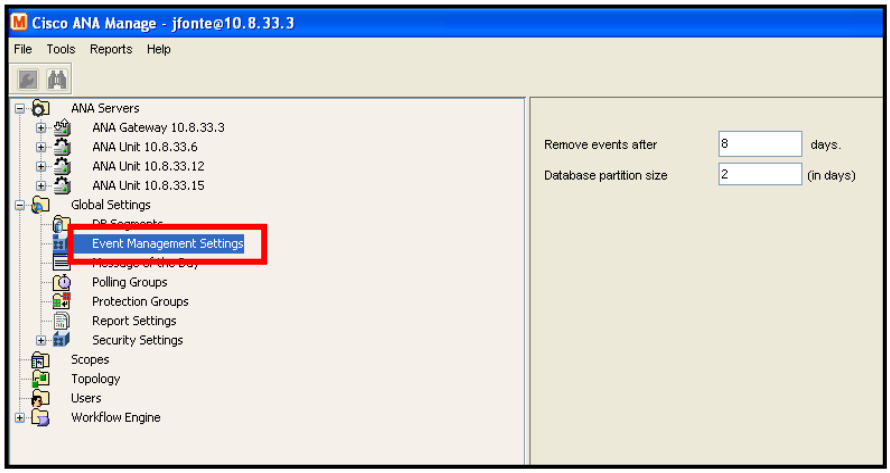


Figura 5.2.21: Events Management Settings[1]

5.2.3.5.3 MESSAGE OF THE DAY

Los administradores pueden definir un mensaje que se muestra cuando el usuario inicia sesión en cualquier aplicación de cliente ANA como se indica en la figura 5.2.22.

El usuario debe aceptar el mensaje antes de iniciar sesión; si el usuario no acepta el mensaje no podrá ingresar al sistema. Se puede aplicar un solo mensaje a la vez.

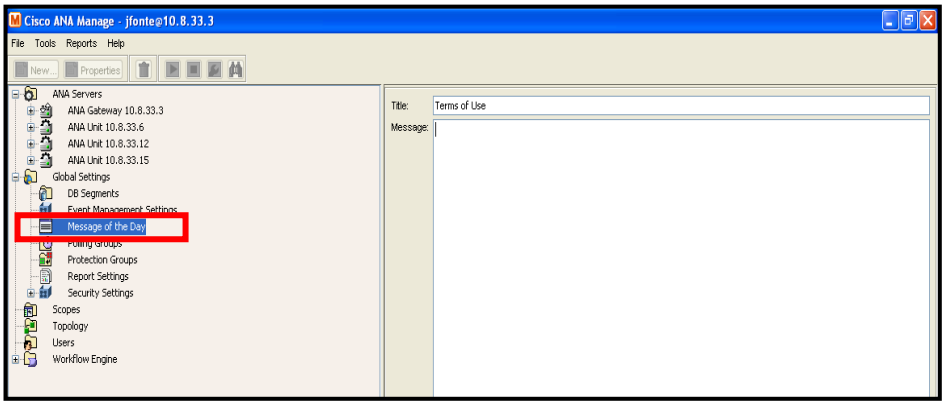


Figura 5.2.22: Message of the day[1]

5.2.3.5.4 POLLING GROUPS

Permite administrar los grupos de sondeo. Diferentes tipos de Polling (sondeo) se pueden ajustar para diferentes grupos de dispositivos a fin de permitir un alto grado de control y flexibilidad.

Los administradores pueden definir varios niveles de Polling (sondeo), y los dispositivos serán consultados de acuerdo a la configuración personalizada del Polling Group.

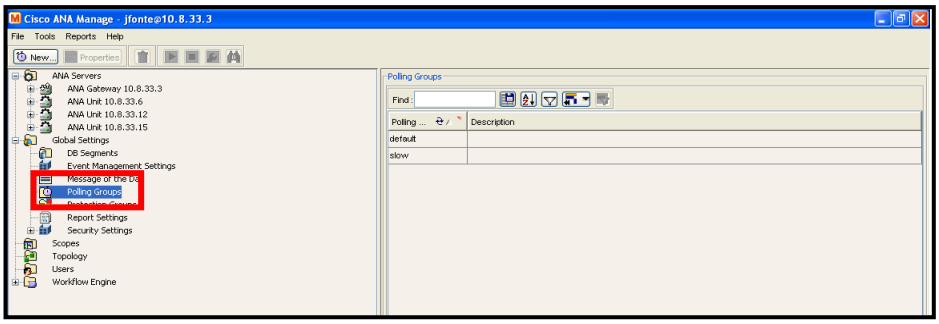


Figura 5.2.23: Polling Group[1]

5.2.3.5.4.1 CREAR UN NUEVO POLLING GROUP

Para la creación de un nuevo Polling Group realizar los siguientes pasos:

1. Seleccionar Polling Group del panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y elegir *New Polling Group*.

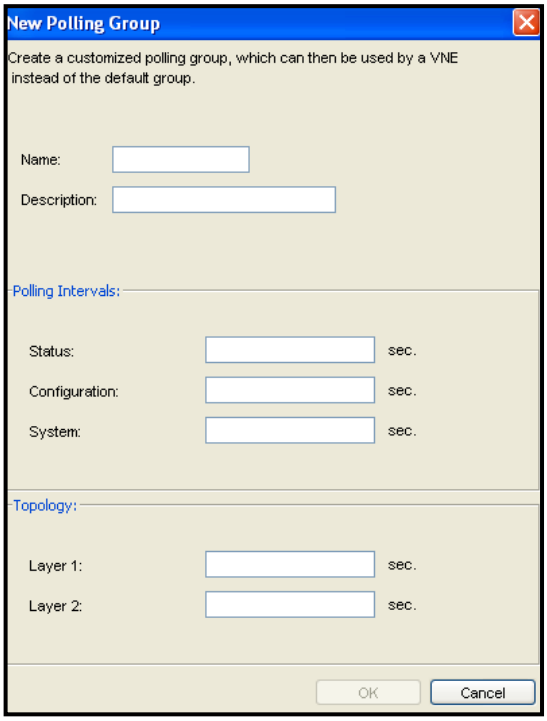


Figura 5.2.24: New Polling Group[1]

2. Colocar el nombre y los valores para cada uno de los 5 intervalos del *Polling Group*.

3. Cualquier cambio realizado en la opción Global Settings se guarda automáticamente y se registra en el registro de Cisco ANA, como se indica en la figura 5.2.24.

5.2.3.5.5 PROTECTION GROUPS

Los administradores pueden crear nuevos grupos de protección y personalizar los servidores de alta disponibilidad. Todas las unidades de Cisco Ana tienen por defecto un grupo de protección (default-pg).

Protection Groups permite manejar diferentes tipos de servidores ó servidores dispersos geográficamente para proporcionar mecanismos de disponibilidad.

5.2.3.5.5.1 CREAR UN NUEVO PROTECTION GROUPS

Para la creación de un nuevo Protection Group seguir los pasos que se muestran a continuación:

1. Seleccionar la opción Protection Groups del panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y elegir *New Protection Groups* y finalmente colocar el nombre y la descripción correspondiente como se muestra en la figura 5.2.25:

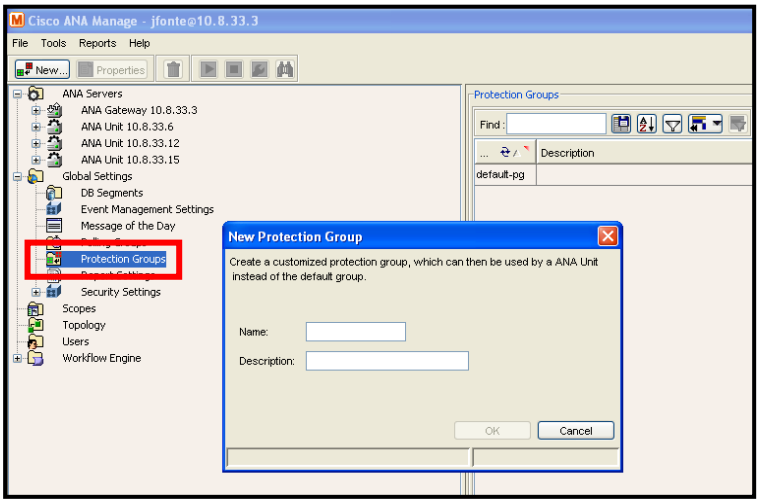


Figura 5.2.25: Protection Group[1]

5.2.3.5.6 REPORT SETTINGS

Permite a los administradores especificar el tiempo en que Cisco ANA debe guardar los informes y si los usuarios pueden crear informes para compartir como indica la figura 5.2.26.

Existen diferentes tipos de reportes que son mostrados en *Network Vision*.

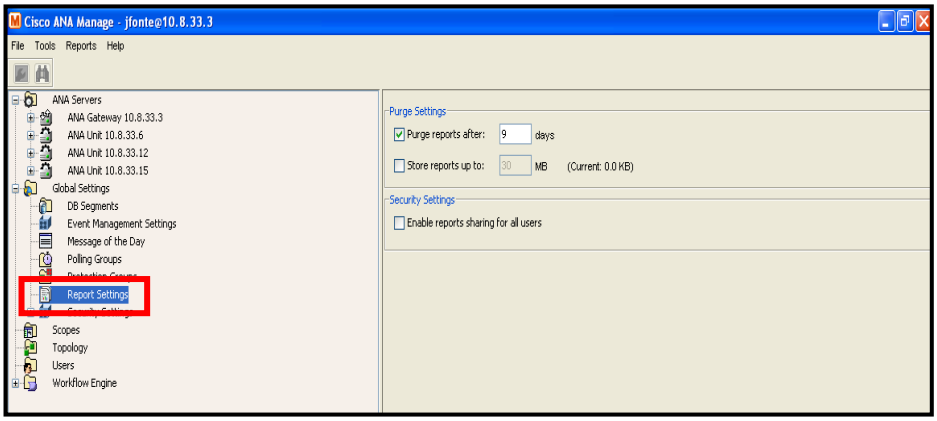


Figura 5.2.26: Report Settings[1]

5.2.3.5.7 SECURITY SETTINGS

Permite a los administradores realizar configuraciones de seguridad las mismas que se describen a continuación.

5.2.3.5.7.1 AUTHENTICATION METHOD

El administrador debe habilitar la opción ANA Authentication como indica la figura 5.2.27:

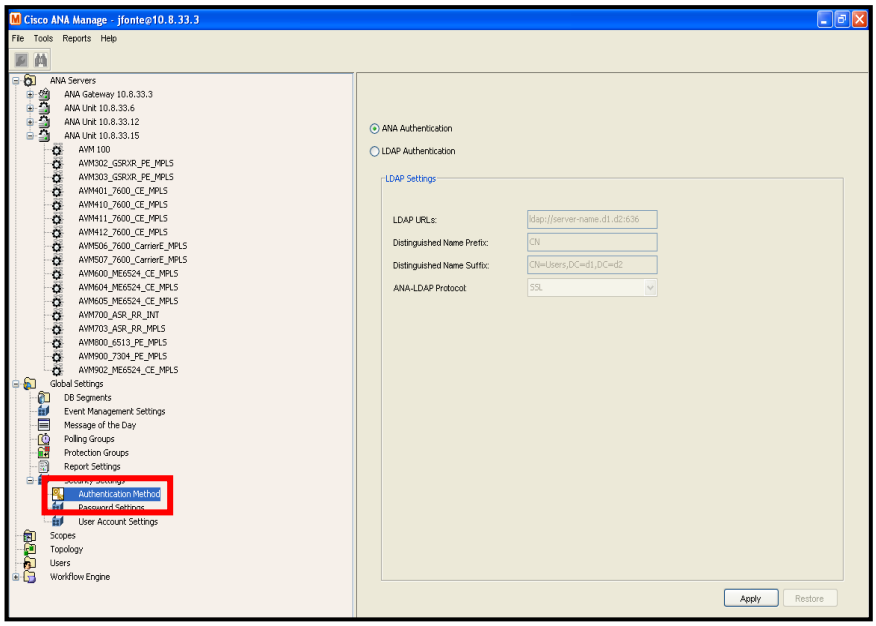


Figura 5.2.27: Authentication Method[1]

5.2.3.5.7.2 PASSWORD SETTINGS

En esta opción se pueden realizar las configuraciones necesarias para las validaciones de contraseñas donde se debe colocar el tiempo de validación y el número de intentos antes de bloquear el acceso, además se debe habilitar todas las secciones *Password Strength*, como se indica en la figura 5.2.28:

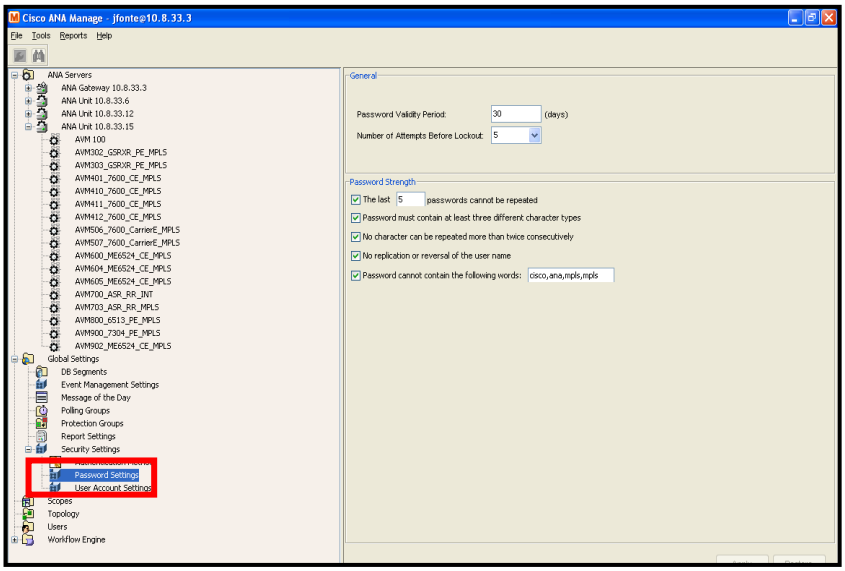


Figura 5.2.28: Password Settings[1]

5.2.3.5.7.3 USER ACCOUNT SETTINGS

Permite determinar el tiempo en que se desactiva una cuenta si se mantiene inactiva como se muestra en la figura 5.2.29:

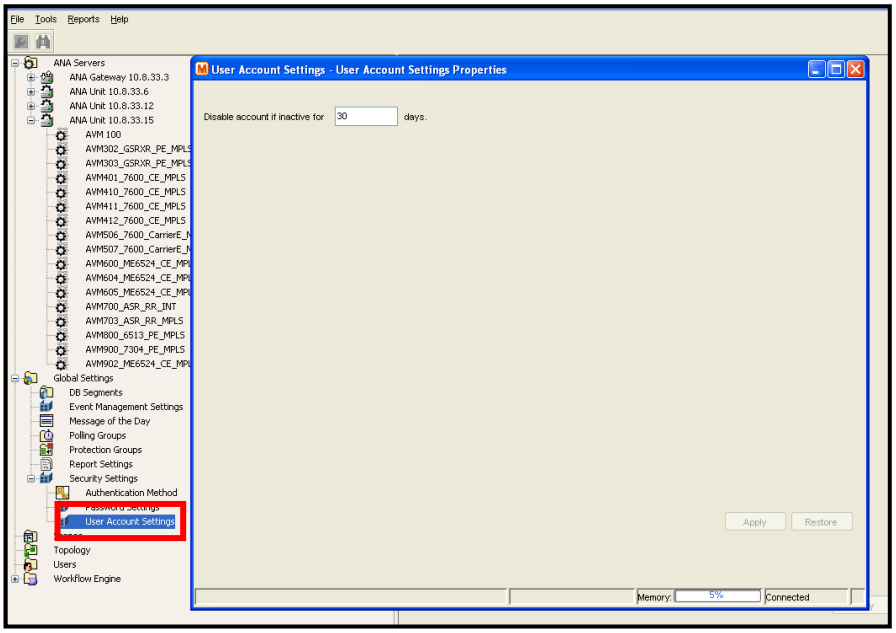


Figura 5.2.29: User Account Settings[1]

5.2.3.5.8 ANA SECURITY

Cisco *ANA Security* se aplica a la administración de dispositivos y la aplicación de funcionalidades.

5.2.3.5.8.1 ADMINISTRACIÓN DE DISPOSITIVOS

Las características de Ana Security pueden ser usadas para limitar a los usuarios a dispositivos específicos y determinadas operaciones en estos dispositivos

- ✓ **Scope:** Define un subconjunto de dispositivos.
- ✓ **Role:** Define un conjunto de operaciones que pueden ser ejecutadas. Los roles (funciones) de usuario se pueden establecer por Scopes.

Cuando un usuario no tiene un rol específico dicha función en ANA está deshabilitada.

5.2.3.5.8.2 APLICACIÓN DE FUNCIONALIDADES

Una role (función) de un usuario por defecto define todas las actividades (no relacionadas con los dispositivos) que un usuario puede ejecutar en las aplicaciones de cliente de ANA.

5.2.3.5.8.3 FUNCIONES DE SEGURIDAD

Cisco ANA ofrece cinco niveles de seguridad previamente establecidos y la administración de usuarios. Además, se les da un role que restringe el acceso a ciertas funciones dentro de la aplicación de ANA se conoce como el rol de usuario por defecto. Para obtener más flexibilidad en la administración de dispositivos, los scopes pueden crear diferentes roles de usuario.

A continuación se describen cada uno de los roles predefinidos para limitar las operaciones en los dispositivos:

 **Administrator:** Administra el sistema de configuración, los usuarios y la topología.

 **Configurator:** Activa los servicios y configura la red.

 **Operator Plus**: Gestiona el ciclo de vida de alarma, administración de las alarmas.

 **Operator:** Muestra información de la red.

Viewer: Muestra la red y la información de negociación de etiquetas.

5.2.3.5.8.4 ADMINISTRACIÓN DE SEGURIDAD

Cisco ANA Security está compuesto por dos bloques principales: Scopes y Users como se indica en la figura 5.2.30:

- ✓ ***Scopes*:** Se refieren a dispositivos o elementos de red gestionados por la plataforma Cisco ANA.
- ✓ ***Users*:** Se refieren a la identificación de los usuarios y la administración de permisos.

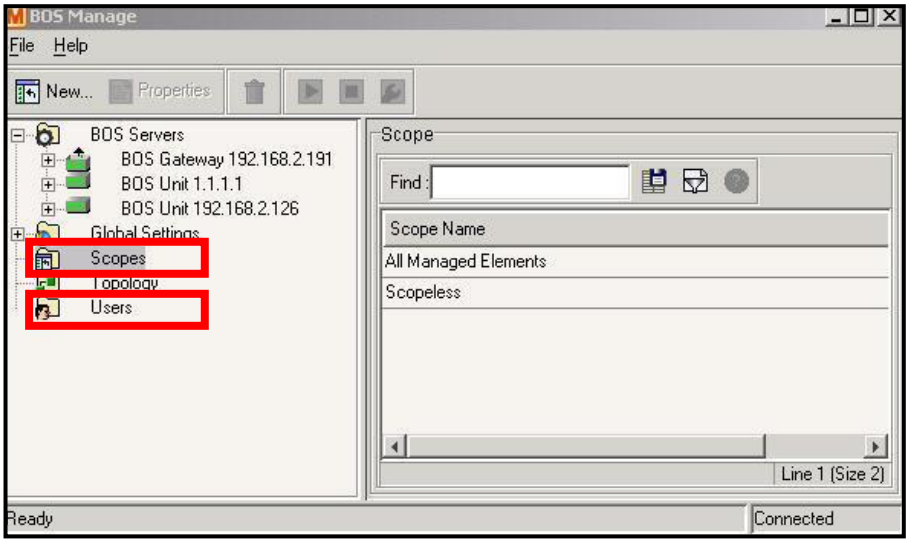


Figura 5.2.30: Scopes y Users[1]

- ➢ **ADMINISTRACIÓN DE SCOPES**

Para la administración de Scope se deben considerar los siguientes puntos:

- ✓ Los Scopes son grupos NE (subgrupos de red).
- ✓ Un Scope puede estar basado en la división organizacional, en la geografía y las reglas de administración de red.
- ✓ Los permisos de usuario pueden variar en diferentes scopes.

- ✓ Los administradores pueden definir nuevos scopes o actualizar los ya existentes.
- ✓ Un dispositivo puede estar en más de un scope.
- ✓ Los usuarios pueden tener diferentes funciones en diferentes Scopes.

➢ CREACIÓN DE UN SCOPE

Para la creación de un nuevo Scope realizar los siguientes pasos:

1. Seleccionar la opción *Scope* en el panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y elegir *New Scope.*

2. Colocar el nombre del Scope y añadir el dispositivo que va a ser parte del Scope como se indica en la figura 5.2.31.

Los usuarios pueden ser asignados a estos Scopes con una función específica.

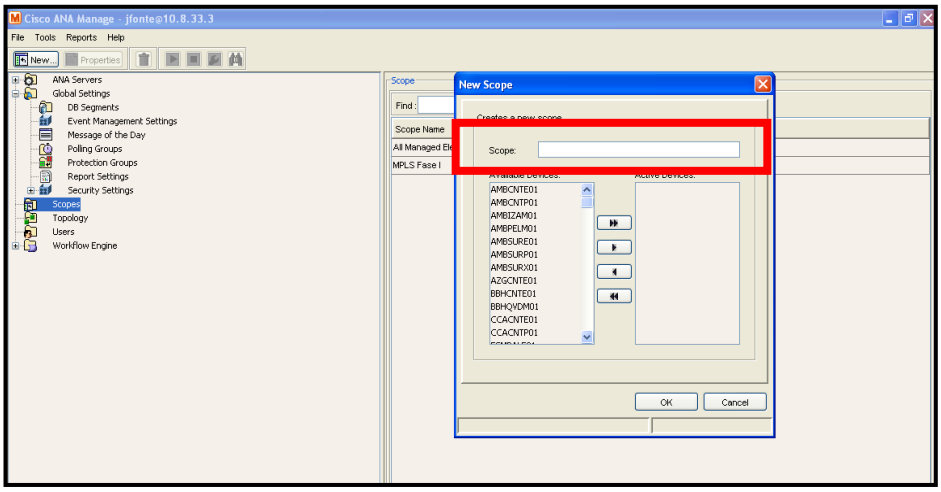


Figura 5.2.31: Nuevo Scope[1]

- **ADMINISTRACIÓN DE USUARIOS**

Para la administración de Usuarios se debe considerar que esta opción permite a los administradores realizar las siguientes funciones:

- ✓ Crear usuarios
- ✓ Eliminar usuarios
- ✓ Cambiar contraseña de usuario.
- ✓ Control de cuenta de usuario y permisos.

- **CREAR USUARIOS**

Es necesario crear usuarios para que puedan ingresar al sistema y realicen actividades de monitoreo, seguridad, levantamiento de mapas, etc

Para la creación de un nuevo Usuario realizar los siguientes pasos:

1. Seleccionar la opción *Users* en el panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y elegir *New User*.

2. En el cuadro de dialogo colocar el nombre, contraseña y la descripción.

3. Seleccionar la función del usuario por defecto.

Todos estos parámetros se indican en la figura 5.2.32:

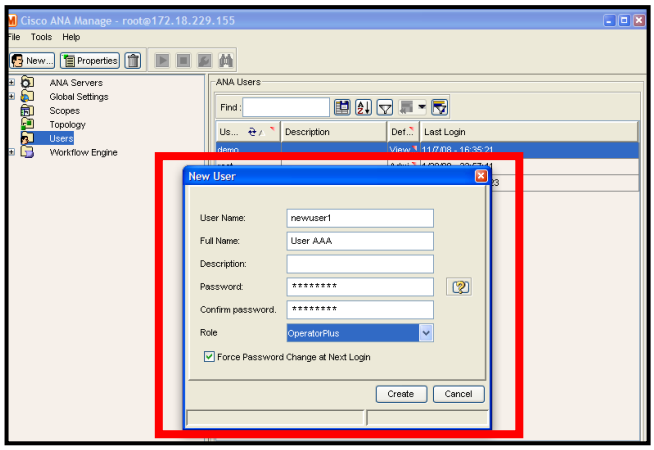


Figura 5.2.32: Nuevo Usuario[1]

4. Para la configuración de roles de usuario seleccionar la opción *User* en el panel de visualización y dar clic en la opción *Properties* o a su vez dar clic derecho y elegir *Properties*.

   A continuación se muestra dos tablas de propiedades:

- **TAB GENERAL**

Permite realizar modificaciones a los nombres de usuario, descripción y propiedades de la cuenta como se indica en la figura 5.2.33:

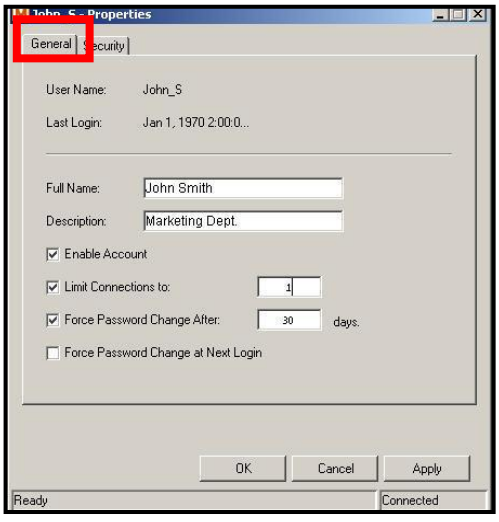


Figura 5.2.33: Tab General[1]

- **TAB SECURITY**

Permite al administrador cambiar las funciones de usuario por defecto y añadir o modificar las funciones asignadas a varios Scopes para ese usuario.

Para añadir una función a un Scope dar clic en la opción *Add*, seleccionar el Scope y elegir un rol (función) para el mismo como se muestra en la figura 5.2.34:

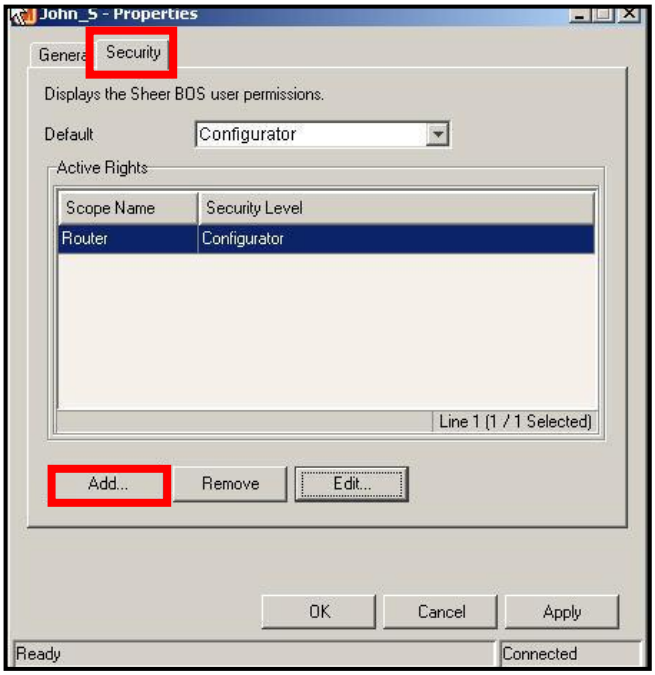


Figura 5.2.34: Tab Security [1]

5.2.3.5.9 TOPOLOGY

ANA Manage tiene la capacidad de crear nuevos enlaces entre dos elementos de red para complementar o reemplazar los ya existentes y auto-descubrir una topología.

El nuevo enlace estático sólo se puede realizar cuando ambos VNEs están activos y accesibles como se indica en la figura 5.2.35:

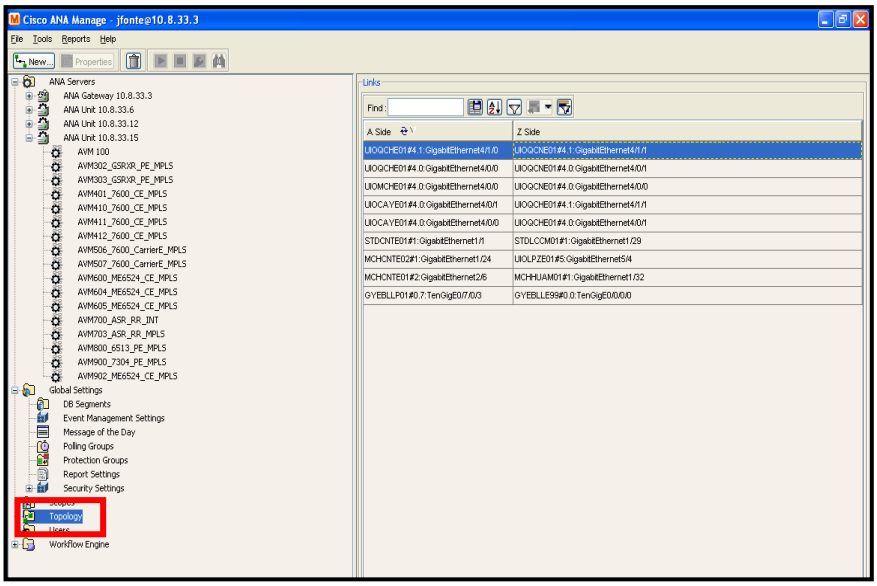


Figura 5.2.35: Topology[1]

5.2.3.5.9.1 CREACIÓN DE NUEVO ENLACE ESTÁTICO

Para crear un nuevo enlace estático seguir los siguientes pasos:

1. Seleccionar la opción Topology en el panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y elegir New Static Link.

2. Seleccionar el sitio de A y Z del enlace estático, expandir el inventario físico de cada elemento y seleccionar la interfaz.

3. Dar clic en *Created.*

Los elementos de la jerarquía de la topología permiten al administrador la gestión (añadir, visualizar y borrar) de los enlaces estáticos. El administrador puede crear un enlace estático entre dispositivos seleccionando dos puertos finales del *Physical Inventoy*.

El enlace es bidireccional y necesita ser añadido una sola vez. El nuevo link es validado después de que los dos puertos son seleccionados, pero antes de que el link sea añadido como se muestra en la figura 5.2.36.

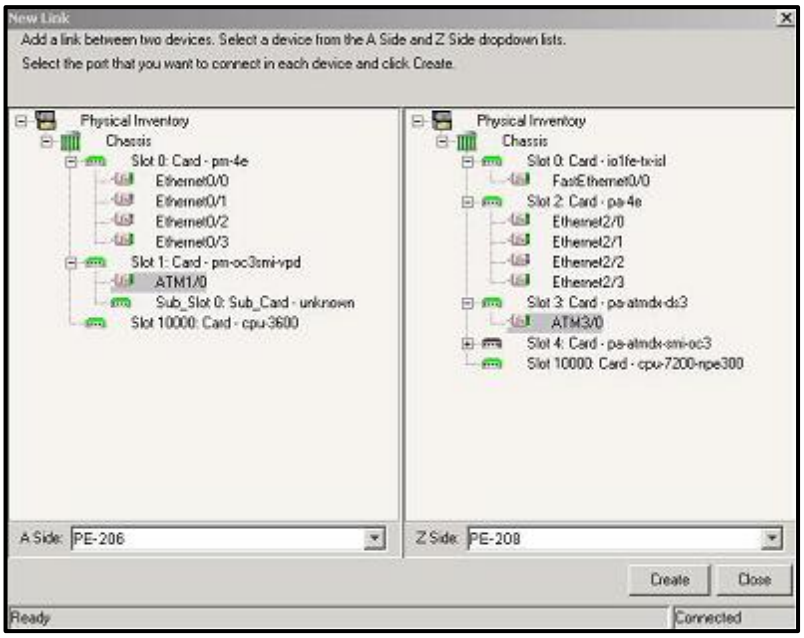


Figura 5.2.36: Nuevo Link[1]

5.2.4 EVENTVISION (VISOR DE SUCESOS ANA)

ANA EventVision es una herramienta de interfaz gráfica de usuario, que sirve como un navegador para ver todas las bases de datos de eventos actuales y pasados que se han producido en la red.

5.2.4.1 INICIALIZACIÓN DE EVENTVISION

1. Ejecutar la aplicación.

2. Ingresar la información en el cuadro de diálogo de inicio de sesión:

   - ✓ Nombre de usuario
   - ✓ Contraseña
   - ✓ Host(ANA GW dirección IP del servidor o nombre de host)

Los controles del cliente para una nueva versión se pueden actualizar automáticamente si es necesario.

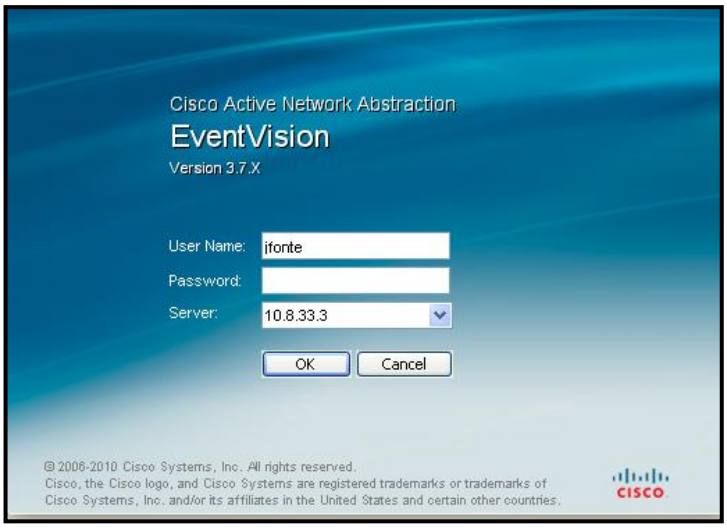


Figura 5.2.37: Inicio EventVision[1]

La ventana EventVision almacena todos los eventos de red de ANA, organizados en categorías.

Las categorías de eventos son las siguientes:

- ✓ Auditoría
- ✓ Aprovisionamiento
- ✓ Seguridad
- ✓ Servicio
- ✓ Syslog
- ✓ Sistema
- ✓ Ticket
- ✓ V1 Trap
- ✓ V2-V3 Trap

EventVision presenta opciones de page, refresh, filter, auto-refresh, split screen, event information y event categories como se indica en la figura 5.2.38.

Cada categoría de eventos contiene un conjunto diferente de campos de información. La ventana EventVision cambia sus columnas dinámicamente, de acuerdo con el tab de la categoría seleccionada.

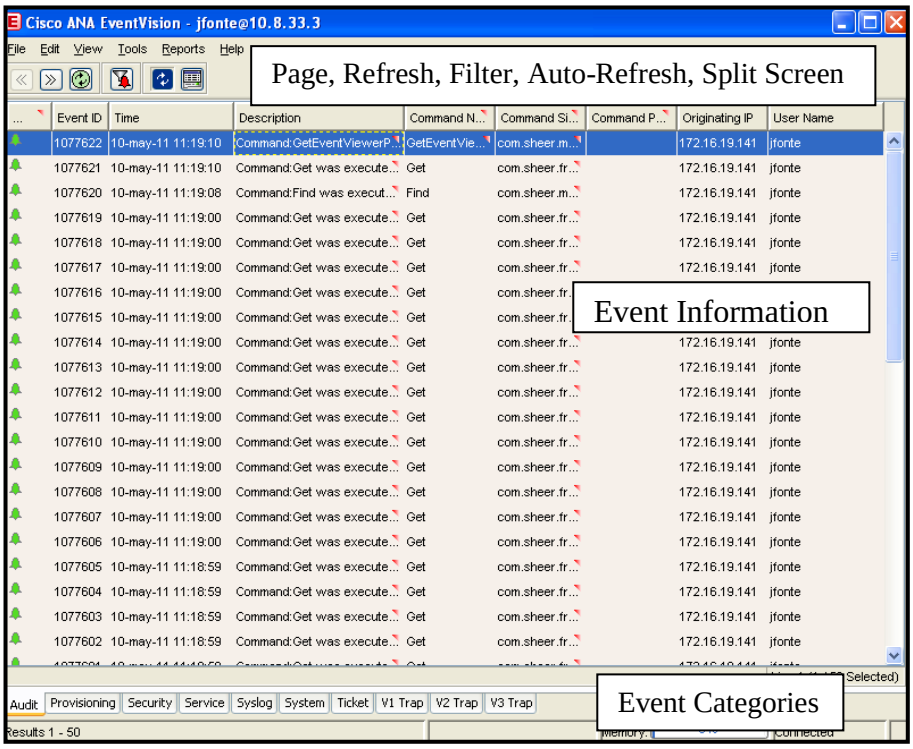


Figura 5.2.38: Ventana Principal EventVision[1]

Cada evento listado incluye información básica como: Gravedad, tiempo y descripción

Todos los eventos contienen una gravedad. Esta gravedad está identificada por un color especifico los mismos que se muestran en la siguiente tabla 5.2.1.

ICONO	COLOR	GRAVEDAD
	ROJO	CRITICO
	NARANJA	MAYOR
	AMARILLO	MENOR

	CELESTE	ADVERTENCIA
	VERDE	AUTORIZADO, NORMALÓ OK.
	AZUL	INFORMACIÓN
	BLANCO	INDETERMINADO

Tabla 5.2.1- Indicadores de estado[1]

5.2.4.2 DETALLES EVENTVISION

Este panel de visualización muestra información básica acerca de cada evento listado como gravedad, tiempo y descripción.

Para visualizar más detalles proceder a dar doble clic en el evento y se desplegará una pantalla con los detalles de dicho evento como se muestra en la figura 5.2.39:

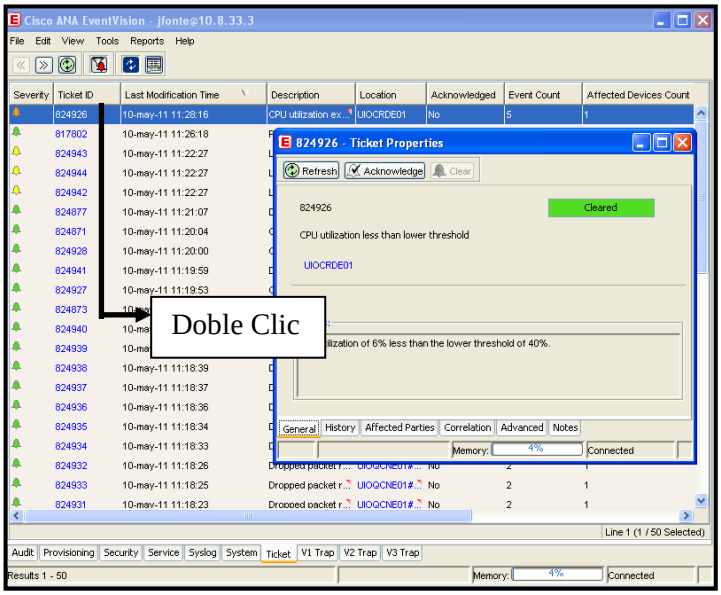


Figura 5.2.39: Detalles EventVision[1]

5.2.4.3 DETALLES -SPLIT SCREEN

Los detalles de los eventos pueden también ser mostrados como parte del panel de visualización.

Seleccionar el ícono *Split Screen* de la barra de herramientas, se mostrará un panel de nivel dos, el panel superior mostrará la lista de eventos para el tab seleccionado y el panel inferior mostrará los detalles del evento seleccionado como se indica en la figura 5.2.40:

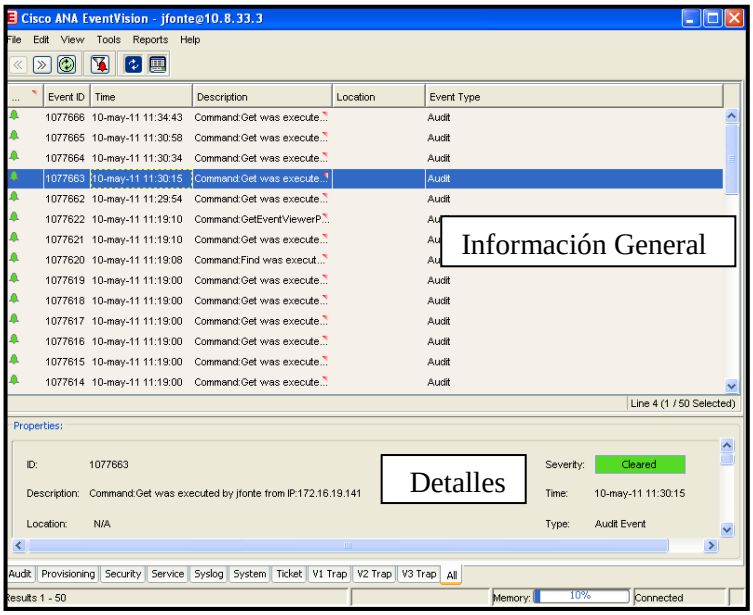


Figura 5.2.40: Split Screen[1]

A continuación se detalla cada una de las pestañas que presenta el tab EventVision.

5.2.4.4 TAB ALL

Muestra los campos de eventos que son comunes a todas las categorías, tales como:

- ✓ Gravedad
- ✓ Identificador de sucesos
- ✓ Descripción del evento

- ✓ Tiempo
- ✓ Tipo de evento

El administrador del sistema puede filtrar los campos que aparecen en la ventana. Los eventos se eliminan automáticamente de la base de datos después de un período de antigüedad definida por el usuario.

A veces la solución a problemas pueden ser asistidos por tener lista cronológica de todos los eventos, esto se puede lograr seleccionando las opciones *File/Open*, *AllTab*, con ello se añade un nuevo tab como se indica en la figura 5.2.41:

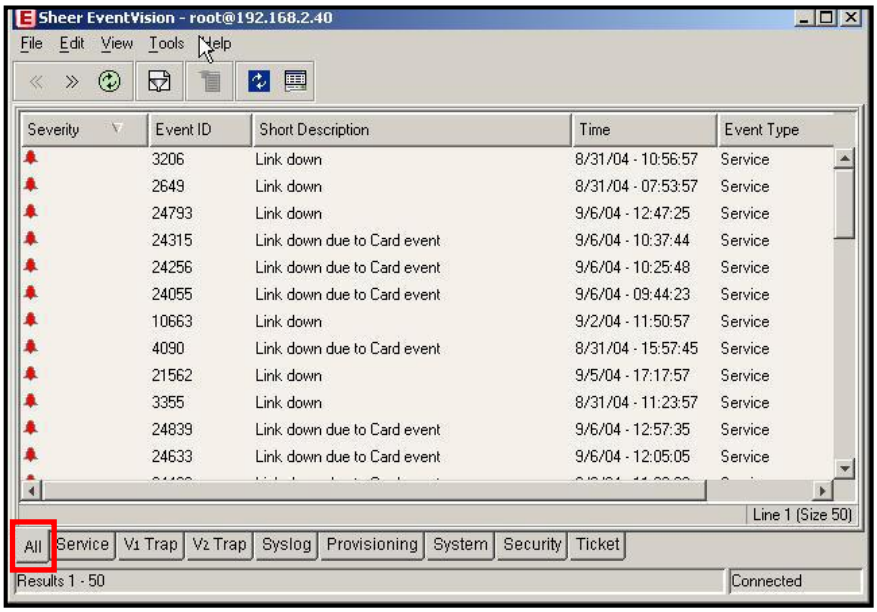


Figura 5.2.41: Tab All[1]

5.2.4.5 TAB AUDIT

Registra todos los comandos que se ejecutan en Cisco ANA Gateway como se indica en la figura 5.2.42:

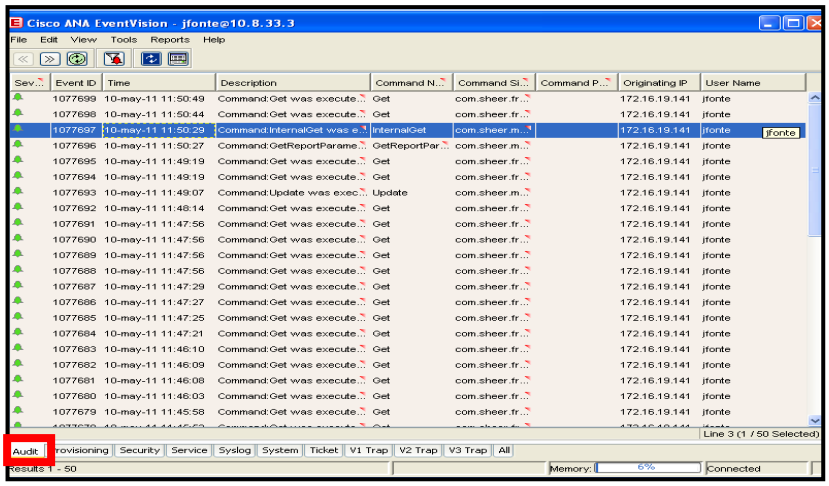


Figura 5.2.42: Tab Audit[1]

5.2.4.6 TAB PROVISIONING

Muestra registros de toda la configuración y aprovisionamiento de las actividades que están relacionadas en un Cisco ANA como se indica en la figura 5.2.43:

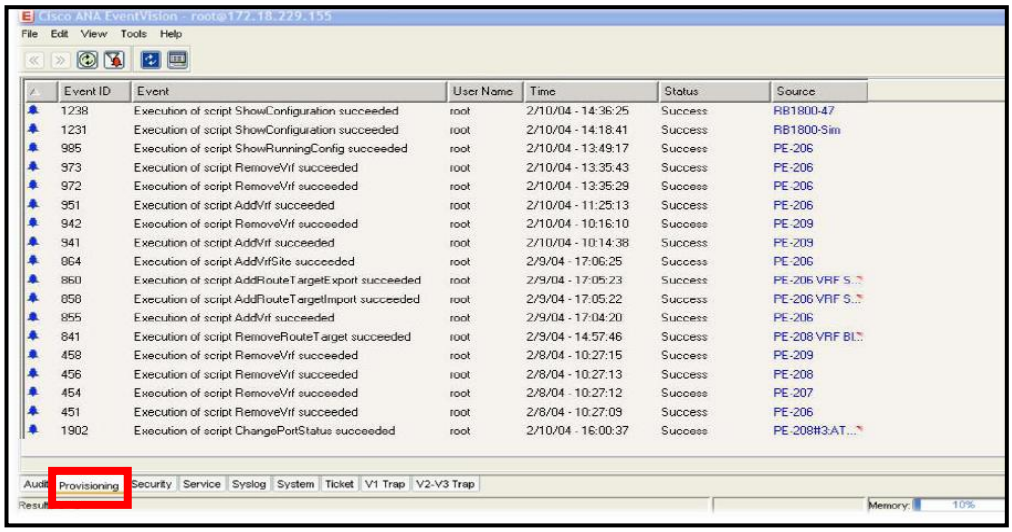


Figura 5.2.43: Tab Provisioning[1]

5.2.4.7 TAB SECURITY

Registra todas las actividades de administración del usuario y acceso del cliente como se muestra en la figura 5.2.44:

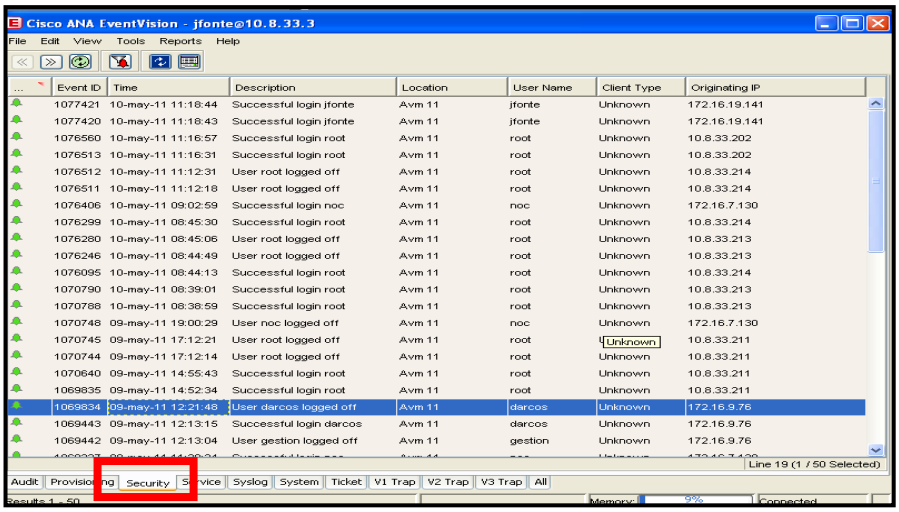


Figura 5.2.44: Tab Security[1]

5.2.4.8 TAB SERVICE

Muestra todos los eventos de alarmas generadas por el sistema Cisco ANA por ejemplo un enlace caído como indica la figura 5.2.45:

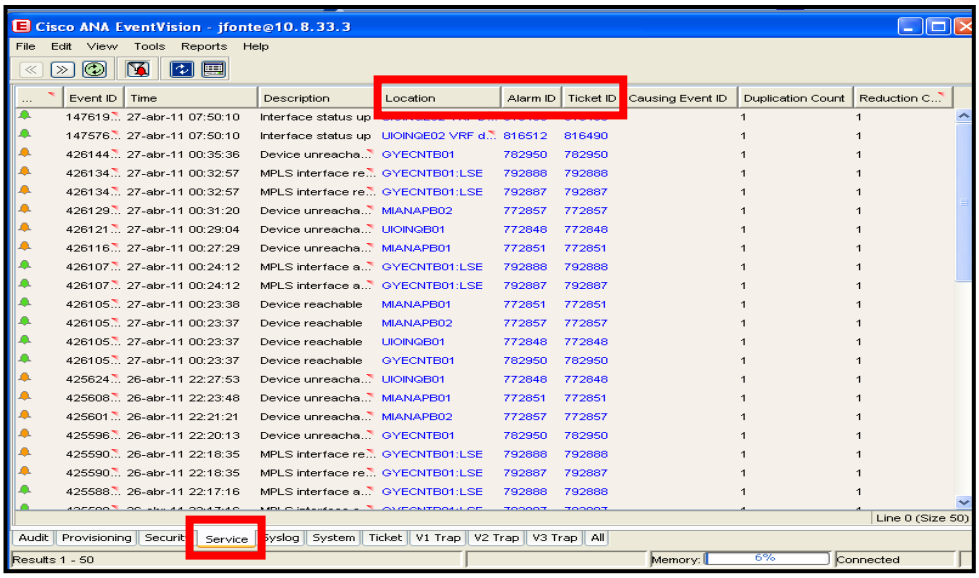


Figura 5.2.45: Tab Service[1]

Al dar doble clic en uno de los equipos en la opción *Location* se despliega una pantalla que muestra información útil de dicho equipo como se indica en la figura 5.2.46:

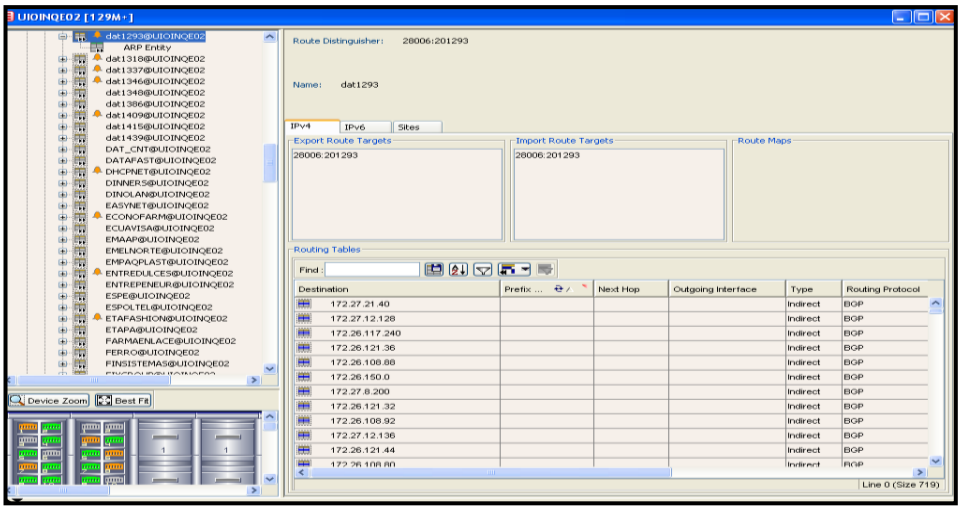


Figura 5.2.46: Location[1]

Al dar doble clic en cualquiera de las alarmas en la opción *Alarm Id* que se muestra en la figura 5.2.45 se despliega una pantalla la misma que contiene información del Ticket Id y de la Localización como se indica en la figura 5.2.47:

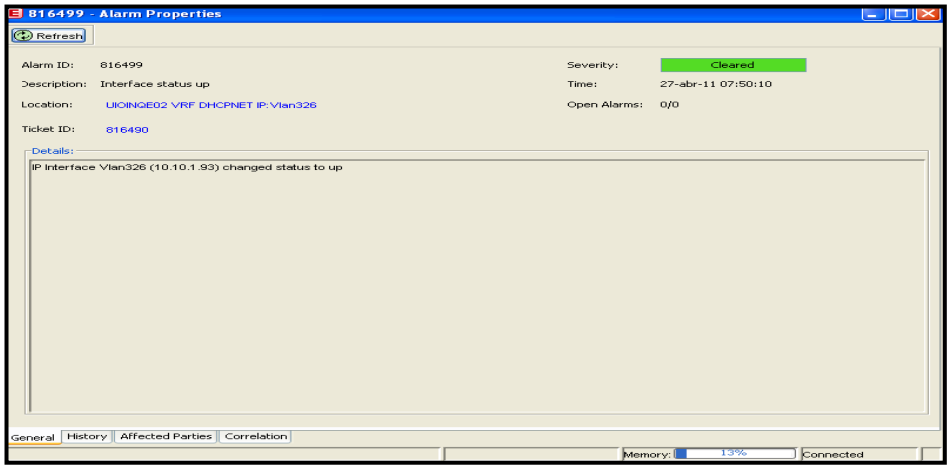


Figura 5.2.47: Información de Alarma Id[1]

Al dar doble clic en el número de *Ticket Id* que se indica en la figura 5.2.45 se despliega otra pantalla con detalles del ticket abierto a causa de la alarma como muestra la figura 5.2.48:

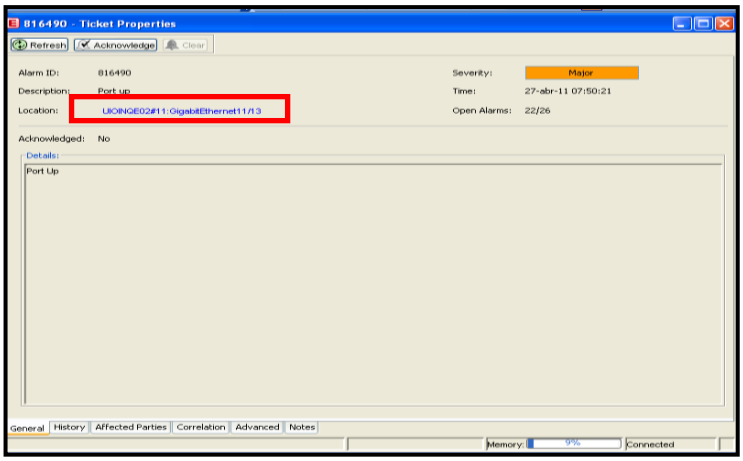


Figura 5.2.48: Información de Ticket Id[1]

Al dar doble clic en la localidad en la que se encuentra el problema se despliega una pantalla con la información del *Phisical Inventory* como: status, puerto, descripción y número del conector, modo de la interface, vlans existentes, tipo de encapsulación y dirección MAC como indica la figura 5.2.49:

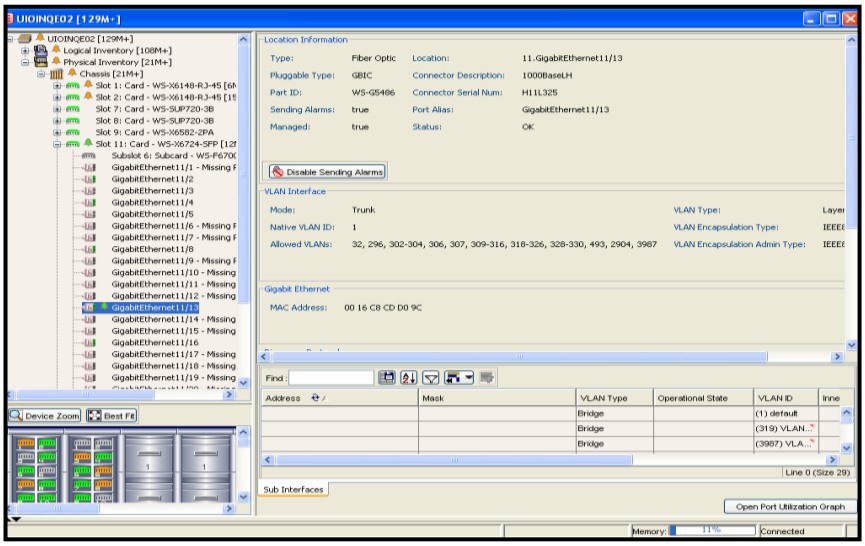


Figura 5.2.49: Phisical Inventory[1]

5.2.4.9 TAB SYSLOG

Contiene la lista de todos los eventos Syslog recibidos de los dispositivos. Los eventos Syslog son mensajes de registro del sistema enviados por los dispositivos y

las VNEs, estos presentan información adicional como el número de alarma, una breve descripción, ubicación y tiempo como se indica la figura 5.2.50:

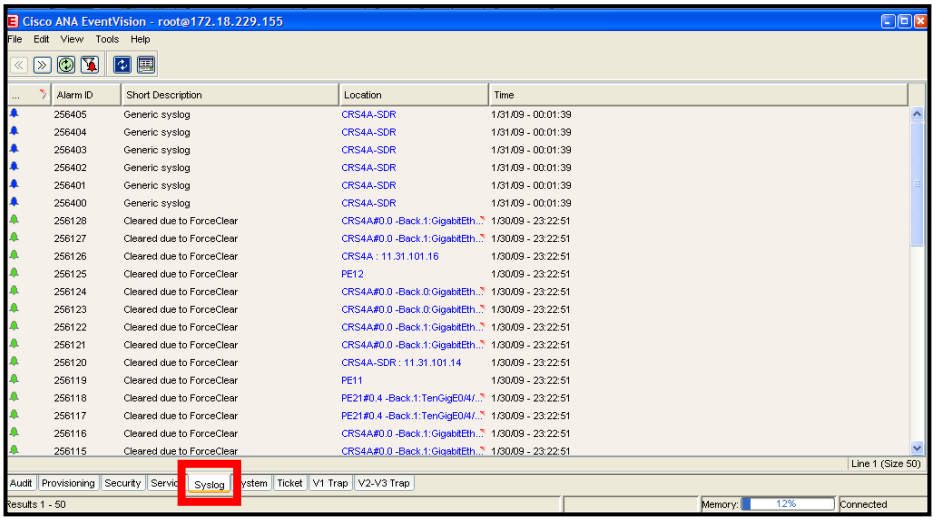


Figura 5.2.50: Tab Syslog[1]

5.2.4.10 TAB SYSTEM

Contiene los registros de todos los recursos del sistema Cisco ANA y está relacionado con los eventos en los servidores de Cisco ANA y sus componentes como se indica en la figura 5.2.51:

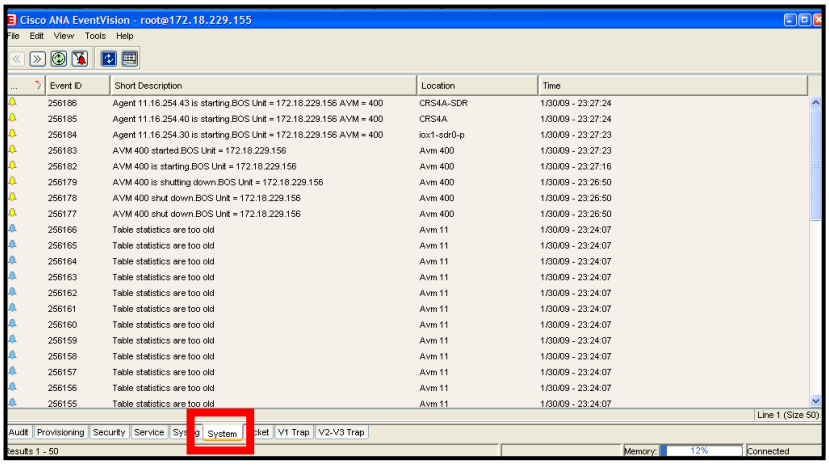


Figura 5.2.51: Tab System[1]

5.2.4.11 TAB TICKET

Registra todos los tickets que se abrieron en Cisco ANA como indica la figura 5.2.52:

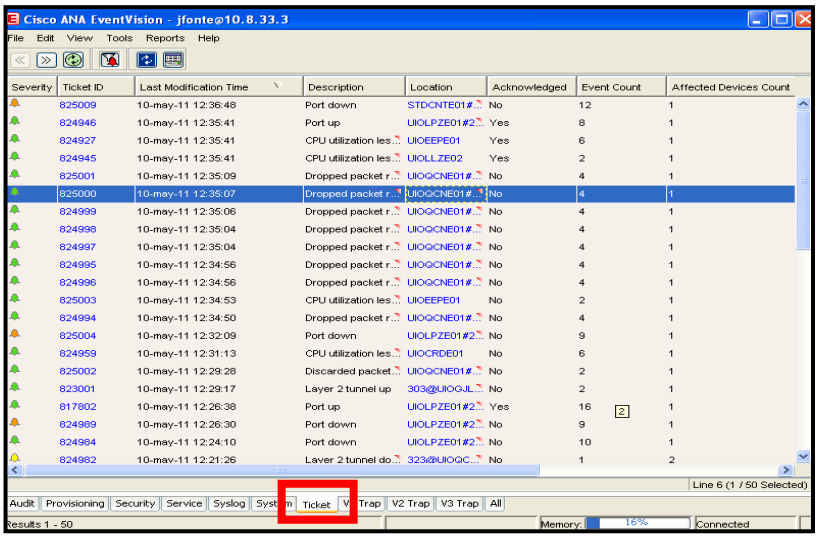


Figura 5.2.52: Tab Ticket[1]

5.2.4.12 TAB SNMP TRAPS

El tab SNMPV1 y V2/3 muestra todos las traps generadas por los dispositivos y recibido por ANA.

Este evento se activa cuando el elemento de red envía un mensaje para reportar ciertas condiciones y cambios de estado de los equipos, presenta información adicional como gravedad, número de alarma, breve descripción del proceso, y la ubicación y el tiempo como se indica en la figura 5.2.53:

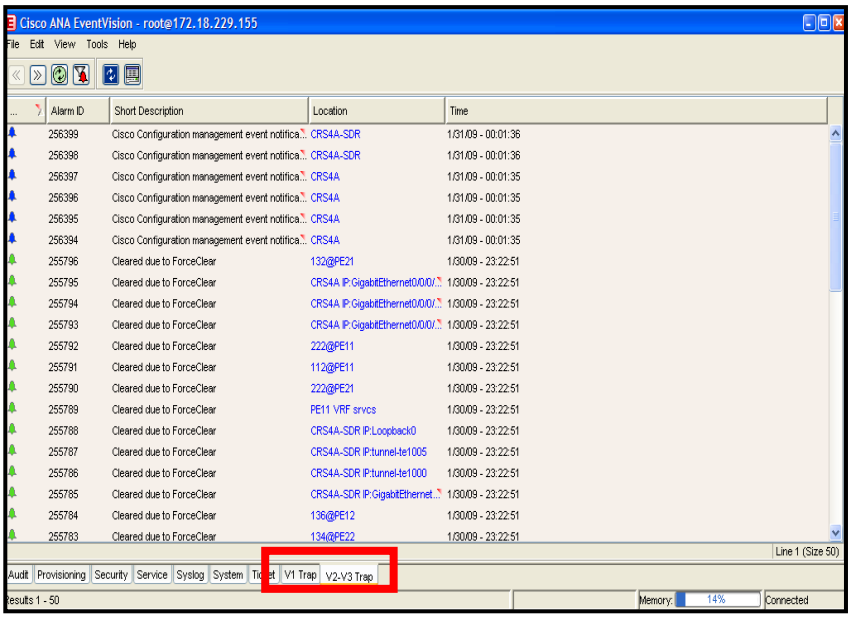


Figura 5.2.53: Tabs Traps[1]

5.2.5 CISCO ANA NETWORKVISION

Es un panorama de funcionalidad básica que permite trabajar con mapas, íconos y símbolos para administrar y personalizar la perspectiva de la red.

5.2.5.1 FUNCIONALIDAD DE NETWORKVISION

NetworkVision es la principal interfaz gráfica de usuario para Cisco ANA y proporciona una visibilidad completa de las redes.

Los usuarios pueden tener varias vistas de la red: árbol, mapa, servicio VPN, mapa de dispositivos o elementos con sus respectivas propiedades, vista de la información del inventario físico y lógico, de las propiedades de enlace así como la administración de las entradas de las alarmas.

5.2.5.2 INICIALIZACIÓN DE NETWORKVISION

Seguir los pasos que se indican:

1. Ejecutar la aplicación.

2. Ingresar la información en el cuadro de diálogo de inicio de sesión:

   - ✓ Nombre de usuario
   - ✓ Contraseña
   - ✓ Host(ANA GW dirección IP del servidor o nombre de host)

Los controles del cliente para una nueva versión se pueden actualizar automáticamente si es necesario.

Figura 5.2.54: Inicio NetworkVision [1]

Una vez que se ha ingresado a NetworkVision se encontrará con la siguiente pantalla principal de esta aplicación denominada workspace.

5.2.5.3 WORKSPACE

Este tab contiene un panel de navegación, contenido, ticket, una barra de herramientas y una de menú como se indica en la figura 5.2.55:

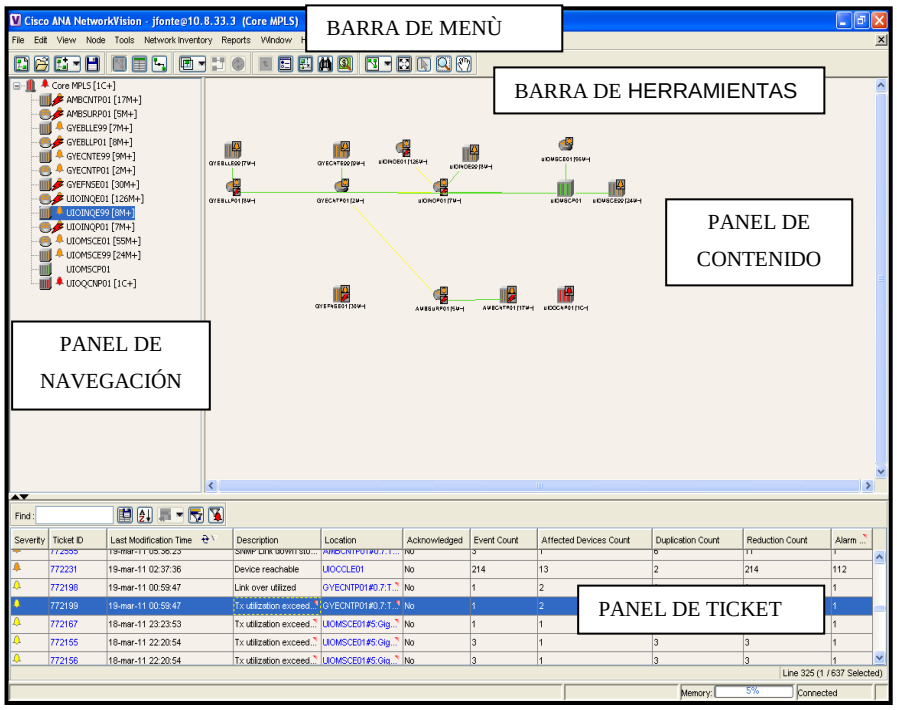


Figura 5.2.55: Pantalla principal de NetworkVision[1]

Después de ingresar a la aplicación NetworkVision el usuario puede personalizar las siguientes configuraciones: *Startup*, *Display* y *Audio* a través de la barra de menú.

Elegir en la barra de menú la opción *Tools/Option* en la cual aparecerá la siguiente pantalla como se indica en la figura 5.2.56:

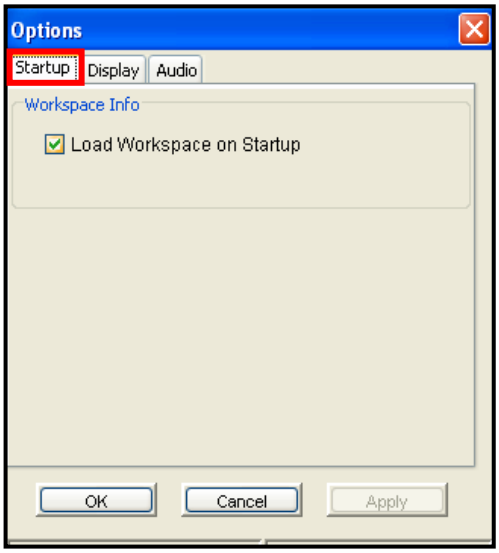


Figura 5.2.56: Pantalla de Opciones[1]

5.2.5.4 TAB STARTUP

Muestra una lista de los mapas que fueron abiertos cuando la última sesión fue cerrada.

5.2.5.5 TAB DISPLAY

Permite modificar las configuraciones de gravedad al momento que una alarma se activa como se indica en la figura 5.2.57:

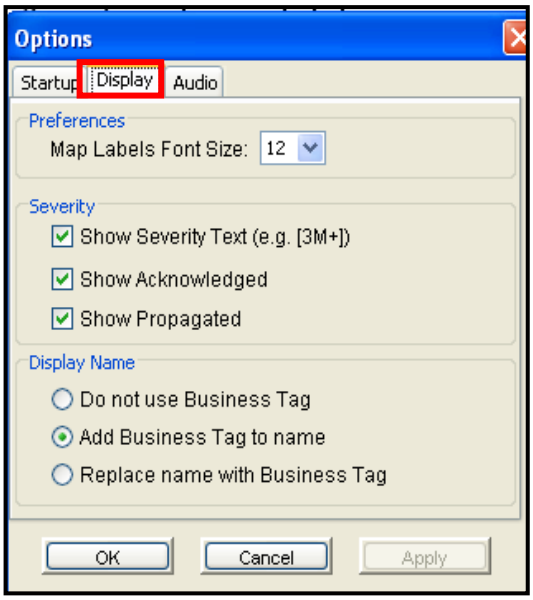


Figura 5.2.57: Display[1]

Las siguientes son las configuraciones que se pueden cambiar:

- **SEVERITY**

Se recomienda habilitar las siguientes opciones:

- ✓ **Show Severity Text:** Muestra las etiquetas de gravedad en el panel de navegación y mapas.
- ✓ **Show Acknowledged:** Muestra la gravedad de una alarma crítica después de que la alarma es conocida.
- ✓ **Show propagated:** Muestra solo las alarmas de una entidad específica.

- **DISPLAY NAME**

Se recomienda habilitar la siguiente opción:

- ✓ **AddbusinessTag:** Muestra el nombre original del elemento de red y el nombre del Business Tag.

5.2.5.6 TAB AUDIO

Permite seleccionar archivos de sonido para ser mostrados cuando una alarma se activa.

Estos archivos de sonidos pueden ser para alarmas de nivel crítico, mayor o menor como se muestra en la figura 5.2.58:

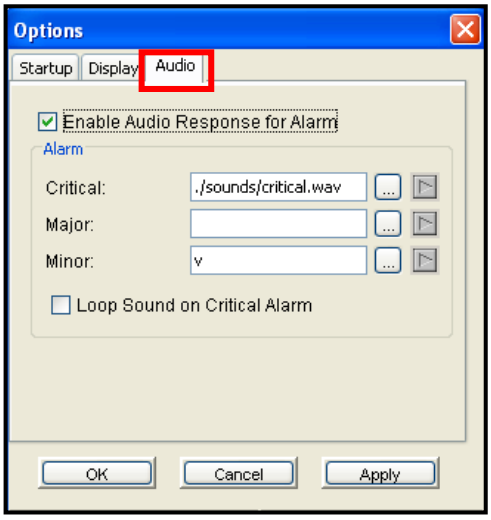


Figura 5.2.58: Audio[1]

5.2.5.7 BARRA DE HERRAMIENTAS NETWORKVISION

La barra de herramientas NetworkVision permite a los usuarios de manera fácil y rápida realizar operaciones diarias. La información sobre las herramientas se muestra al desplazar el puntero del mouse sobre los íconos de la barra de herramientas.

Las opciones disponibles dependen del nivel de permisos de usuario. Las opciones de la barra de herramientas varían dependiendo de su elección. Los ejemplos incluyen: Añadir túnel, inventario, cambio de tamaño, etc. Como indica la figura 5.2.59:

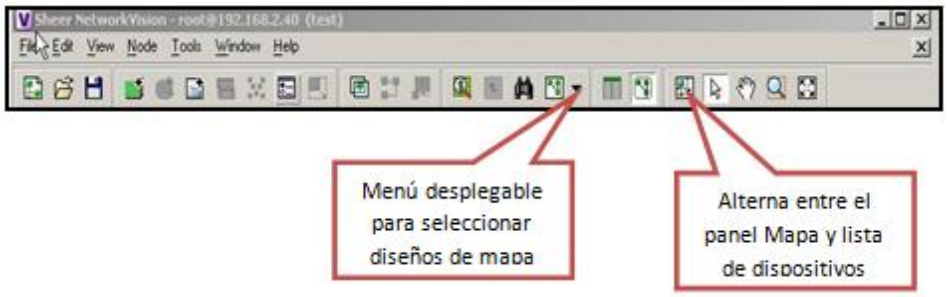


Figura 5.2.59: Barra de herramientas[1]

5.2.5.8 CREACIÓN DE UN MAPA

Para la creación de un mapa seguir los siguientes pasos:

1. En la barra de herramientas dar clic en *New Map* o seleccionar *New Map* del menú *File* como se indica en la figura 5.2.60.

2. Colocar el nombre del mapa el cual debe constar de entre 1 a 65 caracteres.

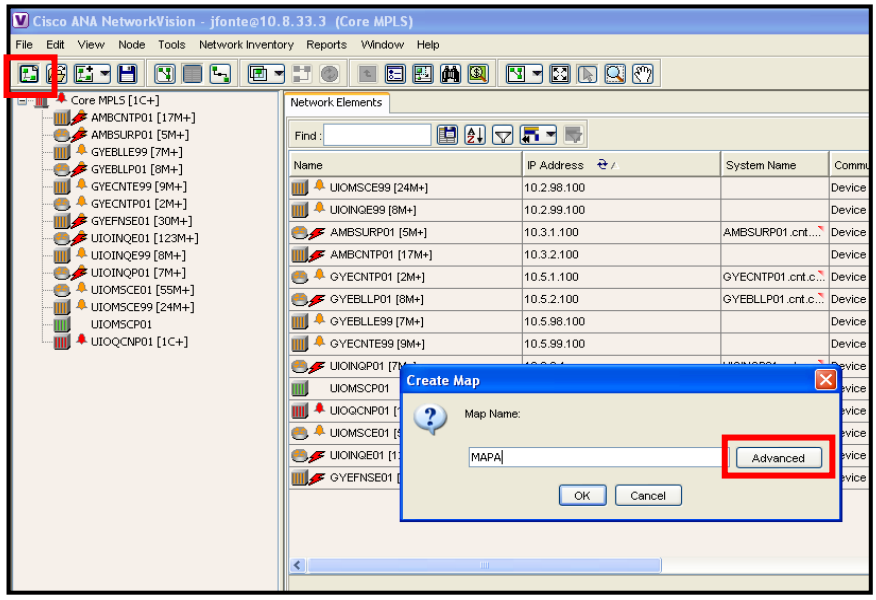


Figura 5.2.60: Nuevo Mapa[1]

3. El botón *Avanced* permite filtrar los enlaces que aparecen en el panel del mapa como se indica en la figura 5.3.60:

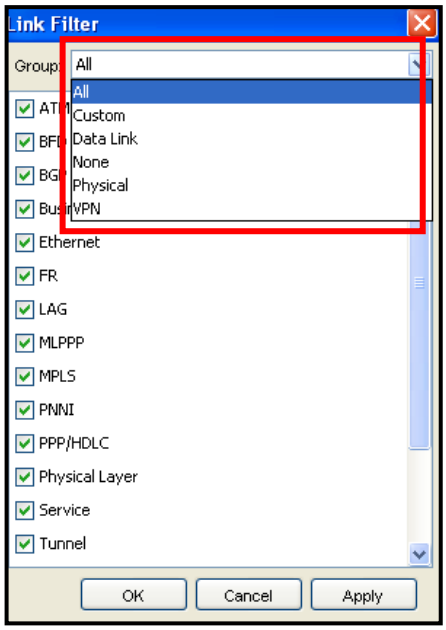


Figura 5.2.61: Link Filter[1]

4. Se puede seleccionar los tipos de enlaces que van a ser filtrados de un grupo predefinido de tipos de enlaces como se indica en la figura 5.2.61. Al colocar el mouse sobre el dispositivo se desplegarán los enlaces establecidos en el mismo.

5.2.5.9 CREACIÓN DE DISPOSITIVOS

Para la creación de un dispositivo seguir los siguientes pasos:

1. En la barra de herramientas dar clic en la opción *AddtoMap* y elegir el elemento de red o dar clic en *File/AddtoMap/Network Element*, como se indica en la figura 5.2.62:

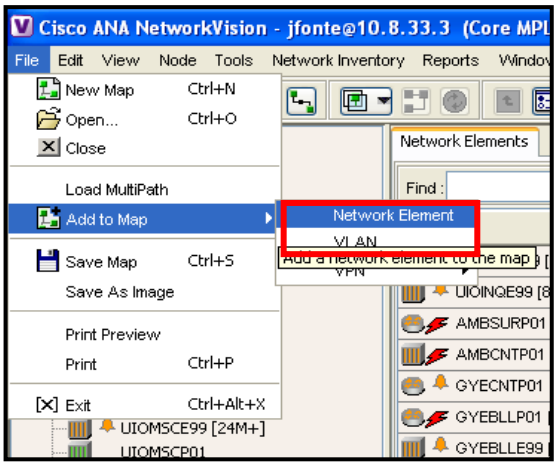


Figura 5.2.62: Opción AddMap[1]

2. En la lista de dispositivos seleccionar el dispositivo que se desee incluir en el mapa. Se puede seleccionar y añadir múltiples dispositivos mediante CTRL o CTRL+, como indica la figura 5.3.63:

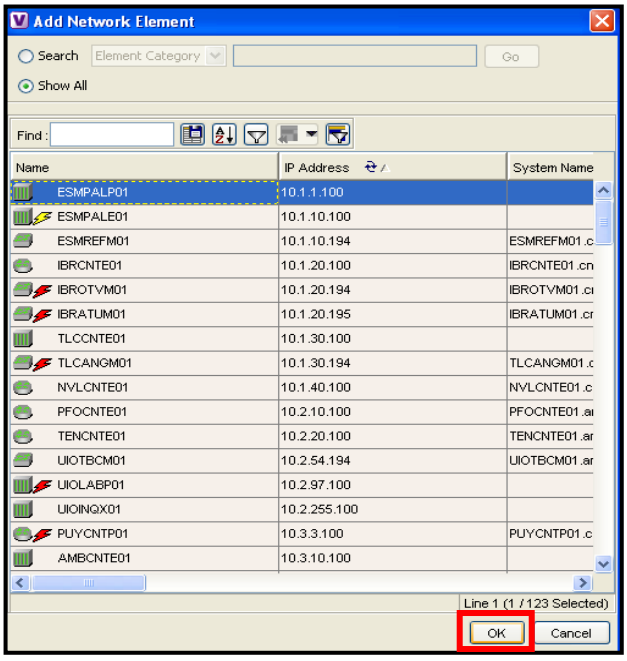


Figura 5.2.63: Selección de dispositivos[1]

5.2.5.10 AÑADIR VPNs A UN MAPA

Para la adición de VPNs a un mapa seguir los siguientes pasos:

1. En la barra de herramientas dar clic en *AddtoMap / VPN / EXISTING.*

2. Seleccionar las VPNs que se requieran incluir en el mapa como se indica en la figura 5.3.64:

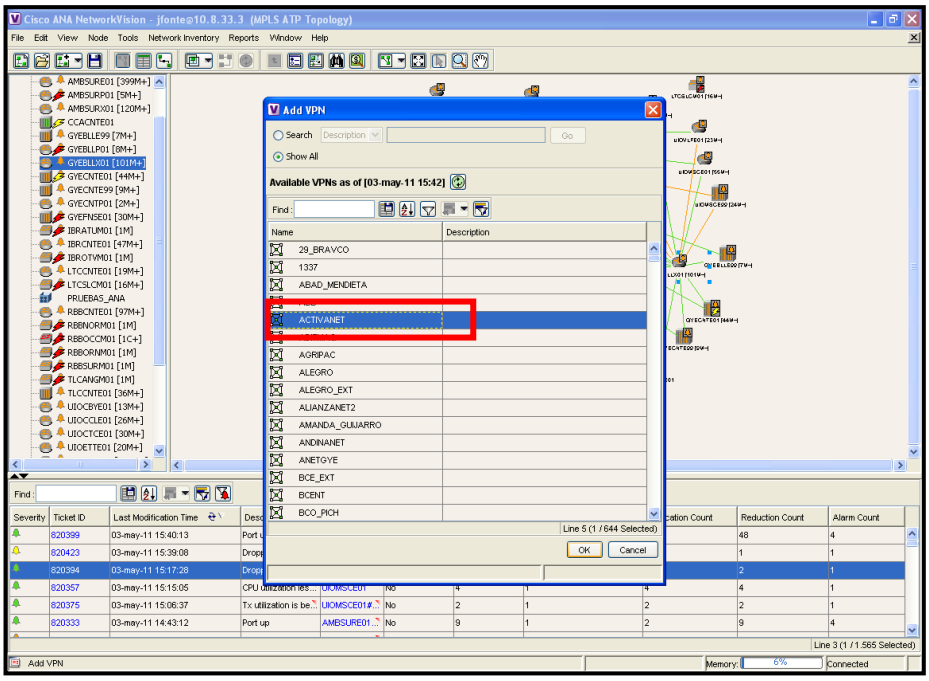


Figura 5.2.64: Adición de una VPN[1]

5.2.5.11 MAP VIEW

Proporciona un panel de árbol jerárquico de los elementos de red incluido en el mapa, así como el diseño topológico de la NEs, los enlaces y las agregaciones.

Cisco Ana Networkvision ofrece la elección de diversas herramientas de visualización que se pueden utilizar para conocer y analizar los mapas y su contenido. Los elementos de la red pueden ser agregados y la información se puede mostrar al colocar el mouse sobre un elemento de enlace o de la red, como se indica en la figura 5.3.65:

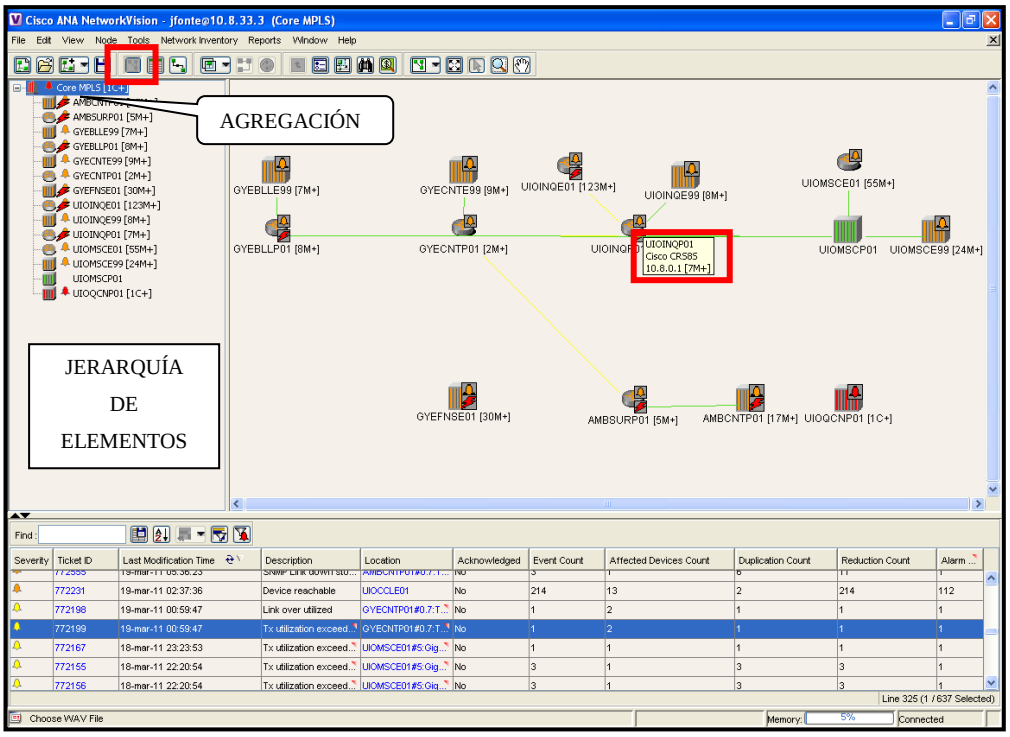


Figura 5.2.65: Map View[1]

El mapa topológico es la principal herramienta utilizada por Cisco ANA Network Vision para mostrar los vínculos y las relaciones entre los elementos de red y los nodos agregados.

5.2.5.11.1 ÍCONOS DE LOS DISPOSITIVOS

Cada elemento de red tiene cinco componentes que conforman el ícono y cada componente representa el estado o los atributos del elemento como se muestra en la figura 5.2.66:

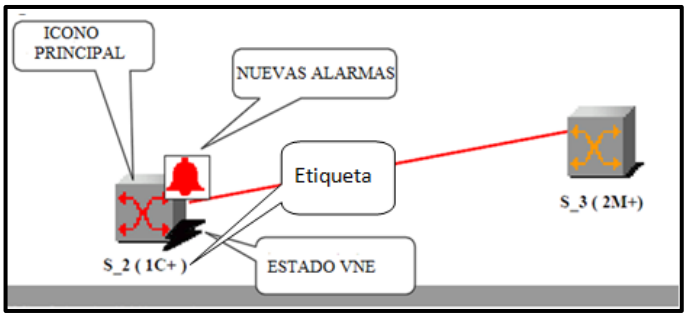


Figura 5.2.66: Icono de dispositivo[1]

- ✓ **Icono del dispositivo:** Indica el tipo de dispositivo.
- ✓ **Color del ícono del dispositivo:** Indica el estado y la gravedad del dispositivo.
- ✓ **Icono de las alarmas:** Indica la presencia de nuevas alarmas.

  Si no hay alarmas, o todas las alarmas activas se reconocen, entonces no se muestra el icono alarmas
- ✓ **Icono del estado de VNE:** Indica el estado de gestión.

  Si una VNE está en pleno funcionamiento entonces el icono VNE no se muestra.
- ✓ **Etiqueta del dispositivo:** Consiste en el nombre del dispositivo y la notación.

  Indica el número de alarmas con la mayor severidad.

  El signo + se utiliza para indicar alarmas adicionales de menor gravedad que también existen.

5.2.5.11.2 ÍCONOS Y SÍMBOLOS

A continuación se presentan los diversos íconos y su representación en el mapa.

ÍCONO	REPRESENTACIÓN
	Red no conocida
	Red, subred o agregación lógica
	Router
	SNMP genérico
	Switch Ethernet

	DSLAM
	ATM switch
	BRAS
	Visible para usuarios con más altos niveles de permiso
	Dispositivo fantasma
	VPN
	Router Virtual
	Site business element

Tabla 5.2.2- Íconos y Símbolos[1]

5.2.5.11.3 NIVELES DE GRAVEDAD

A continuación se muestran en la tabla 5.2.3 los niveles de gravedad que puede presentar un equipo o dispositivo.

ÍCONO	COLOR	GRAVEDAD
	ROJO	CRITICO
	NARANJA	MAYOR
	AMARILLO	MENOR
	CELESTE	ADVERTENCIA
	VERDE	AUTORIZADO,

		NORMAL Ó OK.
	AZUL	INFORMACIÓN
	BLANCO	DESCONOCIDO

Tabla 5.2.3- Niveles de gravedad [1]

5.2.5.11.4 ESTADOS VNE

En la tabla 5.2.4 se muestran los distintos estados que pueden presentar una VNE.

ESTADO	ÌCONO DEL MAPA	DESCRIPCIÓN
	VNE Inalcanzable	El Gateway no recibió ninguna respuesta de la VNE.
	Inicialización VNE	----------
	Equipo Inalcanzable	La VNE no logró alcanzar el equipo.
None	Operacional	----------
	Parcialmente Soportado	Algunos elementos de la VNE no son soportados en su totalidad.
	No compatible	La VNE no es compatible con el hardware del elemento de red, con la versión del software o el módulo del equipo.
	Equipo desconocido	El tipo del equipo es desconocido o la VNE ha sido

		detenida.
	Mantenimiento	El elemento de red se encuentra en up pero no ha sido monitoreada.

Tabla 5.2.4 -Estados de una VNE[1]

5.2.5.12 LIST VIEW

Para desplegar *List View* dar clic en *Show List View* de la barra de herramientas. Muestra los detalles de todos los dispositivos incluidos en el mapa actual de la red o subred como indica en la figura 5.2.67:

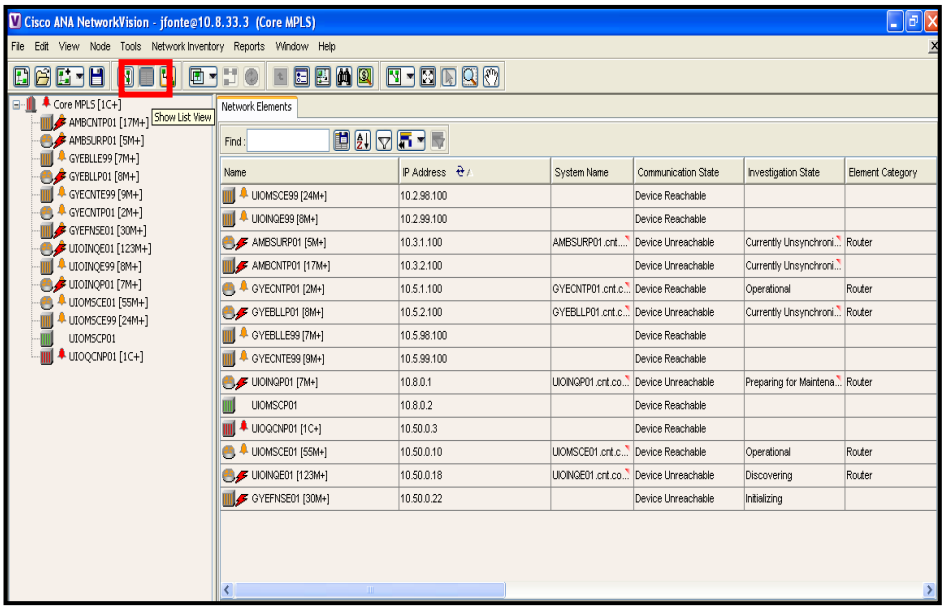


Figura 5.2.67: List View[1]

5.2.5.13 LINK VIEW

Para desplegar *Link View* dar Clic en Show *List View* de la barra de herramientas como se indica en la figura 5.2.68.

Link View muestra los enlaces dependiendo de las configuraciones realizadas en el *Link Filter*, cualquiera de los enlaces añadidos o removidos en el mapa son automáticamente añadidos o removidos al *Link View*.

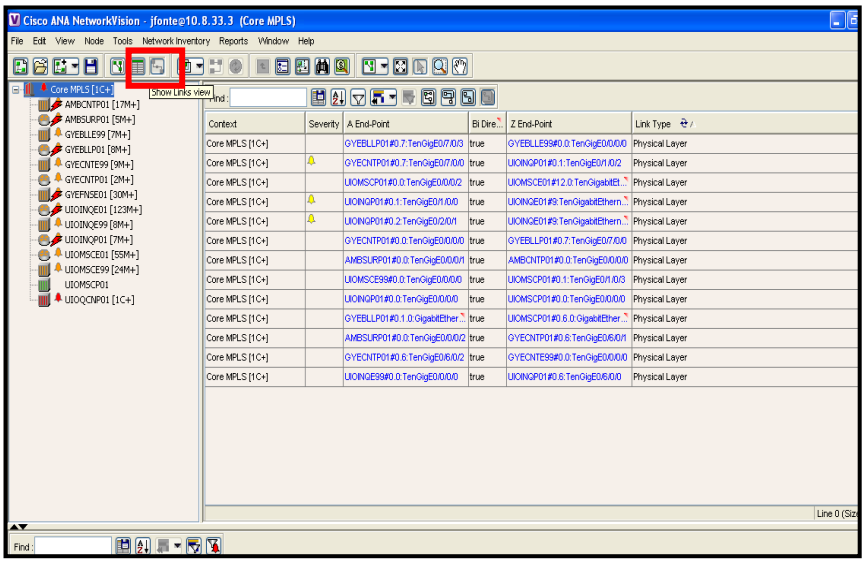


Figura 5.2.68: Link View[1]

5.2.5.14 OVERLAYS

Para desplegar *overlays* dar clic en *Choose overlay Type* de la barra de herramientas como se indica en la figura 5.2.69.

Permite visualizar que dispositivos y enlaces son parte de un servicio específico (VPN ó VLAN).

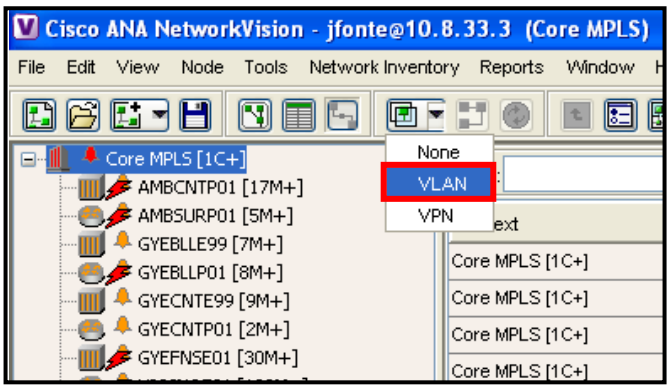


Figura 5.2.69: Overlay[1]

Escoger una VPN ó VLAN específica de acuerdo a los requerimientos como indica la figura 5.2.70:

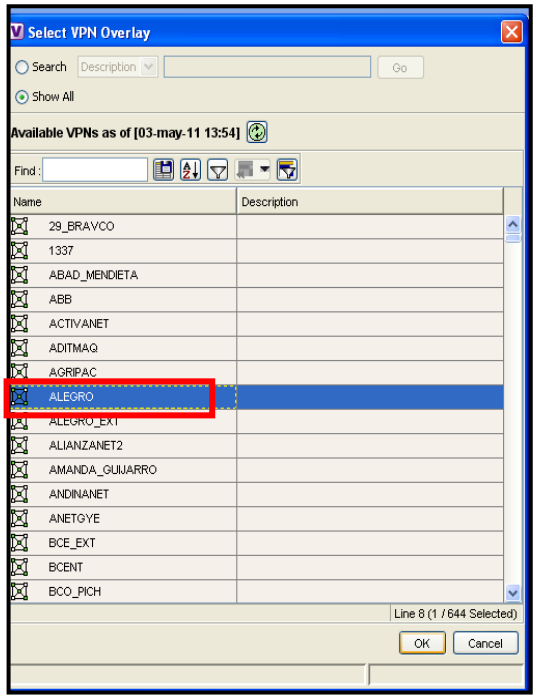


Figura 5.2.70: Selección de Vlan o Vpn[1]

5.2.5.15 LAYOUT MAP

En este mapa se realiza el posicionamiento de la NEs (Network Element) y sus agrupaciones (grupos de NE). Las NEs pueden ser reposicionadas en el mapa. Los elementos pueden ser organizados automáticamente seleccionando el ícono del diseño del mapa, los diseños predefinidos para el mapa son: Circular, Symmetric, Tree, Hierarchical.

Escoger de la barra de herramientas *Layout Map* para elegir cada una de las opciones de mapas que se requiera como se indica en la figura 5.2.71:

Figura 5.2.71: LayoutMap[1]

A continuación se presentan los distintos tipos de topologías que se pueden establecer como se muestra en la figura 5.2.72:

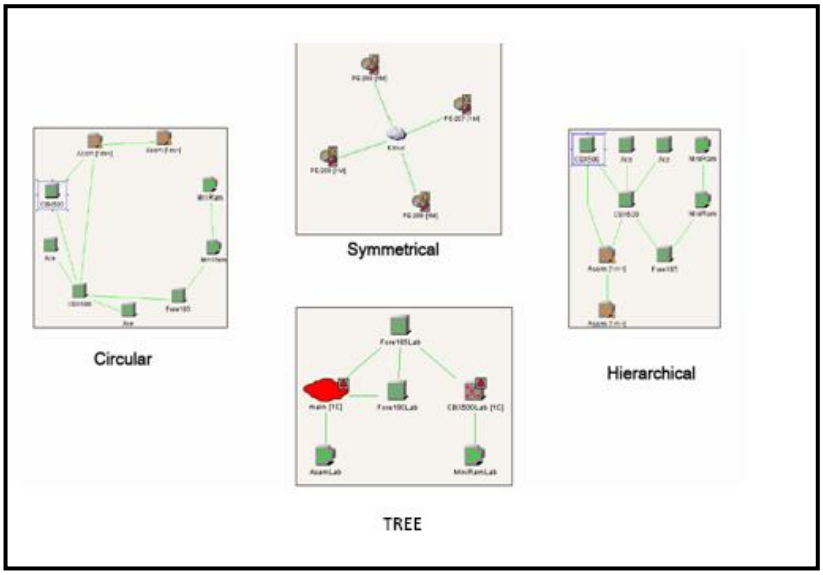


Figura 5.2.72: Tipos de mapas[1]

5.2.5.16 TICKET PANE

Ticket pane muestra todos los tickets abiertos (por causa de alarma). La jerarquía completa de alarmas aparece al visualizar la ventana de *Ticket Properties* dando doble clic en cualquiera de los *ticket ID* como se indica en la figura 5.2.73.

La gravedad se propaga hacia arriba en la jerarquía de la red.

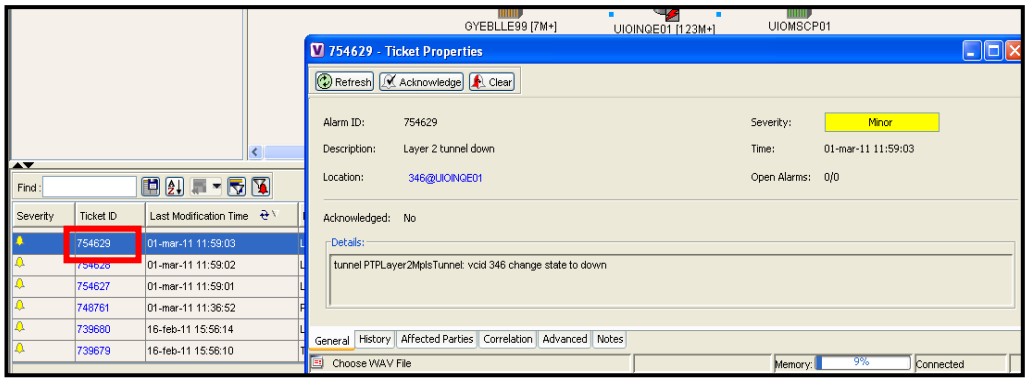


Figura 5.2.73: Ticket Properties[1]

5.2.5.17 VENTANA INVENTORY

Para visualizar esta ventana dar doble clic en el elemento de red del mapa o seleccionar el elemento de red y seleccionar de la barra de menú *Node/Inventory* ó a su vez dar clic derecho en elemento de red del mapa y seleccionar *Inventory*.

A continuación aparecerá la siguiente pantalla como se muestra en la figura 5.2.74:

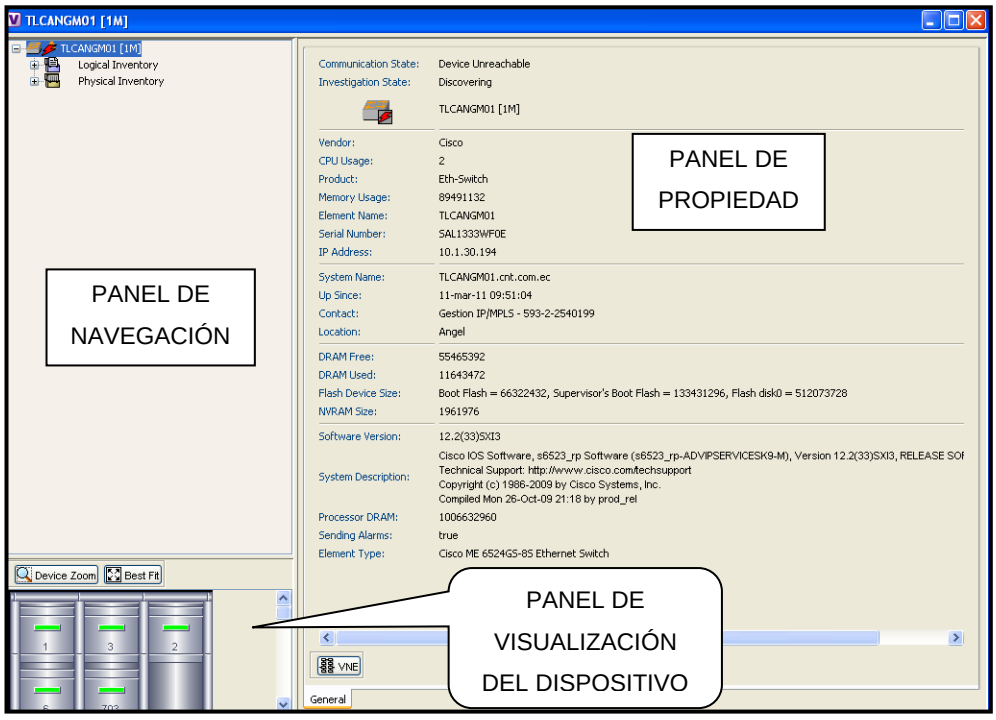


Figura 5.2.74: Inventory [1]

Permite visualizar los componentes físicos y lógicos de un dispositivo y su estado.

- ✓ **Physical Inventory:** Incluye los diferentes componentes del dispositivo como son chasis, tarjetas, subslots entre otros.

- ✓ **Logical Inventory:** Incluye información tal como tráfico ATM, *Access list* y entidades de enrutamiento.

5.2.5.18 BUSSINES TAG

Un *bussiness tag* puede ser usado para etiquetar un componente de un elemento de red. Es un registro que se almacena en la base de datos del Gateway y está asociado con el elemento que se ha configurado.

Un *Bussines Tag* es una construcción u organización de ciertos elementos de la red y sus propiedades en una entidad lógica, para proporcionar capacidad y realizar el seguimiento con una mejor perspectiva, esto incluye elementos de capa 2, capa 3 y routers virtuales.

5.2.3.5.9.2 CREACIÓN DE UN BUSSINESS TAG

Para la creación de un *Bussiness Tag* realizar los siguientes pasos:

1. Elegir un elemento de red y dar clic derecho y escoger *Attach bussiness tag.*

2. En el cuadro de diálogo colocar la información requerida:

   - ✓ Una clave única
   - ✓ Nombre del bussiness tag
   - ✓ Tipo de bussiness tag: *Suscriber, Provider Connection o Label*

3. Guardar los cambios generados

Todos estos parámetros se muestran en la figura 5.2.75.

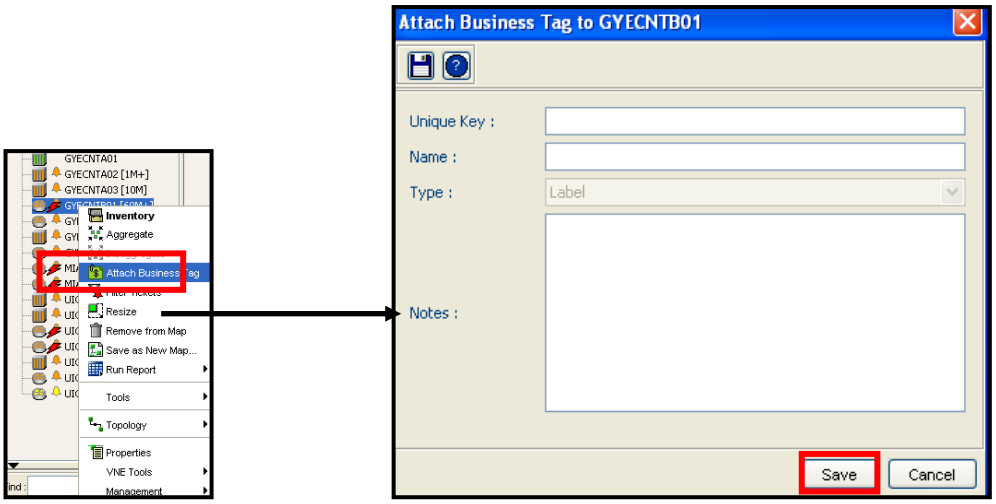


Figura 5.2.75: Bussiness Tag[1]

5.2.5.19 REPORTS OVERVIEW

Cisco ANA proporciona un informe de gestión que le permite generar, visualizar y exportar informes de la información administrada por Cisco ANA.

Se puede guardar los reportes generados en cualquiera de los siguientes formatos: PDF, CSV, HTML, XLS y XMLL.

5.2.5.19.1 TIPOS DE REPORTES

- ✓ **Eventos:** La información relativa de eventos syslog y tickets abiertos.
- ✓ **Inventory (Inventario):** Versión de Software, resumen de la información.

5.2.5.19.2 GENERACIÓN DE INFORMES

En la barra de menú de Networkvision elegir la opción *Reports* en la cual existen dos opciones *Report Manager* y *RunReport* para crear, generar y administrar todos los reportes como se muestra en la figura 5.2.76:

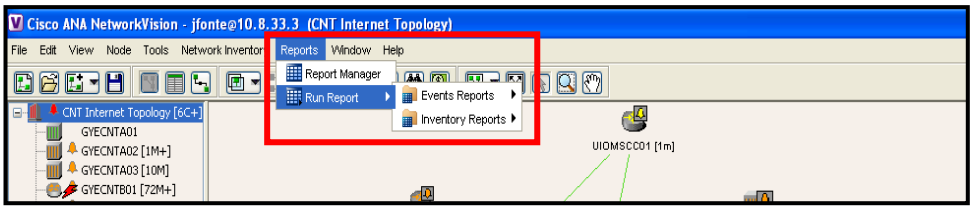


Figura 5.2.76: Reportes[1]

El gestor de informes está disponible en Cisco ANA Networkvision, ANA Manage y EventVision para la elección de informes, escogiendo la opción *Reports/ReportManage.*

Report manage permite ejecutar informes estándar como el número de syslogs por equipo o para definir informes adaptados a su entorno.

El panel de navegación muestra la representación jerárquica de los reportes y sus diferentes tipos como se muestra en la figura 5.2.77:

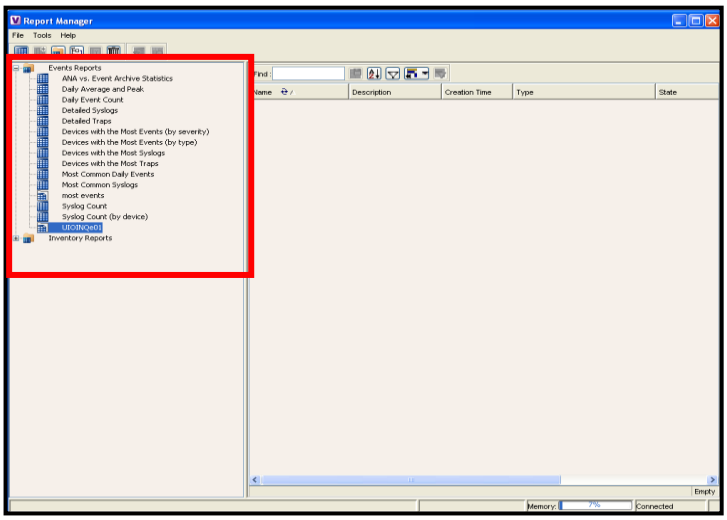


Figura 5.2.77: Reportes en orden jerárquico[1]

Las carpetas de informes normalizadas que figuran en el gestor ANA son de eventos y de inventario. Cada carpeta contiene los tipos de informes que se proporcionan con CISCO ANA, además el usuario definen los mismos.

5.2.5.19.3 CREACIÒN DE UN REPORTE

Para generar un reporte del *Menu Reports* seguir los siguientes pasos:

1. Escoger *Reports/Run, Report/folder/report-type,* donde: *Folder* es el requerimiento del archivo como se indica en la figura 5.2.78:
   Report-type es el requerimiento del tipo de reporte.

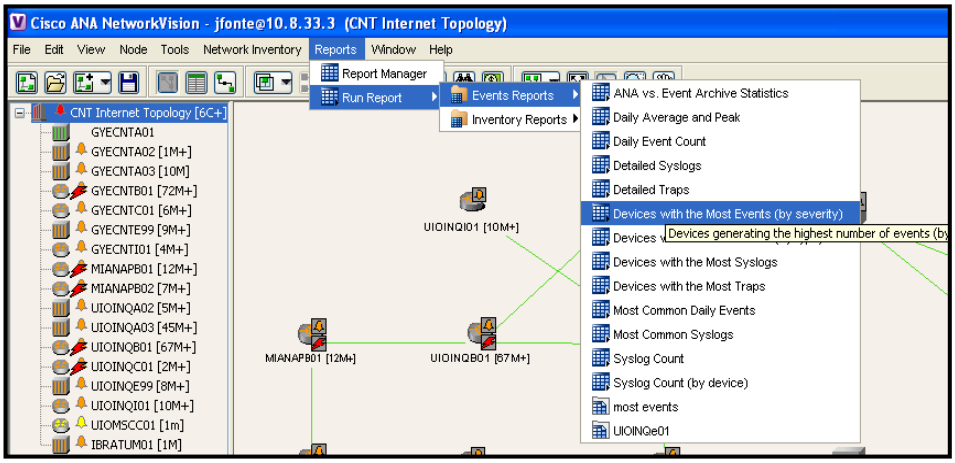


Figura 5.2.78: Tipo de reportes[1]

2. Dar clic derecho en el tipo de reporte y elegir Run.

3. En el cuadro de diálogo del *RunReports* colocar la información requerida y dar clic en Ok.

4. En la opción *Report Settings*, especificar el nombre del reporte la descripción y la seguridad del reporte la misma que puede ser pública o privada.

   Prívate: El reporte puede ser visualizado o usado únicamente por el creador del reporte o el administrador.

   Public: El reporte puede ser visualizado o usado por otros usuarios.

5. En la opción *Data Selection*, especificar el tiempo de concurrencia de los reportes ya sea en segundos, minutos, horas, días, meses y años.

6. En la opción *DeviceSelction*, especificar el equipo que se requiera añadir al reporte mediante la opción *Add*.

Todos estos parámetros se muestran en la figura 5.2.79:

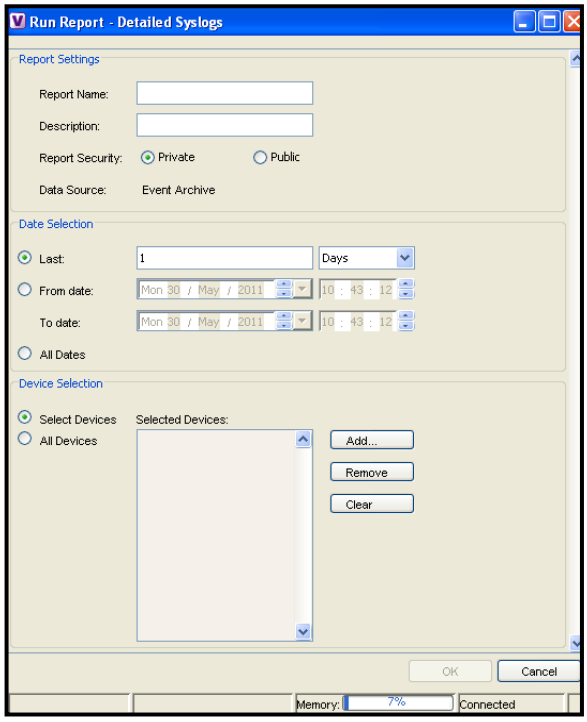


Figura 5.2.79: Run Report[1]

A continuación se presentan los mapas que se encuentran levantados en la red de la Corporación Nacional de Telecomunicaciones:

➢ CNT MPLS NETWORK

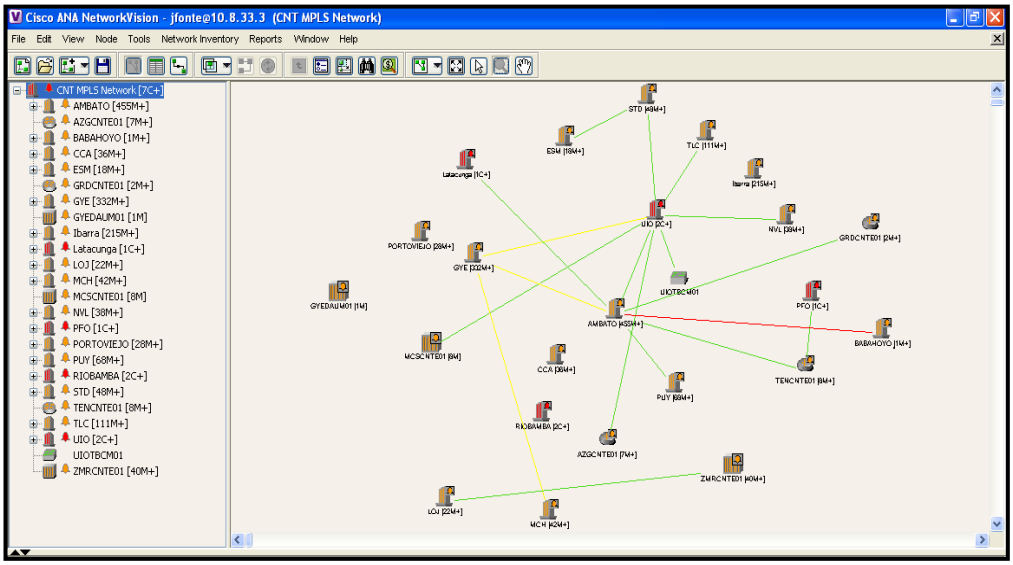


Figura 5.2.80: CNT MPLS NETWORK[1]

➢ CNT INTERNET TOPOLOGY

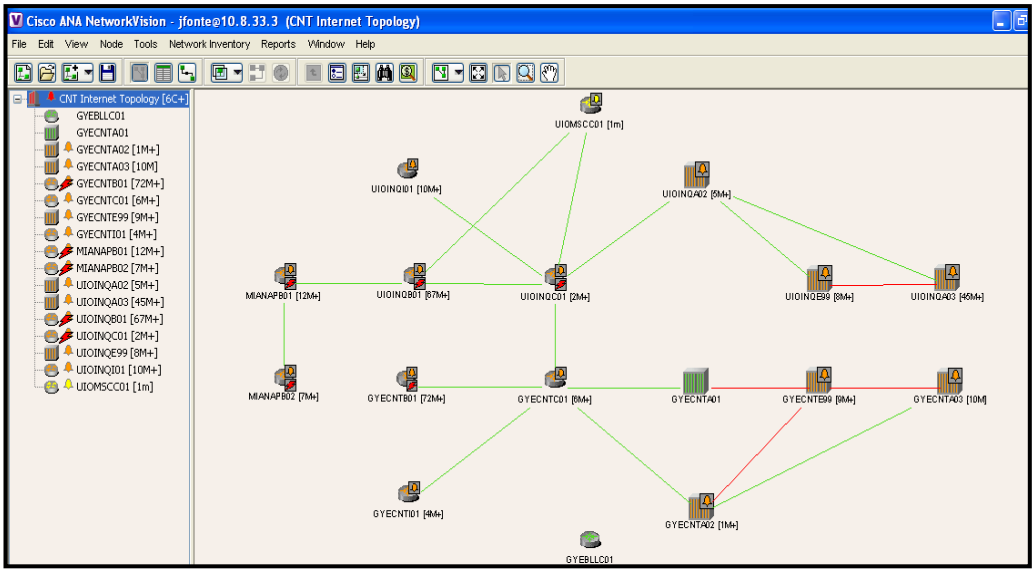


Figura 5.2.81: CNT INTERNET TOPOLOGY[1]

➢ MPLS FASE I

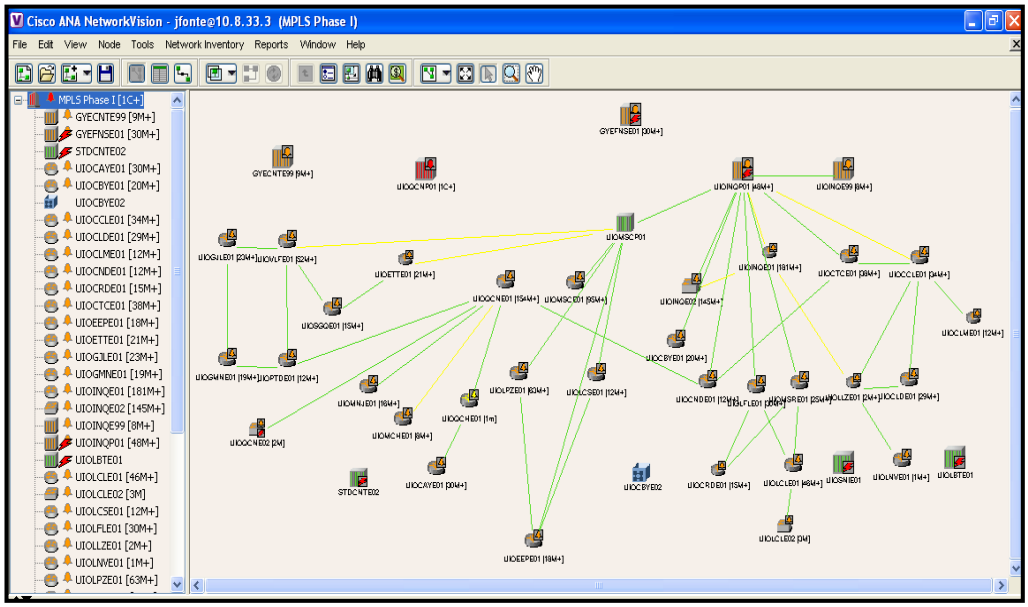


Figura 5.2.82: MPLS FASE I[1]

➢ CORE MPLS

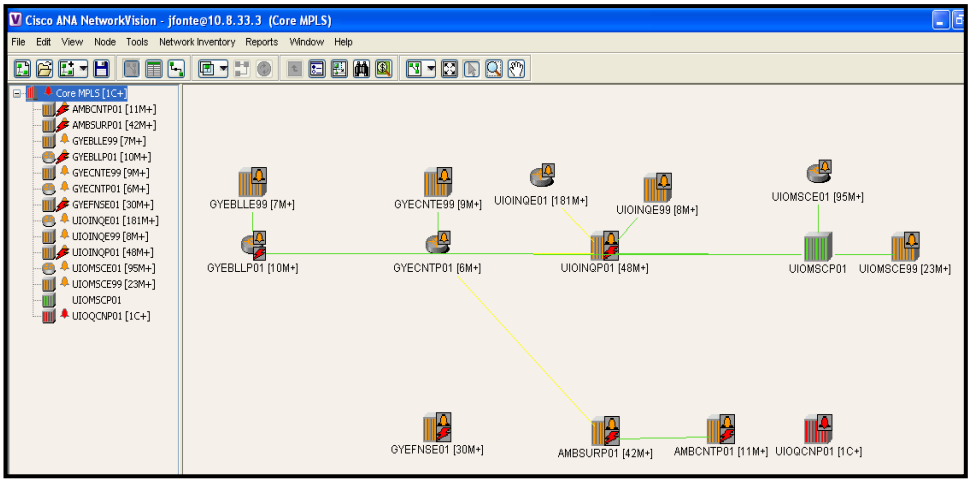


Figura 5.2.83: CORE MPLS[1]

- **VNEs**

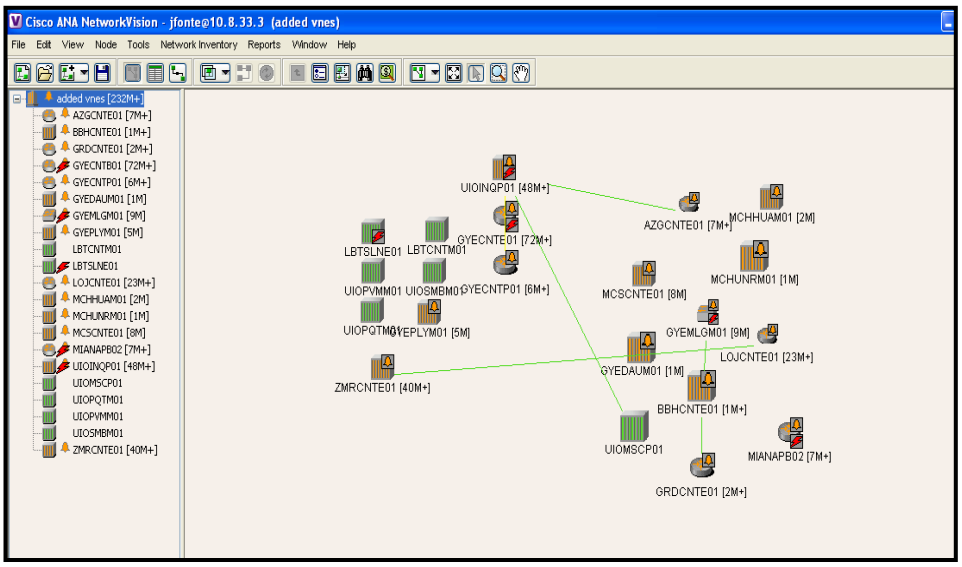


Figura 5.2.84: VNEs[1]

5.3 MANUAL WHATSUP

5.3.1 OBJETIVO

Conocer cada uno de los componentes que conforman la plataforma Whats Up para monitorear y administrar de manera correcta las redes y los servicios que prestan.

5.3.2 INTRODUCCIÓN

WhatsUp es una aplicación que permite mantener un correcto funcionamiento de la red. Con esta plataforma, se puede crear rápidamente un mapa de red, iniciar el monitoreo, y obtener retroalimentación sobre el desempeño de la misma.

Actualmente en esta plataforma se encuentra el mapa principal *Andinatel*, a partir del cual se puede ingresar a los mapas de los equipos 6500, 7600, red IP y BRAS.

5.3.3 INGRESO A LA PLATAFORMA

A continuación se muestran los pasos de ingreso a la plataforma What's Up y sus diferentes mapas como se muestra en la figuras 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5.

Para ingresar a la plataforma se debe colocar la correspondiente dirección del servidor.

1. Para ingresar a los mapas contenidos en *Andinatel* dar doble clic en uno de ellos.

2. Para regresar al mapa principal dar doble clic en la nube (que tiene el contenedor denominado Andinatel).

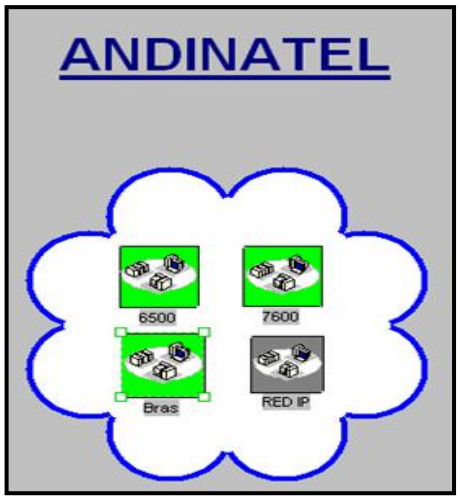


Figura 5.3.1: Red Andinatel[1]

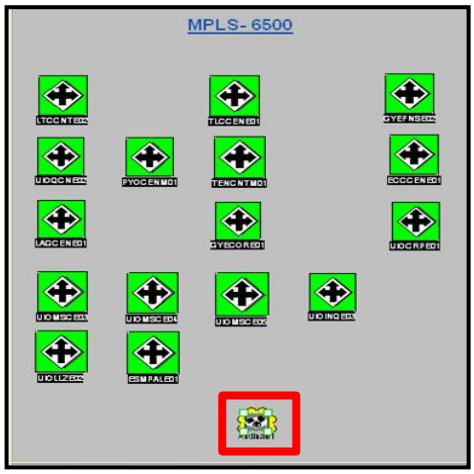


Figura 5.3.2: Equipos MPLS 6500[1]

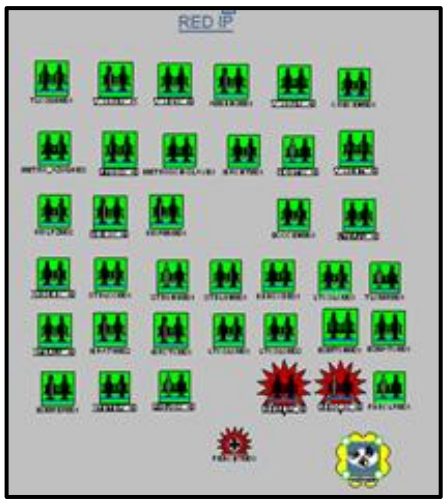


Figura 5.3.3: Red IP[1]

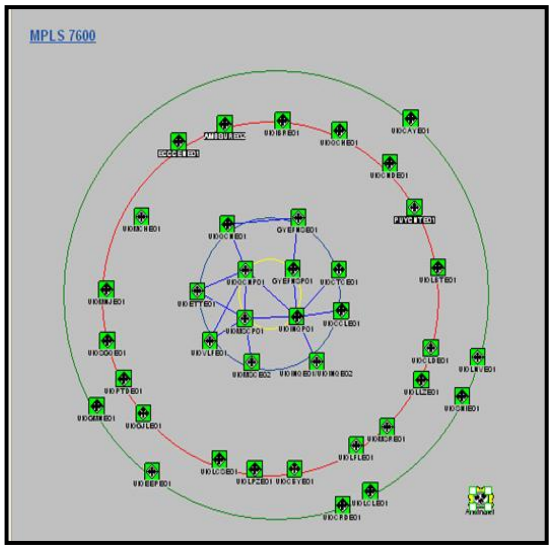


Figura 5.3.4: Equipos MPLS 7600[1]

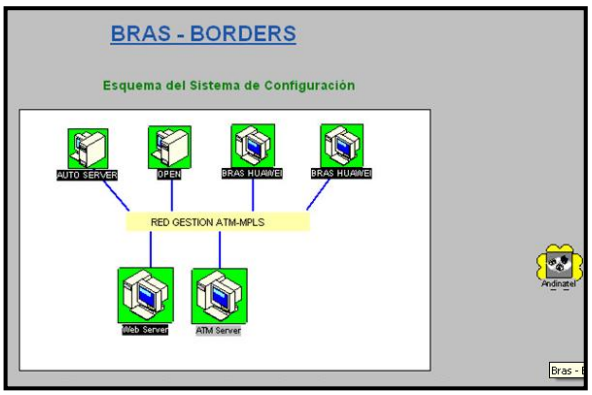


Figura 5.3.5: Equipos BRAS-BORDERS[1]

5.3.4 CREACIÓN DE UN MAPA

Para crear un nuevo mapa, en el menú principal, seguir los siguientes pasos:

1. Seleccionar *File*
2. *New Map Wizard*
3. Seleccionar *Create a blank map*

4. Clic en *Finish*

Se puede establecer las propiedades de sondeo para cada mapa de la red principal y el mapa de subred mediante los siguientes pasos:

1. En el menú principal, seleccionar *Edit.*

2. Seleccionar la opción *Properties* o dar clic derecho en la red y elegir *Properties*, posteriormente aparecerá la siguiente pantalla como se muestra en la figura 5.3.6:

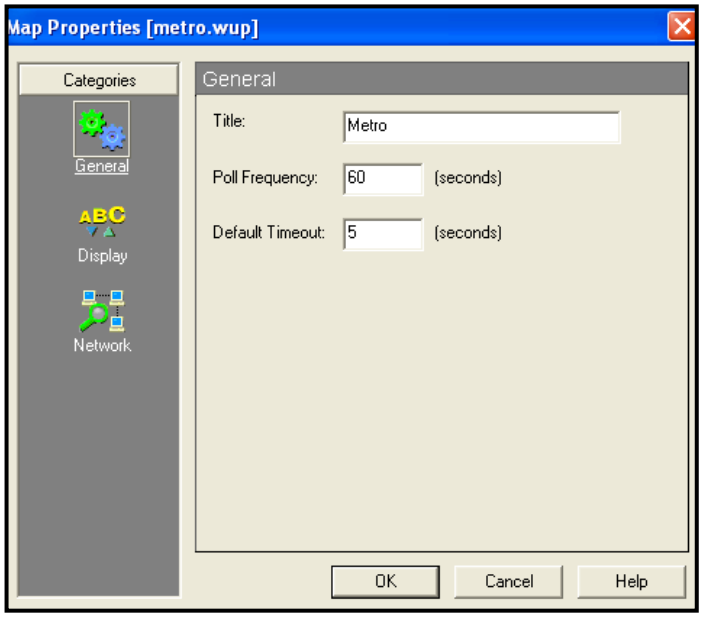


Figura 5.3.6: Propiedades de sondeo de los mapas[1]

Map Properties presenta 3 opciones: *General, Display y Network.*

5.3.4.1 GENERAL

Colocar la información general del mapa, nombre, tiempo de espera predeterminado y frecuencia de sondeo como se muestra en la figura 5.3.7:

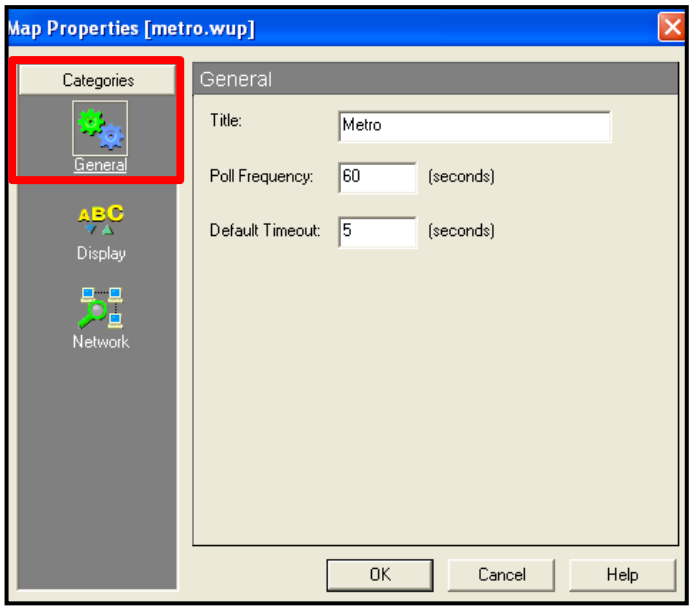


Figura 5.3.7: Opción General[1]

5.3.4.2 DISPLAY

Utilice esta configuración por defecto para los nuevos mapas. Si se selecciona esta opción, WhatsUp aplica esta configuración a todos los nuevos mapas creados como se muestra en la figura 5.3.8.

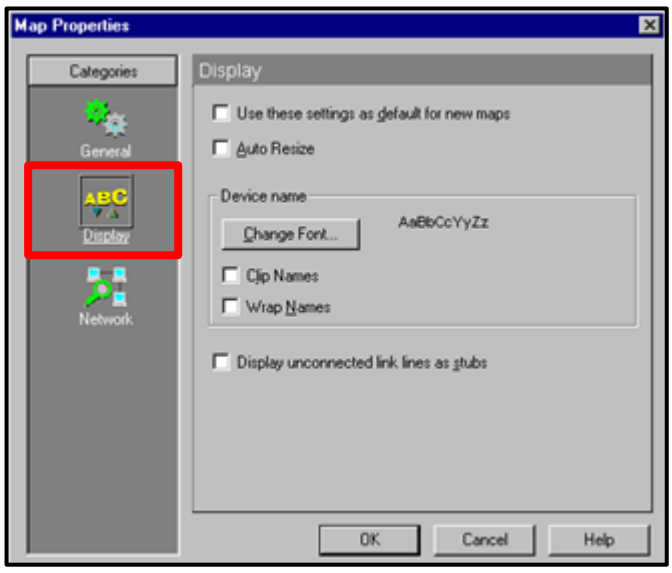


Figura 5.3.8: Opción Display[1]

5.3.4.3 NETWORK

Permite configurar la red y subred del mapa principal, para ello escoger un método de escaneo como se indica en la figura 5.3.9:

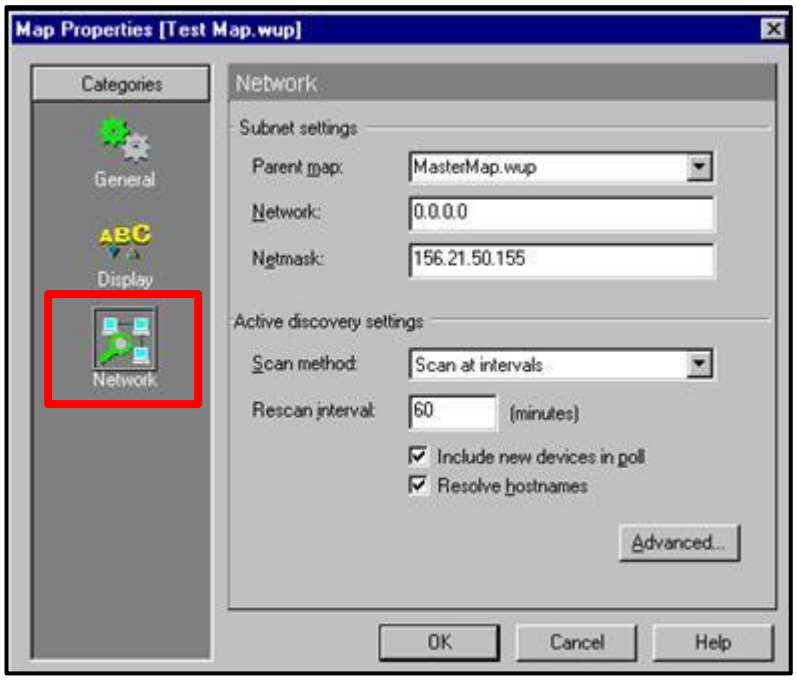


Figura 5.3.9: Opción Network[1]

5.3.5 TAB MAP

Permite visualizar el mapa de la red con cada uno de los dispositivos que se encuentran en estado activo, inactivo o en reconexión como se muestra en la figura 5.3.10:

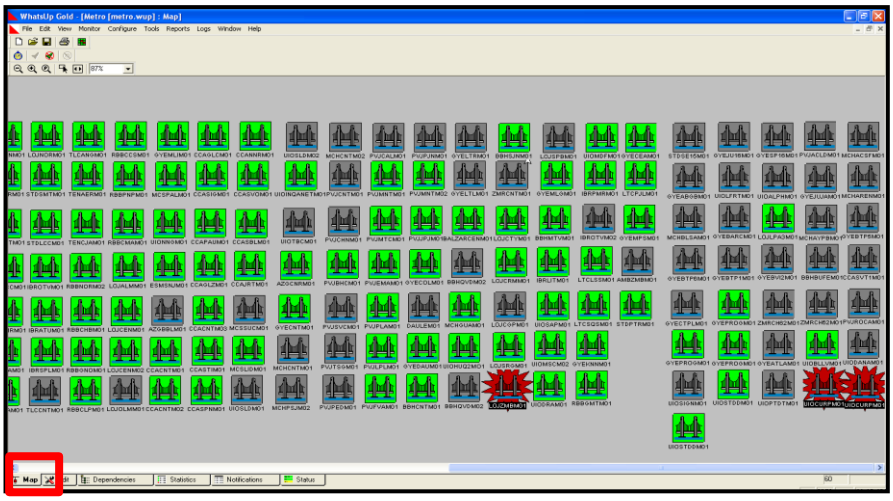


Figura 5.3.10: Tab Map[1]

5.3.6 TAB EDIT

Presenta una barra de herramientas que permitirá añadir y modificar una serie de dispositivos en el mapa como se muestra en la figura 5.3.11:

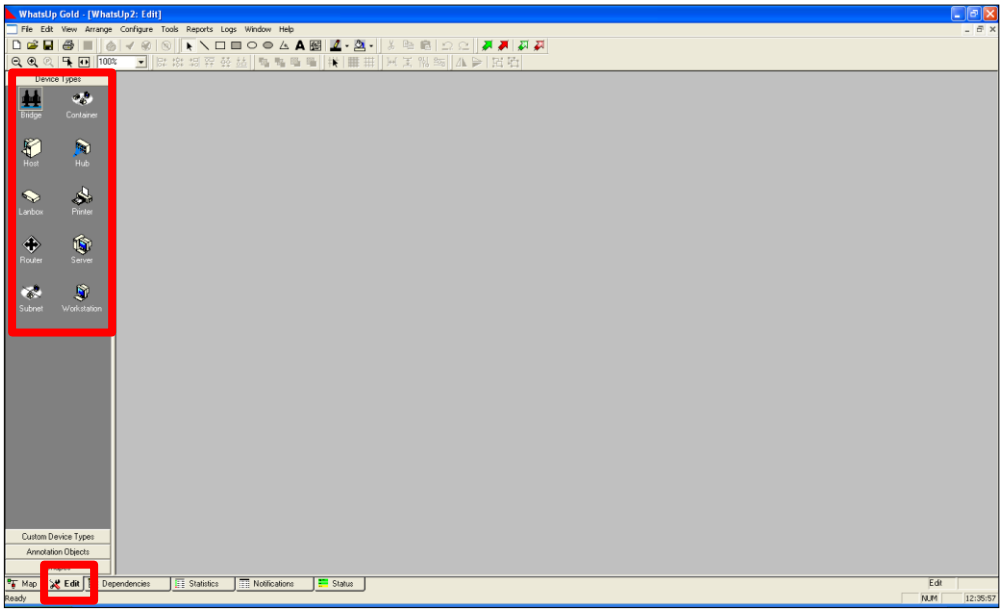


Figura 5.3.11: Tab Edit[1]

Para agregar un objeto en el mapa, seleccionar y arrastrar dicho objeto sobre el mapa. Además se tiene la opción de mover y cambiar el tamaño del objeto.

Para establecer las propiedades de objeto seleccionado realizar los siguientes pasos:

1. Dar clic con botón derecho y seleccione *Item Properties*.

2. En la opción *General*, colocar el nombre, tipo de dispositivo, dirección IP y en la opción *Polling Method*, se recomienda colocar ICMP para verificar la conectividad del equipo como se muestra en la figura 5.3.12:

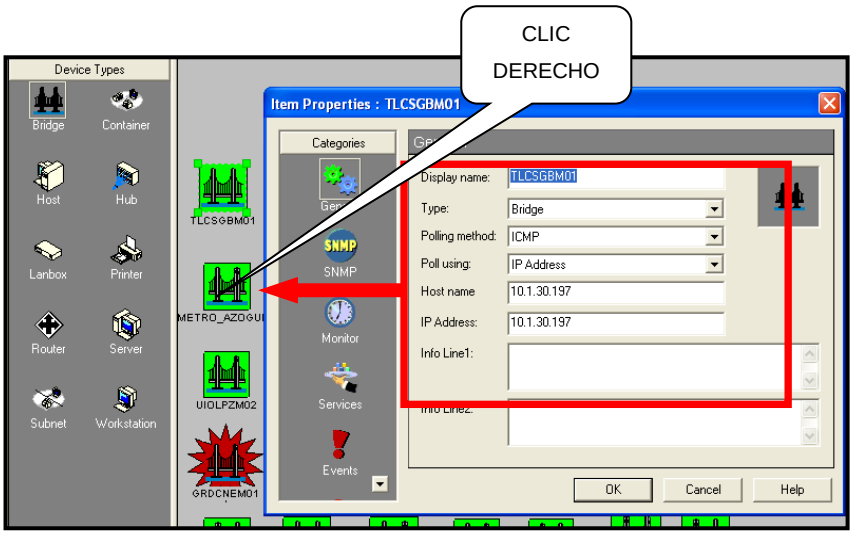


Figura 5.3.12: Propiedades del Objeto[1]

3. Se puede habilitar la opción *SNMP* que permite gestionar los dispositivos que conforman la red, además activa la opción *Logs SMNP* para analizar los sucesos ocurridos como se muestra en la figura 5.3.13:

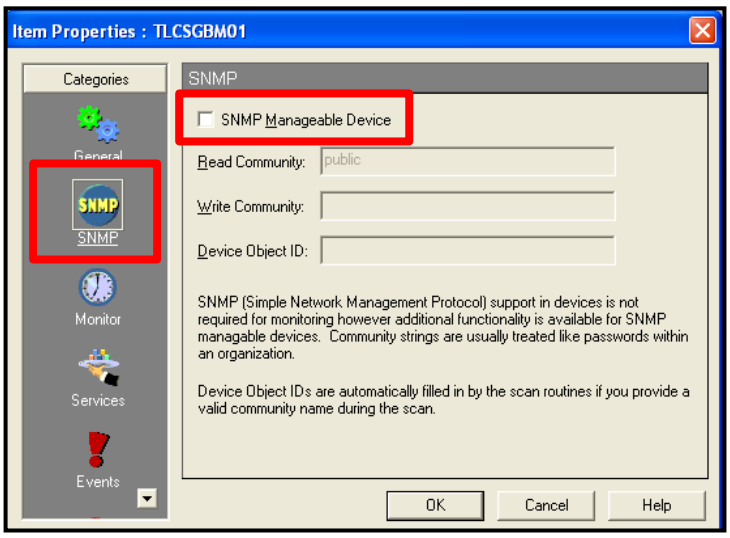


Figura 5.3.13: Habilitación de la opción SNMP[1]

4. En la opción *Monitor* habilitar *Monitor This Device* para especificar cuan a menudo se debe realizar el monitoreo a un dispositivo, además configurar el tiempo en segundos que se debe esperar para una respuesta y verificar si un dispositivo o dependencia se encuentre en up o down como se muestra en la figura 5.3.14:

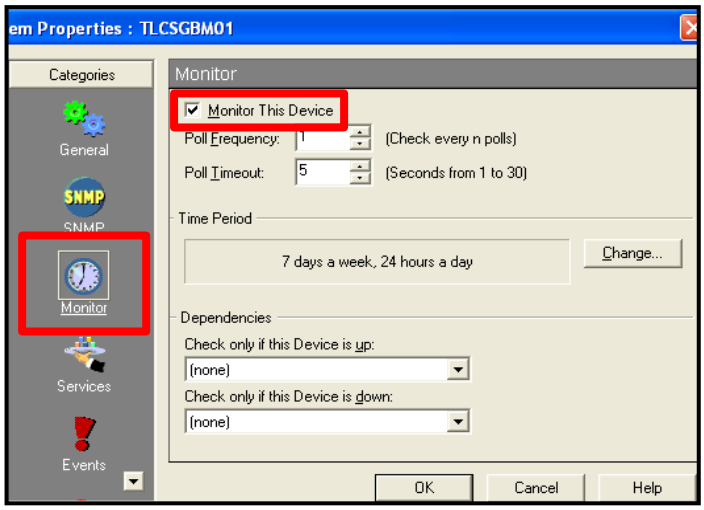


Figura 5.3.14: Opción Monitor[1]

5. Seleccionar la opción *Services* para añadir cualquier servicio que se desee que el equipo monitoree, se sugiere el servicio DNS, como se muestra en la figura 5.3.15:

   Estos servicios son TCP/IP que incluye DNS, FTP, POP3, SMTP, HTTP, IMAP4, NNTP, SNMP.

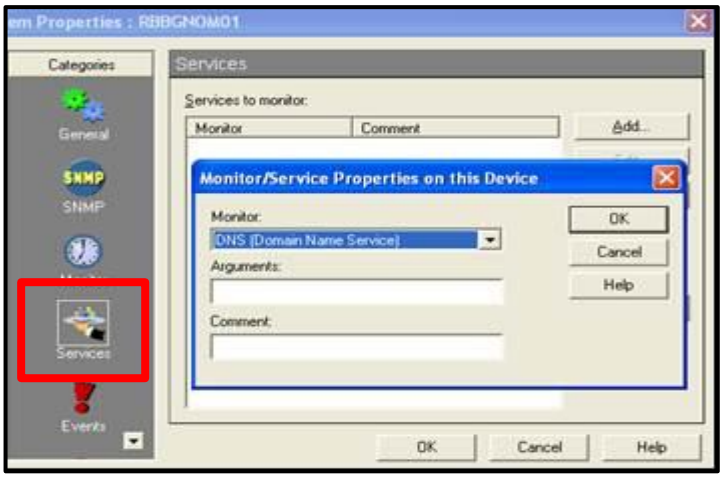


Figura 5.3.15: Opción Services[1]

6. Seleccionar la opción *Events* para añadir cualquier evento que se desee solicitar, se sugiere elegir SNMP Trap como se muestra en la figura 5.3.16:

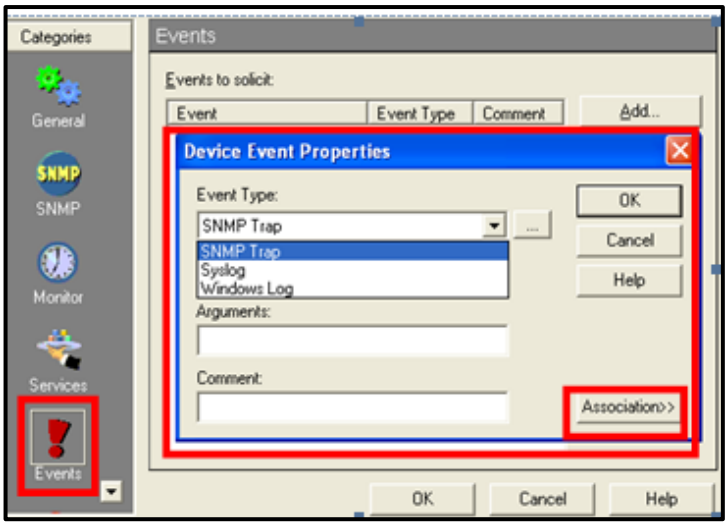


Figura 5.3.16: Opción Events[1]

7. Opcionalmente se puede elegir *Association* para seleccionar un servicio asociado a este evento en el equipo. Además, se puede definir si el servicio asociado entra en modo up o down en el mapa cuando se produce el evento, como se muestra en la figura 5.3.16:

8. Seleccionar la opción *Alerts* y elegir *Enable Logging* el cual permitirá observar los logs del equipo en caso de que exista una incidencia, como se muestra en la figura 5.3.17:

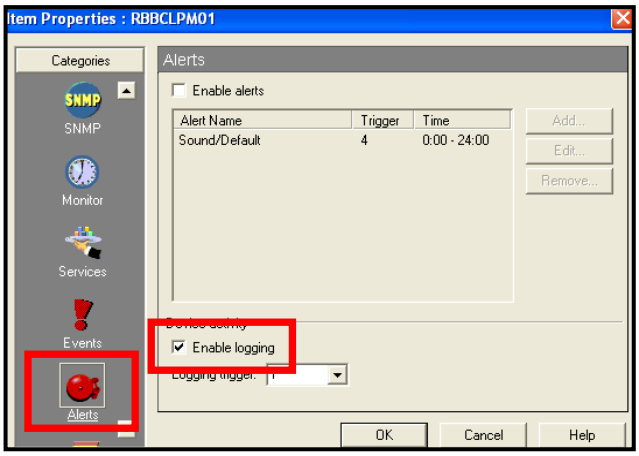


Figura 5.3.17: Opción Alerts[1]

9. Se puede seleccionar la opción *Enable Alerts* para añadir y activar la alerta con un sonido por default, como se muestra en la figura 5.3.18:

Figura 5.3.18: Opción Enable Alerts [1]

10. Si las alertas han sido habilitadas en el dispositivo seleccionado estas aparecerán en la lista de color blanco, si estas son deshabilitadas subsecuentemente la lista aparecerá de color gris.

11. Seleccionar *Notes* en el caso que se requiera colocar algún tipo de descripción del dispositivo o del servicio como se muestra en la figura 5.3.19:

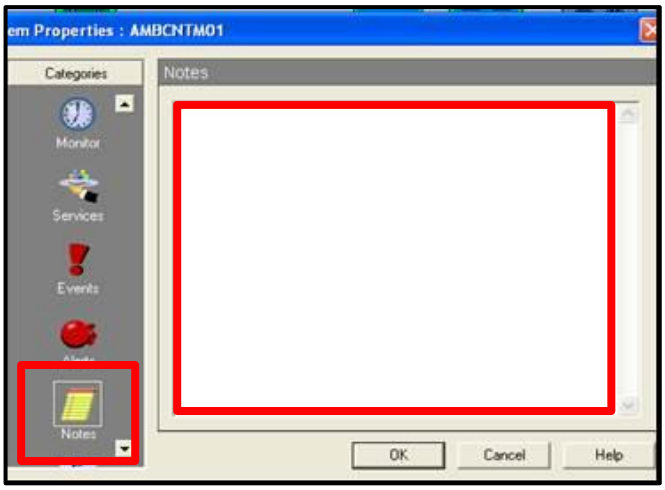


Figura 5.3.19: Opción Notes[1]

12. Seleccionar la opción *Menú* para configurar los comandos que permitan la verificación de conectividad del dispositivo en la red como se muestra en la figura 5.3.20:

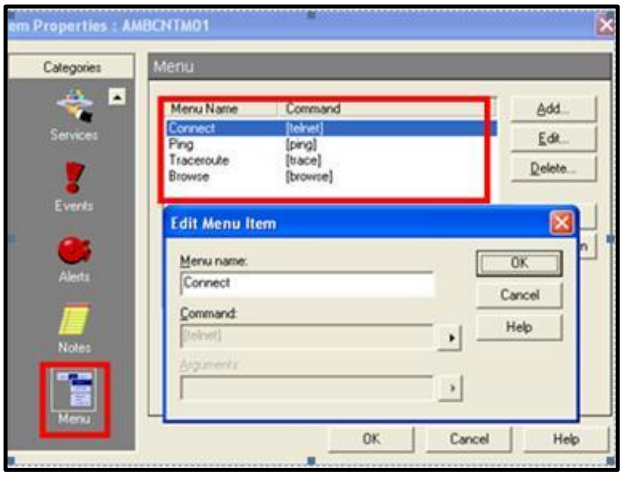


Figura 5.3.20: Opción Notes[1]

5.3.7 TAB DEPENDENCIES

Muestra las dependencias de la red como un árbol jerárquico e indica la secuencia de sondeo, el usuario define si las dependencias se encuentran en Up o Down. El valor entre paréntesis después del nombre del dispositivo es un elemento identificador para resolver nombres ambiguos de los equipos como se muestra en la figura 5.3.21:

Los dispositivos se enumeran en el orden en que son consultados. Se puede arrastrar un dispositivo dentro de la rama para cambiar el orden de sondeo del equipo.

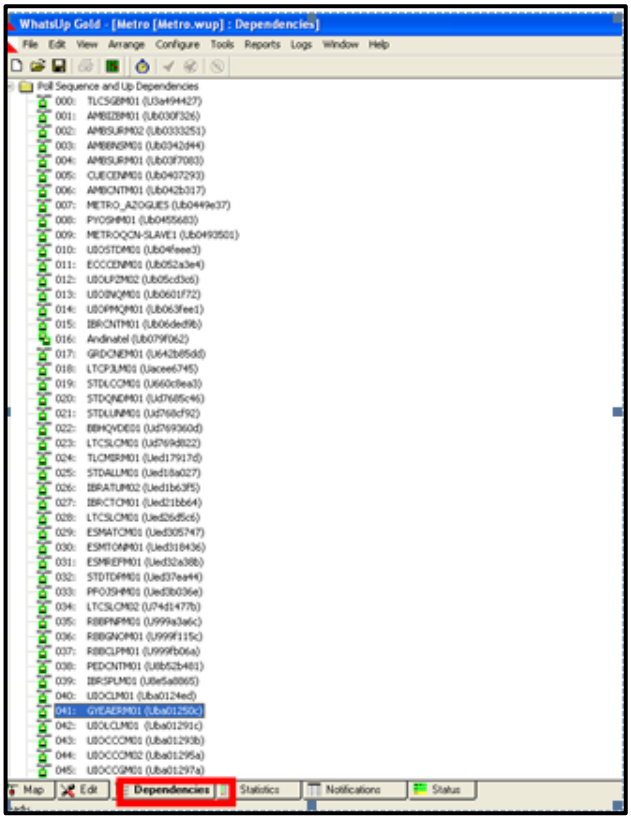


Figura 5.3.21: Tab Dependencies[1]

5.3.8 TAB STATISTICS

Provee un fácil acceso a las estadísticas de sondeo del mapa activo. Se puede verificar las estadísticas acumuladas de cada dispositivo en el mapa de la red activa como se muestra en la figura 5.3.22. Las estadísticas de sondeo se conservan al cerrar o abrir los mapas de la red. Cada mapa tiene un archivo asociado y se registran en el archivo denominado map_name.wui.

Las estadísticas para cada dispositivo son:

- ✓ **Dispositivo:** El nombre del dispositivo.

- ✓ **Dirección:** Dirección del dispositivo (si el método de votación es ICMP o de servicios solamente).
- ✓ **Tipo:** El método de sondeo o monitoreo (ICMP, Servicios solamente, NetBIOS o IPX), creado en el cuadro de diálogo General en las propiedades del dispositivo.
- ✓ Un estado de cero indica que el dispositivo está activo. Cualquier otro valor indica un error.

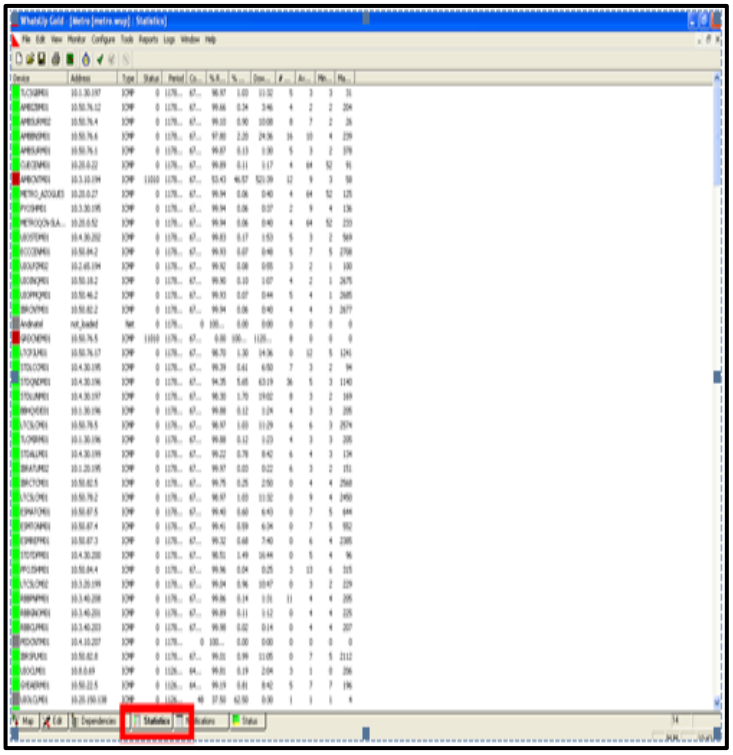


Figura 5.3.22: Tab Statistics[1]

5.3.9 TAB NOTIFICATIONS

Permite observar las notificaciones habilitadas para el mapa activo de la red. Las notificaciones son agrupadas por dispositivo.

Se puede alternar entre orden ascendente y descendente mediante un clic en cualquiera de las columnas como se indica en la figura 5.3.23.

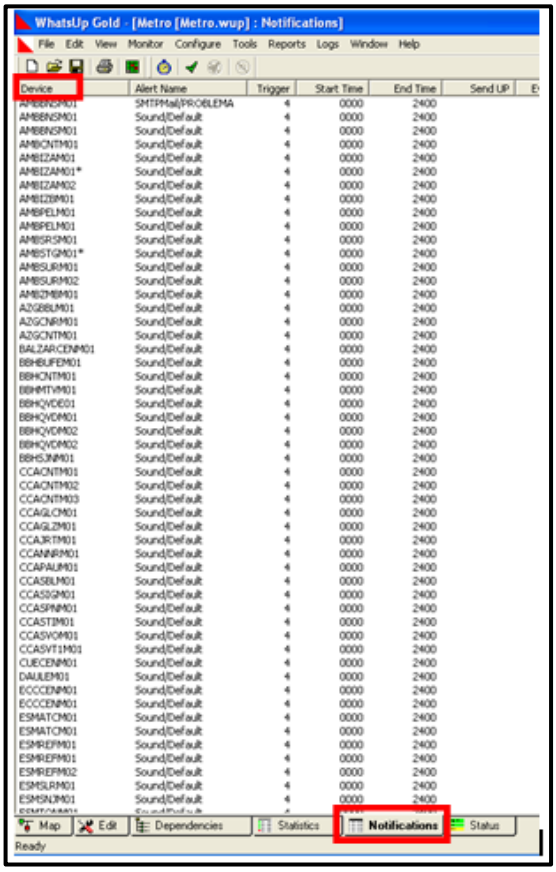


Figura 5.3.23: Tab Notifications[1]

Es importante mencionar que se puede definir los diferentes tipos de notificaciones usando la *Librería de Notificaciones*, para esto ingresar en Menú a la opción *Configure* y seleccionar *Notifications Library*, como se indica en la figura 5.3.24:

Figura 5.3.24: Notifications Library[1]

5.3.10 TAB MINI STATUS

Esta pequeña ventana permite supervisar el estado de la red. Esta es una alternativa para la ventana del mapa y puede ser usada en monitores de baja resolución o cuando se desee guardar espacio en el monitor.

Para visualizar la ventana escoger la opción *View/ Mini Status* como se muestra en la figura 5.3.25, mediante esta opción la ventana de WhatsUp principal se cierra y aparece la vista de los dispositivos en una ventana más pequeña como se indica en la figura 5.3.26.

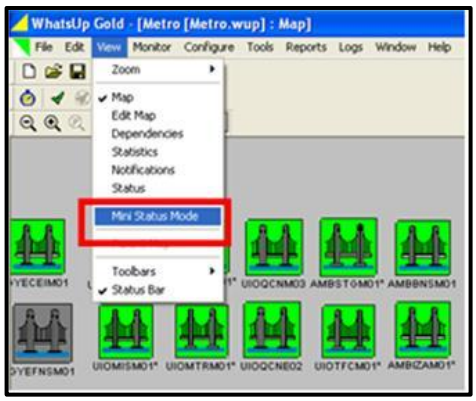


Figura 5.3.25: Selección de la opción Mini Status[1]

La opción *Mini Status* muestra el estado de todos los dispositivos en los mapas actualmente activos, utilizando los mismos colores de la ventana MAP.

Figura 5.3.26: Mini Status[1]

- ✓ Cada mapa abierto es listado en una columna separada. Cualquier servicio que está siendo monitoreado en un dispositivo es mostrado.

- ✓ Dar doble clic en la ventana Mini Status para cerrar esta e ir de regreso a la ventana del mapa.

5.3.11 TAB STATUS

Muestra una lista de todos los equipos que se encuentran activos en el mapa e indica el status de cualquier servicio que está siendo monitoreado como se indica en la figura 5.3.27.

Esta opción presenta la posibilidad de ampliar la ventana de estado con el fin de leer toda la información de monitoreo.

En la barra de herramientas principal haga clic en el botón *Poll* para iniciar un chequeo de cada dispositivo en la ventana Status.

Dar clic en el botón *Stopwatch* para iniciar un sondeo automático de cada dispositivo.

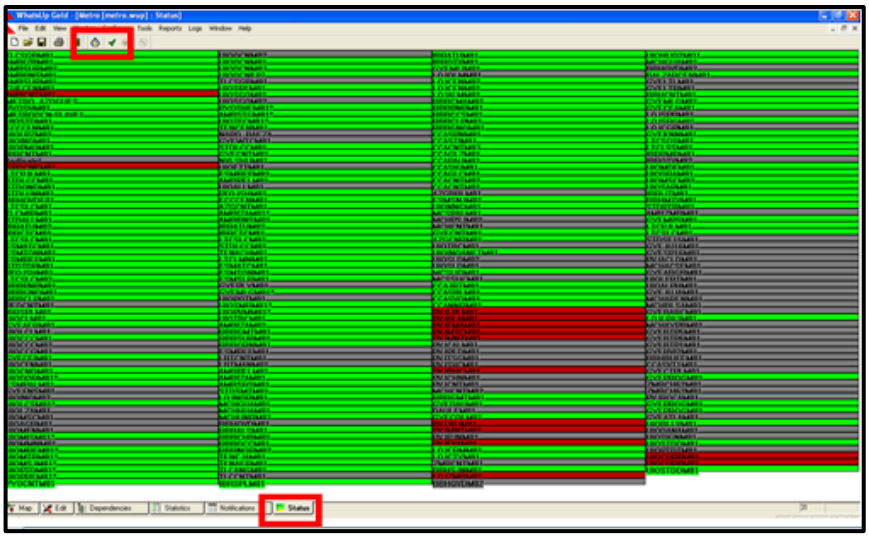


Figura 5.3.27: Tab Status[1]

5.3.12 MONITOREO DEL ESTADO DE LOS EQUIPOS

Al dar clic derecho en el equipo, seleccionar la opción *Quick Status* la misma que despliega una barra de herramientas que muestra las siguientes opciones: *Status, History, Up-Time y Logs History* del equipo.

5.3.12.1 STATUS

Muestra el estado de los paquetes enviados por Whats'up, si el equipo está activo o inactivo y el tiempo de respuesta como se muestra en la figura 5.3.28:

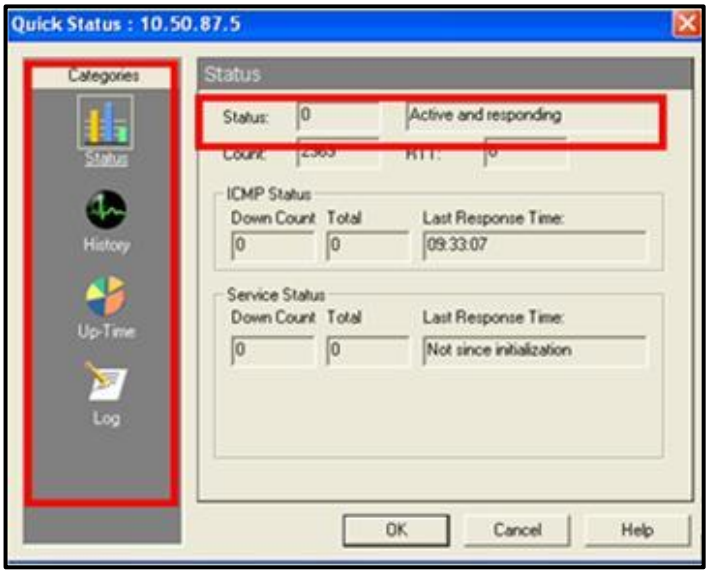


Figura 5.3.28: Status[1]

5.3.12.2 HISTORY

Muestra el tiempo de respuesta relativa del dispositivo sobre los treinta últimos chequeos como se muestra en la figura 5.3.29:

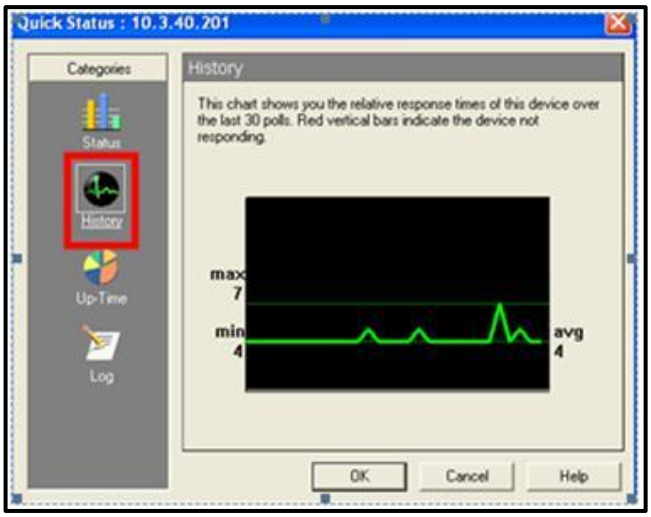


Figura 5.3.29: History[1]

En el caso de presentarse barras verticales de color rojo quiere decir que el equipo no está respondiendo como se indica en la figura 5.3.30:

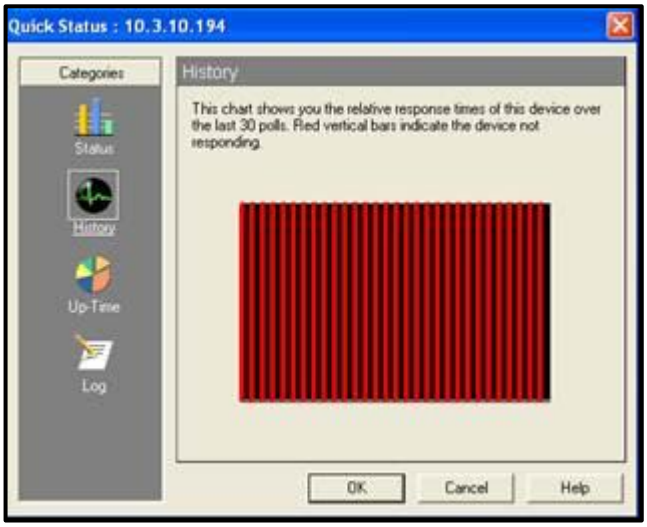


Figura 5.3.30: Equipo sin respuesta[1]

5.3.12.3 UP-TIME

Muestra el porcentaje en el cual el equipo se encuentra en estado up como se muestra en la figura 5.3.31.

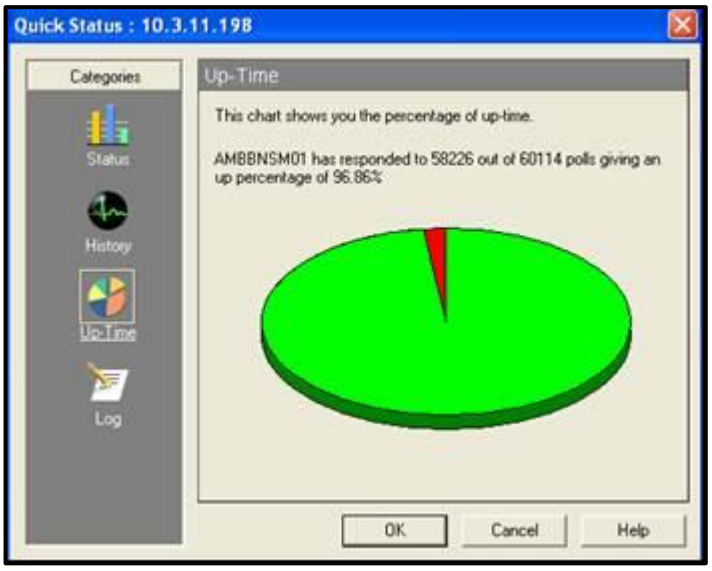


Figura 5.3.31: Estado Up del equipo [1]

5.3.12.4 LOG

Muestra los logs del equipo, el cual permite obtener información útil acerca del procesamiento del equipo y los respectivos sucesos en caso de presentarse un problema como se indica en la figura 5.3.32.

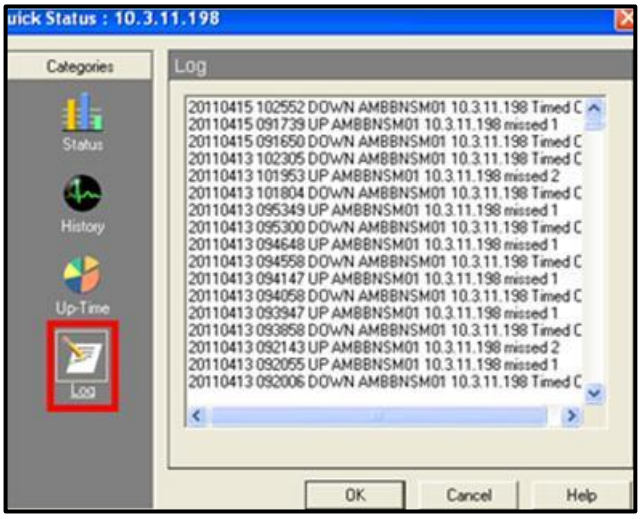


Figura 5.3.32: Logs del equipo[1]

También se puede observar los Logs seleccionando en la barra de herramientas en el menú principal la opción *Activity Logs* como se muestra en la figura 5.3.33:

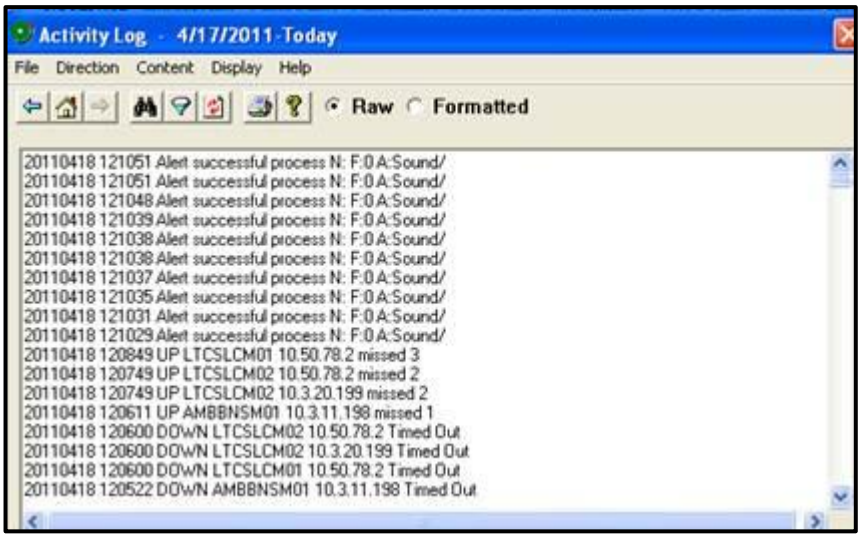


Figura 5.3.33: Activity Log[1]

Para conocer las formas predeterminadas y configurar los colores para el monitoreo de los equipos escoger en el menú las opciones *Configuration /Program Options /Device States.*

Cada uno de los siguientes iconos presenta un estado diferente del equipo:

El color verde encendido indica que el equipo está respondiendo al sondeo.

El color predeterminado verde claro indica que el equipo no ha respondido a un sondeo.

El color predeterminado amarillo sólido indica el equipo no ha respondido a dos sondeos consecutivos.

El color predeterminado amarillo sólido indica que el equipo no ha respondido a tres sondeos consecutivos.

El color predeterminado rojo sólido indica que el equipo no ha respondido de cuatro a siete sondeos consecutivos.

El color predeterminado sólido rojo obscuro indica que el equipo no ha respondido a ocho o más sondeos consecutivos o tiene un error de red.

El color predeterminado sólido púrpura, indica que un servicio se encuentra down en el equipo.

El color predeterminado sólido de color gris obscuro indica que un equipo está inactivo.

5.3.13 VERIFICACIÓN DE CONECTIVIDAD

Al dar clic derecho en el ícono del equipo que se encuentra en el mapa se puede visualizar una serie de herramientas de diagnóstico de red para verificar la conectividad a un sistema particular de la red.

5.3.13.1 CONNECT

Permite realizar conexión remota a un equipo mediante telnet como indica la figura 5.3.34.

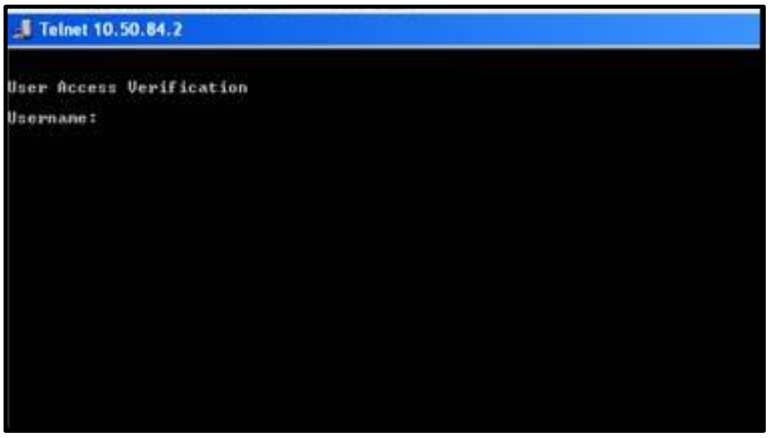


Figura 5.3.34: Connect[1]

5.3.13.2 PING

Es una herramienta de diagnóstico para verificar la conectividad. Ping envía un ICMP en forma de un paquete de datos a un host remoto y muestra los resultados para cada uno. Este intercambio se conoce como "ping". El comando ping muestra

también el tiempo de respuesta de llegada en milisegundos (esto puede variar dependiendo de la carga de red) y depuración de información sobre la interfaz de red como se indica en la figura 5.3.35:

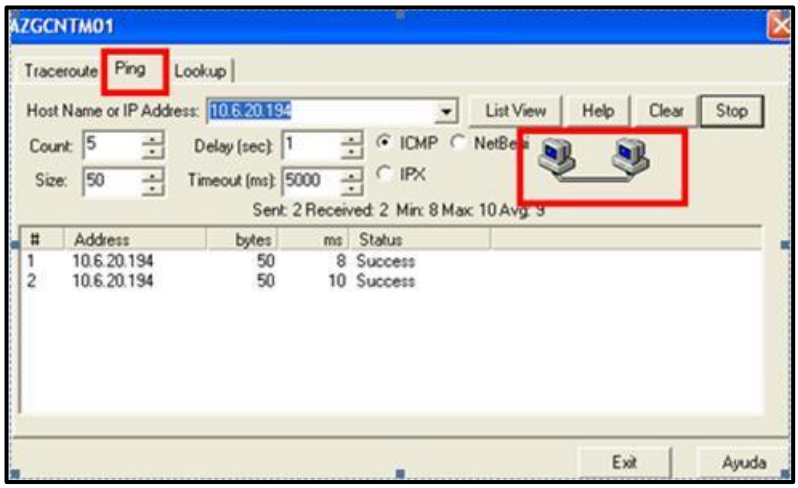


Figura 5.3.35: Ping a un equipo[1]

5.3.13.3 TRACEROUTE:

Permite localizar y ver la ruta real de un paquete IP desde el equipo local a otro host en Internet. Los tiempos de respuesta se muestran en milisegundos y pueden variar dependiendo de la carga de la red. El comando *TraceRoute* es útil para encontrar los puntos donde existan posibles problemas en redes grandes y complejas que están conectadas entre sí por los routers como se indica en la figura 5.3.36:

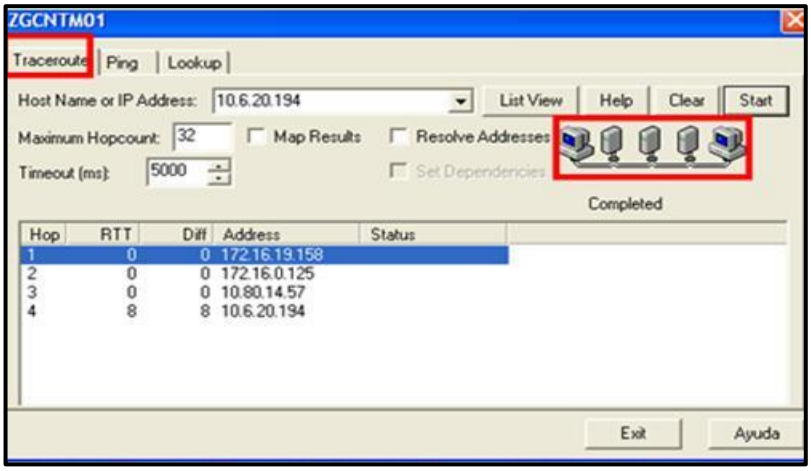


Figura 5.3.36: Traceroute[1]

5.3.13.4 BROWSER

Permite acceder a la cartografía, la vigilancia, y las funciones de notificación vía web de un equipo remoto como indica la figura 5.3.37:

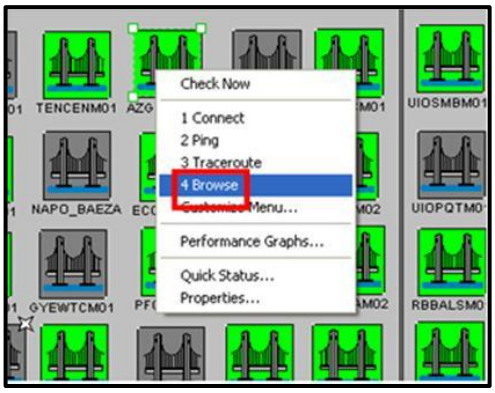


Figura 5.3.37: Browse[1]

Si los paquetes ICMP ping no pueden viajar en la red a su equipo, puede controlar este equipo, monitoreando los servicios configurados anteriormente.

El seguimiento de un servicio siempre implica un handshake[47], un protocolo también puede incluir un intercambio de información adicional entre WhatsUp y el servicio. Estos se pueden verificar en los Logs de los equipos y se pueden identificar los servicios supervisados en el cuadro Services como se indica en la figura 5.3.38:

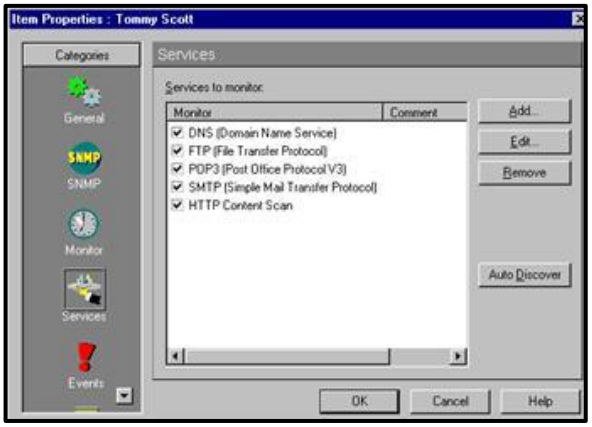


Figura 5.3.38: Services[1]

[47] Handshake: Es el proceso de negociación entre protocolos

Al realizar un mapa que posea un contenedor, dar clic derecho en propiedades y poner el nombre del mapa relacionado con este contenedor.

5.4 MANUAL IPsolutionC

5.4.1 OBJETIVO

- Conocer las herramientas de la plataforma IPsolutionC para configurar y disponer de la conmutación de etiquetas por medio de MPLS y VPNs.

5.4.2 INTRODUCCIÓN

En este manual se mostrarán diversas características que son comunes entre varias aplicaciones, todos los pasos que se indican permitirán realizar múltiples configuraciones para la creación de políticas y otras características en común.

Las secciones tratadas en este manual son las siguientes:

- ✓ Service Inventory
- ✓ Service Desing
- ✓ Monitoring
- ✓ Diagnostics
- ✓ Administration

Es importante mencionar que de la lista de secciones mencionadas anteriormente la más utilizada es la sección *Service Inventory* porque permite realizar configuraciones de customers, providers etc. de forma amigable.

5.4.3 INGRESO A LA PLATAFORMA

Para ingresar a la plataforma colocar la dirección IP correspondiente en el browser, cuando se encuentre en la página principal ingresar el nombre de usuario y contraseña respectivamente, como se indicó anteriormente esta plataforma se

encuentra conformada por diversas secciones las mismas que se muestran a continuación:

5.4.4 OPCIÓN SERVICE INVENTORY

Esta opción contiene herramientas para administrar los elementos del inventario, solicitudes de servicios y dispositivos, como se mencionó anteriormente esta es la sección más utilizada ya que aquí es donde se realizan configuraciones principales como se muestra en la figura 5.4.1.

Para proceder a realizar configuraciones en esta sección seguir los pasos que se muestrana continuación:

1. Dar clic en la sección *Service Inventory* como se muestra en la figura 5.4.1:

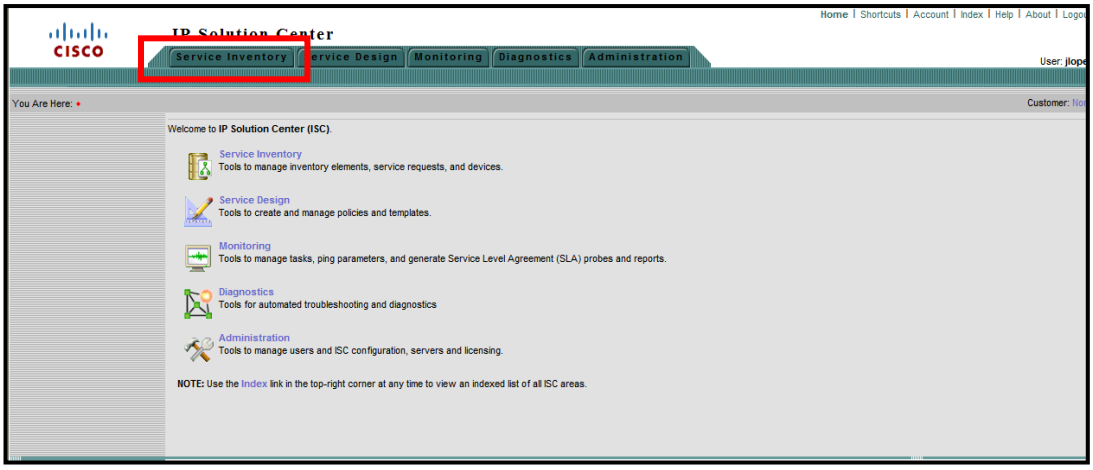


Figura 5.4.1: Ingreso a la plataforma [1]

2. A continuación escoger la opción *Inventory and Connection Manager* para realizar las configuraciones correspondientes como se muestra en la figura 5.4.2:

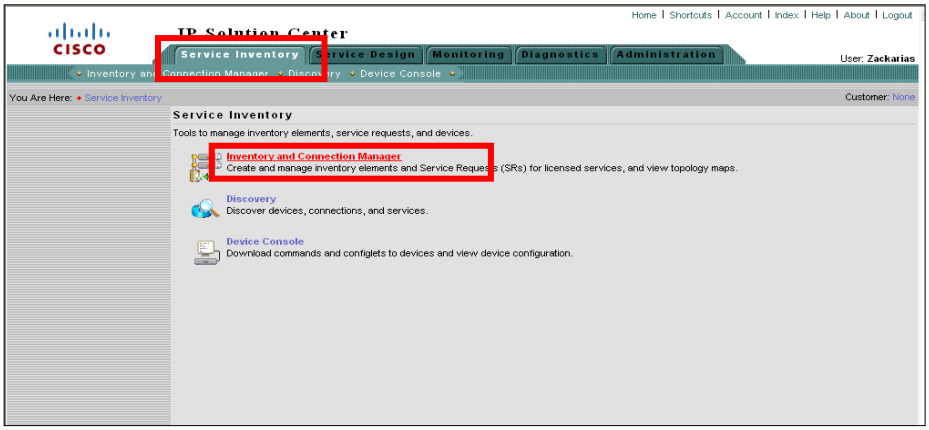


Figura 5.4.2: Opción Service Inventory [1]

Dentro de la opción *Inventory and Connection Manager* se tiene más opciones las cuales permiten realizar configuraciones de usuarios dependiendo de las necesidades del administrador, las mismas que se indican a continuación:

5.4.4.1 CREACIÓN DE CUSTOMERS

Los customers se crean con el fin de poder administrar configuraciones individuales y los servicios que se le asigna a cada uno de ellos.

Para la creación de *Customers* realizar los siguientes pasos:

1. Elegir la opción *Customers* como se muestra en la figura 5.4.3:

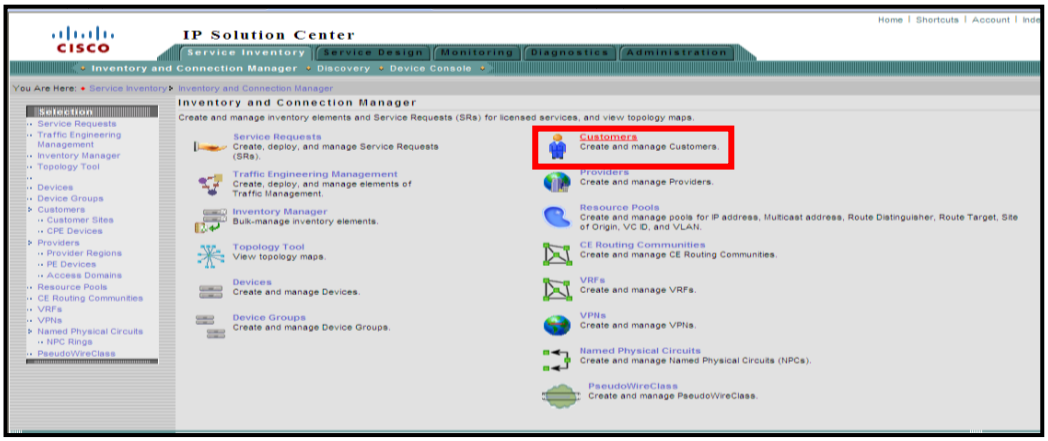


Figura 5.4.3: Opción Customers [1]

2. En la pantalla que aparece a continuación, crear un nuevo *Customer* mediante la opción *Create* como se muestra en la figura 5.4.4:

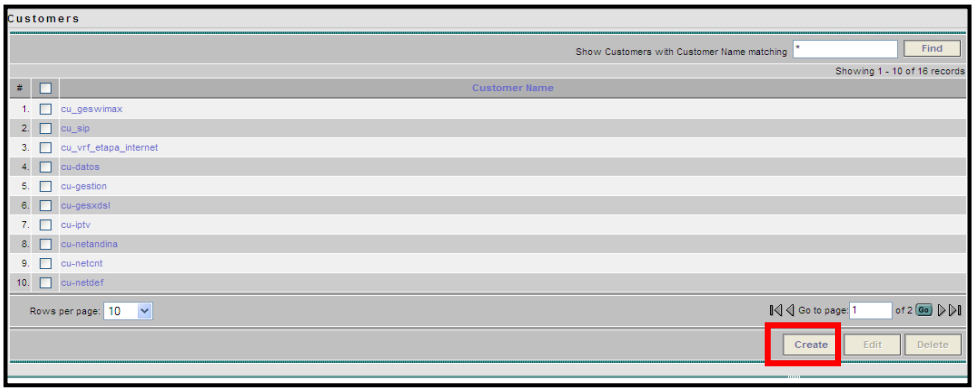


Figura 5.4.4: Creación de un nuevo Customer [1]

3. Colocar el nombre del cliente y la respectiva descripción del mismo, en esta sección se debe colocar cualquier información pertinente sobre el cliente que podría ser útil para los proveedores de servicios, la información se encuentra limitada a 256 caracteres, como se muestra en la figura 5.4.5:

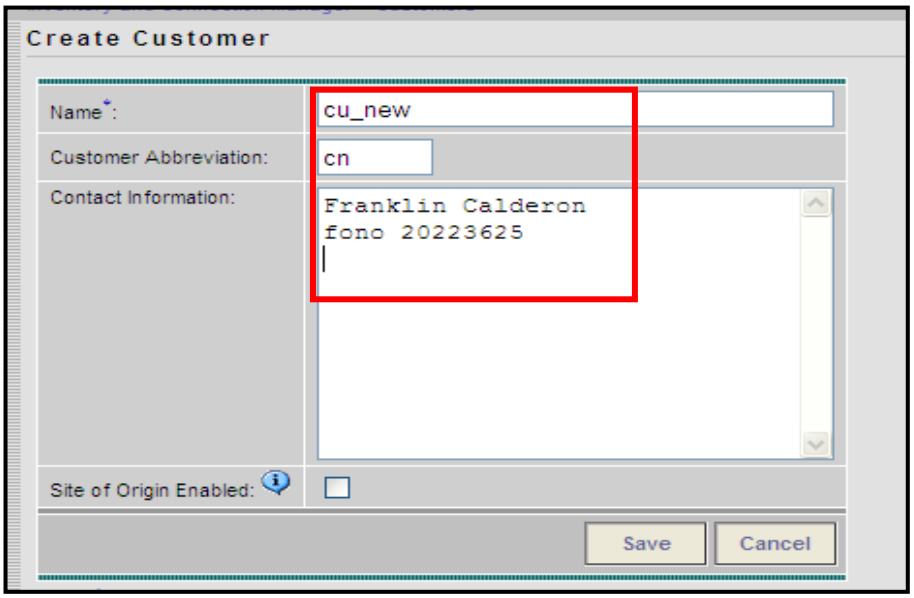


Figura 5.4.5: Colocación del nombre y descripción del cliente [1]

Es importante mencionar que el formato utilizado por los administradores es el siguiente:

- ✓ El nombre se coloca de la siguiente manera: cu_ y el nombre del cliente que ha sido asignado a una VRF[48]. Ejemplo: cu_banco_pichincha

4. Guardar las configuraciones realizadas mediante la opción *Save* y verificar que el customer fue creado y añadido satisfactoriamente como se muestra en la figura 5.4.6:

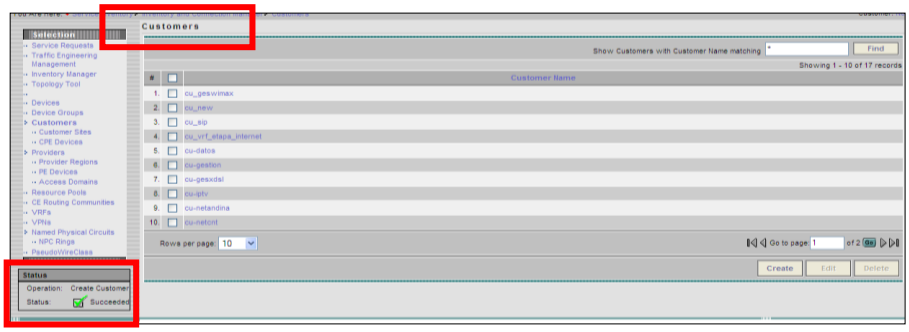


Figura 5.4.6: Verificación de la creación del customer [1]

5.4.4.2 ELIMINAR UN CUSTOMER

Para proceder a eliminar un *Customer* seguir los pasos que se muestran a continuación:

1. Escoger las opciones: *Service Inventory > Inventory and Connection Manager > Customers.*
2. Seleccione uno o más clientes que desee eliminar marcando la casilla de verificación a la izquierda del nombre del cliente.
3. Dar clic en el botón *Delete.* Este botón se activa únicamente si uno o más clientes se han seleccionado, por lo tanto una ventana de confirmación de borrado aparecerá como se muestra en la figura 5.4.7:

[48] Véase Acrónimos

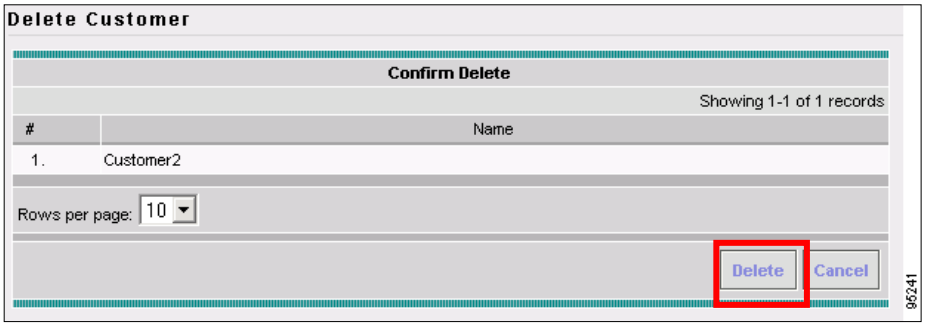


Figura 5.4.7: Opción Delete Customer [1]

5.4.4.3 CREACION DE PROVIDERS

Los *providers* son entidades las cuales tienen asignados un ASN (Número de Sistema Autónomo), los mismos que son creados para que trabajen sobre MPLS. Para la creación de *Providers* seguir los siguientes pasos:

1. Elegir la opción *Providers* en la pantalla como se muestra en la figura 5.4.8:

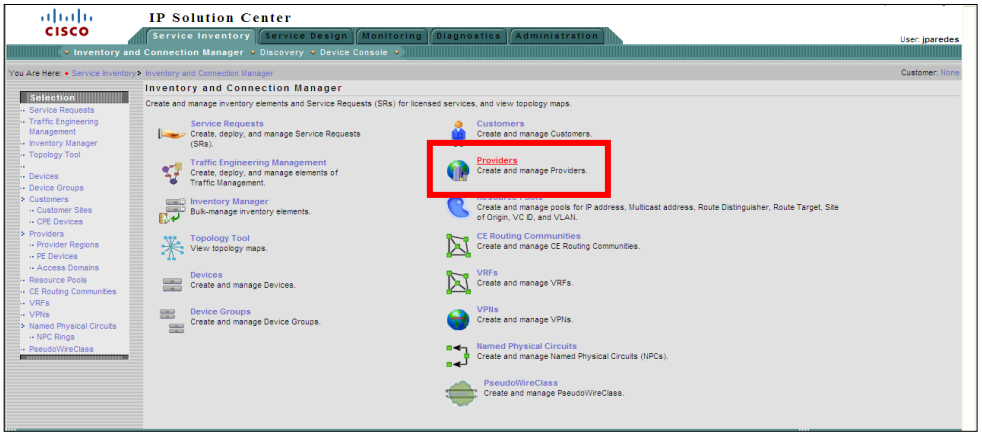


Figura 5.4.8: Opción Providers [1]

2. Crear el Proveedor (VRF) con el nombre del ISP que va a utilizar como se muestra en la figura 5.4.9:

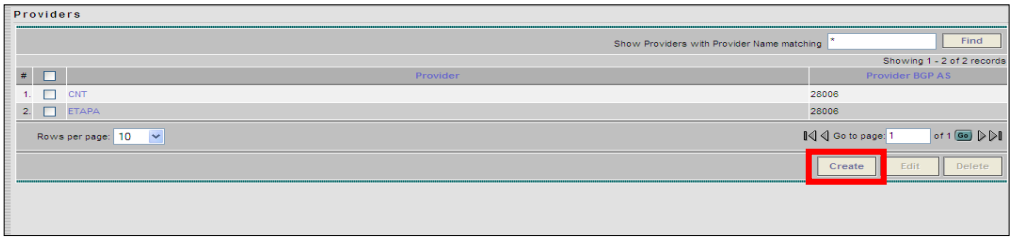


Figura 5.4.9: Colocación de los parámetros para la creación del Provider [1]

3. Colocar el nombre del ISP que va a ocupar la VRF

A cada sistema autónomo BGP se le asigna un único número de 16 bits, es importante recalcar que para este manual el valor del BGP AS se encuentra establecido por defecto para las configuraciones de todas las VRFs. El rango establecido del BGP AS va desde el 1 al 65535.

4. Guardar los cambios efectuados en la configuración como se muestra en la figura 5.4.10:

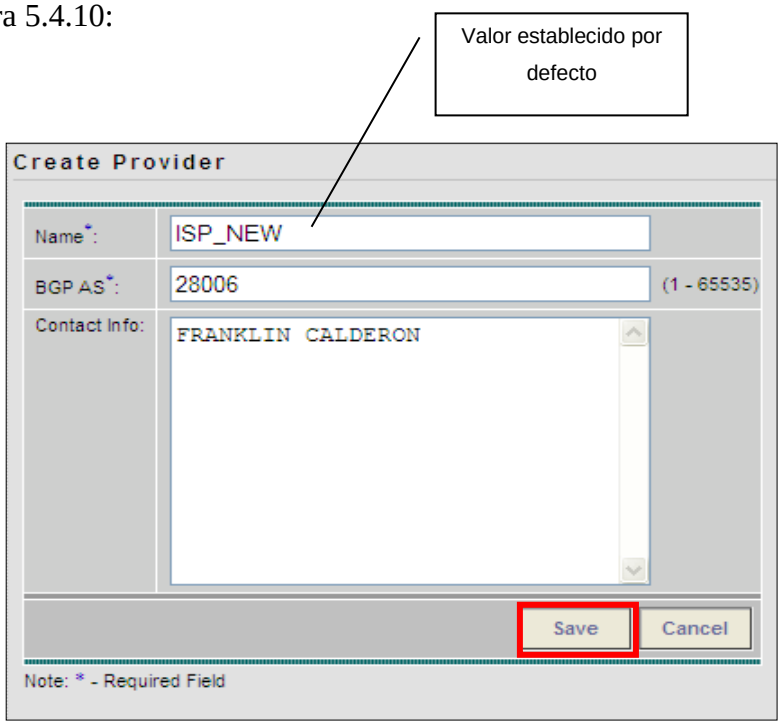


Figura 5.4.10: Opción Create Provider [1]

5. Verificar que el Provider fue creado y añadido satisfactoriamente como se muestra en la figura 5.4.11:

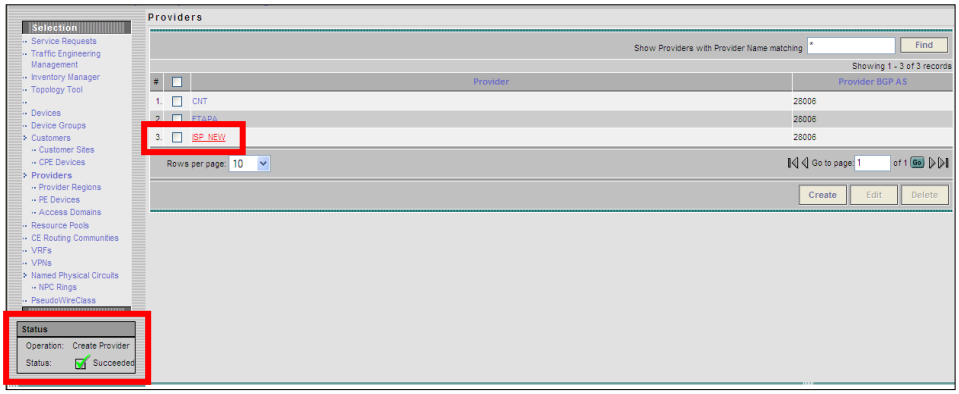


Figura 5.4.11: Verificación de la creación del Provider [1]

5.4.4.4 RESOURCE POOLS

Esta opción define un rango de direcciones IP para proporcionar servicios MPLS. Para la creación de *Resources Pools* seguir los pasos que se muestran a continuación:

1. Elegir la opción Resource Pools como se muestra en la figura 5.4.12:

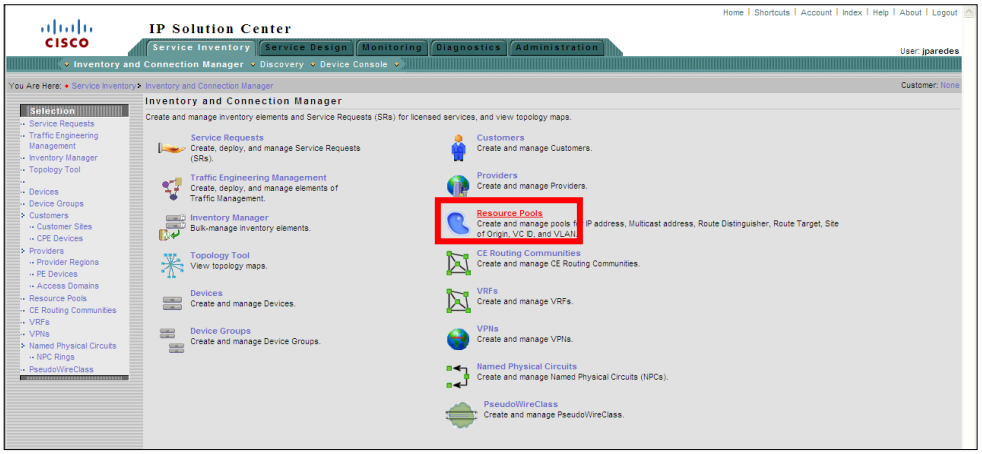


Figura 5.4.12: Opción Resource Pools [1]

2. Reservar un recurso del pool para distinguir qué servicio se va a proporcionar, se recomienda usar la opción *Route Target* porque indica a MPLS cuando las rutas deben ser insertadas en la vrf apropiada, como se muestra en la figura 5.4.13:

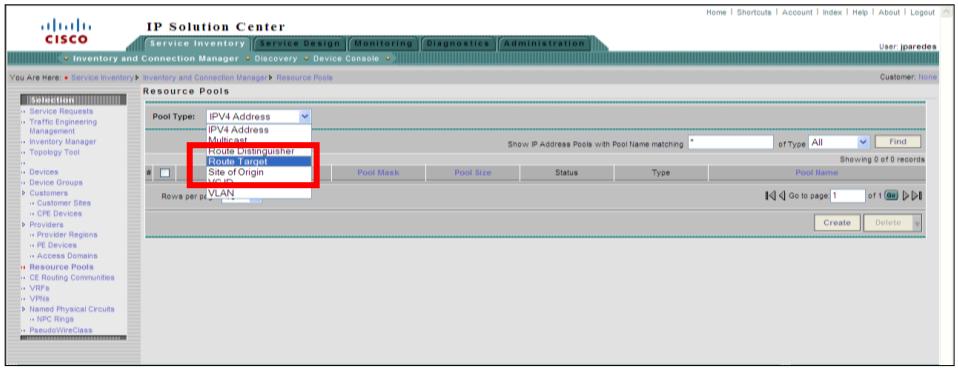


Figura 5.4.13: Opción Route Target [1]

3. A continuación escoger un Start libre o disponible.

Tomar en cuenta que los identificadores de Vrfs están asignados o reservados del 101001 hasta el 101008 y los identificadores que se encuentran disponibles o libres van desde 101009 hasta el siguiente pool.

En la siguiente tabla se aprecia los tipos de servicios que se pueden proporcionar:

TIPO DE SERVICIO	
10xxx	Net Internet
20xxx	Datos
30xxx	Multicast
40xxx	VoIP
50xxx	Gestión

Tabla 5.4.1 -Estados de una VNE Tipo de servicios [1]

4. Dentro de la opción *Route Target* verificar que las configuraciones son correctas como se muestra en la figura 5.4.14:

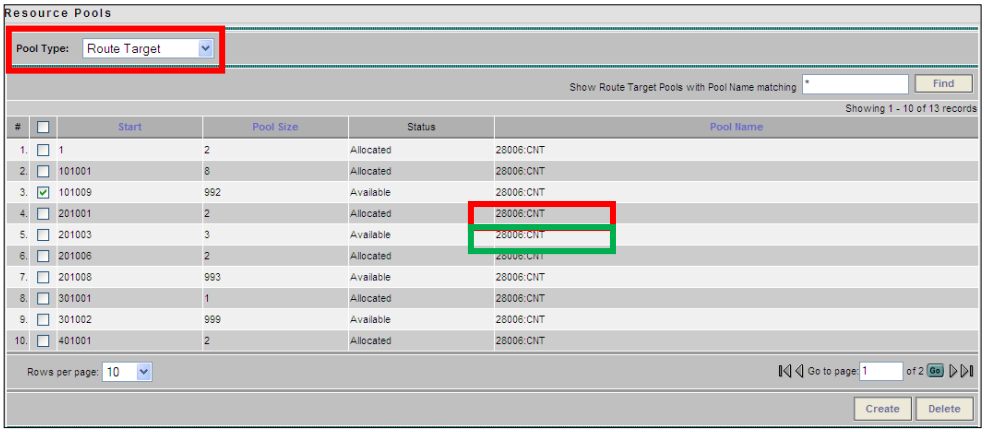


Figura 5.4.14: Verificación de configuraciones [1]

5.4.4.5 CE ROUTING COMMUNITIES

Una VPN puede ser organizada en subgrupos llamados CE Routing Communities, o Cercs. Un CERC describe cómo una VPN se puede comunicar con otra VPN. Por lo tanto, los Cercs describen la topología lógica de la VPN.

Para la creación de CE Routing Communities seguir los pasos que se muestran a continuación:

1. Elegir la opción CE Routing Communities como se muestra en la figura 5.4.15 :

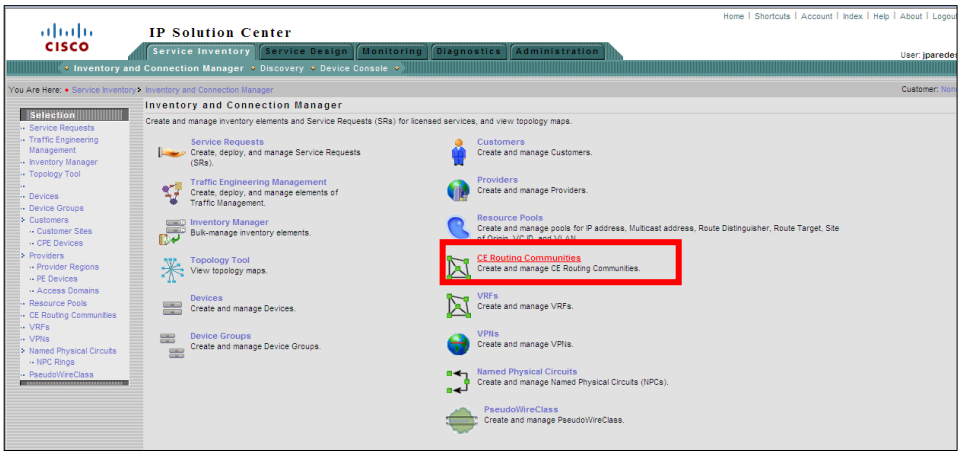


Figura 5.4.15: Opción CE Routing Communities [1]

2. En la pantalla que aparece a continuación crear la nueva Community mediante la opción *Create* como se muestra en la figura 5.4.16:

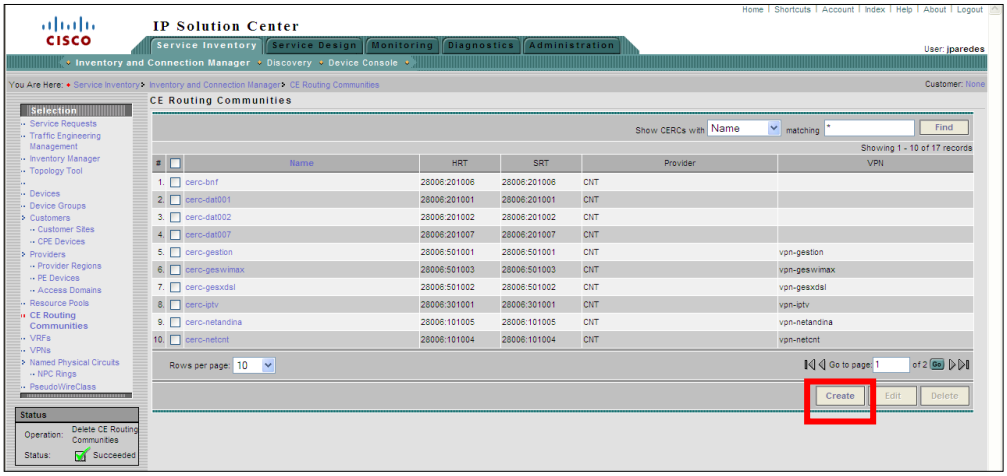


Figura 5.4.16: Creación de una nueva Community [1]

3. Escoger la opción *Select* y elegir el ISP[49] correspondiente como se muestra en la figura 5.4.17:

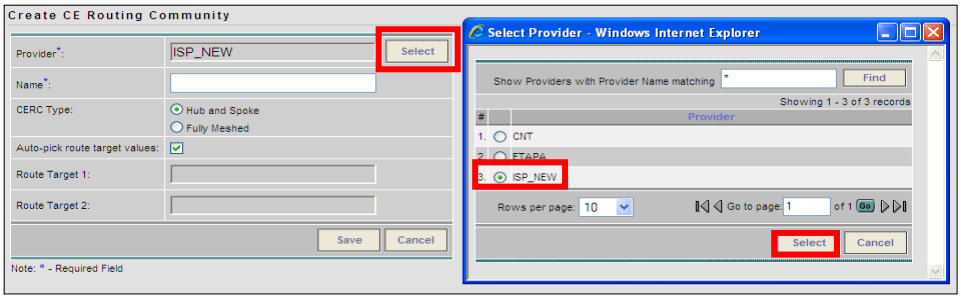


Figura 5.4.17: Selección del ISP [1]

El nombre regido a la norma establecida: Cerc_datxxxx_nombreISP xxxx= Start de Resource Pool.

Ejemplo: Cerc_dat1424_ISP_NEW

4. Elegir *Fully Meshed* para que se puedan ver entre todos los equipos CEs

[49] Véase Acrónimos

5. Colocar el Start libre del Tipo de Servicio que se quiera configurar (Resource Pool).
6. Colocar el BGP AS asignado cuando se creó el PROVIDER
7. Guardar los cambios realizados como se muestra en la figura 5.4.18:

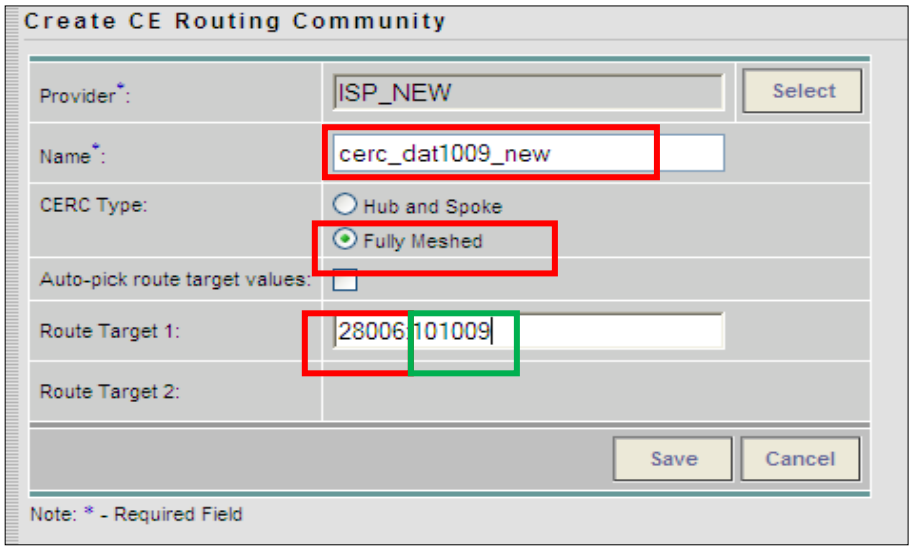


Figura 5.4.18: Configuraciones de una comunidad respectiva [1]

8. Verificar que se creó y añadió satisfactoriamente la Community como se muestra en la figura 5.4.19:

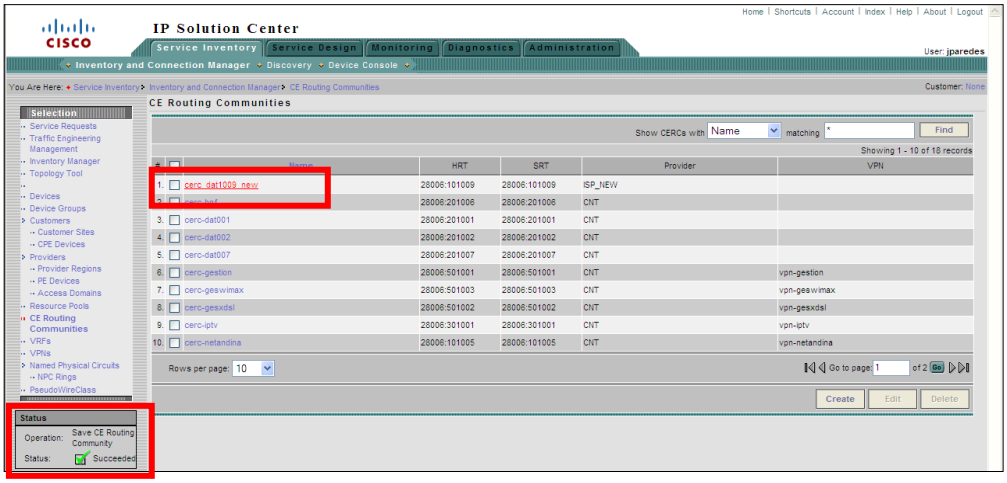


Figura 5.4.19: Verificación de la creación de la comunidad [1]

5.4.4.6 VRFs

Para la creación de una Vrf seguir los pasos que se muestran a continuación:

1. Elegir la opción VRFs como se muestra en la figura 5.4.20:

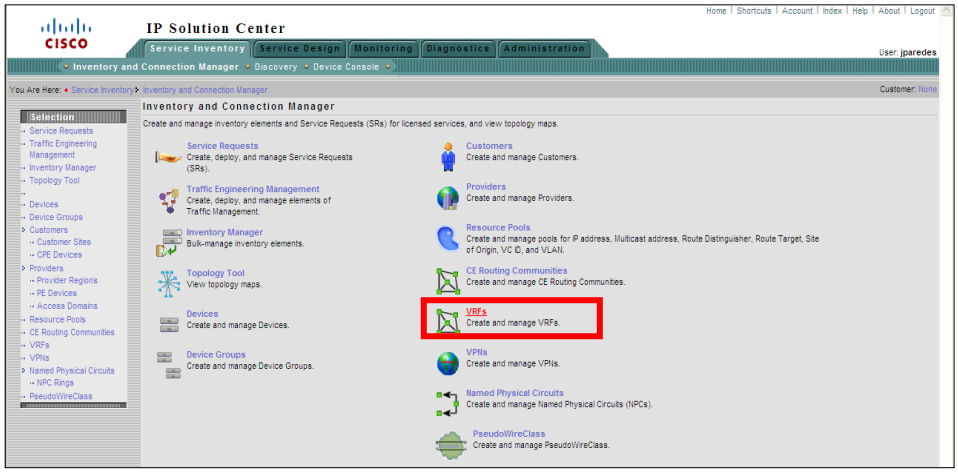


Figura 5.4.20: Opción VRF's [1]

2. Crear la nueva VRF como se muestra en la figura 5.4.21:

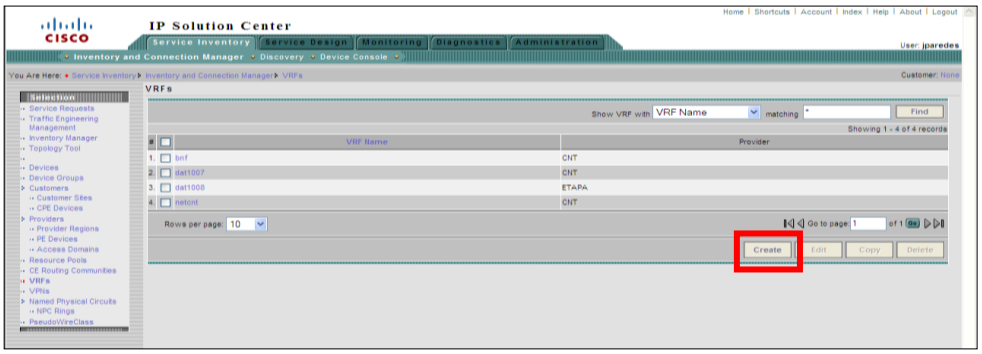


Figura 5.4.21: Creación de una nueva VRF [1]

3. Escoger la opción *Select* para elegir el *Provider* como se muestra en la figura 5.4.22:

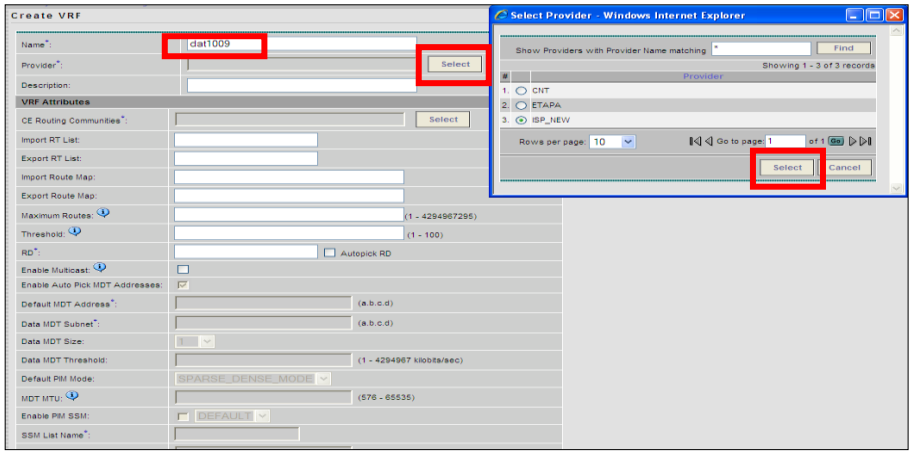


Figura 5.4.22: Selección de un proveedor [1]

- ✓ El nombre establecido: Datxxxx
- ✓ Dat: Para los servicios de datos, el tipo de servicios se muestra en la Tabla 5.4.1
- ✓ xxxx= Start de Resource Pool

Ejemplo: Dat1424, donde Dat=20 y 1424 es el Star de Resorce Pool

4. Colocar el tipo de servicio que se va a implementar, además se puede ubicar datos adicionales como el nombre del cliente como se muestra en la figura 5.4.23:

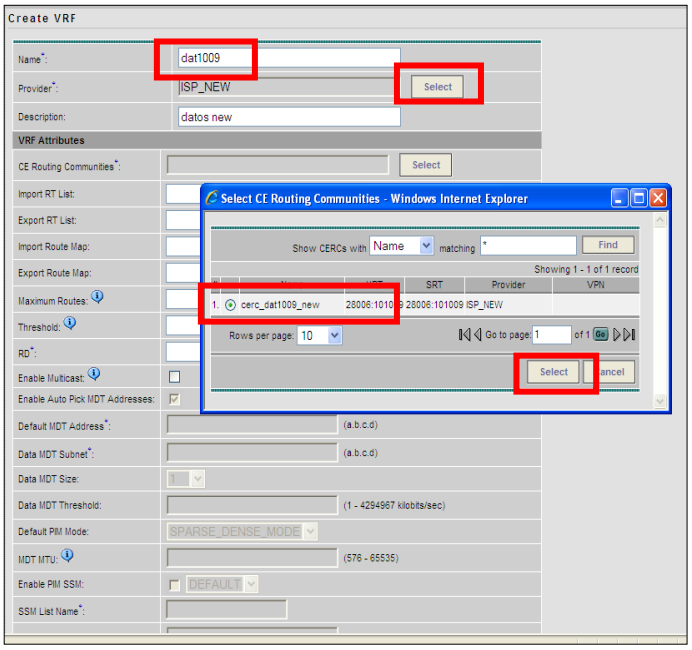


Figura 5.4.23: Parámetros de configuración de una VRF [1]

Es importante mencionar lo siguiente:

- ✓ **IMPORT RT:** Es opcional cuando se crea una nueva VRF pero si ya existe una configurada previamente es necesario colocarlo.
- ✓ **RD*:** Colocar el mismo que se ingresó cuando se creó el CE correspondiente como se muestra en la figura 5.4.24:

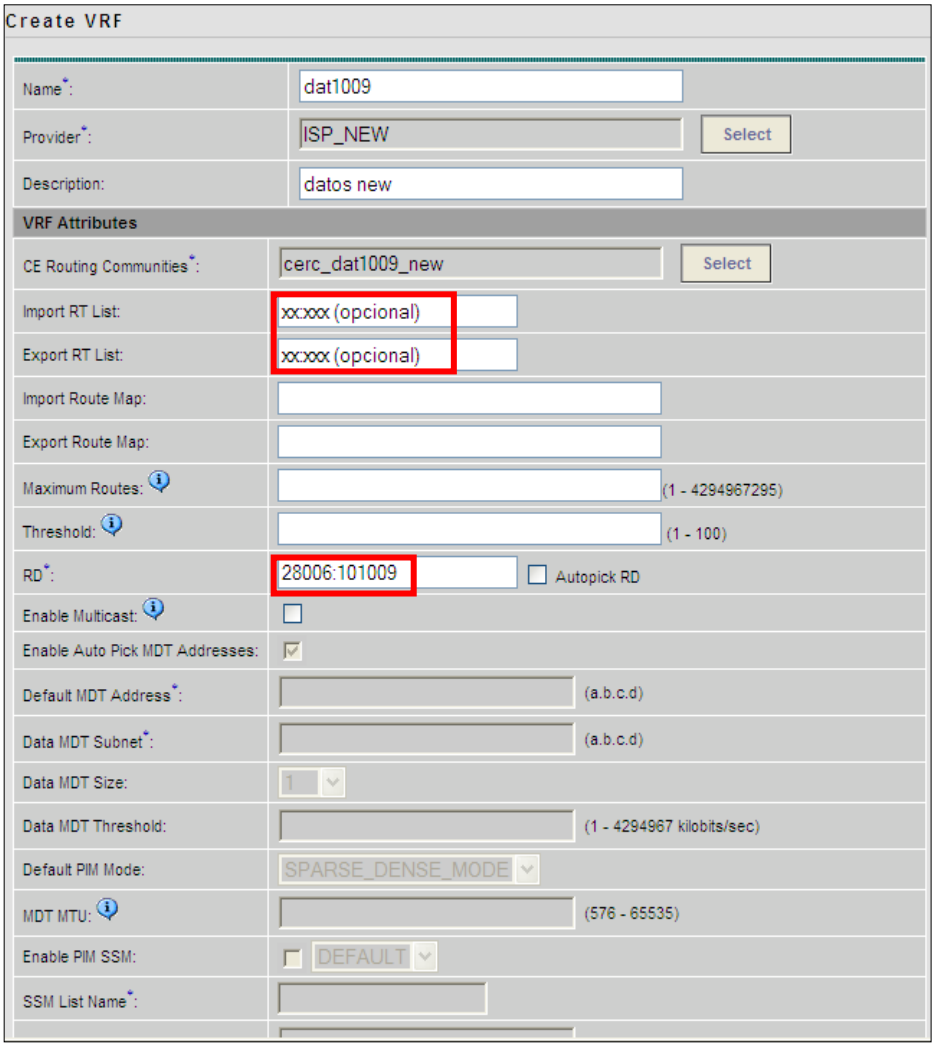


Figura 5.4.24: Parámetros opcionales para la configuración de una VRF [1]

5. Para crear la VRF escoger *Save* como se muestra en la figura 5.4.25:

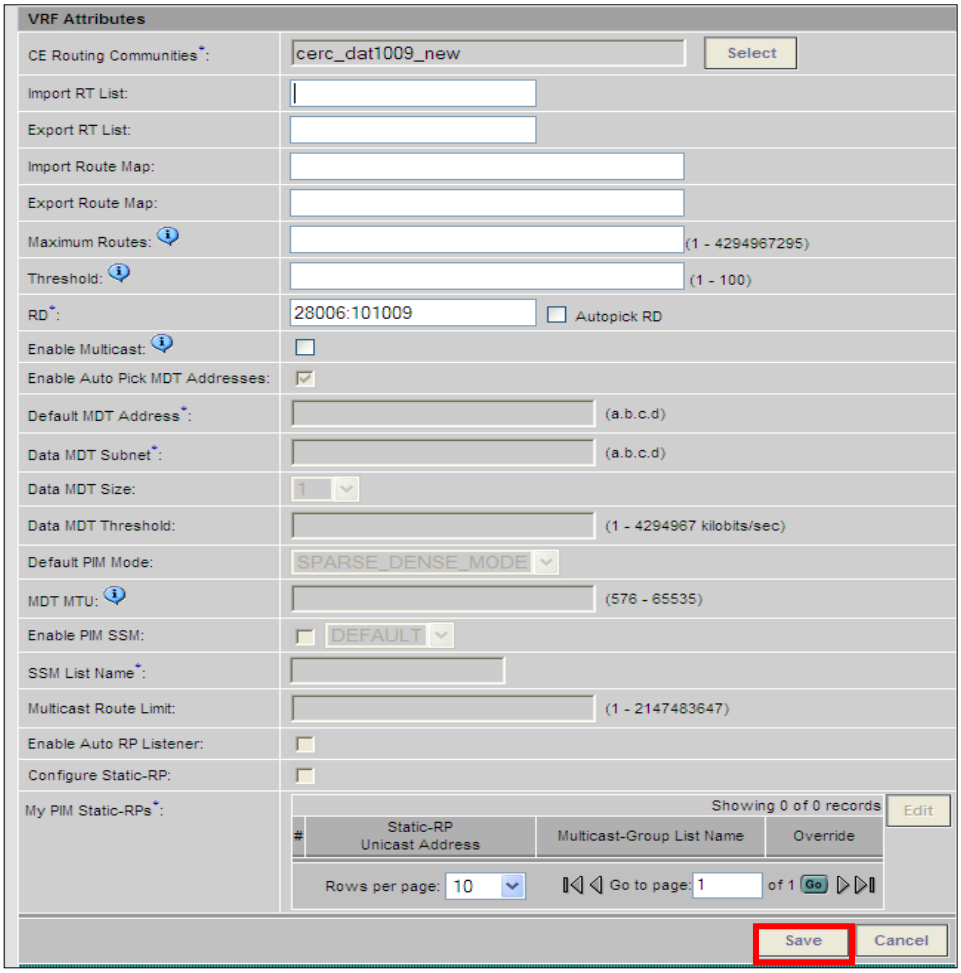


Figura 5.4.25: Guardar las configuraciones de la VRF [1]

6. Es importante verificar si el cliente se creó y se añadió satisfactoriamente como se muestra en la figura 5.4.26:

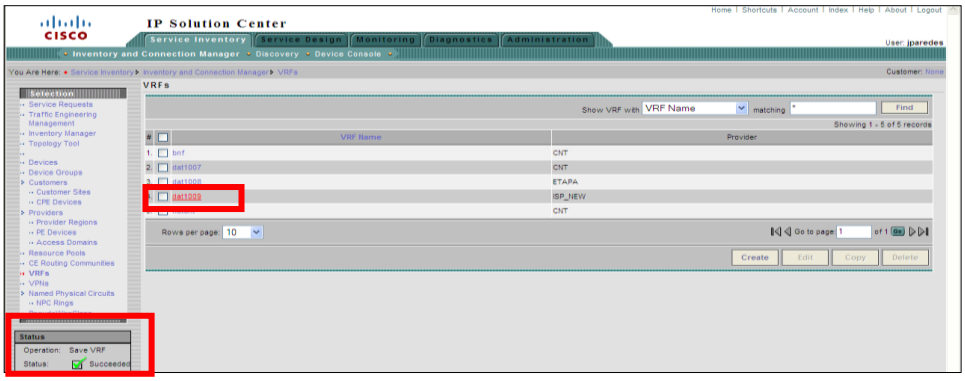


Figura 5.4.26: Verificación del cliente añadido satisfactoriamente [1]

5.4.4.7 VLANS

Para la creación de VLANS seguir con los pasos que se muestran a continuación:

1. Elegir la opción *Service Inventory* y dentro de ésta escoger la opción *Device Console* como se muestra en la figura 5.4.27:

Figura 5.4.27: Opción Device Console [1]

2. Seleccionar la opción *Next* como se muestra en la figura 5.4.28:

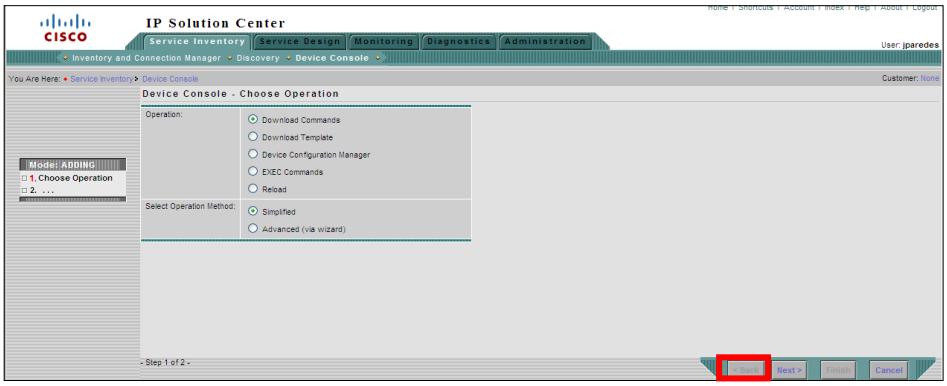


Figura 5.4.28: Opción Next [1]

3. La búsqueda se puede realizar ya sea por Dispositivos o por Grupos.

✓ BÚSQUEDA POR DISPOSITIVO

Para realizar una búsqueda por dispositivo ver la figura 5.4.29:

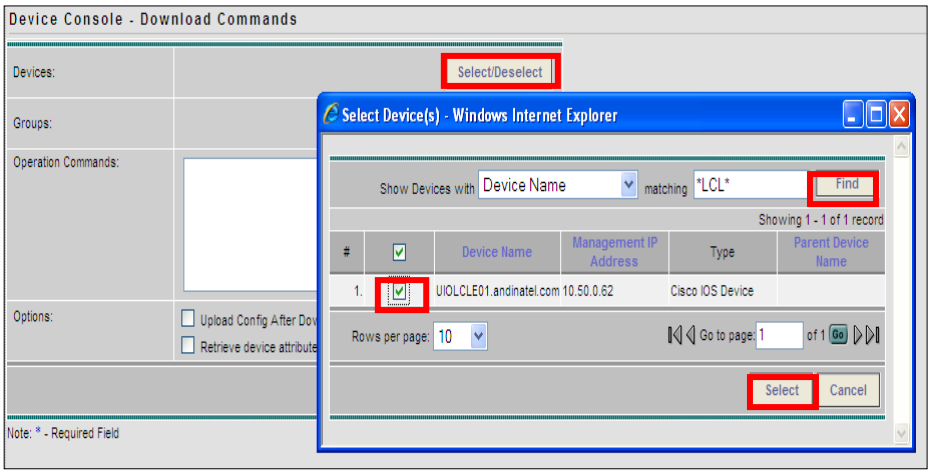


Figura 5.4.29: Búsqueda por Dispositivo [1]

✓ BÚSQUEDA POR GRUPO

Para realizar una búsqueda por grupo ver la figura 5.4.30:

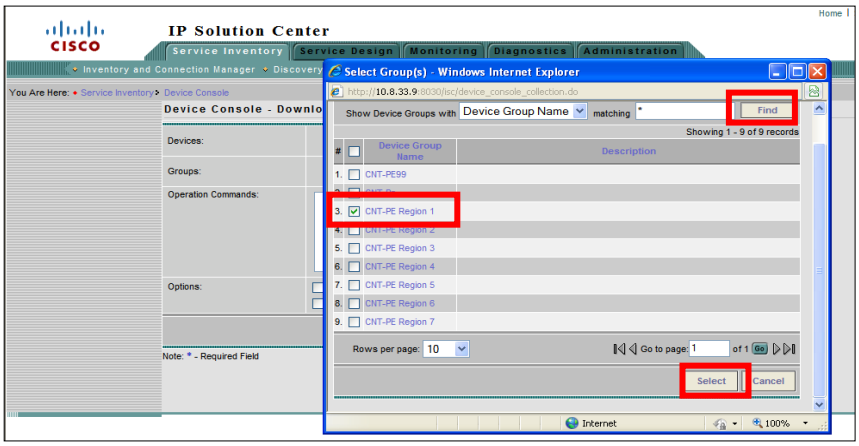


Figura 5.4.30: Búsqueda por Grupo [1]

1. Colocar los siguientes parámetros en el comando de operación como se muestra en el siguiente ejemplo y finalmente seleccionar Ok como se muestra en la figura 5.4.31:

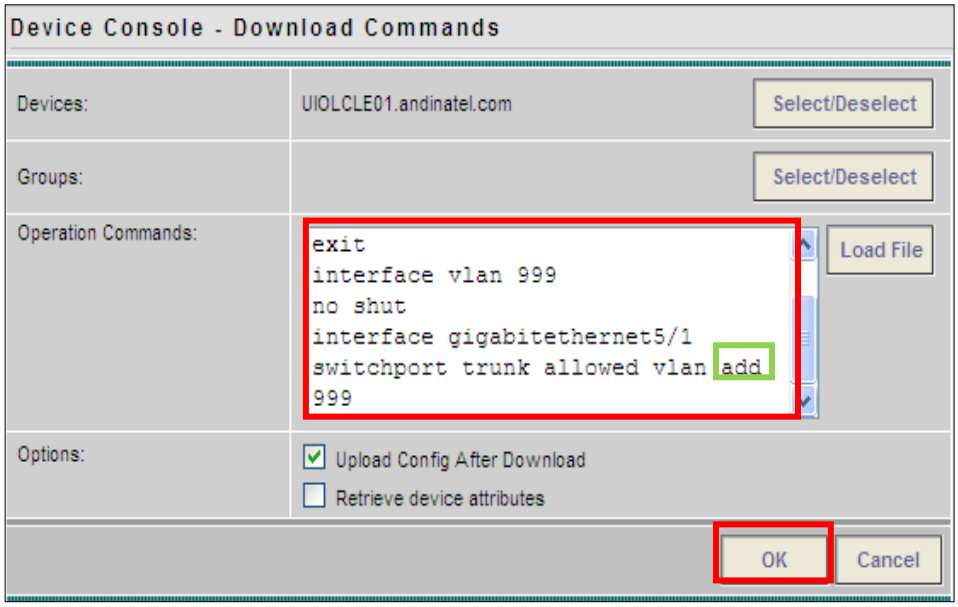


Figura 5.4.31: Selección de parámetros en el comando de operación [1]

✓ Importante: no olvidar poner ADD en los comandos de operación.

2. Finalmente verificar si la vlan ya se encuentra creada como se muestra en la figura 5.4.32:

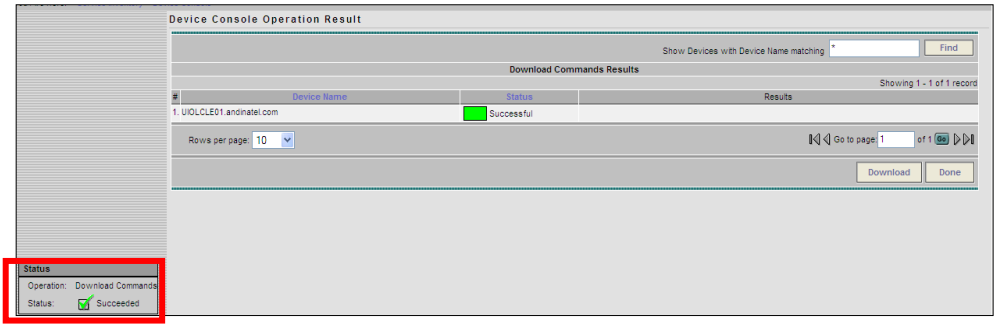


Figura 5.4.32: Verificación de la creación de la VLAN [1]

5.4.4.8 MPLS VPN

Para la creación de MPLS VPN seguir los pasos que se muestra a continuación:

1. En la opción *Service Inventory* escoger la opción *Inventory and Connection Manager* como se muestra en la figura 5.4.33:

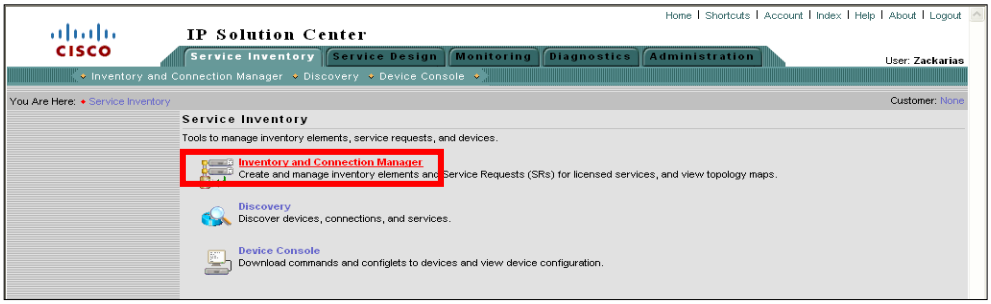


Figura 5.4.33: Opción Inventory and Connection Manager [1]

2. Para crear este servicio elegir la opción *Service Requests* como se muestra en la figura 5.4.34:

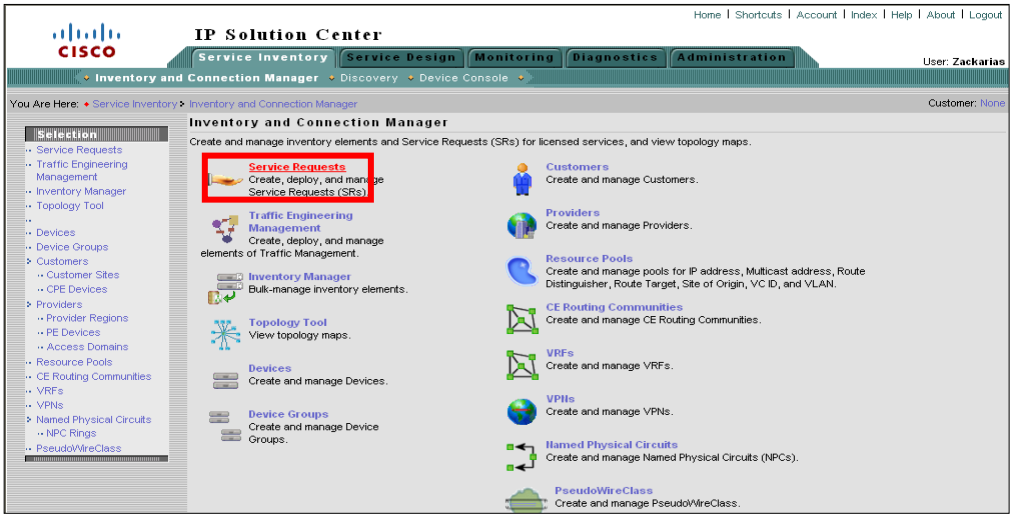


Figura 5.4.34: Opción Service Requests [1]

3. En la barra desplegable en la opción *Create* seleccionar *MPLS VPN* como se muestra en la figura 5.4.35:

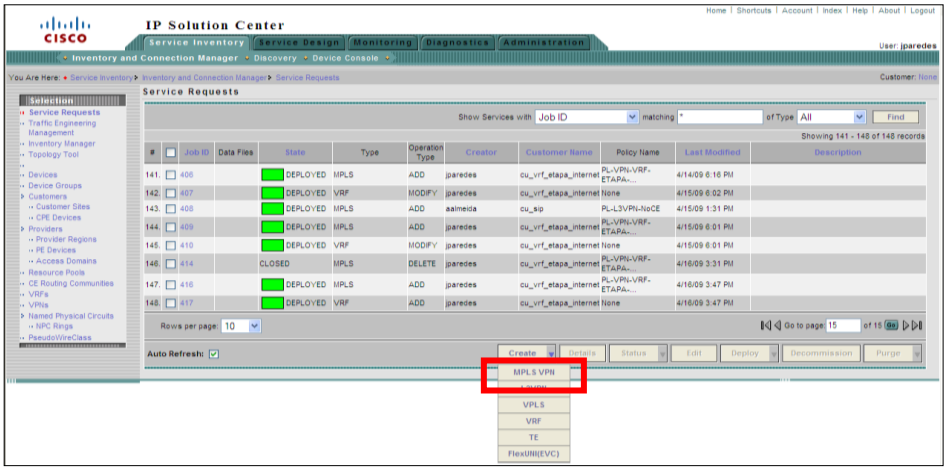


Figura 5.4.35: Selección de la opción MPLS VPN [1]

4. Siempre elegir la política (Policy) para todas las MPLS VPN que se vayan a crear como se muestra en la figura 5.4.36.

   ✓ Se escoge esta política porque es una plantilla de configuraciones base para los servicios MPLS-VPN.

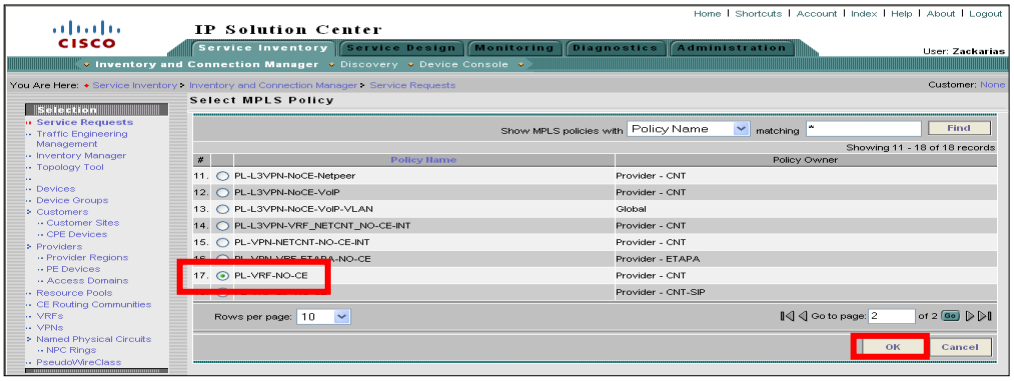


Figura 5.4.36: Selección de la opción Policy [1]

5. Seleccionar el Customer anteriormente creado y escoger Select como se muestra en la figura 5.4.37:

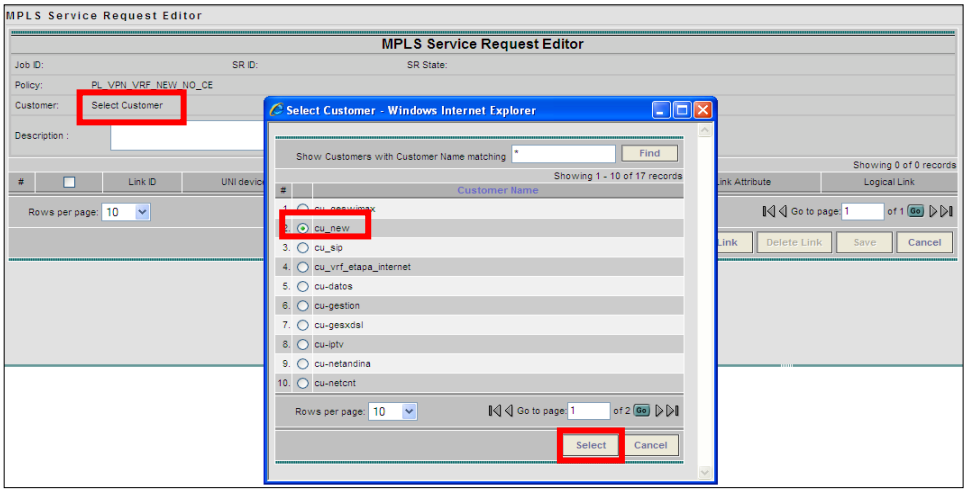


Figura 5.4.37: Selección del Customer anteriormente creado [1]

6. Añadir el enlace como se muestra en la figura 5.4.38:

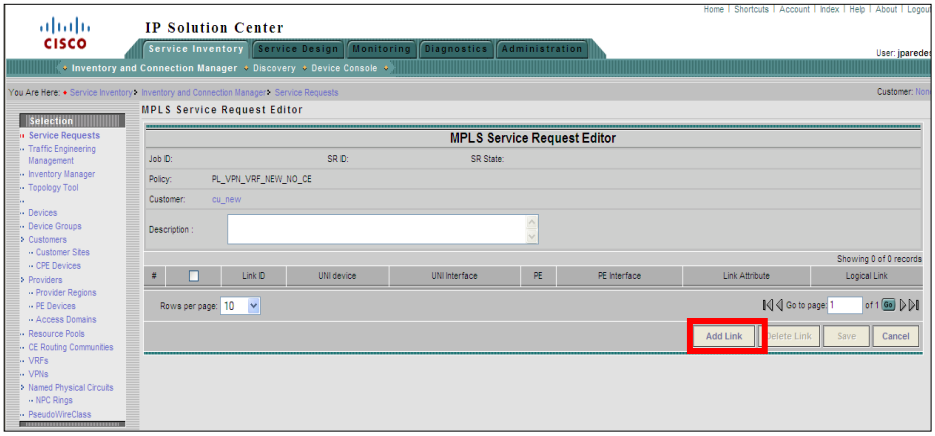


Figura 5.4.38: Adición de un enlace [1]

7. Seleccionar el equipo del provider como se muestra en las figuras 5.4.39 y 5.4.40:

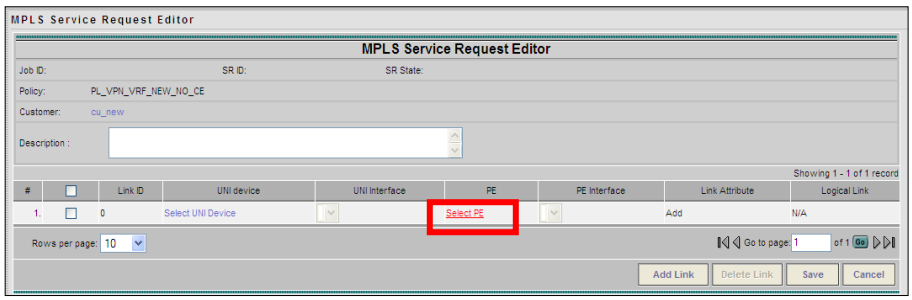


Figura 5.4.39: Selección del equipo del proveedor [1]

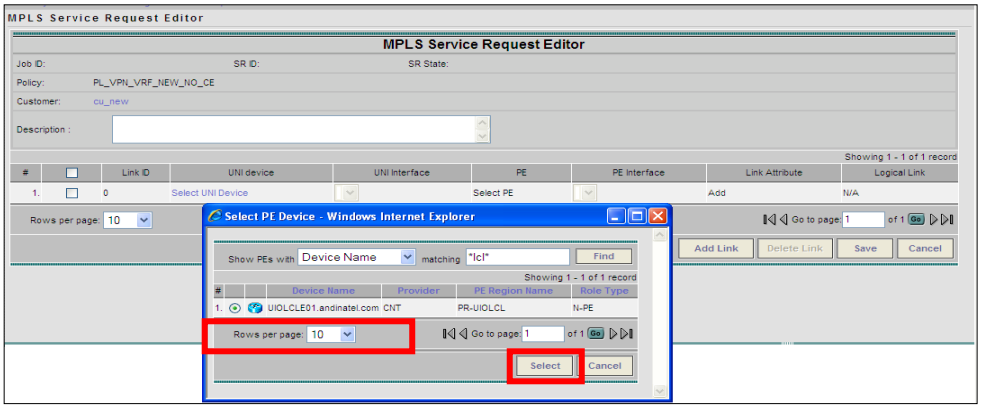


Figura 5.4.40: Opción PE Device [1]

8. Elegir la interface que para este caso será la Vlan.

9. Revisar si la VLAN se encuentra configurada en el equipo correspondiente como se muestra en la figura 5.4.41:

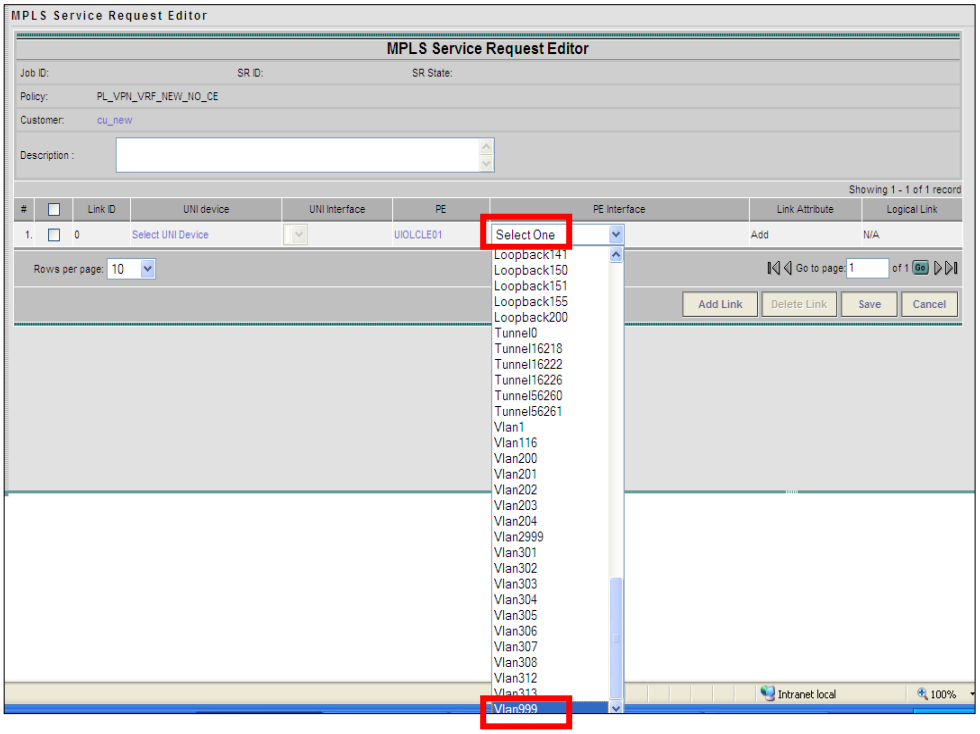


Figura 5.4.41: Selección de la interface vlan [1]

10. Añadir la Vlan creada como se muestra en la figura 5.4.42:

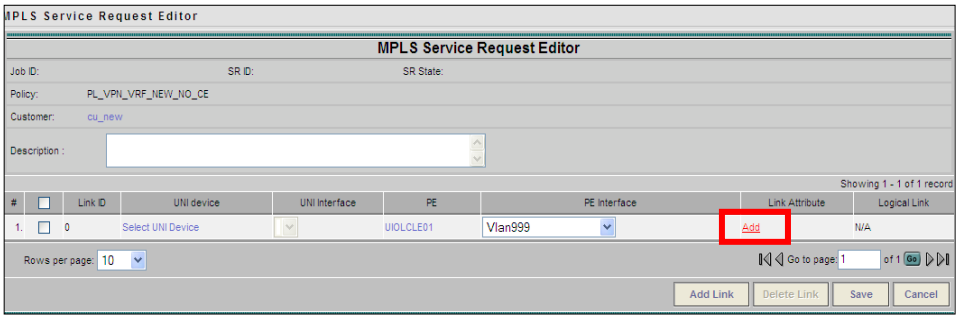


Figura 5.4.42: Adición de una vlan creada [1]

11. En la opción *Interface Description* ingresar el nombre del administrador y número de servicio (NS) como se muestra en la figura 5.4.43.

    ✓ **NS:** El número de servicio es un identificador numérico asignado para la identificación del circuito de un cliente.

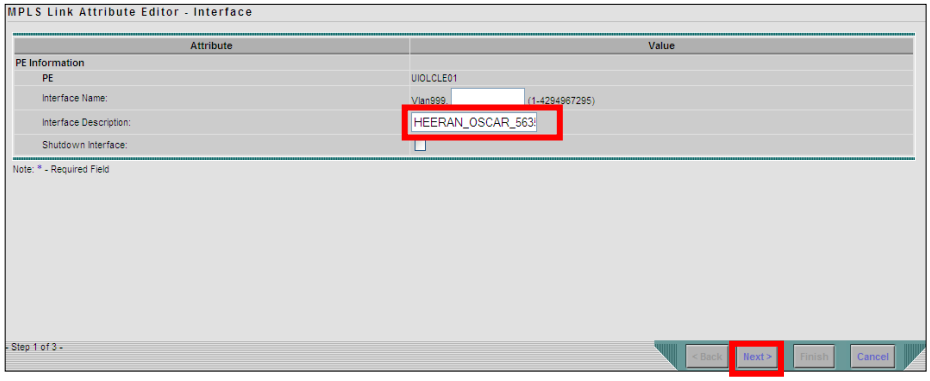


Figura 5.4.43: Opción Interface Description [1]

12. Colocar la IP WAN del equipo del cliente (CE[50]) con su respectiva máscara es importante no dejar espacios como se muestra en la figura 5.4.44:

[50] Véase Acrónimos

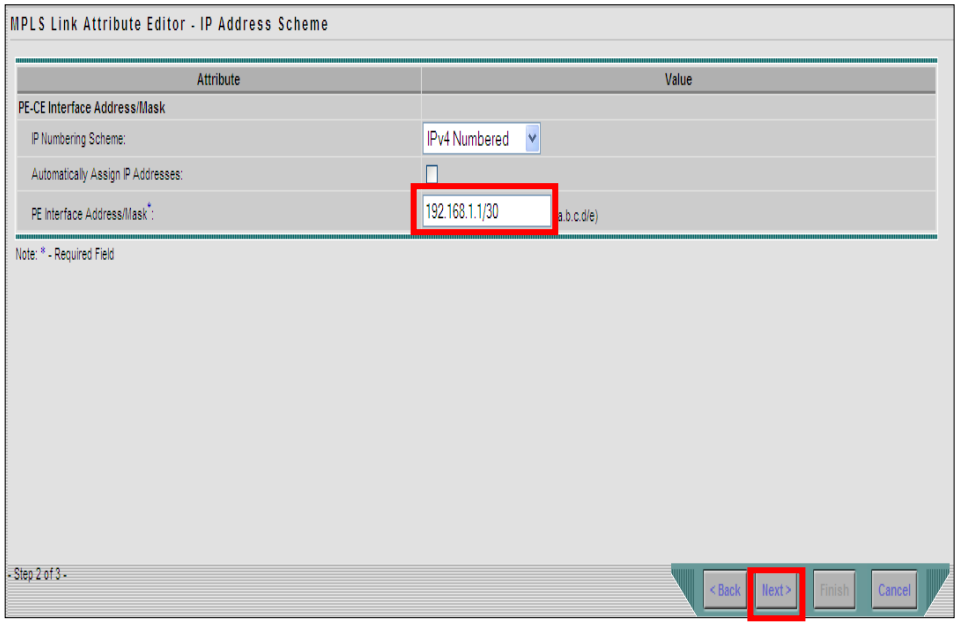


Figura 5.4.44: Colocación de la IP WAN y máscara a un equipo [1]

13. Colocar la IP LAN del equipo del cliente (CE) con su respectiva máscara es importante no dejar espacios además adicionar el tipo de prioridad como se muestra en la figura 5.4.45:

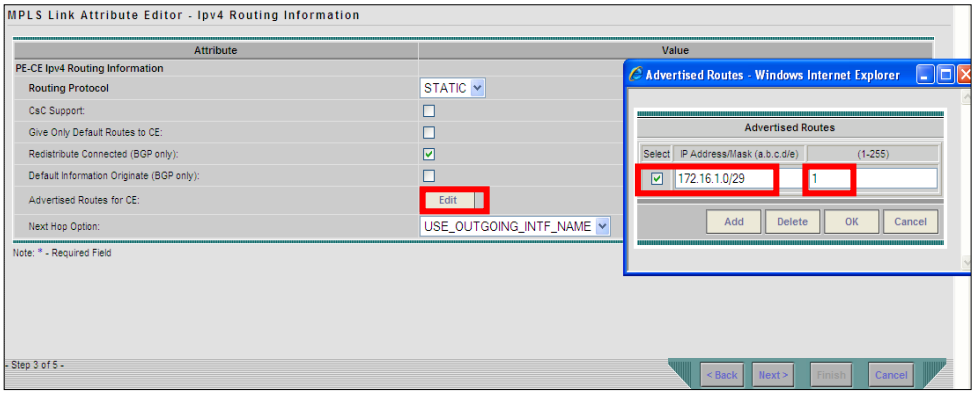


Figura 5.4.45: Colocación de la IP LAN y máscara a un equipo [1]

14. Escoger la opción *USE_ NEXT_ HOP_ IPADDR* la misma que permite cuál será el siguiente salto por donde se puede hallar la red LAN, como se muestra en la figura 5.4.46:

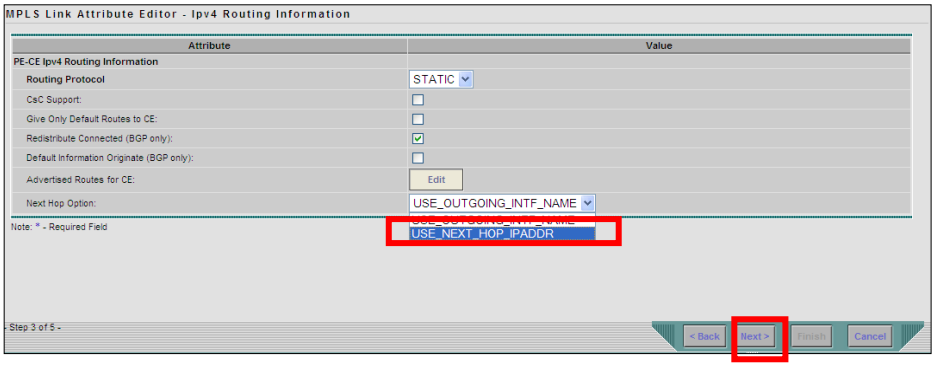


Figura 5.4.46: Opción USE_ NEXT_ HOP_ IPADDR [1]

15. Colocar la dirección IP WAN del siguiente salto del equipo del cliente como se muestra en la figura 5.4.47:

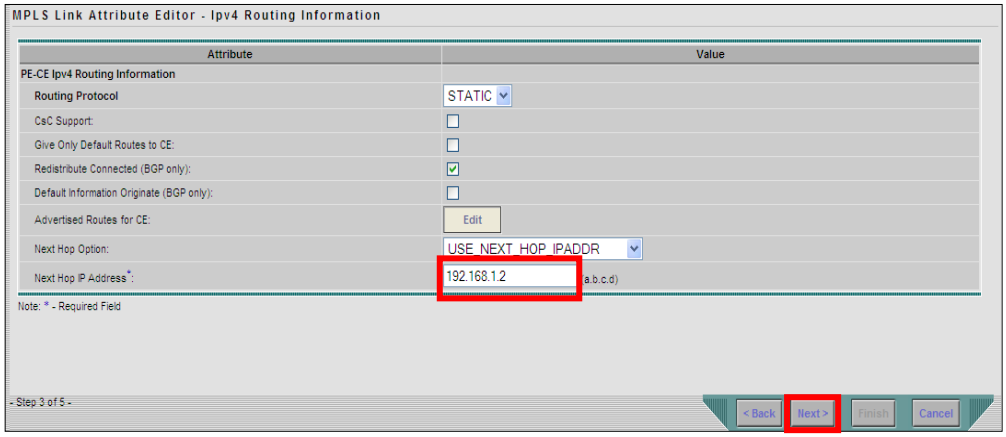


Figura 5.4.47: Colocación de la dirección IP WAN [1]

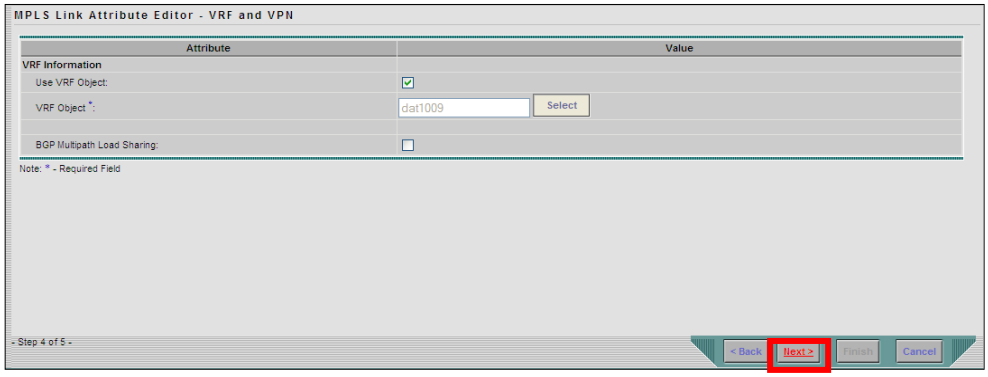


Figura 5.4.48: Opción Next [1]

16. Escoger *Finish* como se muestra en la figura 5.4.49:

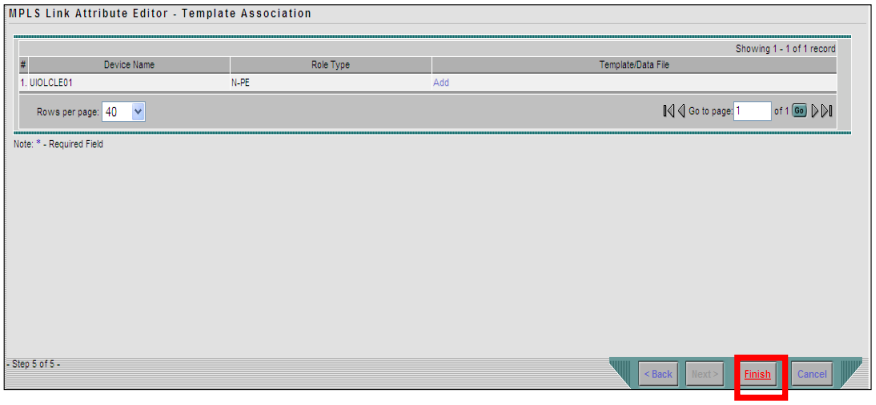


Figura 5.4.49: Opción Finish [1]

Es importante mencionar que cuando se olvida guardar la configuración aparece una advertencia y para ello se debe colocar la opción *Save* como se muestra en la figura 5.4.50:

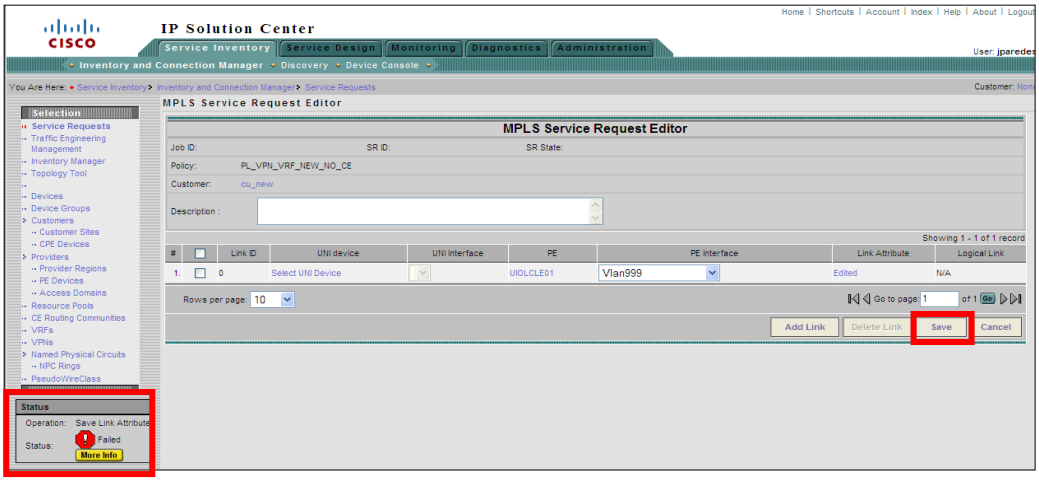


Figura 5.4.50: Advertencia para guardar cambios [1]

5.4.4.9 CREACIÓN DE SERVICIO MPLS-VPN

Cuando se crea una MPLS-VPN automáticamente se crea una VRF pero si solo se desea añadir una VRF se debe seguir los siguientes pasos:

1. Crear la VRF
2. Adjuntar la VRF a la Interface como se muestra en la figura 5.4.51:

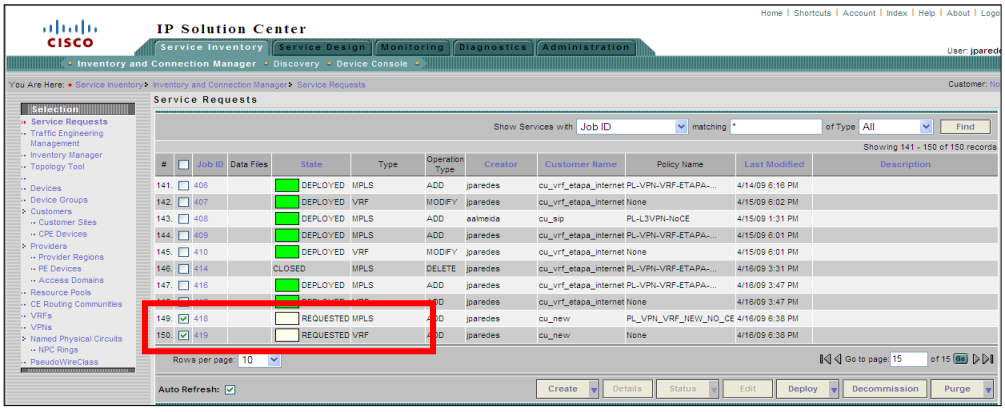


Figura 5.4.51: Adición de la VRF a la interface [1]

3. En la barra desplegable escoger la opción *Deploy* tanto para la VRF como para la interface como se muestra en la figura 5.4.52:

La opción *Deploy* sirve para que se ejecute la información de todos los formularios de configuración del servicio MPLS correspondiente.

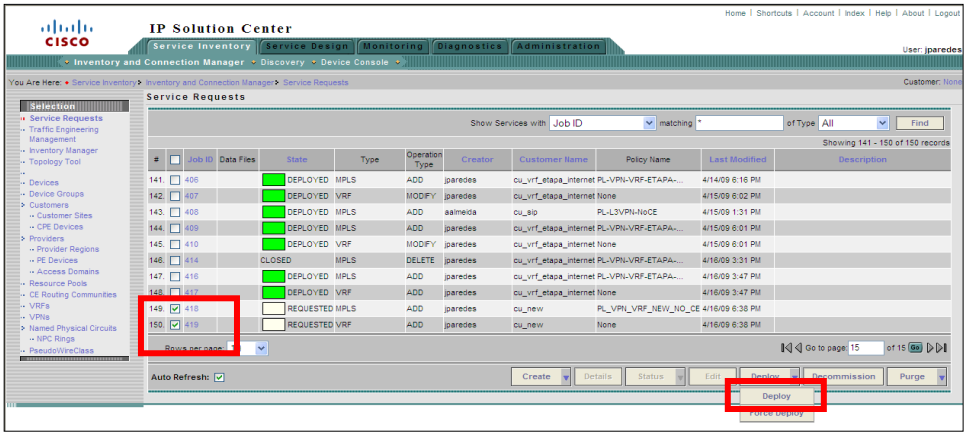


Figura 5.4.52: Opción Deploy [1]

4. Guardar los cambios efectuados como se muestra en la figura 5.4.53:

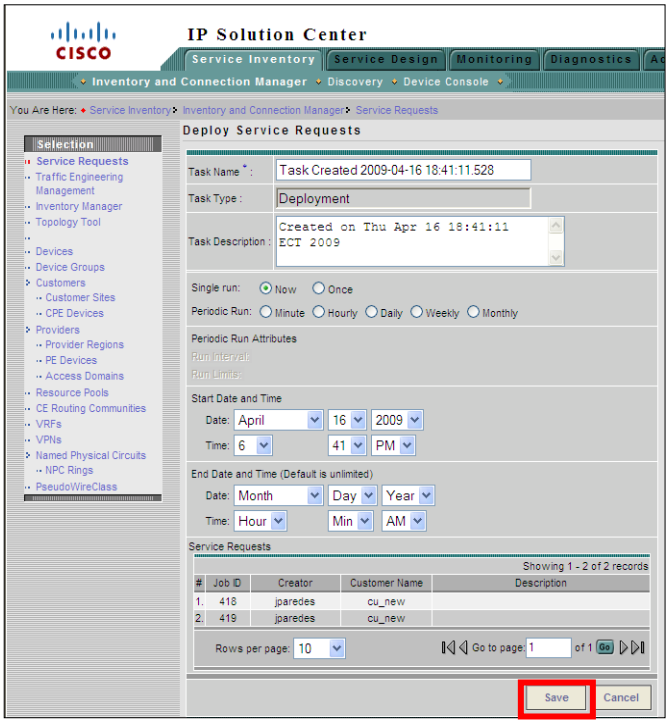


Figura 5.4.53: Guardar cambios efectuados [1]

5. Revisar el cambio de Estado y que se creó satisfactoriamente como se muestra en la figura 5.4.54:

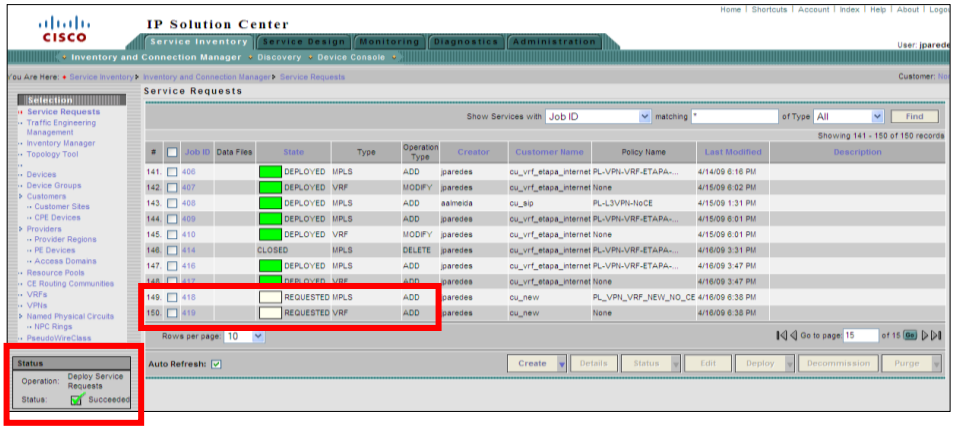


Figura 5.4.54: Revisión de los cambios efectuados [1]

6. Para finalizar verificar que ya se encuentran activas (Up) las interfaces como se muestra en la figura 5.4.55:

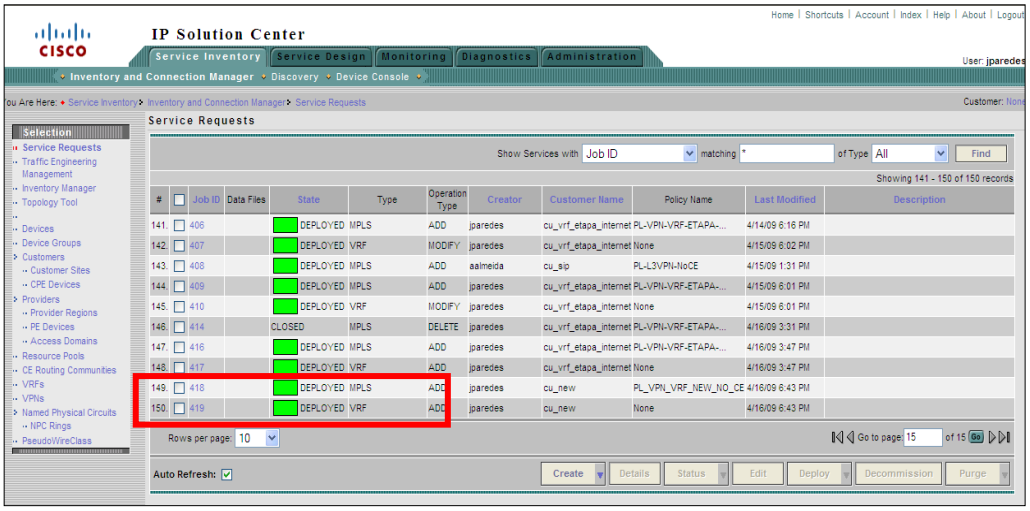


Figura 5.4.55: Verificación del estado de la interface [1]

5.4.4.10 BORRAR VRF'S

Para borrar una VRF realizar los pasos que se muestran a continuación:

1. Elegir una por una las interfaces para proceder a borrarlas y a continuación escoger la opción *Decommission* como se muestra en la figura 5.4.56:

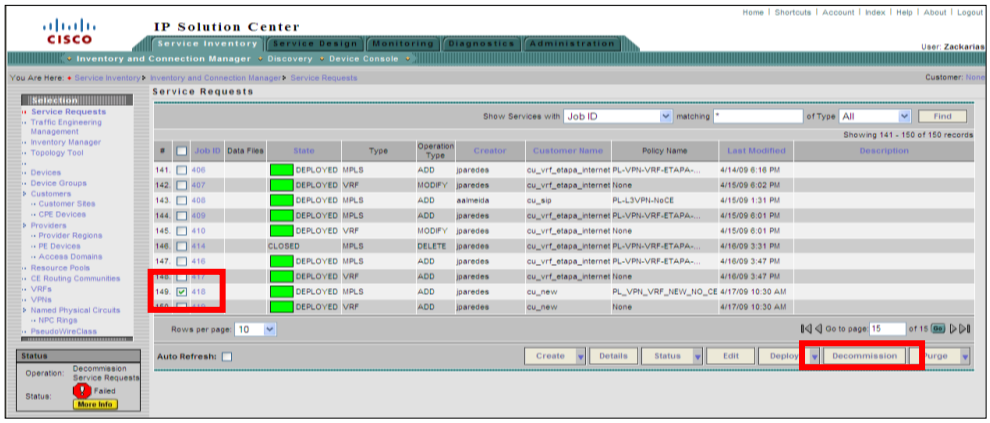


Figura 5.4.56: Opción Decommission [1]

2. Para efectuar los cambios realizados seleccionar OK como se muestra en la figura 5.4.57:

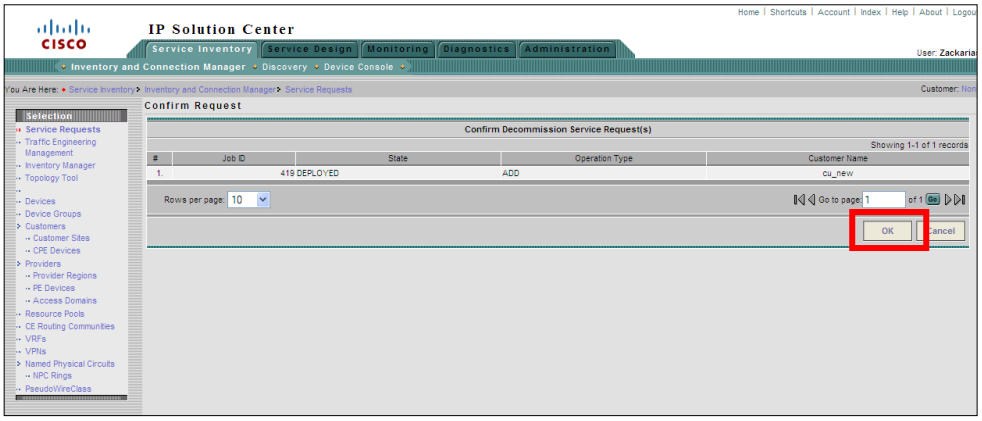


Figura 5.4.57: Validación de cambios efectuados [1]

3. Escoger Deploy para eliminar las configuraciones anteriormente creadas como se muestra en la figura 5.4.58:

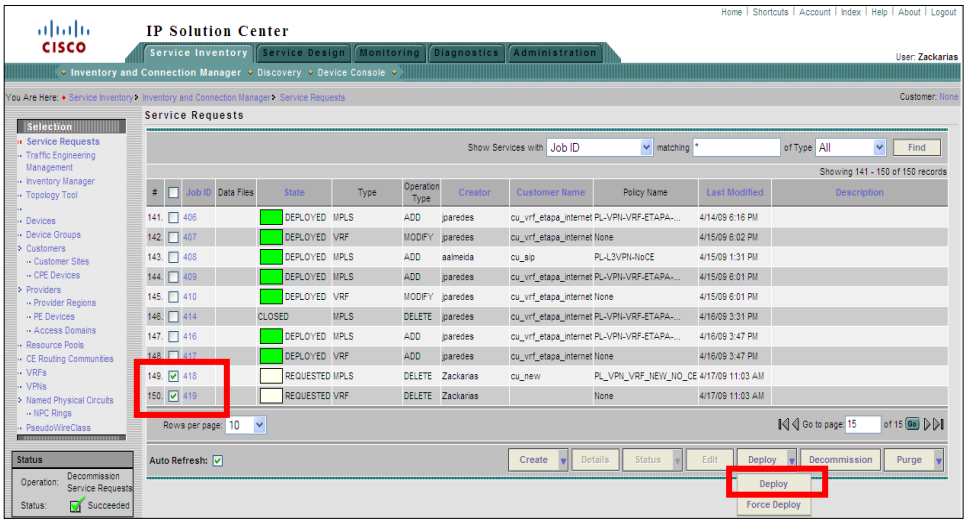


Figura 5.4.58: Opción Deploy para eliminar configuraciones [1]

4. Guardar los nuevos cambios como se muestra en la figura 5.4.59:

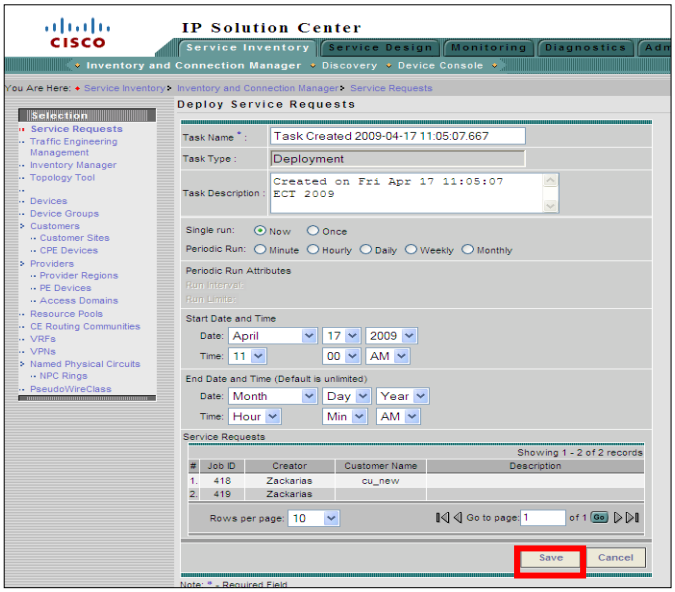


Figura 5.4.59: Guardar nuevos cambios efectuados [1]

5. Revisar que la VRF y la interface estén inhabilitadas como se muestra en la figura 5.4.60:

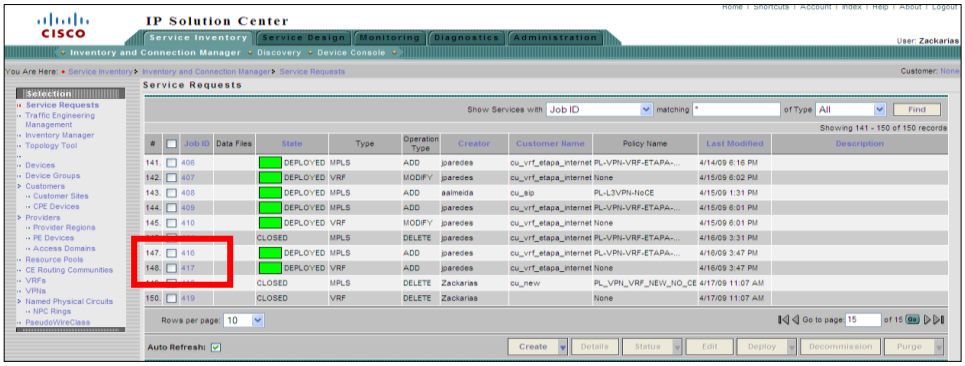


Figura 5.4.60: Verificación de la inactividad de la VRF y la Interface

5.4.5 OPCIÓN SERVICE DESING

La sección *Service Desing* contiene herramientas de administración para crear y administrar políticas y plantillas (Templates) como se muestra en la figura 5.4.61:

Figura 5.4.61: Opción Service Desing [1]

- ✓ **Policies:** Crean y administran las políticas de servicios autorizados.
- ✓ **Templates:** Crean y administran templates y los datos asociados.

5.4.5.1 OPCIÓN POLICIES

Se muestran las diversas configuraciones previamente realizadas como el provider, nombre de la política y tipo de política como se muestra en la figura 5.4.62:

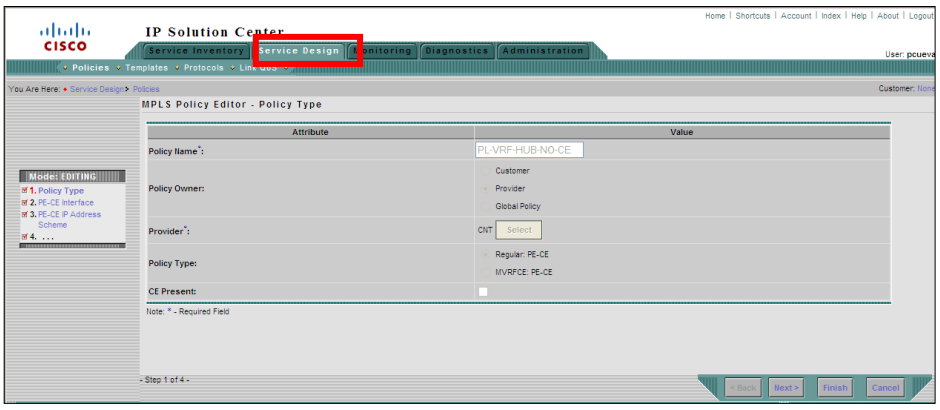


Figura 5.4.62: Opción Policies [1]

Para escoger el nombre de la política dar clic en la casilla que se muestra en la figura 5.4.62 y de la lista que se muestra escoger la opción PL-VRF-HUB-NO-CE como se muestra en la figura 5.4.63:

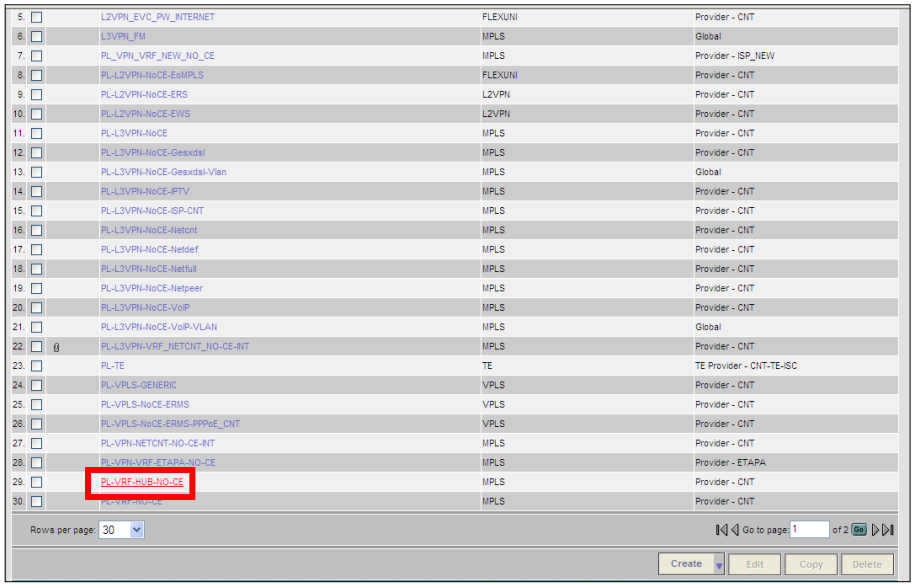


Figura 5.4.63: Selección del nombre de la política [1]

5.4.5.2 OPCIÓN TEMPLATES

Escoger la plantilla que se requiere para la configuración como se muestra en la figura 5.4.64:

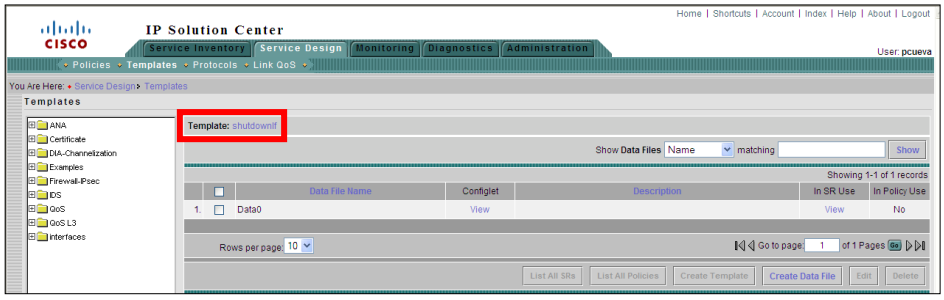


Figura 5.4.64: Opción Templates [1]

5.4.6 OPCIÓN MONITORING

Contiene herramientas de monitoreo para administrar tareas, parámetros de ping, Service Level Agreement (SLA), informes de ingeniería de tráfico de rendimiento y otros informes, como se muestra en la figura 5.4.65:

Figura 5.4.65: Opción Monitoring [1]

5.4.7 OPCIÓN DIAGNOSTICS

Esta opción contiene la solución de problemas y diagnóstico automatizado para VPNs MPLS, como se muestra en la figura 5.4.66:

Figura 5.4.66: Opción Diagnostics [1]

5.4.8 OPCIÓN ADMINISTRATION

Esta opción contiene herramientas que permiten realizar configuraciones para:

- ✓ La gestión de usuarios
- ✓ La configuración del ISC
- ✓ Servidores y licencias
- ✓ Ver los usuarios y el registro de acceso de los usuarios
- ✓ Especificar los atributos de algunos mensajes como se muestra en la figura 5.4.67:

Figura 5.4.67: Opción Administration [1]

Este manual es muy útil para las diferentes configuraciones de usuario porque presenta diversas aplicaciones para la mejor administración de servicios.

5.5 MANUAL NAGIOS

5.5.1 OBJETIVO

Conocer el manejo de la plataforma Nagios, así como la creación de equipos, servicios y alarmas

5.5.2 INSTALACIÓN DEL SERVIDOR NAGIOS

Para poder instalar el servidor Nagios se debe digitar el siguiente comando:

sudo aptitude install –y nagios3

Adicional con Nagios se instalarán otros paquetes necesarios para el funcionamiento eficiente del mismo. En el proceso de instalación se pedirá el ingreso de una contraseña para Nagios, es necesario fijarla, para poder ingresar a la interfaz web.

Una vez que se concluya la instalación se reiniciará el servidor *apache2,* el cual está encargado de subir el sitio web de consulta de Nagios. Para poder acceder a la interfaz web de Nagios se debe digitar:

- ✓ http://ip-del-servidor/nagios3/

El directorio donde se ejecuta Nagios es: */etc/nagios3/*. Dentro de la carpeta nagios3 se encuentra un directorio llamado *conf.d,* aquí se alojan los archivos de configuraciones de host, grupos de host y servicios.

Se debe cambiar los permisos del directorio */etc/nagios3/conf.d/*, así:

sudo chmod 777 /etc/nagios3/conf.d/

Aquí se va a crear los equipos, servicios y demás definiciones que van a ser utilizados por el servidor Nagios.

A continuación se presenta una pequeña guía de creación de equipos.

5.5.3 CREACIÓN DE EQUIPOS PARA NAGIOS

Para la creación de equipos seguir los pasos que se indican a continuación:

1. Se debe crear un archivo con extensión .cfg en el directorio */etc/nagios3/conf.d/*

Ejemplo: A continuación se presenta un ejemplo del archivo a crear

```
sudo nano /etc/nagios3/conf.d/equipos.cfg
```

2. Se copia la siguiente plantilla al archivo creado:

```
define host {
use  generic-host
host_name “NOMBRE”
alias     “NOMBRE”
addresss 1.1.1.1
```

3. Se modifican los campos *host_name*, *alias*, *address* como se requiera.
4. Para guardar los cambios se debe presionar en el teclado **CRTL+O** y dar *Enter* para confirmar la grabación del archivo.

Ejemplo:

```
# ARCHIVO PARA WAN DE INTERNET

define host{
        use             generic-host          ; Inherit default values from a template
        host_name       WAN INTERNET - PRESIDENCIA DE LA REPUBLICA ; The name we're giving to this switch
        alias           WAN INTERNET - PRESIDENCIA DE LA REPUBLICA ; A longer name associated with the switch
        address         201.219.63.130
        icon_image      cisco-logo.gif          ; IP address of the switch
        }

define host{
        use             generic-host          ; Inherit default values from a template
        host_name       WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES ; The name we're giving to this switch
        alias           WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES ; A longer name associated with the switch
        address         201.219.62.90
        icon_image      cisco-logo.gif          ; IP address of the switch
        }

define host{
        use             generic-host          ; Inherit default values from a template
        host_name       WAN INTERNET - MINISTERIO DE AGRICULTURA  ; The name we're giving to this switch
        alias           WAN INTERNET - MINISTERIO DE AGRICULTURA  ; A longer name associated with the switch
        address         201.219.63.226
        icon_image      cisco-logo.gif          ; IP address of the switch
        }

define host{
        use             generic-host          ; Inherit default values from a template
        host_name       WAN INTERNET - MINISTERIO DE INCLUSION ECON. Y SOCIAL  ; The name we're giving to this switch
        alias           WAN INTERNET - MINISTERIO DE INCLUSION ECON. Y SOCIAL  ; A longer name associated with the switch
        address         190.152.88.234
        icon_image      cisco-logo.gif          ; IP address of the switch
        }
```

Figura 5.5.1: Creación de equipos [1]

5.5.4 CREACIÓN DE SERVICIOS PARA NAGIOS

Para crear un servicio se debe tener al menos un equipo registrado que pueda ser señalado en algún archivo de configuración, cuando ya se cuenta con el o los equipos se debe seguir el siguiente proceso:

1. Crear un archivo con extensión *.cfg* en el directorio */etc/nagios3/conf.d/*

sudo nano /etc/nagios3/conf.d/servicios.cfg

2. Copiar la siguiente plantilla al archivo creado

```
define service {
    use  generic-service
    host_name “NOMBRE HOST”
    service_description     “NOMBRE SERVICIO”
    check_command  check_(servicio)! (parámetros)
```

Ejemplo: A continuación se presenta un ejemplo del archivo a crear

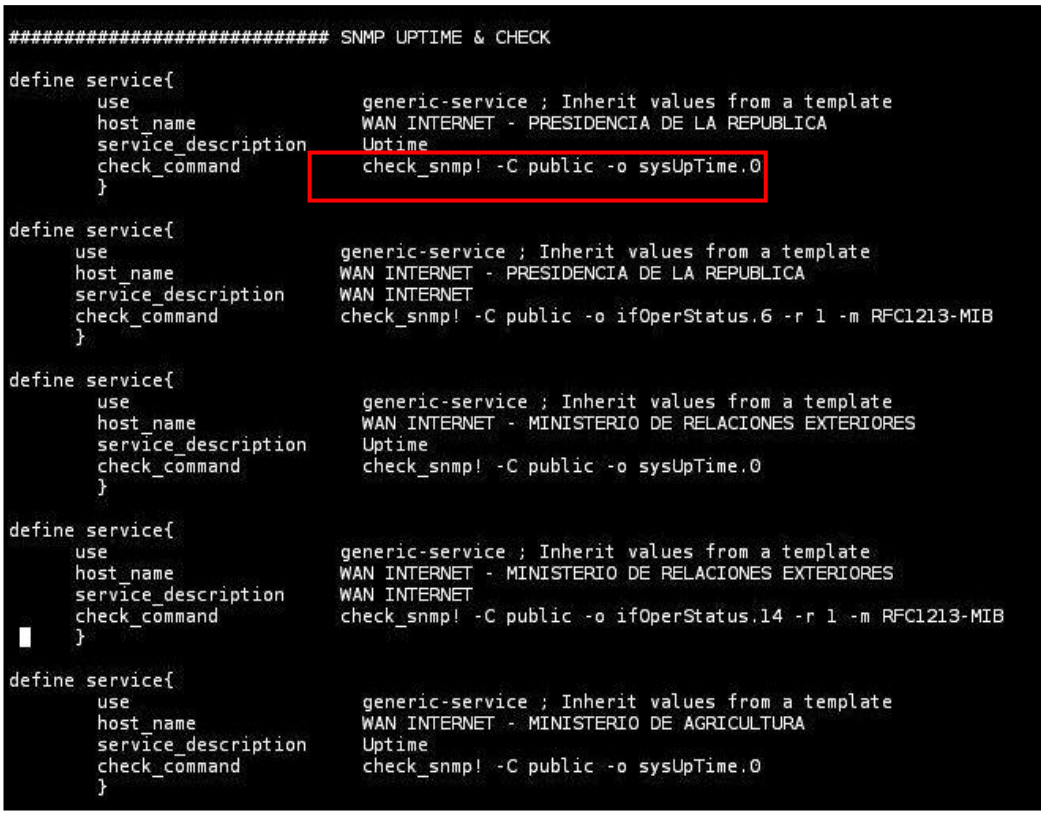


Figura 5.5.2: Creación se servicios [1]

Es recomendable que se revise la documentación o ejemplos de las definiciones de los *check_command* ya que dependiendo de los servicios los parámetros pueden cambiar o la misma definición de llamada del servicio. Esta documentación se puede encontrar en Internet o buscando los archivos *check_*, para esto se puede buscar con el comando *locate check_** en un Terminal.

Los tipos de servicios pueden ser SNMP[51], PING[52], FTP[53] entre otros dependiendo de las necesidades de monitoreo.

No se incluyen estas definiciones por que se refieren como a 35 diferentes tipos de checks.

1. Cambiar los parámetros *host_name*, *service_description* y *check_command* acorde a las necesidades.

[51] Véase Acrónimos
[52] Véase Acrónimos
[53] Véase Acrónimos

2. Para guardar los cambios se debe presionar en el teclado **CRTL+O** y dar *Enter* para confirmar la grabación del archivo.

5.5.5 CREACIÓN DE ALERTAS POR EMAIL DE NAGIOS

Para que las alertas se puedan enviar de forma adecuada, se deben configurar algunos paquetes extras.

1. Instalar un paquete denominado *postfix*¸ que es una herramienta de gestión de correo muy reducida.
2. Para instalar el paquete se debe digitar el siguiente comando:

```
sudo aptitude install –y postfix
```

3. Una vez que este paquete se haya instalado, se debe configurar/crear un archivo denominado *main.cf* que debe encontrase en el directorio */etc/postfix/main.cf/*
4. Añadir las siguientes definiciones al *main.cf:*

```
biff=no
append_dot_mydomain=no
myhostname= NOMBRE-SERVIDOR-DNS
alias_maps= hash:/etc/aliases
alias_database= hash:/etc/aliases
mydestination= DOMINIO1, DOMINIO2, DOMINION, localhost
relayhost= IP-SERV-SMTP:PUERTO
```

Todos los valores en color azul deben ser cambiados según se requiera.

5. Para guardar los cambios se debe presionar en el teclado **CRTL+O** y dar *Enter* para confirmar la grabación del archivo

6. Abrir el archivo *commands.cfg* en la carpeta */etc/nagios3/* y verificar que existan las definiciones ***'notify-host-by-email'*** y ***'notify-service-by-email'***. Por defecto suelen estar habilitadas.

7. Finalmente en la carpeta */etc/nagios3/conf.d/* se encuentra el archivo *contact-nagios2.cfg*, en donde se debe abrir y modificar la dirección de correo electrónico del root por una cuenta de correo real.

5.5.6 INSTALACIÓN DE HERRAMIENTAS DE NAGIOS - NDOUTILS

La herramienta *ndoutils* es un complemento desarrollado para que la información manejada de Nagios, pueda ser guardada en una base de datos *mysql*, esta herramienta debe ser instalada luego de que Nagios haya sido instalado completamente.

1. Para instalar este complemento se debe digitar el siguiente comando:

sudo aptitude install –y ndoutils

2. Junto a estos cambios se deben digitar los siguientes comandos

sudo nano /etc/nagios3/nagios.cfg

Es un *plugin* que permite que los datos de Nagios se correlacionen en una base de datos.

5.5.7 CONFIGURACIÓN DE DISPOSITIVOS

```
# ARCHIVO PARA WAN DE INTERNET

define host{
        use             generic-host          ; Inherit default values from a template
        host_name       WAN INTERNET - PRESIDENCIA DE LA REPUBLICA ; The name we're giving to this switch
        alias           WAN INTERNET - PRESIDENCIA DE LA REPUBLICA ; A longer name associated with the switch
        address         201.219.63.130
        icon_image      cisco-logo.gif          ; IP address of the switch
        }

define host{
        use             generic-host          ; Inherit default values from a template
        host_name       WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES ; The name we're giving to this switch
        alias           WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES ; A longer name associated with the switch
        address         201.219.62.90
        icon_image      cisco-logo.gif          ; IP address of the switch
        }

define host{
        use             generic-host          ; Inherit default values from a template
        host_name       WAN INTERNET - MINISTERIO DE AGRICULTURA  ; The name we're giving to this switch
        alias           WAN INTERNET - MINISTERIO DE AGRICULTURA  ; A longer name associated with the switch
        address         201.219.63.226
        icon_image      cisco-logo.gif          ; IP address of the switch
        }

define host{
        use             generic-host          ; Inherit default values from a template
        host_name       WAN INTERNET - MINISTERIO DE INCLUSION ECON. Y SOCIAL  ; The name we're giving to this switch
        alias           WAN INTERNET - MINISTERIO DE INCLUSION ECON. Y SOCIAL  ; A longer name associated with the switch
        address         190.152.88.234
        icon_image      cisco-logo.gif          ; IP address of the switch
        }
```

Figura 5.5.3: Configuración de dispositivos [1]

5.5.8 CONFIGURACIÓN DE SERVICIOS

```
############################## SNMP UPTIME & CHECK

define service{
        use                     generic-service ; Inherit values from a template
        host_name               WAN INTERNET - PRESIDENCIA DE LA REPUBLICA
        service_description     Uptime
        check_command           check_snmp! -C public -o sysUpTime.0
        }

define service{
        use                     generic-service ; Inherit values from a template
        host_name               WAN INTERNET - PRESIDENCIA DE LA REPUBLICA
        service_description     WAN INTERNET
        check_command           check_snmp! -C public -o ifOperStatus.6 -r 1 -m RFC1213-MIB
        }

define service{
        use                     generic-service ; Inherit values from a template
        host_name               WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES
        service_description     Uptime
        check_command           check_snmp! -C public -o sysUpTime.0
        }

define service{
        use                     generic-service ; Inherit values from a template
        host_name               WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES
        service_description     WAN INTERNET
        check_command           check_snmp! -C public -o ifOperStatus.14 -r 1 -m RFC1213-MIB
        }

define service{
        use                     generic-service ; Inherit values from a template
        host_name               WAN INTERNET - MINISTERIO DE AGRICULTURA
        service_description     Uptime
        check_command           check_snmp! -C public -o sysUpTime.0
        }
```

Figura 5.5.4: Configuración de servicios [1]

5.6 MANUAL ACS (ACCESS CONTROL SERVER)

5.6.1 OBJETIVOS

- Conocer las herramientas de la plataforma ACS para mejorar le seguridad en cuanto al control de acceso de la administración de los equipos de la red IP/MPLS.
- Investigar cómo se realiza la asignación de privilegios a determinados usuarios.

5.6.2 INTRODUCCIÓN

La plataforma ACS[54] es utilizada para proporcionar una aplicación centralizada de accesos, privilegios y políticas. Proporciona autenticación y autorización de punto de control entre dispositivos de red que utilizan TACACS + RADIUS, y un grupo de bases de datos que residen en los servidores.

5.6.3 INGRESO A LA PLATAFORMA

Para poder ingresar a esta plataforma de autentificación y seguridad seguir los pasos que se muestran a continuación:

1. Colocar la dirección IP del servidor correspondiente en el browser.
2. A continuación aparecerá la pantalla de inicio de la plataforma.
3. Colocar el nombre de usuario y la contraseña respectivamente como se muestra en la figura 5.6.1:

[54] **ACS (ACCESS CONTROL SERVER):** Permite controlar el acceso del usuario a la red, autorizar los diferentes tipos de servicios de red para los usuarios o grupos de usuarios, y llevar un registro de todas las acciones de la red del usuario.

Figura 5.6.1: Pantalla de ingreso a la plataforma [1]

5.6.4 PANTALLA PRINCIPAL

En esta pantalla se encuentran todas las herramientas para la administración del ACS.

En el Panel de Navegación se encuentran diversas opciones usadas para la configuración de usuarios, grupo de usuarios, perfiles, dispositivos, protocolos, bases de datos externos y logs como se muestra en la figura 5.6.2:

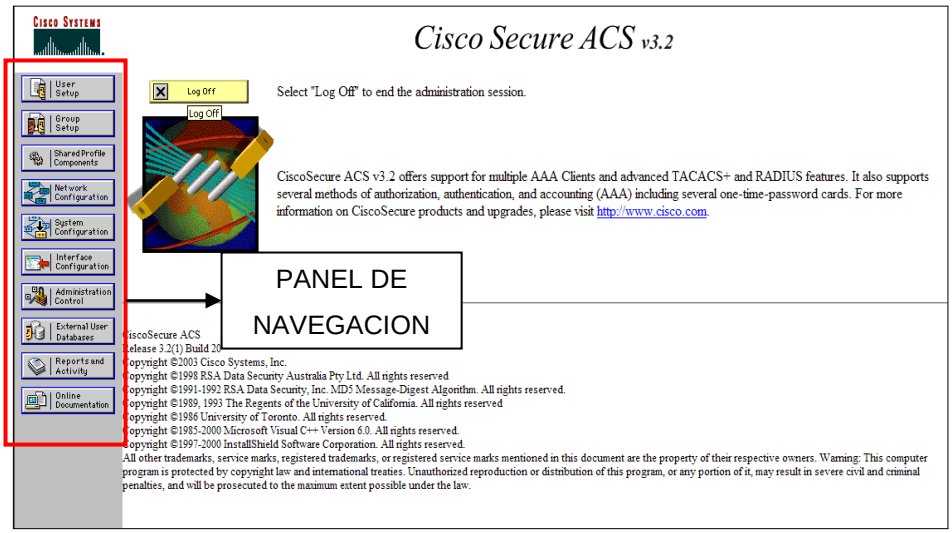


Figura 5.6.2: Pantalla principal [1]

Para la correcta administración de los ACS's se debe seguir la siguiente secuencia de configuración:

1. Perfiles de autorización
2. Dispositivos de red
3. Grupos de usuarios
4. Usuarios dentro de un grupo

A continuación se mostrará las opciones más utilizadas para la asignación de privilegios a los administradores así como también el establecimiento de seguridades:

5.6.5 TAB USER SETUP

Esta opción permite configurar la información de cada usuario, añadir uno nuevo o eliminarlo de la base de datos como se muestra en la figura 5.6.3:

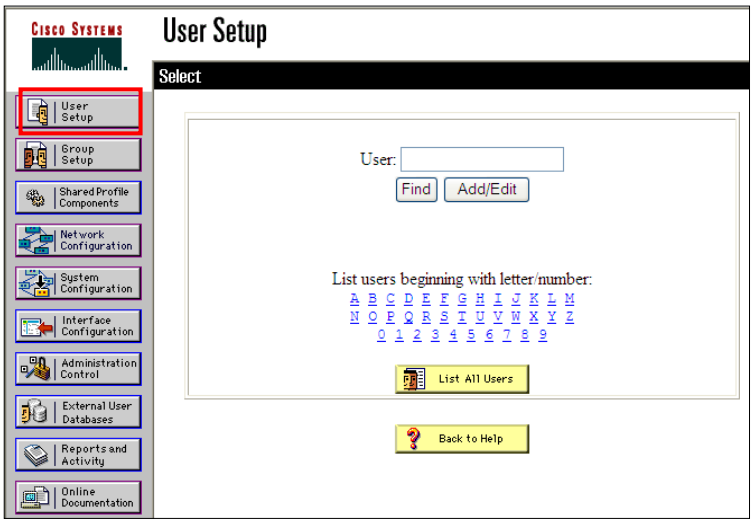


Figura 5.6.3: Tab user setup [1]

5.6.5.1 CONFIGURACIÓN DE USUARIOS EN UNA BASE DE DATOS EXTERNA

El servidor ACS puede autenticar a los usuarios en una base de datos externa para ello se debe tomar en cuenta que se debe realizar las configuraciones previas en dicha base de datos.

Es importante mencionar que en el tab *User Setup* no se puede añadir o eliminar nombres de usuario de la base de datos externa.

5.6.5.2 ENCONTRAR UN USUARIO ESPECÍFICO EN LA BASE DE DATOS

Para buscar un usuario que ya se encuentra en la base de datos realizar los siguientes pasos:

1. Colocar la primera letra del nombre en el campo de usuario.
2. A continuación agregar un asterisco (*) como comodín para realizar la búsqueda correspondiente.
3. Finalmente dar un clic en Buscar.
4. Posteriormente aparecerá la lista de nombres de usuario en la parte derecha de la pantalla, haga clic en el nombre de usuario cuya información desea ver o cambiar como se muestra en la figura 5.6.4:

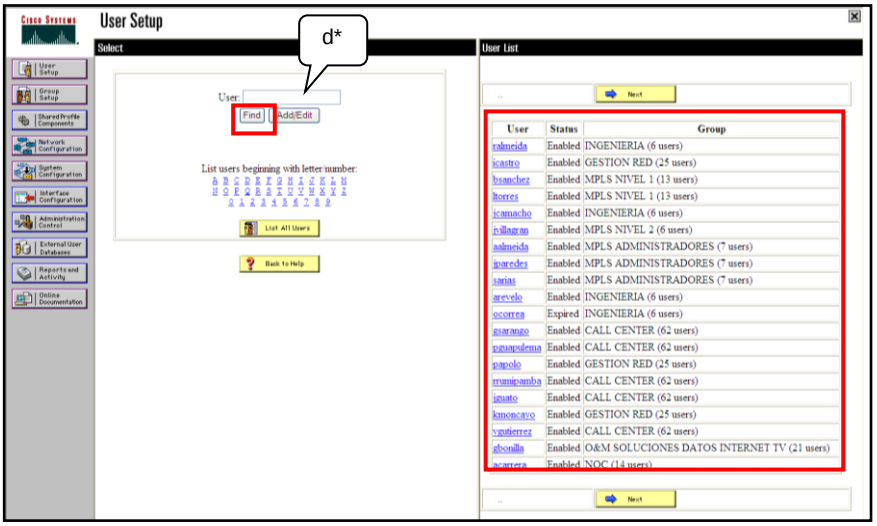


Figura 5.6.4: Ubicación de usuarios en la base de datos [1]

5.6.5.3 LISTADO DE NOMBRES QUE EMPIEZAN CON UN CARACTER PARTICULAR

Para mostrar una lista de los nombres de usuario que comienzan con una letra o un número específico realizar los siguientes pasos:

1. Dar clic en la letra que se encuentra en la lista alfanumérica, o escriba el caracter en el campo de usuario seguido de un asterisco (*).
2. Dar clic en *Find*, posteriormente aparecerá una lista de usuarios en la parte derecha de la pantalla con los nombres que comienzan con la letra o número escogido anteriormente.
3. A continuación haga clic en el nombre del usuario cuya información desea ver o cambiar como se muestra en la figura 5.6.5:

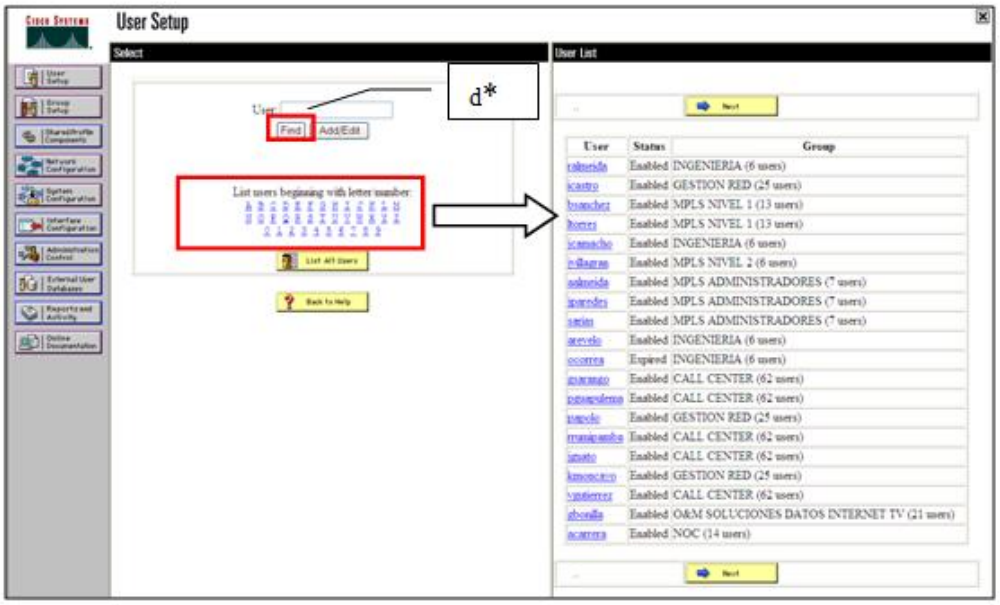


Figura 5.6.5: Listado de los nombres de usuario que empiezan con un carácter en particular. [1]

5.6.5.4 CAMBIO DE UN NOMBRE DE USUARIO EN LA BASE DE DATOS

Los nombres de usuario no pueden ser cambiados o modificados en la base de datos es preferible eliminar el nombre de usuario y agregar uno nuevo.

5.6.5.5 CONFIGURACIÓN DE UN USUARIO

Para realizar la configuración de un usuario específico es necesario en primer lugar seleccionar el nombre de usuario que se desea configurar en la lista correspondiente

y posteriormente aparecerá una ventana en donde se deberá colocar los parámetros necesarios como se muestra en la figura 5.6.6:

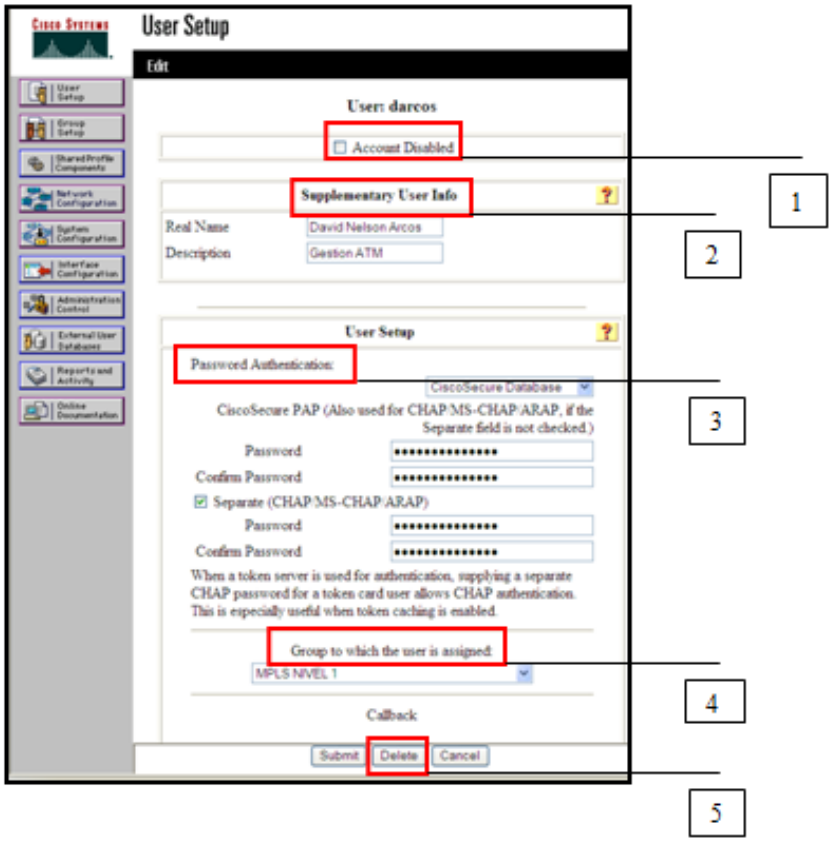


Figura 5.6.6: Configuración de un usuario [1]

1. **ACCOUNT DISABLED STATUS**

Coloque un visto en esta casilla para deshabilitar esta cuenta o desactive la casilla para activar la cuenta nuevamente.

2. **SUPPLEMENTARY USER INFO**

Escribir la información correspondiente en los cuadros que aparecen en esta opción. Para agregar o cambiar los campos, haga clic en la opción *Interface Configuration*, y luego dar clic en la opción *User Data Configuration*. Se puede realizar la configuración de hasta cinco campos.

3. **PASSWORD AUTHENTICATION**

Colocar una contraseña de autenticación de acuerdo a una base de datos para proceder a su validación y colocar las confirmaciones de dichas contraseñas como se indica en la figura 5.6.6.

4. **GRUPO AL CUAL EL USUARIO ES ASIGNADO (GROUP TO WHICH THE USER IS ASSIGNED)**

En la lista, seleccione el grupo al que pertenece el usuario para definir el tipo de servicios que le estarán permitidos usar. Para configurar la información del grupo, haga clic en la opción *Group Setup*.

5. **ELIMINACIÓN DE UN USUARIO**

El botón *Delete* sólo aparece cuando se está editando una cuenta de usuario, o cuando se va a agregar uno nuevo.

Para eliminar la cuenta de usuario actual de la base de datos haga clic en la opción *Delete,* cuando se le pregunte que confirme la acción dar clic en Aceptar como se muestra en la figura 5.6.6.

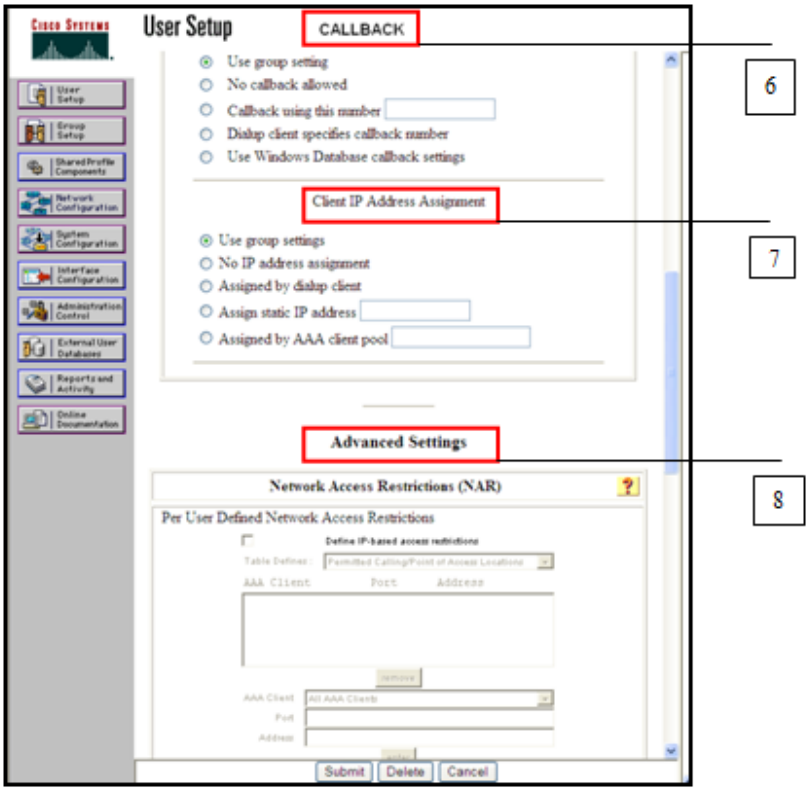


Figura 5.6.7: Eliminación de un usuario [1]

6. **CALLBACK**

Es una cadena de comandos que son pasados al servidor de acceso. Se puede utilizar una cadena de callbacks para inicializar un módem y realizar llamadas al usuario mediante un número específico. Esta opción se encuentra conformada por varios campos para lo cual se recomienda colocar los parámetros apropiados de acuerdo a los privilegios que se les vaya a dar a cada uno de los usuarios.

7. **CLIENT IP ADDRESS ASSIGNMENT**

Ubicar la dirección IP que ha sido asignada para el usuario, esta opción se encuentra conformada por varios campos para lo cual se recomienda colocar los parámetros apropiados de acuerdo a los privilegios que se les vaya a dar a cada uno de los usuarios.

8. **ADVANCED SETTINGS**

Permite realizar configuraciones avanzadas tales como permitir o denegar el acceso a un usuario utilizando un filtro de acceso etc., estas opciones deben ser marcadas de acuerdo a los requerimientos de cada uno de los usuarios como se muestra en la figura 5.6.7

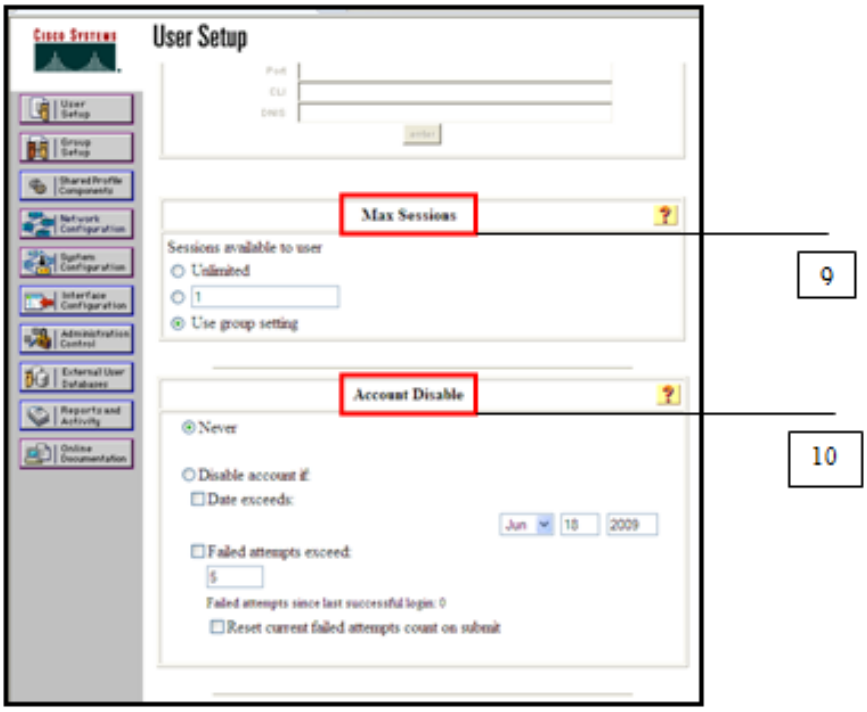


Figura 5.6.8: Opción Advanced Settings [1]

9. **MAX SESSIONS**

Establece el número máximo de conexiones simultáneas para este usuario. Existen tres opciones para establecer las sesiones de usuario tales como:

- ✓ **Unlimited:** Seleccionar esta opción para permitir que un usuario tenga un número ilimitado de sesiones simultáneas.
- ✓ **n:** Escriba el número máximo de sesiones simultáneas permitidas para este usuario.
- ✓ **Use group setting:** Seleccionar esta opción si se desea utilizar el valor máximo de sesiones para el grupo.

10. **ACCOUNT DISABLE**

Define las circunstancias en que esta cuenta de usuario se desactivará. Se encuentra conformado por varias opciones las cuales deben ser seleccionadas de acuerdo a los requerimientos como se muestra en la figura 5.6.8.

- ✓ **Disable account if:** Seleccionar esta opción para deshabilitar la cuenta.
- ✓ **Date exceeds:** Para desactivar una cuenta después de una fecha determinada, seleccione la casilla de verificación y especifique la fecha.
- ✓ **Failed attempts exceed:** Permite desactivar una cuenta después de un cierto número de intentos fallidos de conexión, para ello seleccione la casilla de verificación y escriba el número de intentos fallidos que deshabilitarán la cuenta.
- ✓ **Failed attempts since last successful login:** Este contador muestra el número de intentos fallidos de ingreso desde la última vez que el usuario fue registrado con éxito.
- ✓ **Reset current failed attempts count on submit:** Si una cuenta está deshabilitada porque el número de intentos fallidos se ha superado, seleccione la casilla de verificación y seleccione ***Submit*** para reiniciar el contador de intentos fallidos para este usuario y así restablecer la cuenta.

5.6.6 TAB GROUP SETUP

La configuración de grupo se utiliza para activar y configurar las autorizaciones específicas asignadas a todo un grupo de usuarios. El grupo se le asigna a un usuario y este se configura en la sección *User Setup.*

5.6.6.1 CREACIÓN DE UN GRUPO DE USUARIO

Para la creación de un grupo de usuarios seguir los pasos que se muestras a continuación:

1. Seleccionar del panel de navegación la opción Group Setup.
2. Seleccionar un número libre en la barra desplegable como se muestra en la figura 5.6.9:

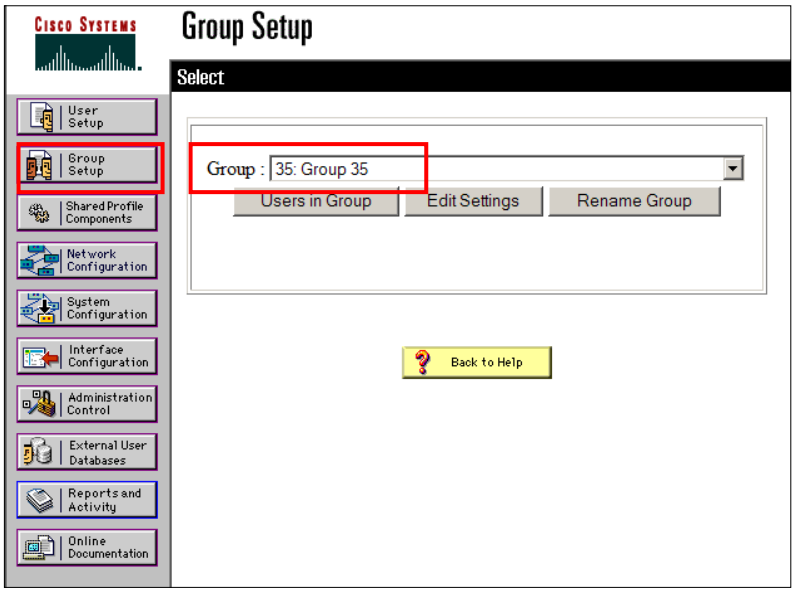


Figura 5.6.9: Creación de un grupo de usuario [1]

3. Dar clic en *User in Group* para observar la lista de todos los usuarios asignados al grupo seleccionado como se muestra en la figura 5.6.10:

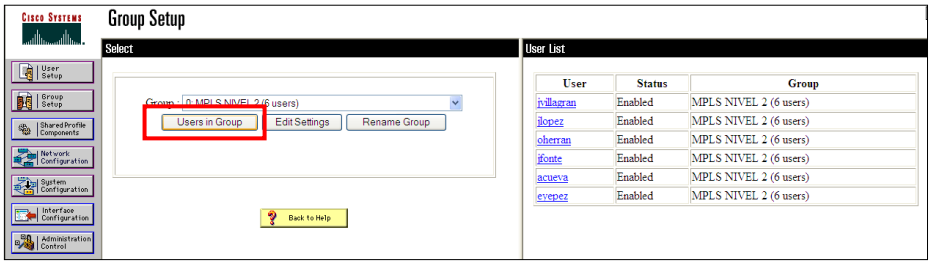


Figura 5.6.10: Opción User in Group [1]

4. Dar clic en *Edit Settings* para modificar los privilegios de autorización del grupo seleccionado como se muestra en la figura 5.6.11:

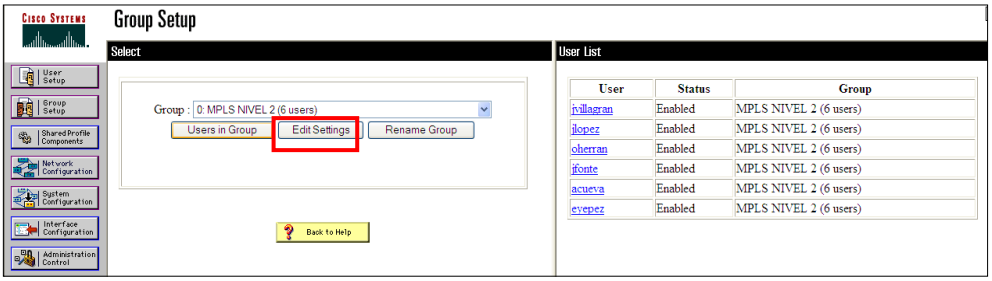


Figura 5.6.11: Opción Edit Settings [1]

5.6.6.2 RENOMBRAR UN GRUPO

Elegir la opción *Renaming Group* para escribir un nuevo nombre de grupo y haga clic en Submit para asignar un nombre más descriptivo para el perfil de grupo. Haga clic en Cancelar para volver a la ventana de configuración de grupo sin guardar un nombre de grupo como se muestra en la figura 5.6.12:

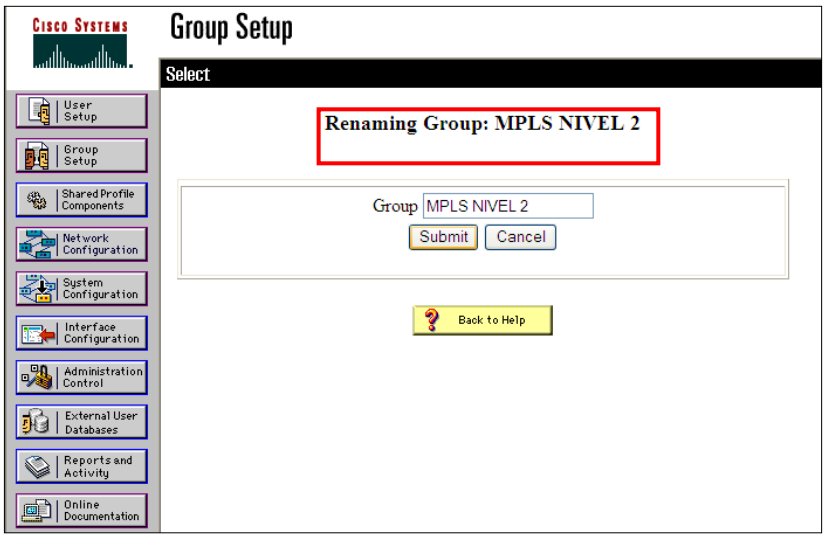


Figura 5.6.12: Renombrar un grupo [1]

5.6.7 TAB SHARE PROFILE COMPONENTS

Esta opción permite realizar configuraciones para añadir a los grupos creados, para ello realizar los siguientes pasos:

1. Seleccionar la opción *Shell Command Authorization Sets* que permite utilizar múltiples tipos de comandos de autorización como se muestra en la figura 5.6.13:

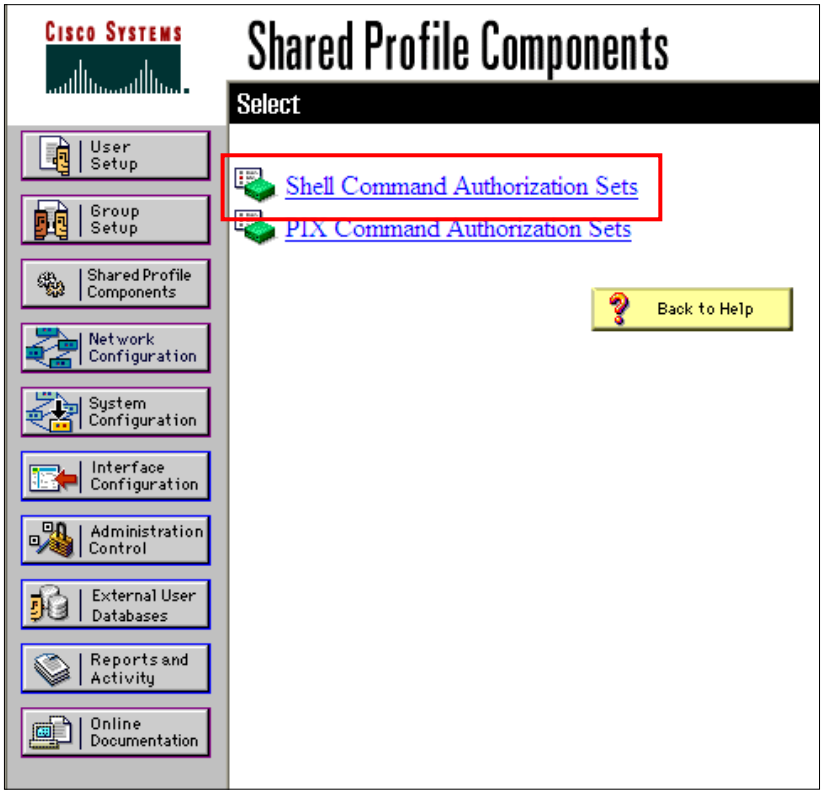


Figura 5.6.13: Opción Shell Command Authorization [1]

2. Posteriormente aparecerá el siguiente recuadro que muestra todos los grupos que se encuentran previamente configurados con sus respectivas descripciones como se muestra en la figura 5.6.14:

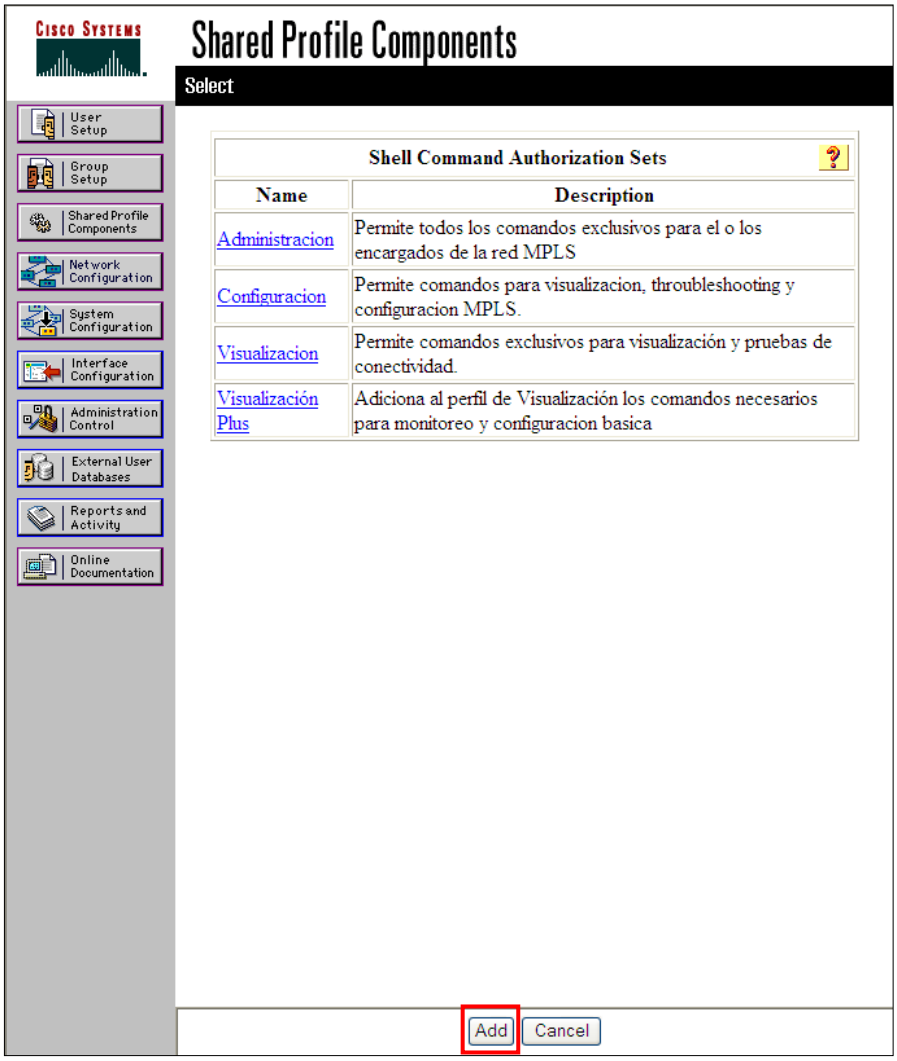


Figura 5.6.14: Grupos configurados previamente [1]

5.6.7.1 CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Es un conjunto de configuraciones de reglas de autorización emitidas durante el uso de una aplicación de administración de dispositivos.

5.6.7.2 AÑADIR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Para agregar un conjunto de comandos de autorización dar haga clic en la opción *Add* y seguidamente aparecerá una ventana en donde se permiten o se deniegan dichos comandos.

5.6.7.3 EDITAR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Para editar un conjunto de comandos de autorización existente realizar los siguientes pasos:

1. En la columna *Name* dar haga clic en el nombre del grupo que se desee configurar.
2. En la página que aparece, se puede agregar o quitar los comandos de acuerdo a los requerimientos de cada uno de los usuarios como se muestra en la figura 5.6.15:

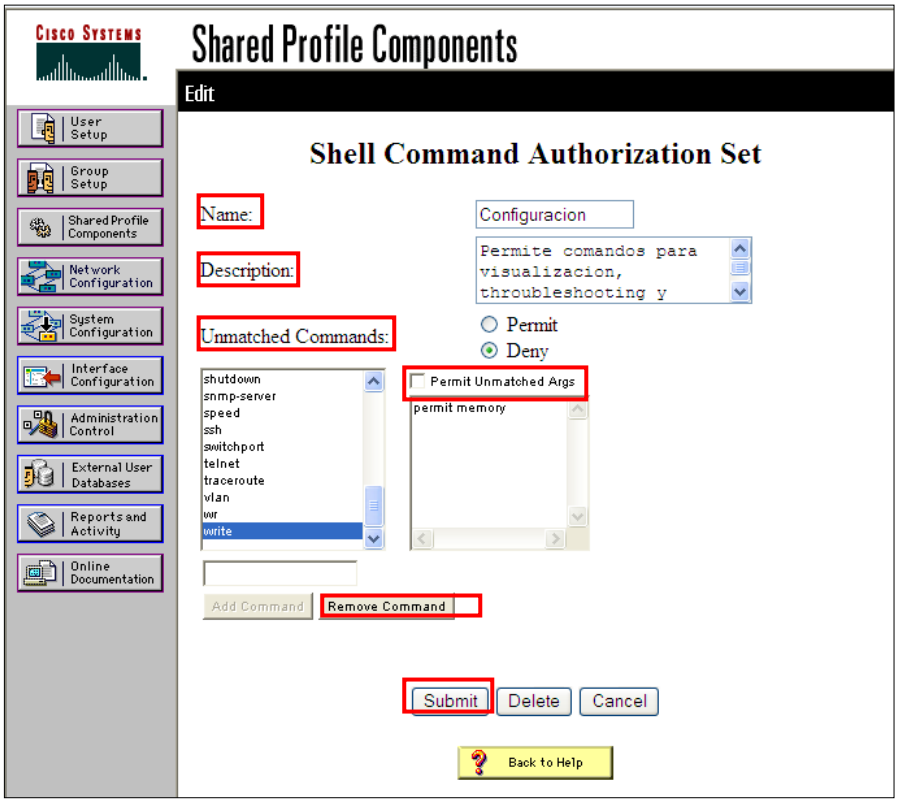


Figura 5.6.15: Edición de un conjunto de comandos de autorización [1]

5.6.7.4 AÑADIR Y EDITAR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Para agregar o editar un comando de autorización, completar las siguientes pasos y posteriormente dar clic en *Submit*.

1. **Name:** Escribir el nombre del conjunto de comandos de autorización.
2. **Description:** Colocar una descripción del conjunto de comandos de autorización.
3. **Unmatched Commands:** Niega o permite comandos de autorización en este caso se da de la siguiente manera:
   - ✓ Seleccionar la opción Permit cuando se desee denegar el uso de un comando.
   - ✓ Seleccionar la opción Deny cuando se desee permitir el uso de un comando.
4. **Permit Unmatched Args:** Permite o deniega argumentos que no están seleccionados en la lista de argumentos.
5. **Add Command:** Permite añadir nuevos comandos en la lista.
6. **Remove Command:** En la lista de comandos, seleccione el comando que se desee eliminar y finalmente dar clic en la opción *Remove Command.*

5.6.7.5 ELIMINAR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Para eliminar un conjunto de comandos de autorización realizar los siguientes pasos:

1. En la columna Name dar clic en el nombre del grupo que se desee eliminar.
2. Posteriormente en la ventana que aparece se procede a eliminar los comandos de acuerdo a las necesidades del usuario.
3. Finalmente confirmar la eliminación del comando dando clic en OK.

5.6.8 TAB NETWORK CONFIGURATION

Esta opción permite realizar configuraciones a los grupos de dispositivos que se encuentran en la red.

5.6.8.1 CONFIGURACIÓN DE DISPOSITIVOS

Para configurar un dispositivo seguir los pasos que se indican a continuación:

1. Seleccionar del panel de navegación la opción *Network Configuration.*
2. Antes de iniciar la configuración cabe destacar que los equipos se encuentran divididos en MPLS e INTERNET los mismos que se encuentran en la lista de *Network Device Group.*

   En MPLS se encuentran los equipos, IP (Core), PE [55](Border), L2(Acceso)

   En INTERNET se encuentran Core, Borde, Acceso, Route Reflector, BRAS (autentificación).También se encuentran configurados los equipos de gestión ISC, ANA, CACTI, NAGIOS, etc.
3. Para agregar un nuevo grupo seleccionar la opción *Add/Entry* como se muestra en la figura 5.6.16:

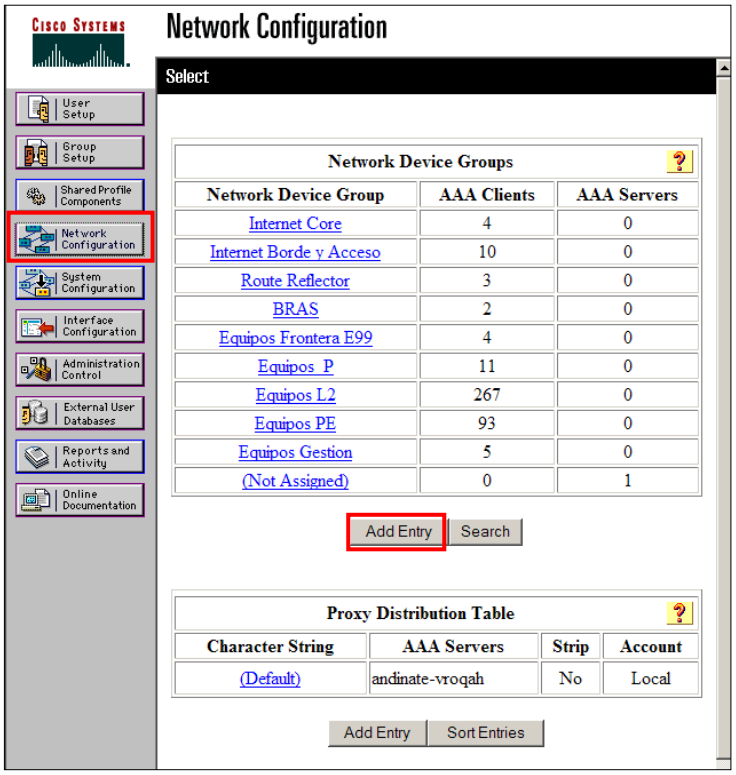


Figura 5.6.16: Configuración de dispositivos [1]

[55] Véase Acrónimos

4. Colocar el nombre del grupo y dar clic en *Submit* como se muestra en la figura 5.6.17:

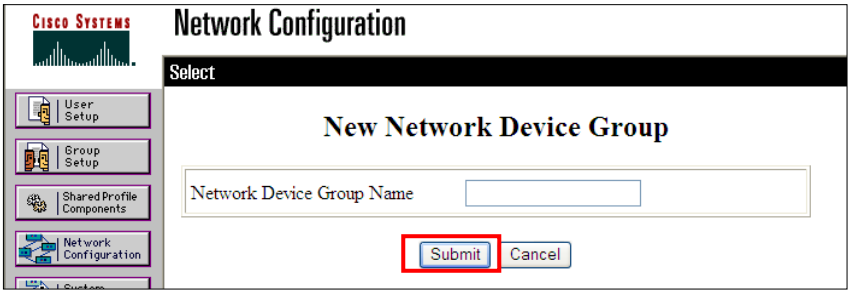


Figura 5.6.17: Opción Submit [1]

5. Una vez creado el grupo se procede a configurar cada uno de los equipos que van a estar dentro de dicho grupo, para ello elegir la opción *Add Entry* como se muestra en la figura 5.6.18:

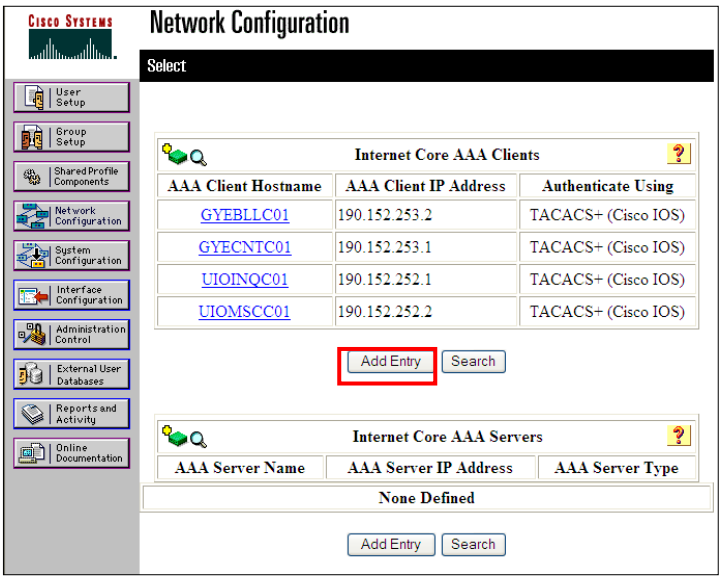


Figura 5.6.18: Opción Add Entry [1]

6. A continuación aparecerá una ventana en la cual se debe colocar los parámetros correspondientes al equipo como se muestra en la figura 5.6.19:

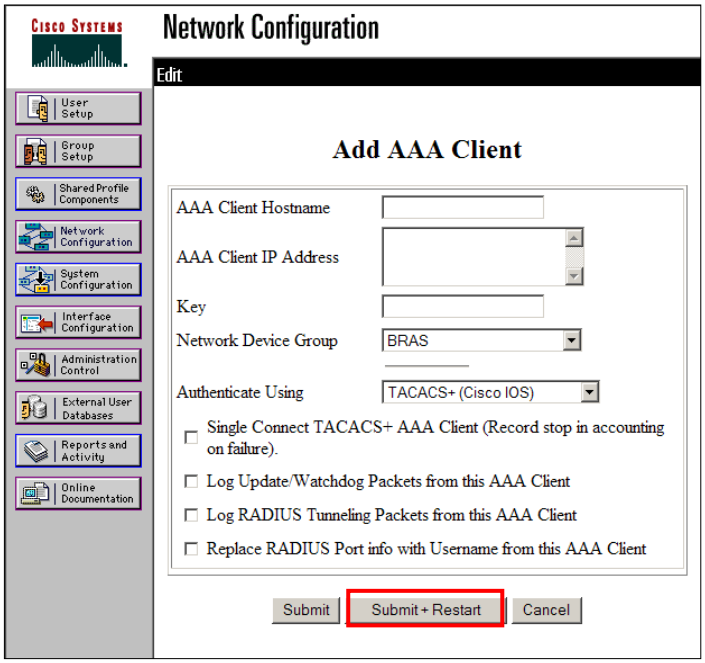


Figura 5.6.19: Configuración de los parámetros del equipo [1]

7. Colocar el nombre del equipo
8. Colocar la dirección IP
9. Clave de autenticación con el ACS
10. En la lista, haga clic en el nombre del grupo de dispositivos de red a la que pertenece el cliente AAA.
11. Colocar el protocolo para la autenticación, en el caso de dispositivos Cisco elegir el protocolo TACACS-CISCO IOS y en el caso de dispositivos Huawei elegir el protocolo RADIUS
12. Para que los cambios efectuados se guarden correctamente elegir la opción *Submit+Restart*.

5.6.9 TAB SYSTEM CONFIGURATION

Este tab se encuentra conformado por un conjunto de opciones como se muestra en la figura 5.6.20, los mismos que permiten la correcta configuración del sistema.

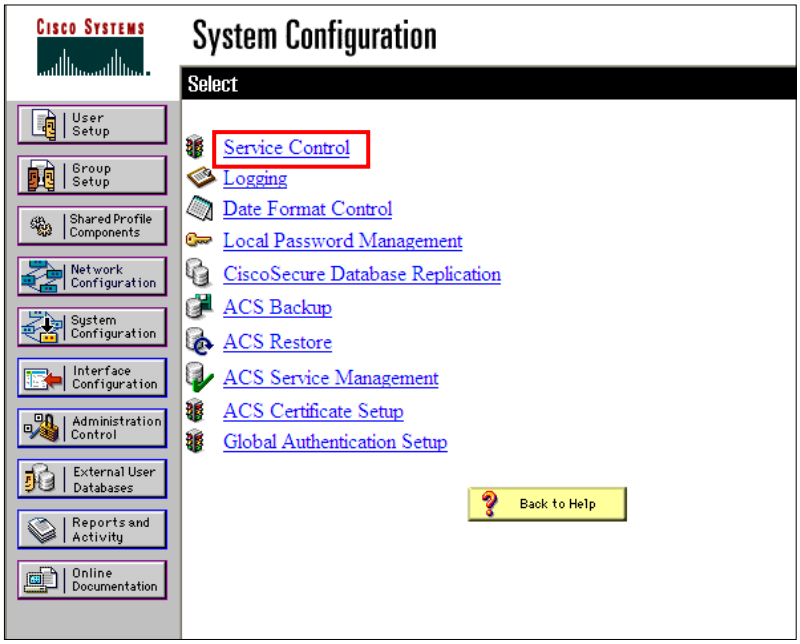


Figura 5.6.20: Tab System Configuration [1]

La única opción usada en este tab es *Service Control* ya que las demás opciones no se encuentran implementadas.

5.6.9.1 Service Control

Seleccionar esta opción para realizar configuraciones para el control de servicios como se muestra en la figura 5.6.21:

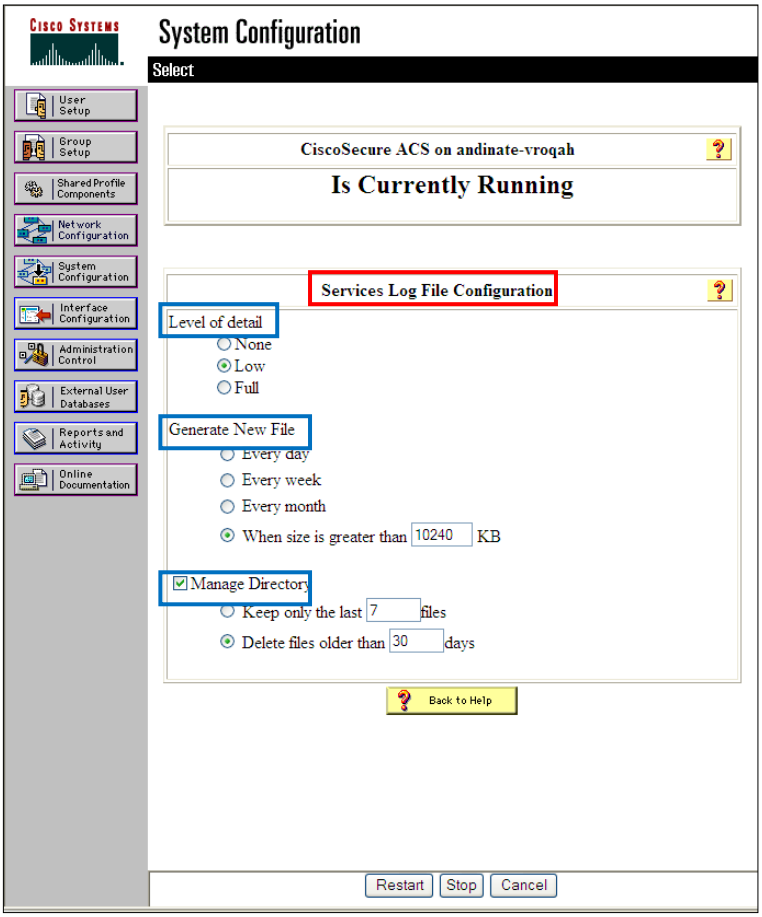


Figura 5.6.21: Opción Service Control [1]

5.6.9.1.1 Services Log File Configuration

Las opciones de esta sección de control establecen los parámetros de registro del servicio y el directorio.

- **Level of detail:** Dar clic en una de las opciones siguientes para determinar el nivel de detalle que aparecerá en el archivo de registro.
  - ✓ **None:** Cuando no hay archivo de registro generado.
  - ✓ **Low:** Inicia y detiene las acciones en el sistema.
  - ✓ **Full:** Todas las acciones de los servicios se registran.
- **Generate New File:** Si ha seleccionado la opción Low o Full para el nivel de detalle proceder a dar clic en una de las opciones que se muestran en la ventana para configurar el nuevo archivo de registro. Para este caso

seleccionar la opción *When size is greater than X KB* que tiene un valor por defecto de 2048 KB.

- **Manage Directory:** Para configurar los parámetros del directorio de los archivos de registro, seleccione la casilla *Manage Directory* y chequee las siguientes opciones:
  - ✓ **Keep only the last *X* files:** El valor predeterminado es 7 ficheros.
  - ✓ **Delete files older than *X* days:** El valor predeterminado es 7 días.

5.6.10 TAB INTERFACE CONFIGURATION

Esta opción permite configurar las opciones de protocolos de Autenticación, en este caso se usa TACACS+ (Cisco IOS) para equipos cisco y Radius(Alcatel) para equipos Alcatel como se muestra en la figura 5.6.22:

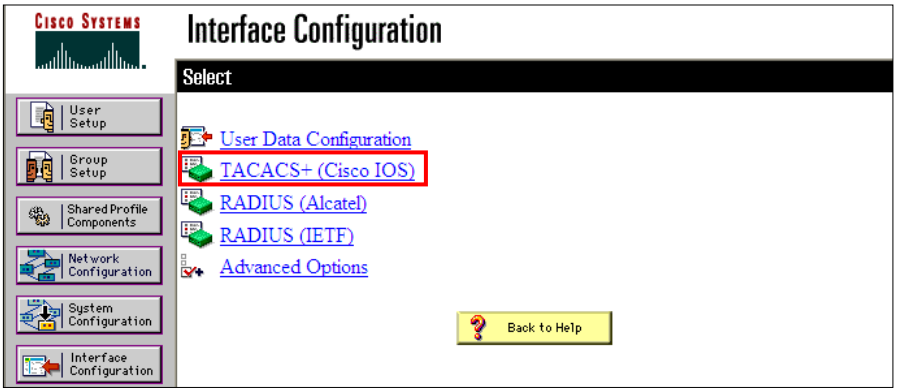


Figura 5.6.22: Tab Interface Configuration [1]

5.6.10.1 CONFIGURACION DEL PROTOCOLO TACAS+ (CiscoIOS)

Para su configuración seguir los pasos que se muestran a continuación:

1. Seleccionar la opción TACACS+ (Cisco IOS)
2. Seleccione la casilla de verificación, ya sea para usuarios y / o de grupo para cada TACACS + Services que desea que aparezca como una opción

configurable en la configuración del usuario y / o en la ventana de configuración de grupo, en consecuencia.

3. Cuando haya terminado de seleccionar las opciones, haga clic en *Submit*, en este caso se considera el servicio *Shell.*

4. En *Advanced Configuration Options* elegir la opción que permite visualizar una ventana por cada servicio seleccionado en el momento que ingresan a TACAS+Attributes.

5. Dar clic en *Submit* para guardar los cambios efectuados como se muestra en la figura 5.6.23:

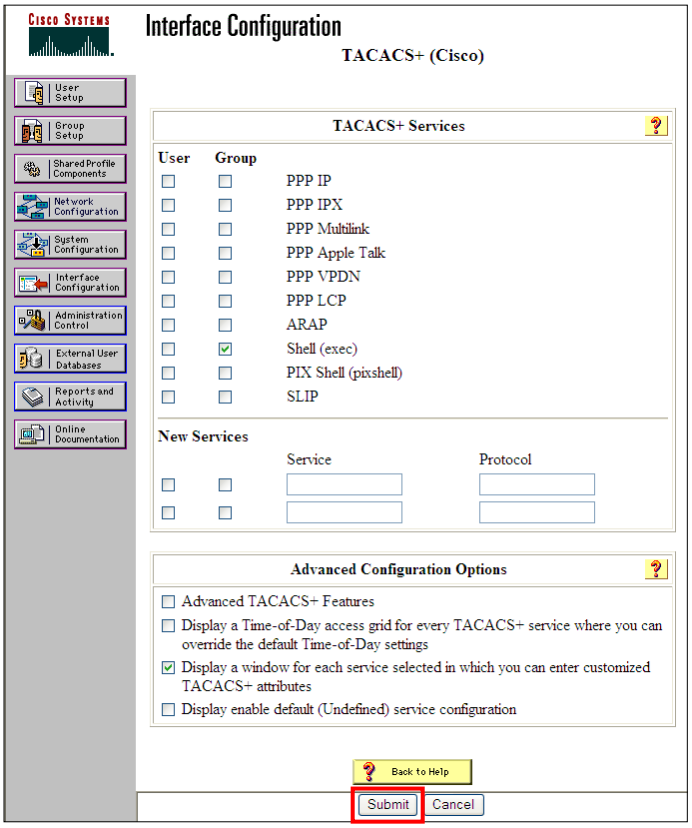


Figura 5.6.23: Configuración del protocolo tacas+ (Cisco IOS) [1]

5.6.10.2 CONFIGURACIÓN DEL PROTOCOLO RADIUS (Alcatel)

Cabe mencionar que se colocó un parche para que el servidor ACS reconozca equipos Alcatel. Para la configuración de este protocolo seguir los pasos se muestran a continuación:

1. Seleccionar la opción RADIUS(Alcatel)
2. Habilite los atributos específicos del protocolo RADIUS para los equipos Alcatel RADIUS ya sea en la configuración de usuario y / o en la ventana de configuración de grupo.
3. Cuando haya terminado, haga clic en *Submit* para guardar los cambios como se muestra en la figura 5.6.24:

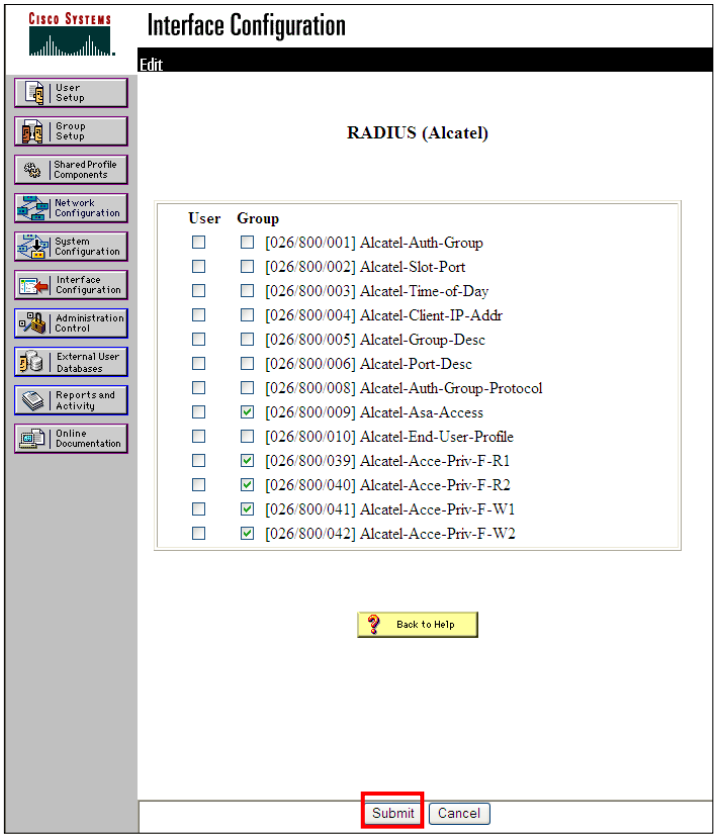


Figura 5.6.24: Configuración del protocolo Radius (Alcatel) [1]

5.6.11 TAB ADMINISTRATION CONTROL

Este tab presenta opciones que permiten agregar o editar las cuentas administrativas y editar o establecer acceso, sesión y políticas de auditoría.

Para visualizar esta ventana dar clic en la opción *Administration Control* como se muestra en la figura 5.6.25:

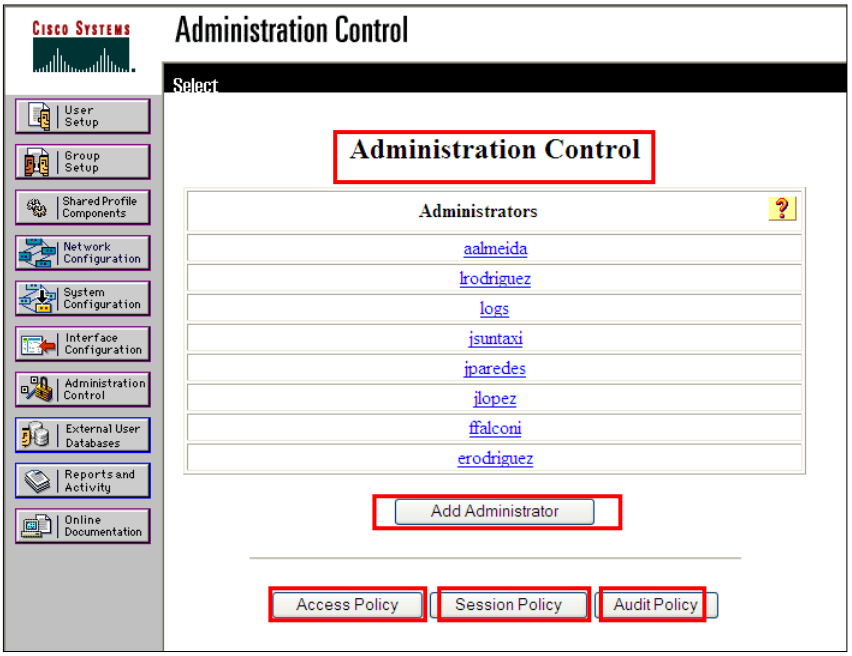


Figura 5.6.25: Opción Administration Control [1]

En la ventana del *Administration Control* se puede visualizar una serie de opciones para las respectivas configuraciones, las mismas que se describen a continuación:

5.6.11.1 Add Administrator

Dar clic en esta opción para agregar un nuevo administrador, a continuación aparecerá la ventana que se muestra en la figura 5.6.26, aquí se deberán realizar las configuraciones respectivas.

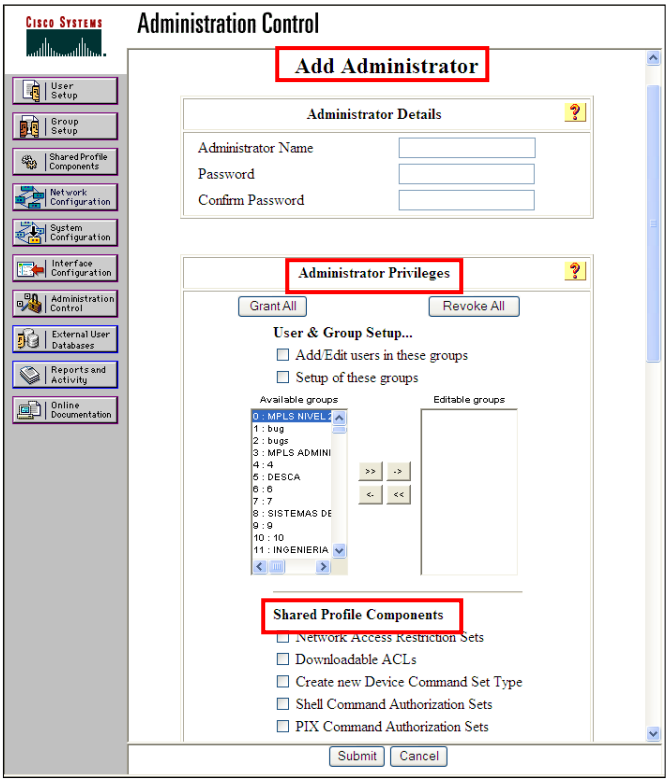


Figura 5.6.26: Opciones Administration Control [1]

- **Administrator Details:** Utilice esta tabla para configurar el nombre y la contraseña del administrador que está agregando.
- **Administrator Privileges:** Seleccione cualquiera o todos los siguientes privilegios que desea permitir para este administrador.
- **Shared Profile Components:** En esta opción se puede escoger los parámetros que se indican en la figura 5.6.26, pero para este caso no se habilita esta opción.

5.6.11.2 Access Policy

Dar clic en esta opción para configurar las políticas de acceso que permiten a los administradores del servidor ACS limitar el acceso de un intervalo de direcciones IP. En la pantalla que aparece seleccionar las opciones adecuadas como se muestra en la figura 5.6.27:

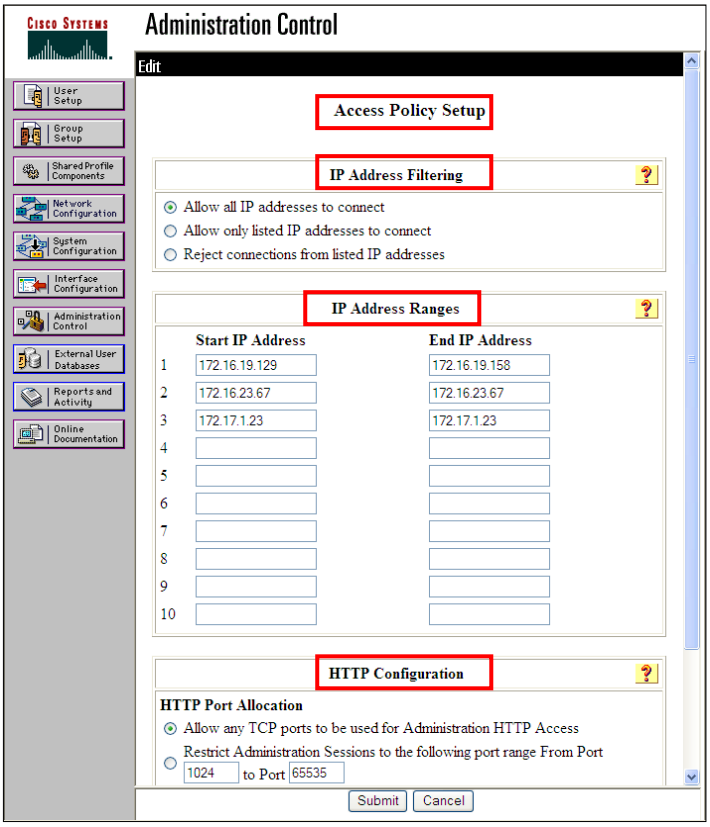


Figura 5.6.27: Opción Access Policy [1]

- **IP Address Filtering:** De las opciones que se muestran en la figura dar clic en la opción *Allow all IP addresses to connect* que es por defecto, esta opción indica cuando no hay filtrado en cualquier dirección IP por lo tanto se efectúa cuando el administrador tiene acceso al servidor ACS de forma remota.

- **IP Address Ranges:** En esta opción especificar el rango de direcciones IP para permitir o denegar el acceso.

- **HTTP Configuration:** Se recomienda escoger la opción *Allow any TCP [56]ports to be used for Administration HTTP[57] Access* para permitir que los puertos TCP sean usados para sesiones de administración remotas. La opción *Restrict Administration Sessions to the following port range From Port X to Port Y*, permite restringir los puertos TCP utilizados para las sesiones de administración remotas a un rango específico, para ello dar clic en esta opción y completar los siguientes campos:

[56] Véase Acrónimos
[57] Véase Acrónimos

- ✓ **X:** Número de puerto del extremo inferior del rango de puertos TCP
- ✓ **Y:** Número de puerto del extremo superior del rango de puertos TCP

5.6.11.3 Session Policy

Dar clic en esta opción para establecer el tiempo de espera de la sesión para permitir una sesión local automática y habilitar o deshabilitar respuestas de acceso remoto de las direcciones IP no válidas como se muestra en la figura 5.6.28:

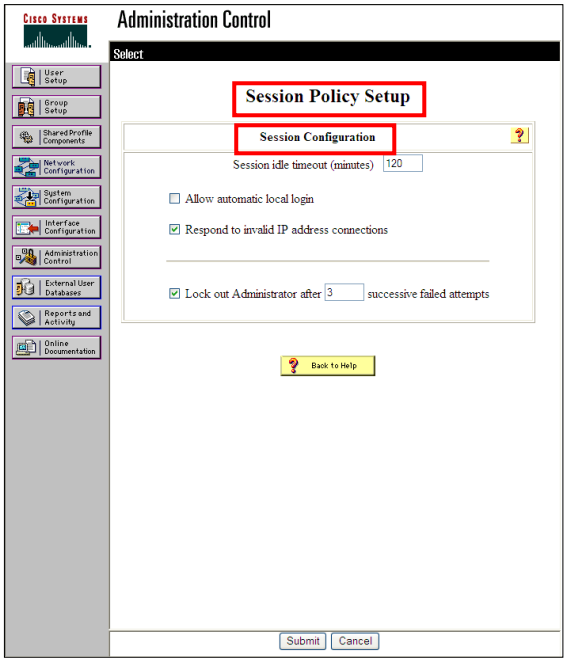


Figura 5.6.28: Opción Session Policy [1]

A continuación se muestran las respectivas configuraciones de las políticas de sesión como se indican en la figura 5.6.28.

- ➢ **Session idle timeout (minutes):** Colocar el número de minutos de inactividad, después del cual el navegador finaliza la conexión de administración remota. El valor por defecto es de 60 minutos.
- ➢ **Allow automatic local login:** Dar clic en esta opción para desactivar esta casilla con el fin de forzar a los administradores iniciar sesión en la interfaz de usuario en el servidor ACS. Esta opción está seleccionada por defecto.

- **Respond to invalid IP address connections:** Si esta casilla de verificación está activada, el servidor ACS responde con un mensaje de error en el administrador remoto cuando la estación está en un intervalo no válido. Si esta casilla está desactivada, ningún mensaje de error se generará. Los administradores pueden deshabilitar esta opción para evitar la identificación no autorizada del servidor ACS. Esta opción está seleccionada por defecto.
- **Lock out Administrator after x successive failed attempts:** Permite bloquear a un administrador después de una serie de intentos de conexión fallidos, para ello seleccionar esta opción y luego, en el cuadro X, escriba un número de intentos fallidos para el ingreso, después de lo cual el administrador será bloqueado.

5.6.12 TAB EXTERNAL USER DATABASE

Esta opción por el momento no se maneja pero permite tener una base de datos de las distintas configuraciones y cargarlas en los equipos de manera automática y de esta manera ahorra tiempo como se muestra en la figura 5.6.29:

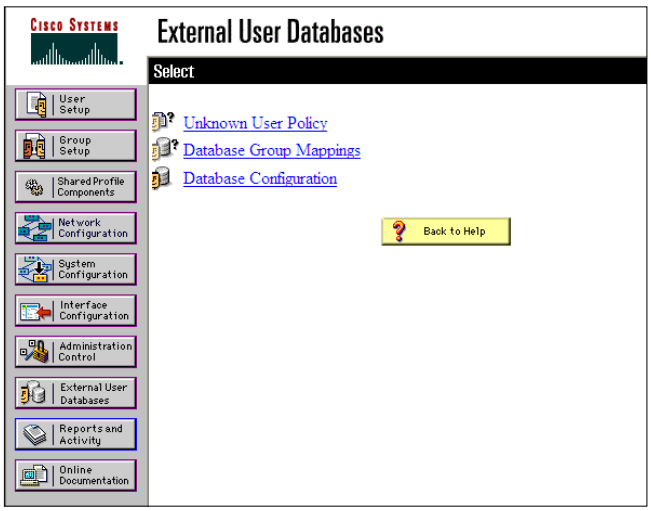


Figura 5.6.29: Opción External User Database [1]

- **Unknown User Policy**

Permite realizar un proceso de autenticación de usuarios desconocidos que no se encuentran configurados en la base de datos.

- **Database Group Mappings**

Permite configurar privilegios de autorización a un grupo de usuarios en una base de datos externa.

- **Database Configuration**

Permite configurar un tipo particular de base de datos externa para que los usuarios puedan autenticarse.

5.6.13 TAB REPORT AND ACTIVITY

Esta opción permite visualizar los informes que genera ACS.

- ✓ Seleccione el informe que desee dando clic en la opción correspondiente en la parte derecha de la ventana.

Los informes están disponibles para TACACS + y / o RADIUS si un cliente de la AAA se ha configurado para utilizar el protocolo como se muestra en la figura 5.6.30:

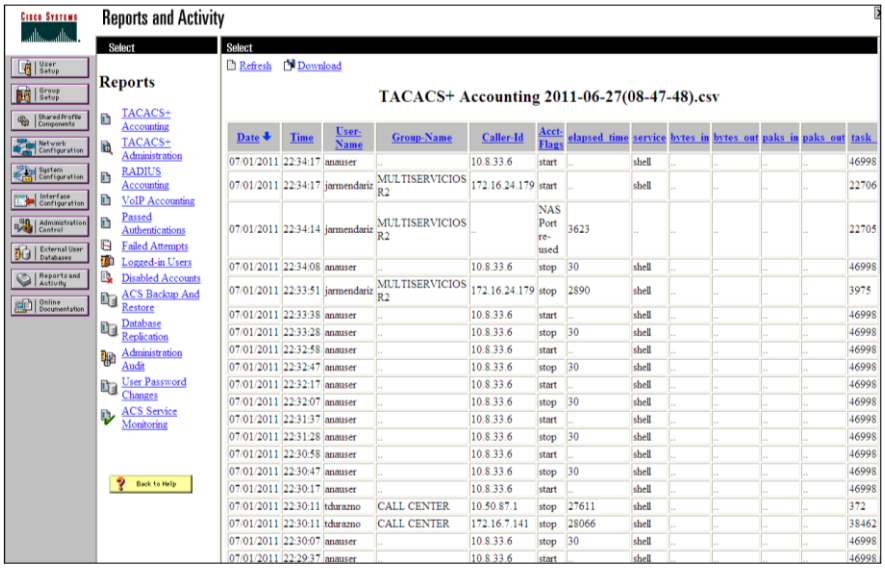
Figura 5.6.30: Opción Report and Activity [1]

Estos informes se pueden importar a hojas de cálculo y base de datos con la extensión .csv, así como también se los puede descargar eligiendo el archivo que requiera.

A continuación se presenta una descripción de los informes actualmente manejados por el área:

5.6.13.1 TACACS+ Accounting

Contiene un registro de todas las autenticaciones que se han realizado con éxito. La información capturada incluye fecha / hora, nombre de usuario, tipo de conexión, la cantidad de tiempo conectado, y bytes transferidos como se muestra en la figura 5.6.31:



Date	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	elapsed_time	service	bytes_in	bytes_out	paks_in	paks_out	task_
07/01/2011	22:34:17	anauser	..	10.8.33.6	start	..	shell	..	..	..	..	46998
07/01/2011	22:34:17	jarmendariz	MULTISERVICIOS R2	172.16.24.179	start	..	shell	..	..	..	..	22706
07/01/2011	22:34:14	jarmendariz	MULTISERVICIOS R2	..	NAS Port re-used	3623	..	..	..	..	..	22705
07/01/2011	22:34:08	anauser	..	10.8.33.6	stop	30	shell	..	..	..	..	46998
07/01/2011	22:33:51	jarmendariz	MULTISERVICIOS R2	172.16.24.179	stop	2890	shell	..	..	..	..	3975
07/01/2011	22:33:38	anauser	..	10.8.33.6	start	..	shell	..	..	..	..	46998
07/01/2011	22:33:28	anauser	..	10.8.33.6	stop	30	shell	..	..	..	..	46998
07/01/2011	22:32:58	anauser	..	10.8.33.6	start	..	shell	..	..	..	..	46998
07/01/2011	22:32:47	anauser	..	10.8.33.6	stop	30	shell	..	..	..	..	46998
07/01/2011	22:32:17	anauser	..	10.8.33.6	start	..	shell	..	..	..	..	46998
07/01/2011	22:32:07	anauser	..	10.8.33.6	stop	30	shell	..	..	..	..	46998
07/01/2011	22:31:37	anauser	..	10.8.33.6	start	..	shell	..	..	..	..	46998
07/01/2011	22:31:28	anauser	..	10.8.33.6	stop	30	shell	..	..	..	..	46998
07/01/2011	22:30:58	anauser	..	10.8.33.6	start	..	shell	..	..	..	..	46998
07/01/2011	22:30:47	anauser	..	10.8.33.6	stop	30	shell	..	..	..	..	46998
07/01/2011	22:30:17	anauser	..	10.8.33.6	start	..	shell	..	..	..	..	46998
07/01/2011	22:30:11	tduranno	CALL CENTER	10.50.87.1	stop	27611	shell	..	..	..	..	372
07/01/2011	22:30:11	tduranno	CALL CENTER	172.16.7.141	stop	28066	shell	..	..	..	..	38462
07/01/2011	22:30:07	anauser	..	10.8.33.6	stop	30	shell	..	..	..	..	46998
07/01/2011	22:29:37	anauser	..	10.8.33.6	start	..	shell	..	..	..	..	46998

Figura 5.6.31: Opción TACACS+ Accounting [1]

5.6.13.2 TACAS+ ADMINISTRATION

Registra todos los comandos que el usuario ha ejecutado en los equipos. Esto se suele utilizar cuando Cisco Secure ACS se está utilizando para gestionar el acceso a los routers como se muestra en la figura 5.6.32:

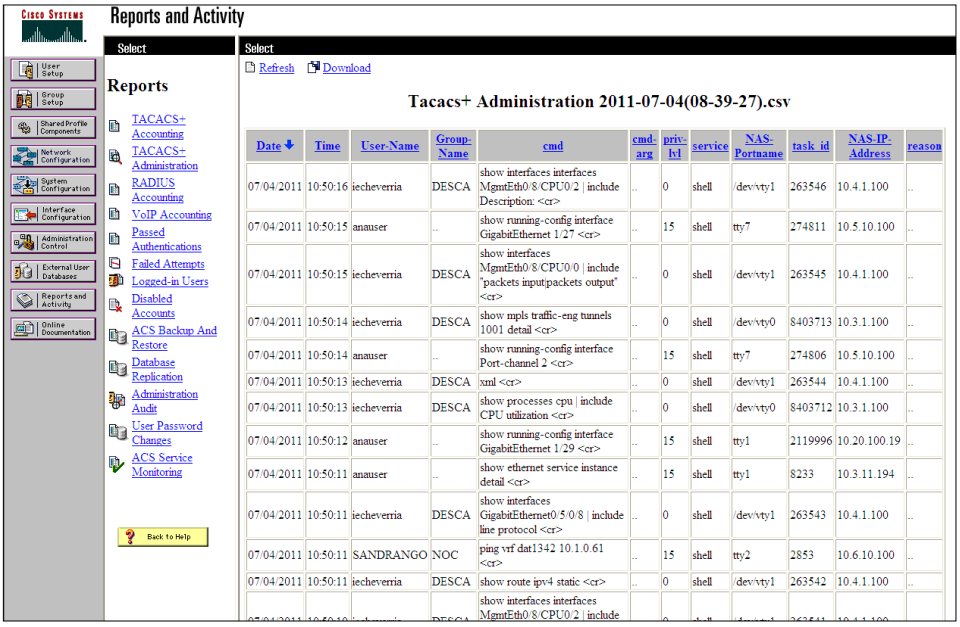


Figura 5.6.32: Opción TACAS+ ADMINISTRATION [1]

5.6.13.3 LOGGED IN USERS

Registra todos los usuarios AAA que se han logueado[58] en los equipos, no genera ningún archivo .csv pero este reporte puede ser impreso como se muestra en la figura 5.6.33:

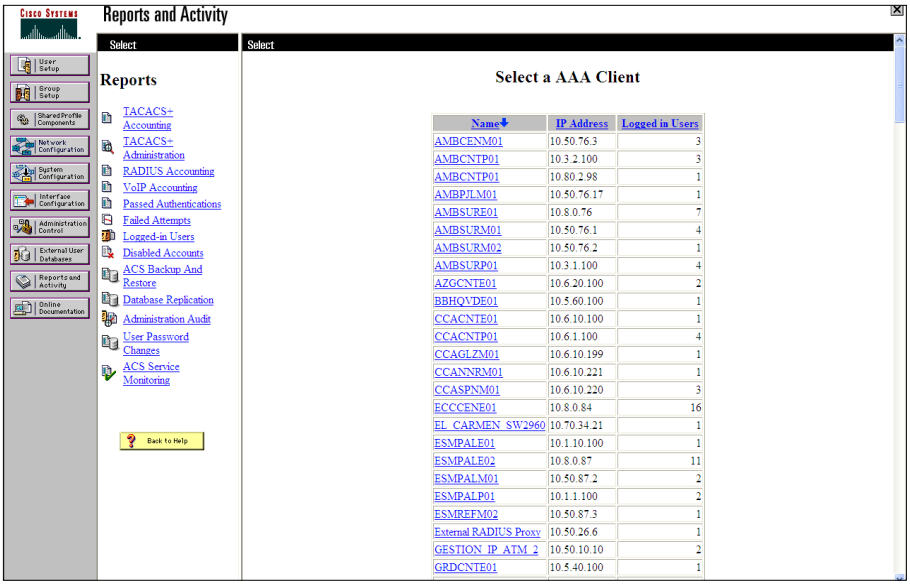


Figura 5.6.33: Opción Logged in Users [1]

[58] **Loguearse**: Identificarse para ingresar a un sitio restringido

5.6.13.4 ADMINISTRATION AUDIT

Este reporte contiene una lista de los administradores que han accedido a Cisco Secure ACS en la fecha que corresponda, las acciones que hizo o intentó hacer, y el tiempo de la acción. Ejemplos de acciones registradas incluyen iniciar y detener la sesión de administración, edición de datos de usuarios y grupos, y cambiar la configuración de la red como se muestra en la figura 5.6.34:

Select

Refresh Download

Administration Audit.csv

Date	Time	Name	Browser IP	Message
06/07/2011	16:46:14	lrodriguez	127.0.0.1	Viewed "Reports & Activity - Passed Authentications" report 'Passed Authentications active.csv'
06/07/2011	16:44:38	lrodriguez	127.0.0.1	Viewed "Reports & Activity - TACACS+ Administration" report 'Tacacs+ Administration active.csv'
06/07/2011	16:43:55	lrodriguez	127.0.0.1	Viewed "Reports & Activity - TACACS+ Administration" report 'Tacacs+ Administration active.csv'
06/07/2011	16:42:38	lrodriguez	127.0.0.1	Viewed "Reports & Activity - TACACS+ Accounting" report 'TACACS+ Accounting active.csv'
06/07/2011	16:42:27	lrodriguez	127.0.0.1	Viewed "Reports & Activity - TACACS+ Accounting" report 'TACACS+ Accounting active.csv'
06/07/2011	16:35:17	jlopez	172.16.19.148	Administration session finished
06/07/2011	16:25:45	jlopez	172.16.19.148	Viewed "Reports & Activity - TACACS+ Administration" report 'Tacacs+ Administration 2011-06-07(11-14-30).csv'
06/07/2011	16:24:47	jlopez	172.16.19.148	Viewed "Reports & Activity - TACACS+ Administration" report 'Tacacs+ Administration 2011-06-07(07-29-10).csv'
06/07/2011	16:24:33	jlopez	172.16.19.148	Administration session started
06/07/2011	16:03:28	lrodriguez	127.0.0.1	Administration session started

Figura 5.6.34: Opción Administration Audit [1]

5.6.13.5 ACS SERVICE MONITORING

Este reporte contiene un registro de los eventos producidos en Cisco Secure ACS cuando trata de controlar los servicios, tales como CSAdmin. Este reporte está activado por defecto como se muestra en la figura 5.6.35:

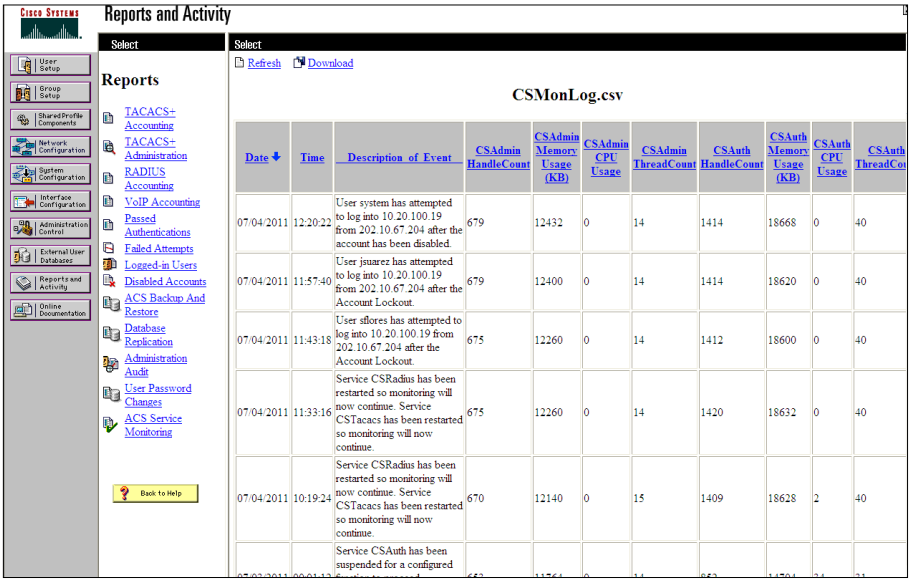


Figura 5.6.35: Opción Acs Service Monitoring [1]

5.7 PROCESOS O&M/MPLS

Los manuales de usuario personalizados de las plataformas de gestión y monitoreo anteriormente descritos son necesarios y complementarios para el siguiente diagrama general que abarca los procedimientos correspondientes para los cuatro incidentes(Pérdidas de paquetes por intermitencias de enlace, fallos en equipos de acceso, conectividad limitada o nula, problemas en configuración de plataformas) más comunes en la red, para reducir los tiempos de respuesta y resolver de manera más eficiente los problemas y dar mayor satisfacción al cliente.

5.7.1 DIAGRAMA GENERAL DE LOS PROCESOS Y USO DE LAS PLATAFORMAS.

En este diagrama se podrá observar las secciones en las cuales se encuentran los procedimientos de las plataformas correspondiente a cada ítem de verificación en caso de incidentes.

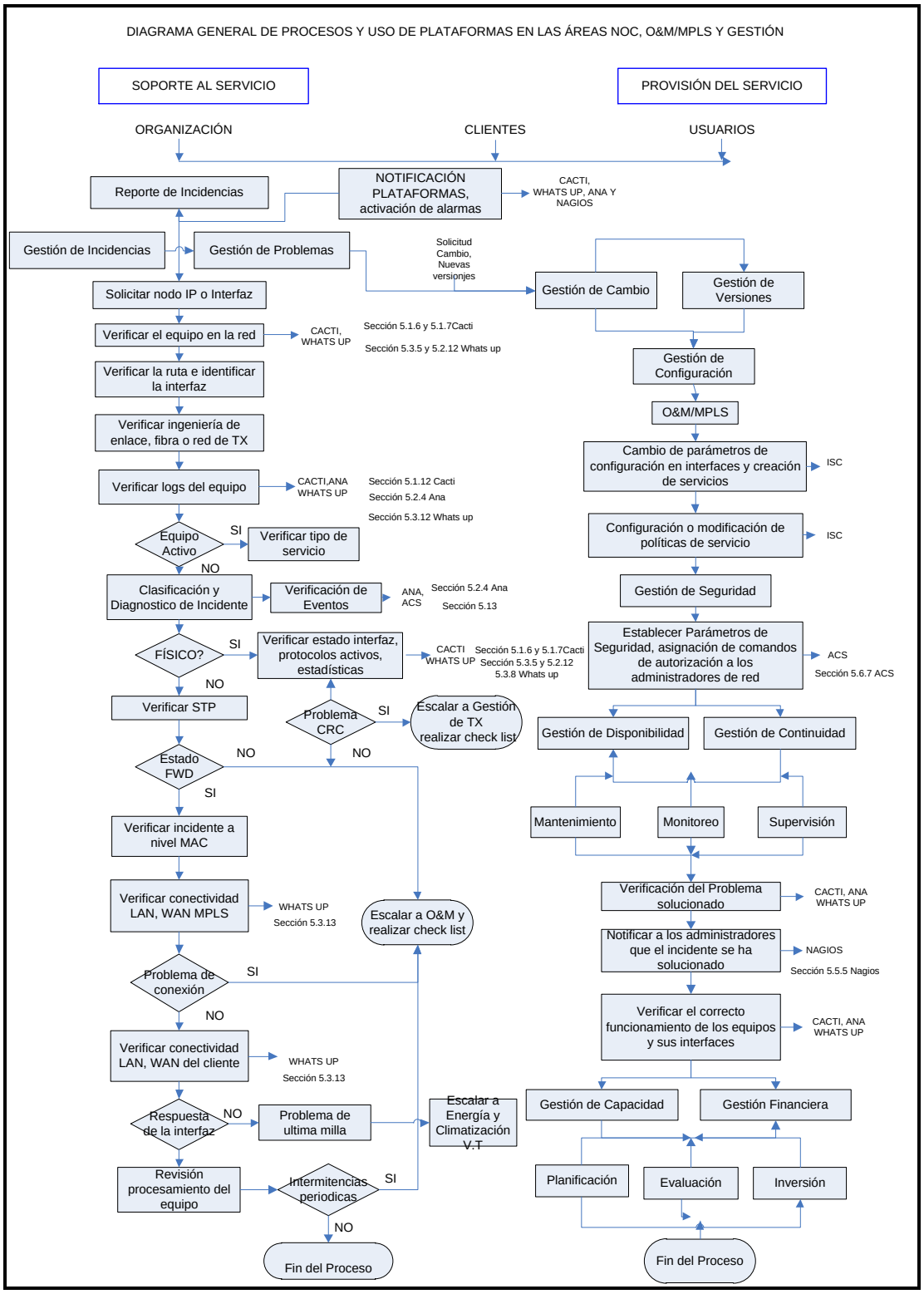


DIAGRAMA GENERAL DE PROCESOS Y USO DE PLATAFORMAS EN LAS ÁREAS NOC, O&M/MPLS Y GESTIÓN
SOPORTE AL SERVICIO
PROVISIÓN DEL SERVICIO
ORGANIZACIÓN
CLIENTES
USUARIOS
Reporte de Incidencias
NOTIFICACIÓN PLATAFORMAS, activación de alarmas
CACTI, WHATS UP, ANA Y NAGIOS
Gestión de Incidencias
Gestión de Problemas
Solicitud Cambio, Nuevas versionjes
Gestión de Cambio
Gestión de Versiones
Solicitar nodo IP o Interfaz
Verificar el equipo en la red
CACTI, WHATS UP
Sección 5.1.6 y 5.1.7Cacti
Sección 5.3.5 y 5.2.12 Whats up
Verificar la ruta e identificar la interfaz
Gestión de Configuración
Verificar ingeniería de enlace, fibra o red de TX
O&M/MPLS
Verificar logs del equipo
CACTI,ANA WHATS UP
Sección 5.1.12 Cacti
Sección 5.2.4 Ana
Sección 5.3.12 Whats up
Cambio de parámetros de configuración en interfaces y creación de servicios
ISC
Equipo Activo
SI
Verificar tipo de servicio
NO
Configuración o modificación de políticas de servicio
ISC
Clasificación y Diagnostico de Incidente
Verificación de Eventos
ANA, ACS
Sección 5.2.4 Ana
Sección 5.13
Gestión de Seguridad
FÍSICO?
SI
Verificar estado interfaz, protocolos activos, estadísticas
CACTI WHATS UP
Sección 5.1.6 y 5.1.7Cacti
Sección 5.3.5 y 5.2.12
5.3.8 Whats up
Establecer Parámetros de Seguridad, asignación de comandos de autorización a los administradores de red
ACS
Sección 5.6.7 ACS
NO
Verificar STP
Problema CRC
SI
Escalar a Gestión de TX realizar check list
Gestión de Disponibilidad
Gestión de Continuidad
Estado FWD
NO
NO
SI
Mantenimiento
Monitoreo
Supervisión
Verificar incidente a nivel MAC
Verificar conectividad LAN, WAN MPLS
WHATS UP
Sección 5.3.13
Escalar a O&M y realizar check list
Verificación del Problema solucionado
CACTI, ANA WHATS UP
Notificar a los administradores que el incidente se ha solucionado
NAGIOS
Sección 5.5.5 Nagios
Problema de conexión
SI
NO
Verificar el correcto funcionamiento de los equipos y sus interfaces
CACTI, ANA WHATS UP
Verificar conectividad LAN, WAN del cliente
WHATS UP
Sección 5.3.13
Gestión de Capacidad
Gestión Financiera
Respuesta de la interfaz
NO
Problema de ultima milla
Escalar a Energía y Climatización V.T
Planificación
Evaluación
Inversión
Revisión procesamiento del equipo
Intermitencias periodicas
SI
NO
Fin del Proceso
Fin del Proceso

5.7.2 PÉRDIDAS DE PAQUETES POR INTERMITENCIAS DE ENLACES

Para escalar un problema de intermitencias al MPLS previamente se debe disponer de al menos los siguientes datos:

- ✓ NODO IP: Ejemplo. UIOMSCE01, PVJCALM01, etc.
- ✓ INTERFAZ: Ejemplo. Interface vlan xx, interfaces gi13/43, etc.

Para verificar pérdidas de paquetes por intermitencias siga las siguientes instrucciones:

1. Verificar mediante las herramientas SNMP (CACTI) que no exista saturación en dicha interfaz.

2. Verificar la ingeniería del enlace que tiene problemas para identificar si pasa por fibra oscura o por una red de transmisión.

3. Revisar si se obtiene alguna información útil en el log del equipo mediante el comando UIOINQE01#show logging.

PARA IDENTIFICAR SI ES UN PROBLEMA A NIVEL FÍSICO SIGA LAS SIGUIENTES INSTRUCCIONES:

1. Verificar mediante el comando *show interface* si existe intermitencia (up, down, up, down) y repetir este procedimiento varias veces para observar si se presentan problemas en la transmisión.

2. Verificar los parámetros de la interface

    a. Verificar que el estado de la interfaz y del protocolo estén activos.

b. Verificar que exista flujo de tráfico de datos.

c. Verificar que no se presenten errores en las interfaces (CRC).

d. Verificar la velocidad y negociación del puerto.

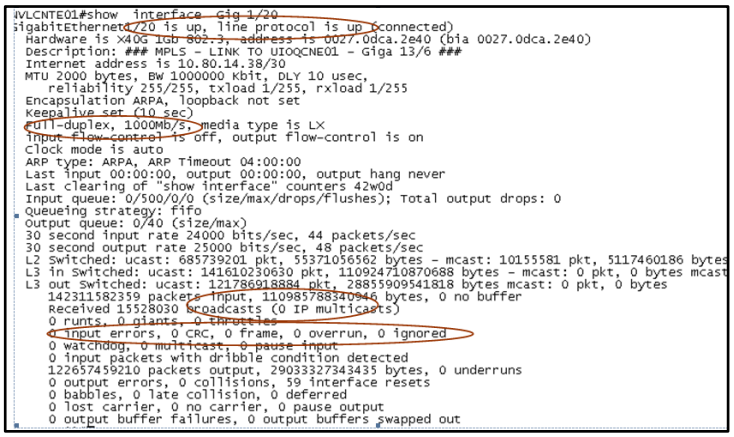


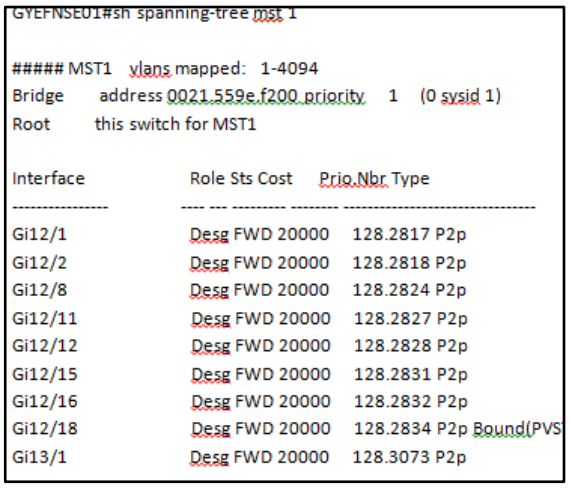
Figura 5.7.1: Show Interface[1]

3. En caso de que exista problemas de transmisión como por ejemplo CRC. Escalar a transmisiones y seguir el Check list de Transmisión.

4. Una vez realizados los pasos anteriores y la interfaz continúe flapeando (cambiando de estado de UP a DOWN), y que no se presenten inconvenientes de CRC además que TRANSMISIONES (RTFO, Radio, etc) haya descartado un problema físico procedemos a verificar el estado de las interfaces a nivel lógico.

Para la verificación a nivel lógico en enlaces capa 2 siga las siguientes instrucciones:

1. Verificar Spanning Tree mediante el comando *show spanning-tree mst 1*. En MPLS en su mayoría el tipo de STP usado es el de MSTP (Multiple STP) y todas las vlans se mapean sobre la instancia 1.

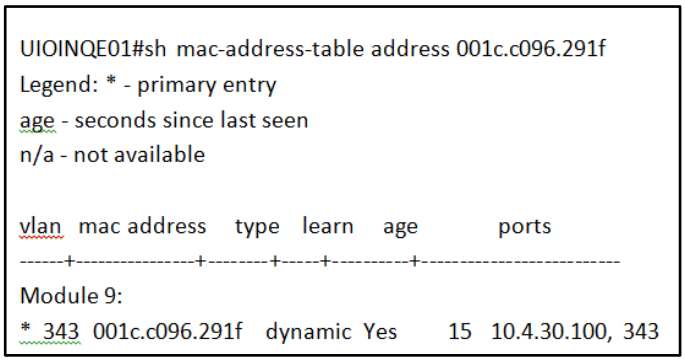


```
GYEFNSE01#sh spanning-tree mst 1

##### MST1   vlans mapped:   1-4094
Bridge      address 0021.559e.f200 priority    1    (0 sysid 1)
Root        this switch for MST1

Interface              Role Sts Cost      Prio.Nbr Type
---------------        ---- --- --------- -------- --------------------------------
Gi12/1                 Desg FWD 20000     128.2817 P2p
Gi12/2                 Desg FWD 20000     128.2818 P2p
Gi12/8                 Desg FWD 20000     128.2824 P2p
Gi12/11                Desg FWD 20000     128.2827 P2p
Gi12/12                Desg FWD 20000     128.2828 P2p
Gi12/15                Desg FWD 20000     128.2831 P2p
Gi12/16                Desg FWD 20000     128.2832 P2p
Gi12/18                Desg FWD 20000     128.2834 P2p Bound(PVS
Gi13/1                 Desg FWD 20000     128.3073 P2p
```

Figura 5.7.2: Spanning Tree

2. Revisar que el estado del STP se mantenga en FWD, en el caso de que este estado cambie de FWD a BLK varias veces escalar a MPLS debido a que es un problema de intermitencia.

3. Es posible que se presente un flaping a nivel de macs para verificar dicha incidencia usar el comando *show mac-address-table address <dir mac>*.



```
UIOINQE01#sh mac-address-table address 001c.c096.291f
Legend: * - primary entry
age - seconds since last seen
n/a - not available

vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Module 9:
* 343  001c.c096.291f   dynamic  Yes        15   10.4.30.100, 343
```

Figura 5.7.3: Mac Address

Se recomienda repetir este comando varias veces; si realmente existe flapeo se observa que la entrada de la mac desaparece o cambia de puerto como se observa en el siguiente ejemplo.

```
UIOINQE01#sh mac-address-table address 0024.13e1.7c19
Legend: * - primary entry
age - seconds since last seen
n/a - not available
vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Module 13:
*  343   0024.13e1.7c19    dynamic  Yes          0   Gi13/39


UIOINQE01#sh mac-address-table address 0024.13e1.7c19
Legend: * - primary entry
age - seconds since last seen
n/a - not available
vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Module 9:
*  343   0024.13e1.7c19    dynamic  Yes          0   10.4.30.100, 343
```

Figura 5.7.4: Ejemplo de flapeo por Mac

En este caso procedemos a escalar a MPLS.

Si no se observa cambio en el estado del STP, ni flapeo de macs se procede a verificar conectividad con una interfaz vlan (SVI).

4. Verificar conexión hacia la WAN (Si es enlace capa 3) o hacia una interfaz vlan (SVI) (si es enlace capa 2) con las diferentes variaciones del comando como por ejemplo con carga (size→MTU), sin carga, sin desfragmentación (df-bit), con muchas repeticiones, etc. Ejemplo de un ping extendido.

```
UIOMSCE01#ping 10.80.10.254  size 1900 df-bit repeat 1000
Type escape sequence to abort.
Sending 1000, 1900-byte ICMP Echos to 10.80.10.254,  timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000),  round-trip min/avg/max = 1/1/4 ms
```

Figura 5.7.5: Ping Extendido

Lo ideal es que se observe el mismo comportamiento con todos estos parámetros; por ejemplo pase un MTU de 1900 sin desfragmentar.

Este procedimiento es válido para revisión de clientes, lo única que cambia es los escalamientos y que algunos de los comandos deben ser cambiados con la opción vrf como se muestra en los siguientes ejemplos.

4.1 Para verificar la conexión WAN del MPLS realizarlo mediante el siguiente comando: *ping vrf <nombre de la vrf ><ip wan>*.

```
NVLCNTE01#ping vrf netcnt 186.42.165.185

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 186.42.165.185, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Figura 5.7.6: Conexión WAN MPLS

En el caso de que existan problemas con la conexión de esta interfaz ESCALAR AL MPLS.

4.2 Verificar conexión hacia la WAN del cliente *ping vrf <nombre de la vrf> <ip wan>*.

```
NVLCNTE01#ping vrf netcnt 186.42.165.186

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 186.42.165.186, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms
NVLCNTE01#
```

Figura 5.7.7: Conexión WAN del cliente

En el caso de no tener respuesta de la interfaz, el problema es de última milla.

4.3 Verificar la ruta del cliente *show ip route vrf <nombre de la vrf ><ip wan>*.

```
NVLCNTE01#show ip route vrf netdef 190.152.88.90

Routing Table: netdef
Routing entry for 190.152.88.88/30
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Redistributing via bgp 28006
  Advertised by bgp 28006
  Routing Descriptor Blocks:
  * directly connected, via Vlan427
      Route metric is 0, traffic share count is 1
```

Figura 5.7.8: Ruta- Cliente

En este punto se debe verificar si existe duplicación de rutas ya que esto puede presentar intermitencias.

4.4 Verificar conexión hacia la LAN del cliente *ping vrf <nombre de la vrf > <ip LAN>*.

```
NVLCNTE01#PING vrf netdef 201.219.33.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 201.219.33.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Figura 5.7.9: Conexión LAN

En caso de no tener respuesta de la interfaz el problema pasa a ser de última milla.

4.5 Verificar la conexión a la LAN y WAN desde otro equipo PE.

```
UIOQCNE01#PING vrf netdef 201.219.33.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 201.219.33.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
UIOQCNE01#PING vrf netdef 190.152.88.90

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 190.152.88.90, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
```

Figura 5.7.10: Conexión LAN – WAN

Después de tener respuestas satisfactorias en los pasos 7.3 - 9 y no tener respuesta desde otro equipo PE proceder a ESCALAR AL MPLS.

5. En caso de que las intermitencias sean aleatorias revisar el procesamiento del equipo mediante el comando show processes cpu history.

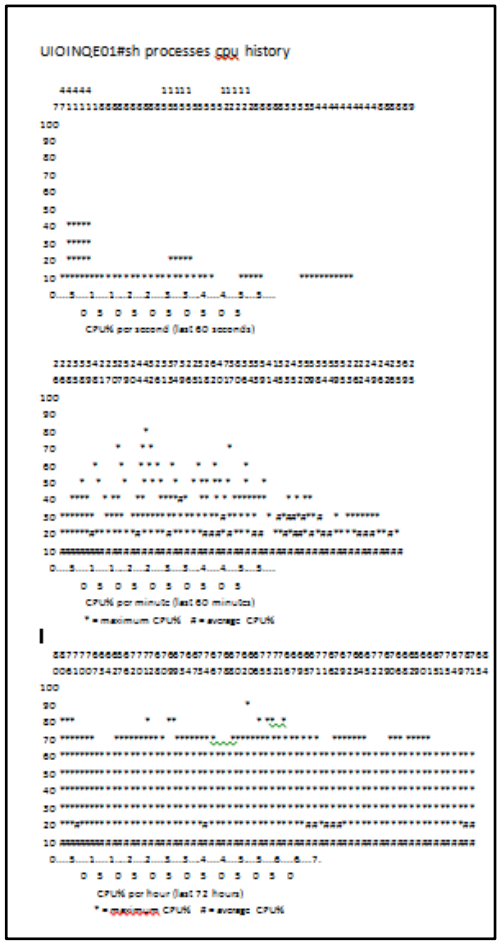


Figura 5.7.11: Procesamiento del Equipo

Si en el grafico histórico se observa picos mayores a 89% significa que existe alto procesamiento del equipo

6. Si detecta que el 100% de CPU se dispara por el proceso ARP Input y IP Input mediante el comando en el show processes cpu sorted significa que hay un ataque desde la LAN hacia el router, ocasionando que haya pérdida de paquetes, por ende intermitencias con ICMP (ping).

```
AMBSURE01#sh processes cpu sorted
CPU utilization for five seconds: 4%/1%; one minute: 8%; five minutes: 11%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
 489   345681560 532034553        649  1.03%  0.65%  0.54%   0 PDU DISPATCHER
 490   9487887762379843942          0  0.39%  1.21%  1.28%   0 SNMP ENGINE
 202   4265576884262272056          0  0.31%  0.52%  0.62%   0 IP Input
  98         188       826        227  0.31%  0.03%  0.00%   2 Virtual Exec
  94   135914584 150239626        904  0.31%  1.42%  3.88%   6 SSH Process
  76    70404460  92753892        759  0.31%  0.14%  0.17%   0 IPC LC Message H
  83   132203188  15500125       8529  0.23%  0.23%  0.23%   0 Compute load avg
  10   501538924 568200034        882  0.23%  0.66%  0.71%   0 ARP Input
 488    94467004 983185136         96  0.07%  0.16%  0.15%   0 IP SNMP
 142         732     16197         45  0.07%  0.00%  0.00%   4 Virtual Exec
 436     1590100   1573149       1010  0.07%  0.10%  0.09%   0 RPC pm-mp
  11      205432  39420714          5  0.00%  0.00%  0.00%   0 ARP Background
  12           0         3          0  0.00%  0.00%  0.00%   0 ATM Idle Timer
   9           0         2          0  0.00%  0.00%  0.00%   0 Timers
  15           0         1          0  0.00%  0.00%  0.00%   0 Policy Manager
  13           0         1          0  0.00%  0.00%  0.00%   0 ATM ASYNC PROC
  14           0       161          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  16        1456      2524        576  0.00%  0.00%  0.00%   0 Entity MIB API
  19         116    627030          0  0.00%  0.00%  0.00%   0 IPC Dynamic Cach
  20       21072   7519972          2  0.00%  0.00%  0.00%   0 IPC Service NonC
  21           0         3          0  0.00%  0.00%  0.00%   0 VTEMPLATE Backgr
  22       36244  37544550          0  0.00%  0.00%  0.00%   0 IPC Periodic Tim
  17       88256   4210825         20  0.00%  0.00%  0.00%   0 EEM ED Syslog
  18           0         1          0  0.00%  0.00%  0.00%   0 IFS Agent Manage
  25     7606840  47085013        161  0.00%  0.01%  0.00%   0 IPC Seat Manager
  23      214624 163862266          1  0.00%  0.00%  0.00%   0 IPC Managed Time
  27      119096   7535854         15  0.00%  0.00%  0.00%   0 IPC Loadometer
  28           8        58        137  0.00%  0.00%  0.00%   0 RO Notify Timers
  29           0         1          0  0.00%  0.00%  0.00%   0 RMI RM Notify Wa
```

Figura 5.7.12: Procesamiento del cpu

7. En caso de que las intermitencias sean periódicas escalar a MPLS, puede deberse a afinamiento del control plane (arquitectura interna de routers) o afinamiento en las políticas de QoS; debido a que el ping (ICMP) no tiene preferencia.

NOTA: El ping no es una buena referencia para verificar la disponibilidad de un servicio.

5.7.3 FALLO DE EQUIPOS DE ACCESO

Estos fallos se pueden dar por las siguientes causas:

- ✓ Cuando una vlan no esté creada.
- ✓ Cuando la vlan no pasa por una interfaz
- ✓ Cuando un puerto está mal configurado
- ✓ Cuando la vlan no está aprendiendo la dirección Mac
- ✓ Por problemas de Spanning Tree
- ✓ En ciertos casos problemas con la MTU

PARA VERIFICAR EL FALLO EN EQUIPOS DE ACCESO SIGA LAS SIGUIENTES INTRUCCIONES:

1. Verificar que se encuentre creada la vlan mediante el comando show vlan id <vlan>.

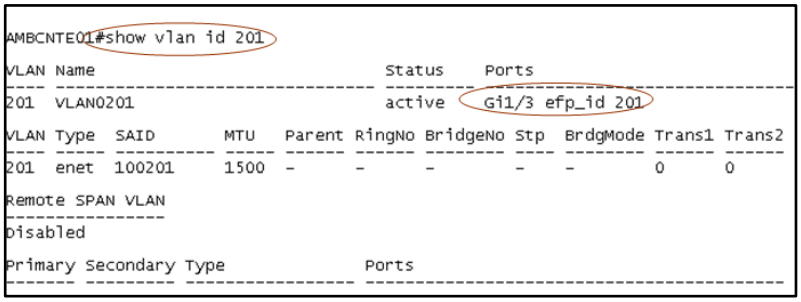


Figura 5.7.13: Parámetros de Vlan

En el caso que la vlan no se encuentre pasada por algún puerto solicitar dicha operación al área O&M.

2. Revisar la interfaz usando el comando *show interface <interface>* y verificar los siguiente parámetros:

a. Verificar que el estado de la interfaz y del protocolo estén activos.

b. Verificar que exista flujo de tráfico de datos.

c. Verificar que no se presenten errores en las interfaces (CRC).

d. Verificar la velocidad y negociación del puerto.

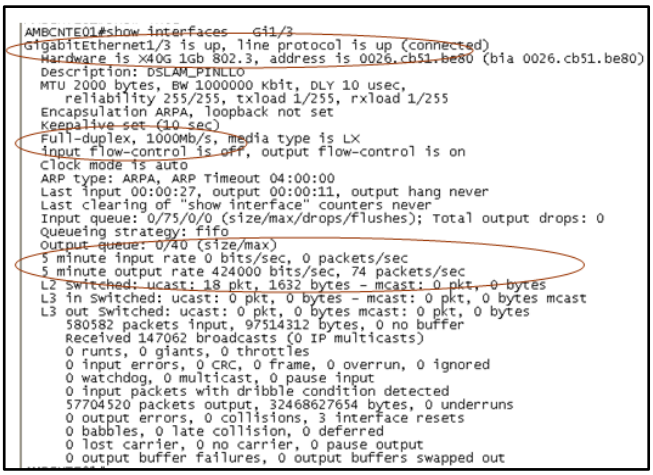


Figura 5.7.14: Verificación de la Interfaz

3. Verificar que la vlans están aprendiendo direcciones mac, mediante comando *show mac address-table vlan<vlan>*.

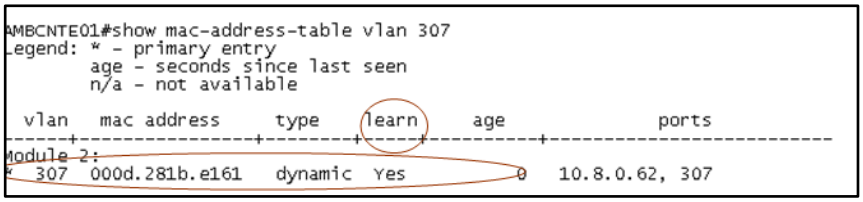


Figura 5.7.15: Recepción de Mac

4. En el caso que se tenga el dato de la dirección mac del equipo se puede verificar la interfaz usando el comando *show mac address-table address <dir mac>*.

```
AMBCNTE01#show mac-address-table address 000d.281b.e161
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------------
Module 2:
*  307   000d.281b.e161   dynamic  Yes          0   10.8.0.62, 307
```

Figura 5.7.16: Verificación con la dirección Mac

En clientes corporativos por lo general se presentan problemas de Spanning Tree para verificarlos seguimos los siguientes pasos:

1. Ingresamos el comando *show spanning-tree interface <interface>*.

```
UIOQCNE01#show spanning-tree interface fa6/5

Mst Instance        Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
MST0                Desg FWD 200000    128.1285 P2p
MST1                Desg FWD 200000    128.1285 P2p
UIOQCNE01#
```

Figura 5.7.17: Spanning Tree

2. Verificar que el estado de la interface se encuentre en FWD (Forwarding) que es el más óptimo. En el caso de que el estado sea BLK (Bloqueado) ocasiona que el e protocolo pase a un estado de Error Disable, se produce bloqueo de la vlan y como consecuencia de ello presentarse un fallo en el acceso a los equipos.

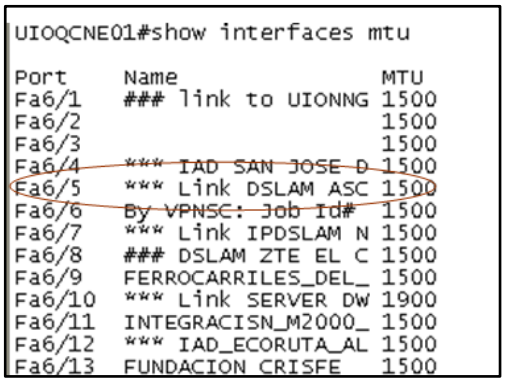
3. Verificar que los puertos estén configurados correctamente ya sea como modo troncal o acceso mediante el comando: *show run interface <interface>*.

```
UIOQCNE01#show run interface fa6/5
Building configuration...

Current configuration : 238 bytes
!
interface FastEthernet6/5
 description *** Link DSLAM ASCAZUBI ***
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 200,201,300-331,333-342,344,345,704
 switchport mode trunk
 switchport nonegotiate
end
```

Figura 5.7.18: Verificación de puertos

En ciertas ocasiones se pueden presentar problemas con la mtu ya sea porque se encuentra configurado con un menor valor del requerido lo cual también produce un fallo en los equipos de acceso.

4. Verificar las mtu configuradas para las interfaces mediante el comando *show interface mtu*.



```
UIOQCNE01#show interfaces mtu

Port      Name                MTU
Fa6/1     ### link to UIONNG 1500
Fa6/2                         1500
Fa6/3                         1500
Fa6/4     *** IAD SAN JOSE D 1500
Fa6/5     *** Link DSLAM ASC 1500
Fa6/6     By VPNSC: Job Id#  1500
Fa6/7     *** Link IPDSLAM N 1500
Fa6/8     ### DSLAM ZTE EL C 1500
Fa6/9     FERROCARRILES_DEL_ 1500
Fa6/10    *** Link SERVER DW 1900
Fa6/11    INTEGRACISN_M2000_ 1500
Fa6/12    *** IAD_ECORUTA_AL 1500
Fa6/13    FUNDACION CRISFE   1500
```

Figura 5.7.19: MTU de la interfaces

5.7.4 CONECTIVIDAD LIMITADA O NULA

Estas incidencias se pueden presentar a nivel de Corporativos y Masivos

PARA VERIFICAR CONECTIVIDAD EN CORPORATIVOS SIGA LAS SIGUIENTES INTRUCCIONES:

1. Verificar la vlan del cliente mediante el comando *show vlan*.

```
BBHCNTE01# show run int vlan 862
Building configuration...

Current configuration : 147 bytes
!
interface Vlan862
 description By VPNSC: Job Id# = 8378 (SISTEMAS MPLS)
 ip vrf forwarding dat1311
 ip address 172.18.32.94 255.255.255.252
end
```

Figura 5.7.20: Comprobación de la VLAN

2. Verificar la vrf asignada al cliente mediante el comando *show run vrf <vrf>*.

```
BBHCNTE01#show run vrf dat1311
Building configuration...

Current configuration : 594 bytes
ip vrf dat1311
 rd 28006:201311
 route-target export 28006:201311
 route-target import 28006:201311
!
!
interface Vlan862
 description By VPNSC: Job Id# = 8378 (SISTEMAS MPLS)
 ip vrf forwarding dat1311
 ip address 172.18.32.94 255.255.255.252
!
router bgp 28006
 !
 address-family ipv4 vrf dat1311
  no synchronization
  redistribute connected
  redistribute eigrp 20
 exit-address-family
```

Figura 5.7.21: Comprobación de la VRF

3. Revisar si la interface se encuentra activa mediante el comando *show interface <interface>*.

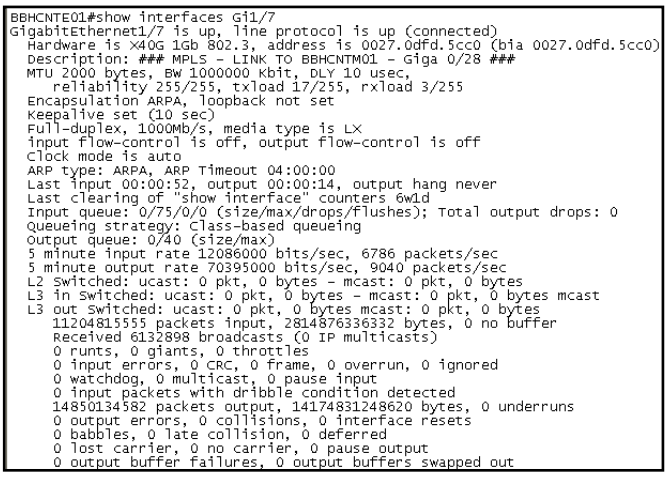


Figura 5.7.22: Verificación de Interfaz

4. Realizar un ping a la vrf

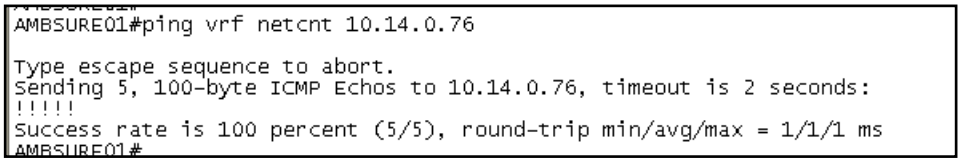


Figura 5.7.23: Ping a la vrf

Si después de haber realizado este procedimiento verificando que la interfaz, la vlan y la vrf se encuentran en un estado óptimo y la conectividad aun es limitada se procede a:

5. Verificar el enrutamiento mediante el comando *show ip route <vrf>* para determinar si el router está activo para enrutamiento.

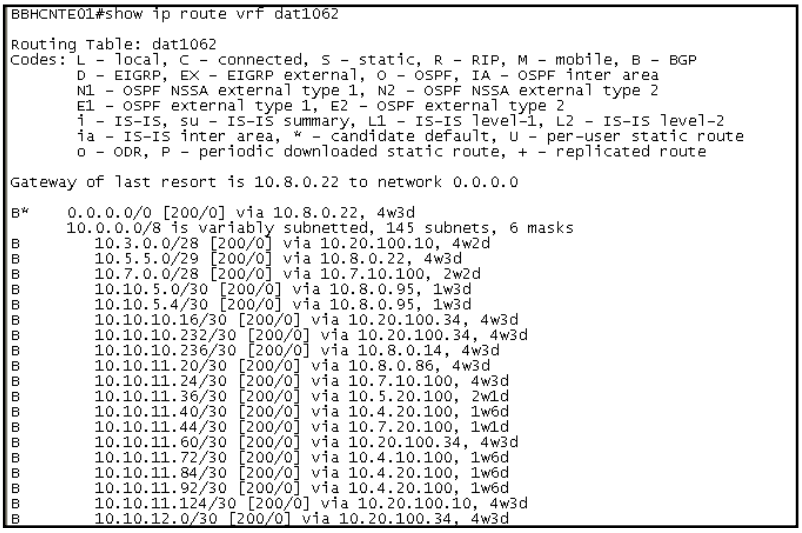


Figura 5.7.24: Enrutamiento VRF

6. Identificar los puertos troncales y de acceso mediante el comando *show run interface <interface>*.

7. Realizar un ping al router de siguiente salto.

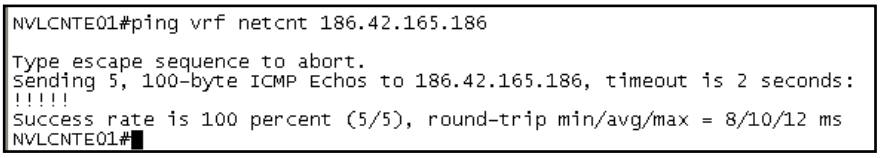


Figura 5.7.25: Ping al siguiente salto

En caso de no tener respuesta satisfactoria el problema se debe a las siguientes causas

- ✓ Vlan no configurada en el dslam
- ✓ Vlan no forma parte de una interfaz
- ✓ El puerto asignado para la vlan se encuentre mal configurado ya sea como modo troncal o de acceso.

8. Verificar que el puerto configurado en el switch tenga una ruta estática.

5.7.5 PROBLEMAS DE CONFIGURACIÓN EN PLATAFORMAS

Estos fallos se pueden dar por las siguientes causas:

- ✓ Cambio de velocidad en la vlan
- ✓ Cambio de la vrf de un cliente
- ✓ Cambios de clientes a otra troncal por problemas de transmisión

PARA VERIFICAR PROBLEMAS DE CONFIGURACION EN PLATAFORMAS SIGA LAS SIGUIENTES INTRUCCIONES:

1. Verificar el estado actual de la vlan mediante el comando *show run in vlan*.

2. Revisar la velocidad configurada en la vlan.

3. Verificar que las Políticas de Servicio estén correctamente configuradas.

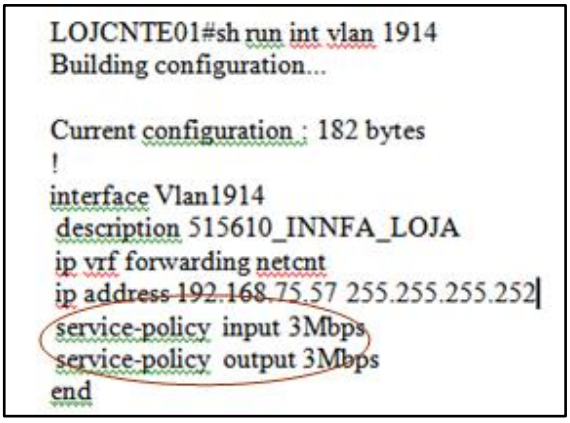


Figura 5.7.26: Verificación de Políticas

En el caso de que la velocidad configurada no sea la requerida solicitar al área O&M el cambio de velocidad

En el caso de un problema de configuración en la vrf e ip de un cliente siga las siguientes instrucciones:

1. Verificar el estado actual de la vrf configurada mediante el comando *show run vrf<vrf>*.

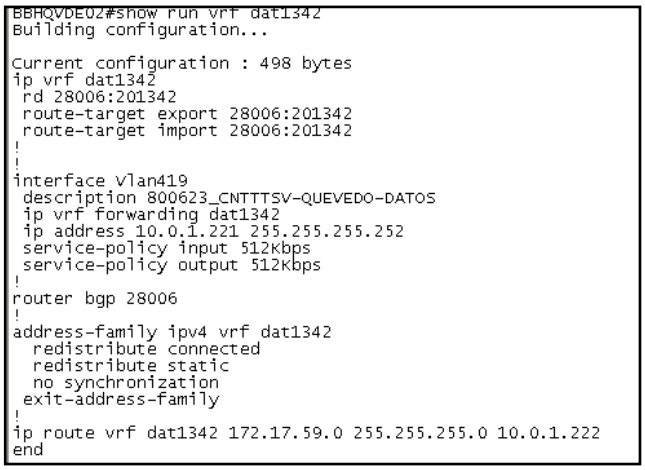


Figura 5.7.27: Estado actual VRF

2. Verificar la ip de la LAN de la vrf usando el dato de la ip de la WAN del Router del cliente.

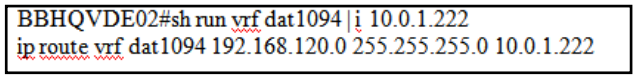


Figura 5.7.28: Verificación de la LAN

En el caso que la vrf y la ip no coincidan con lo requerido se solicita un cambio de vrf y de la ip de la LAN.

3. Verificar el camino por la cual está saliendo la vrf configurada mediante el comando *show ip route vrf <vrf>*.

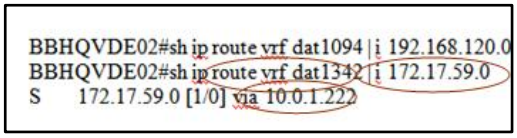


Figura 5.7.29: Ruta VRF

4. En ocasiones se puede presentar que un enlace de la troncal tuvo problemas de transmisión, es necesario verificar el estado de la interfaz que presenta incidencias mediante el siguiente comando *show int Gi2/28 | i line | rate | errors*.

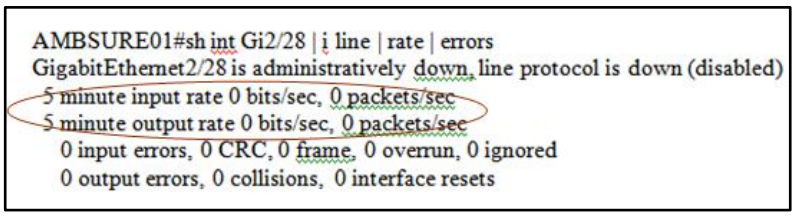


Figura 5.7.30: Estado de la interfaz

Como se puede observar existe problemas en la transmisión de datos por esta razón es preciso cambiar el enlace para que todo el tráfico se envié por el nuevo enlace.

5. Verificar que la interfaz con incidencias ha sido bloqueado por spinning tree lo hacemos mediante el comando *show spanning tree mts*.

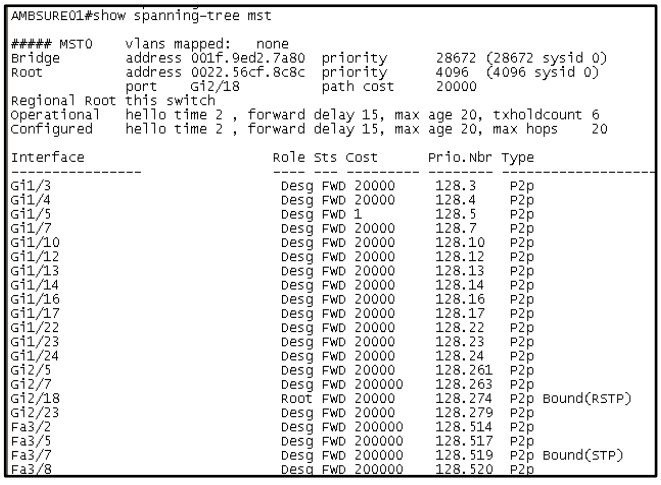
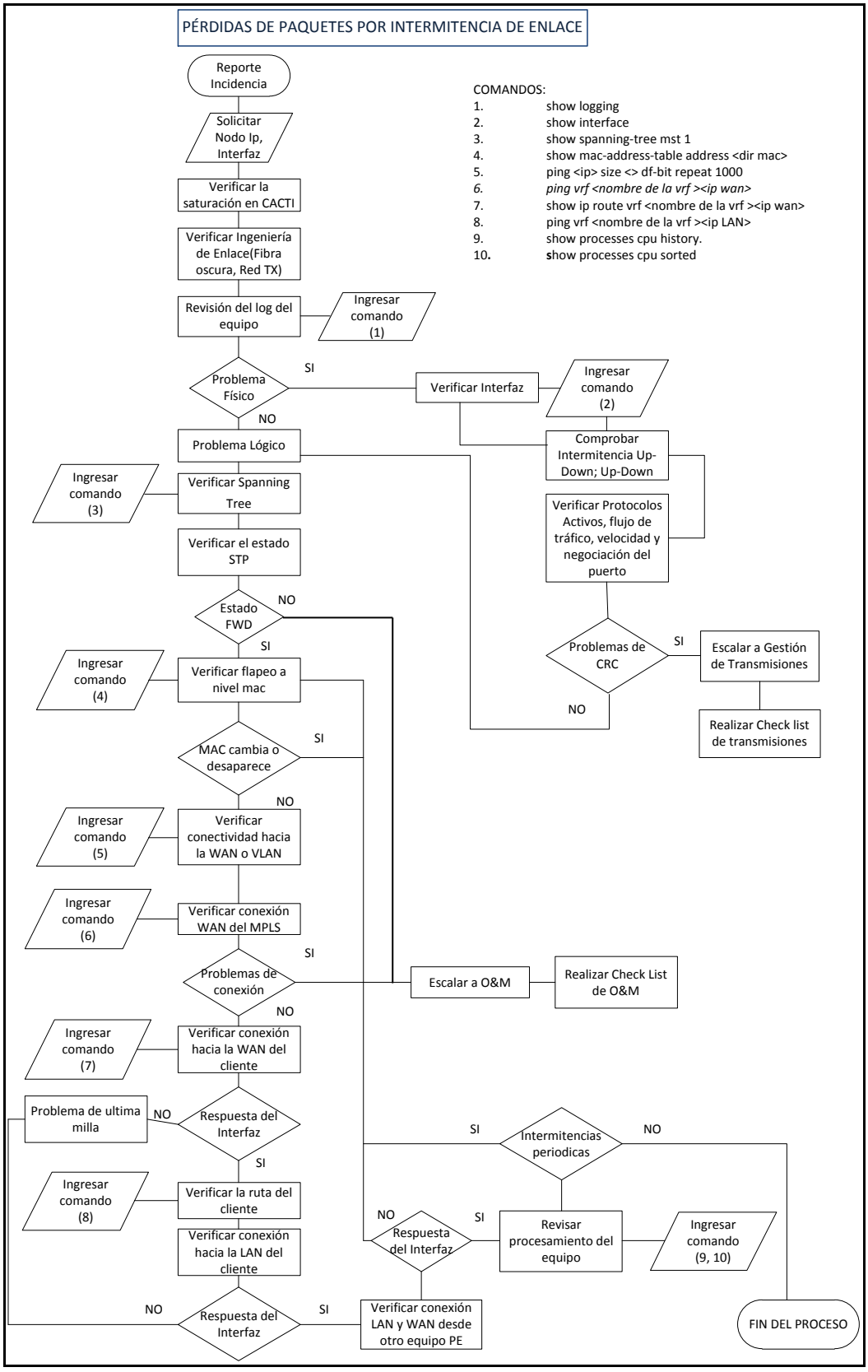
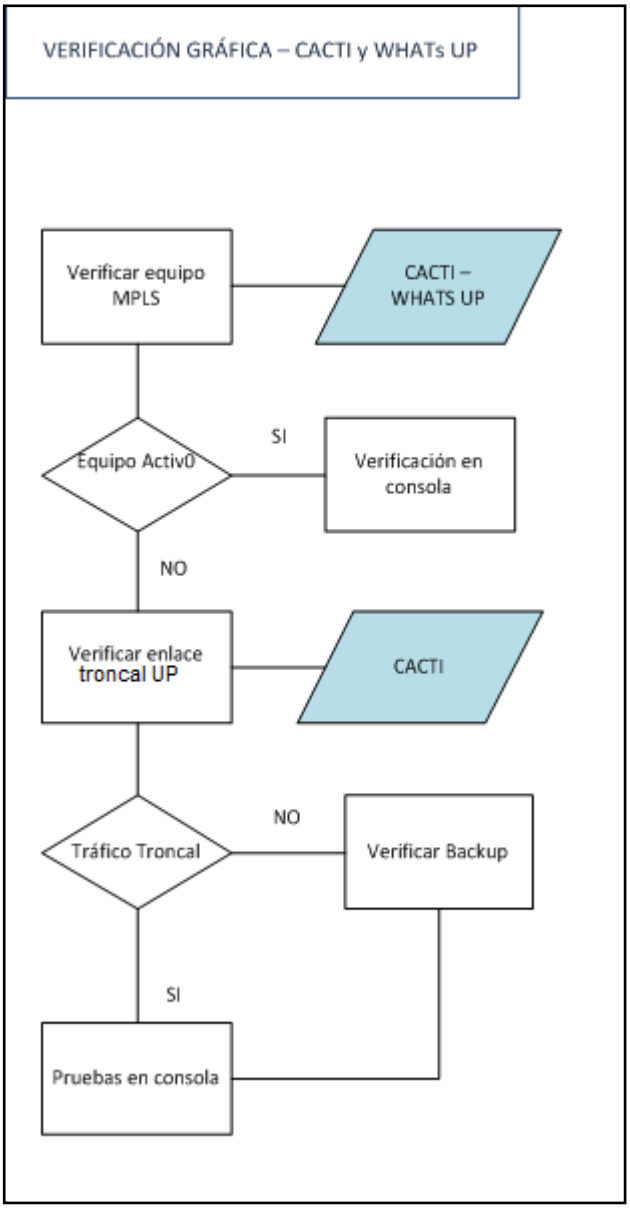


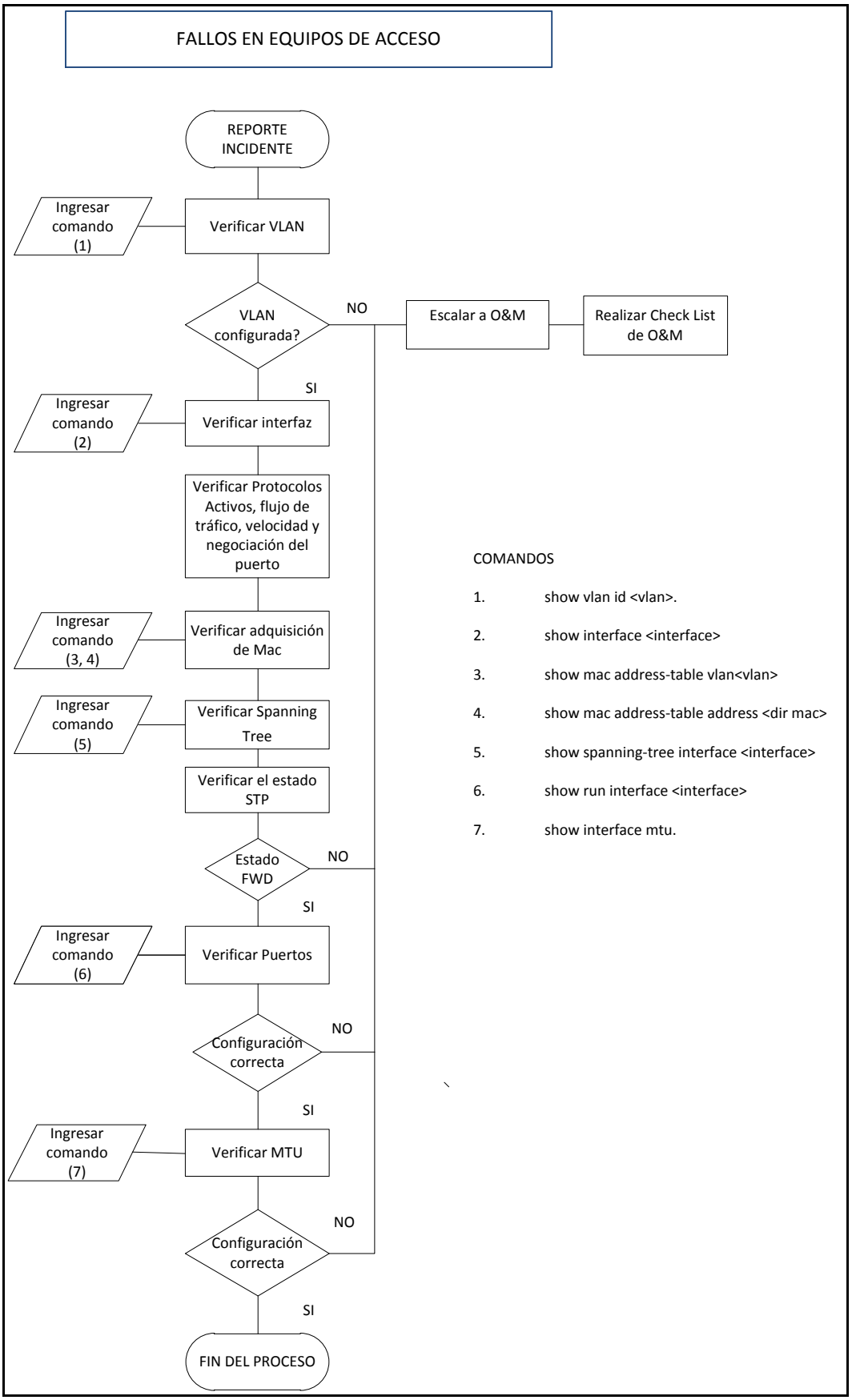
Figura 5.7.31: Spanning Tree

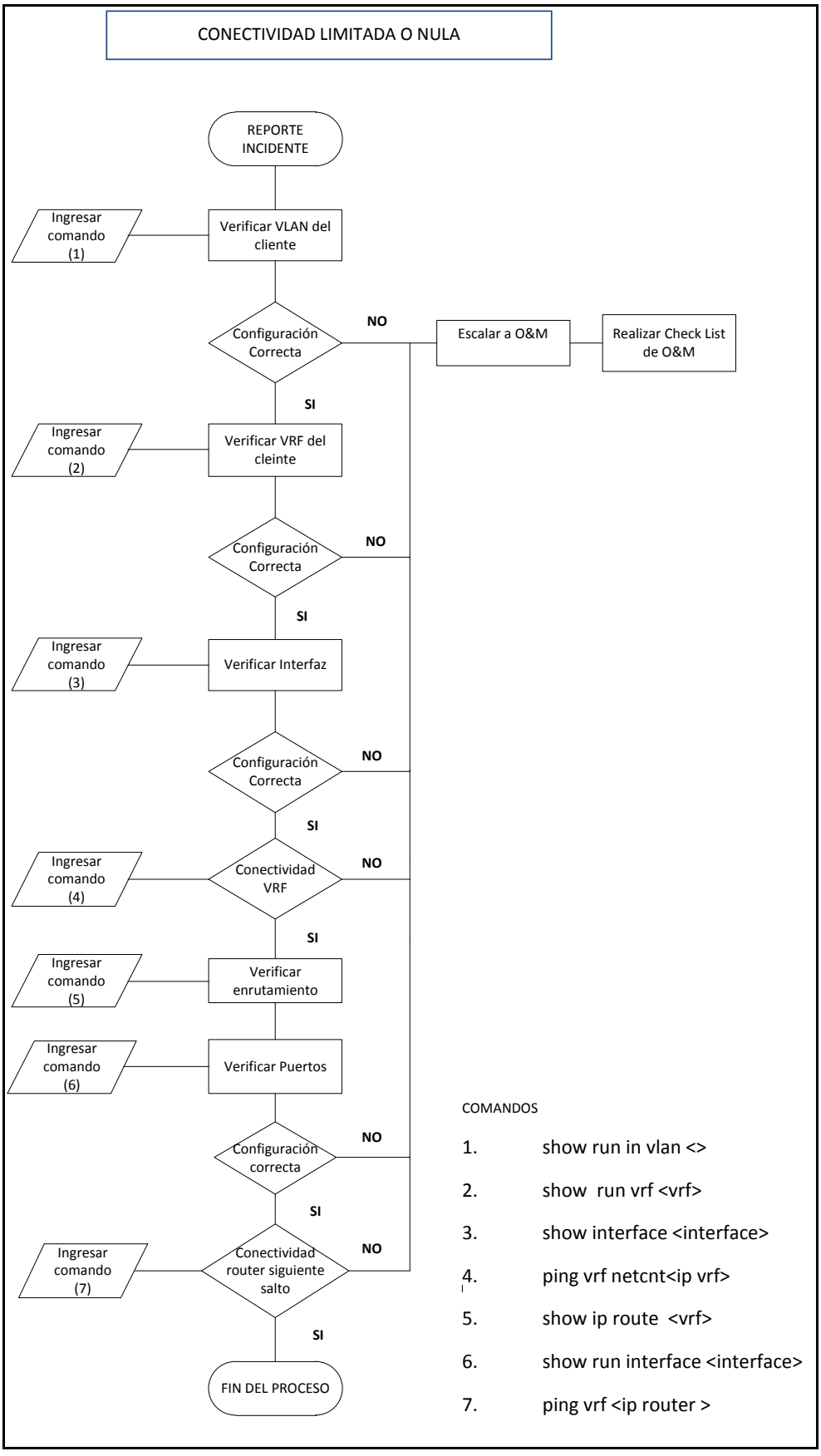
Si en el estado STP cambia de FWD a BLK varias veces escalar a MPLS.

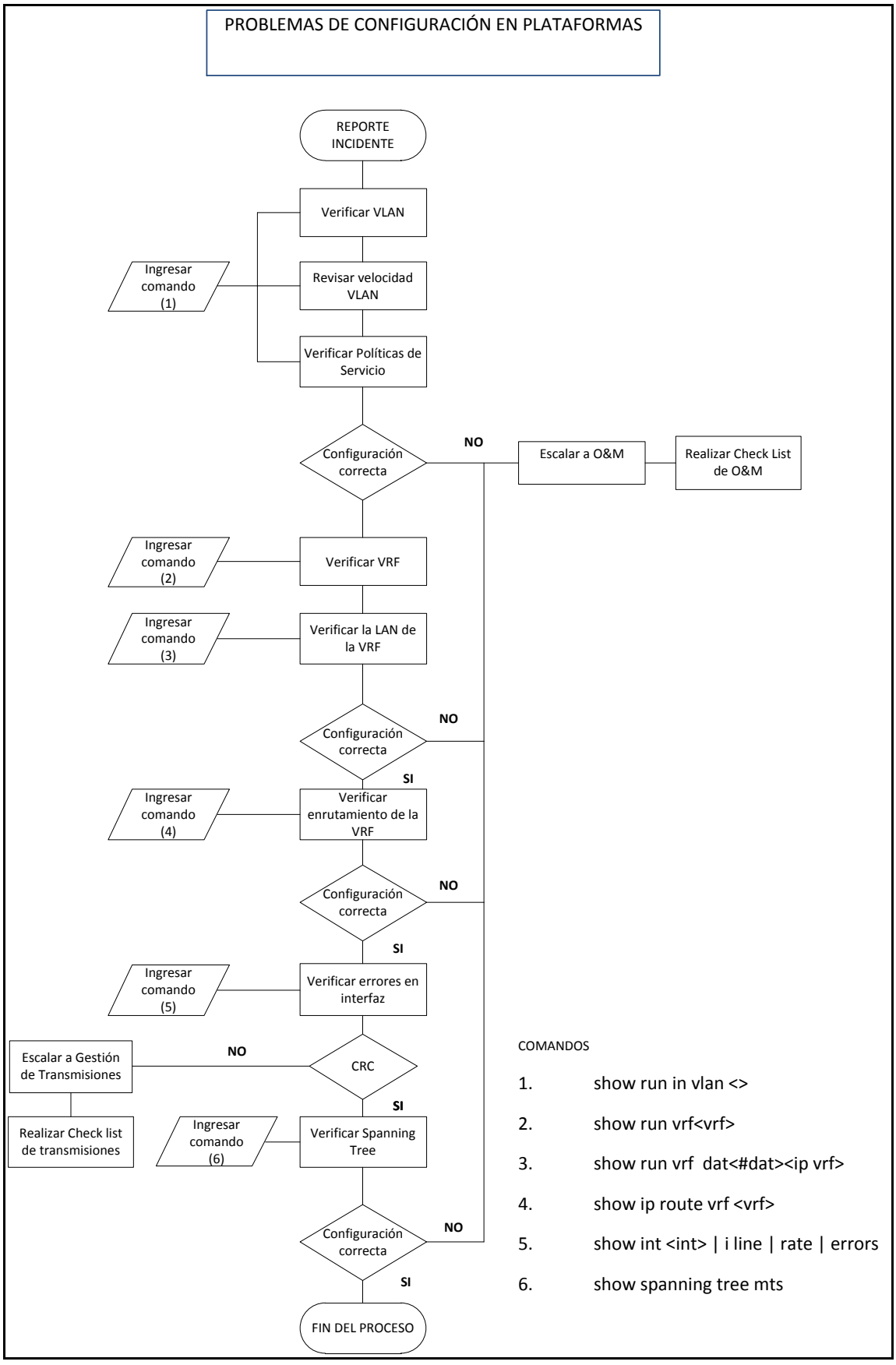
A continuación se presentan los diagramas de flujo de los procesos anteriormente descritos.




VERIFICACIÓN GRÁFICA – CACTI y WHATs UP
Verificar equipo MPLS
CACTI – WHATS UP
Equipo Activ0
SI
Verificación en consola
NO
Verificar enlace troncal UP
CACTI
Tráfico Troncal
NO
Verificar Backup
SI
Pruebas en consola


FALLOS EN EQUIPOS DE ACCESO
REPORTE INCIDENTE
Ingresar comando (1)
Verificar VLAN
VLAN configurada?
NO
Escalar a O&M
Realizar Check List de O&M
SI
Ingresar comando (2)
Verificar interfaz
Verificar Protocolos Activos, flujo de tráfico, velocidad y negociación del puerto
Ingresar comando (3, 4)
Verificar adquisición de Mac
Ingresar comando (5)
Verificar Spanning Tree
Verificar el estado STP
Estado FWD
NO
SI
Ingresar comando (6)
Verificar Puertos
Configuración correcta
NO
SI
Ingresar comando (7)
Verificar MTU
Configuración correcta
NO
SI
FIN DEL PROCESO
COMANDOS
1. show vlan id <vlan>.
2. show interface <interface>
3. show mac address-table vlan<vlan>
4. show mac address-table address <dir mac>
5. show spanning-tree interface <interface>
6. show run interface <interface>
7. show interface mtu.


CONECTIVIDAD LIMITADA O NULA
REPORTE INCIDENTE
Ingresar comando (1)
Verificar VLAN del cliente
Configuración Correcta
NO
Escalar a O&M
Realizar Check List de O&M
SI
Ingresar comando (2)
Verificar VRF del cleinte
Configuración Correcta
NO
SI
Ingresar comando (3)
Verificar Interfaz
Configuración Correcta
NO
SI
Ingresar comando (4)
Conectividad VRF
NO
SI
Ingresar comando (5)
Verificar enrutamiento
Ingresar comando (6)
Verificar Puertos
Configuración correcta
NO
SI
Ingresar comando (7)
Conectividad router siguiente salto
NO
SI
FIN DEL PROCESO
COMANDOS
1. show run in vlan <>
2. show run vrf <vrf>
3. show interface <interface>
4. ping vrf netcnt<ip vrf>
5. show ip route <vrf>
6. show run interface <interface>
7. ping vrf <ip router >


PROBLEMAS DE CONFIGURACIÓN EN PLATAFORMAS
REPORTE INCIDENTE
Verificar VLAN
Ingresar comando (1)
Revisar velocidad VLAN
Verificar Políticas de Servicio
Configuración correcta
NO
Escalar a O&M
Realizar Check List de O&M
Ingresar comando (2)
Verificar VRF
Ingresar comando (3)
Verificar la LAN de la VRF
Configuración correcta
NO
SI
Ingresar comando (4)
Verificar enrutamiento de la VRF
Configuración correcta
NO
SI
Ingresar comando (5)
Verificar errores en interfaz
Escalar a Gestión de Transmisiones
NO
CRC
SI
Realizar Check list de transmisiones
Ingresar comando (6)
Verificar Spanning Tree
Configuración correcta
NO
SI
FIN DEL PROCESO
COMANDOS
1. show run in vlan <>
2. show run vrf<vrf>
3. show run vrf dat<#dat><ip vrf>
4. show ip route vrf <vrf>
5. show int <int> | i line | rate | errors
6. show spanning tree mts

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- MPLS es una tecnología orientada a paquetes con etiquetas IP muy flexible que proporciona la ventaja de poder usar las características de los protocolos de las capas enlace y de red sin ningún tipo de restricción, además permite la implementación de una serie de aplicaciones como Ingeniera de tráfico, QoS, VPNs para de esta manera optimizar el proceso de routing y forwarding dentro de una red.

- Las medidas de seguridad que presta la plataforma ACS son de gran utilidad con lo que respecta al control de acceso de los equipos de la red IP/MPLS así como también para establecer privilegios a cada uno de los administradores de acuerdo a sus requerimientos. El presente manual será de gran ayuda para los administradores ya que les permitirá manejar las herramientas de la plataforma de forma fácil y rápida.

- Las Plataformas de Gestión y Monitoreo son de gran utilidad para organizaciones que poseen una estructura de red bien definida y que requieren establecer comunicación entre usuarios de diferentes sedes ya que por medio de ésta utilidad el administrador de red podrá tener un control sobre todos los dispositivos y servicios que la integran; así como también mantener información actual acerca de diversos sucesos o eventos que se ejecuten dentro de la red y fallas de algún componente de hardware.

- IPsolutionC es una herramienta que permite realizar diversas configuraciones de equipos y usuarios, este manual es de gran utilidad para los administradores ya que proporciona toda la información necesaria para realizar dichas configuraciones de forma fácil y rápida

- Nagios brinda ayuda a los administradores para que puedan tener siempre el control de qué está pasando en la red y conocer los problemas que ocurren en la infraestructura que administran antes de que los usuarios de la misma los perciban, vigila los equipos y servicios que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

- La información contenida en ITIL son esenciales para una eficiente administración de las TI, debido a que proveen a los profesionales de la informática los conocimientos y recursos necesarios para dirigir y mantener una infraestructura tecnológica de forma efectiva, con el objetivo fundamental de cubrir las necesidades de los clientes, mediante la mejor utilización de los recursos disponibles.

- ITIL define las mejores prácticas en la gestión de servicios TI mediante la aplicación de procesos los mismos que tienen que ser implementados, esto implican tiempo, cambio en la cultura de trabajo y requiere soporte, compromiso y disciplina para su adopción, además el personal debe entender, saber y usar la herramienta que los soporta

- La generación de los manuales de usurario de las plataformas de gestión y monitoreo son esenciales para el personal que trabajan en las áreas O&M, Gestión y NOC ya que contienen la información detallada de cada una de estas herramientas para su correcto uso y de esta manera solucionar los problemas de forma eficiente y rápida para dar mayor satisfacción al usuario.

6.2 RECOMENDACIONES

- Es importante que el personal del área de O&M, NOC y GESTIÓN de la Corporación Nacional de Telecomunicaciones actualice de manera periódica cada uno de los manuales de las plataformas de gestión y monitoreo, para que en caso de presentarse algún inconveniente se pueda solucionar de forma rápida y eficaz.

- El área NOC debe realizar correctamente el check list que se ha elaborado en conjunto con el área O&M, el mismo que reúne una serie de procesos para resolver problemas comunes que se presentan a diario en los equipos que conforman la red CNT y como efecto ofrecer una mayor disponibilidad a los usuarios.

REFERENCIAS BIBLIOGRÁFICAS

BIBLIOGRAFÍA CAPITULO UNO

[1] http://www.cnt.gob.ec/

[2] Autores Tesis

BIBLIOGRAFIA CAPITULO DOS

[1]RUBIANO, Gina y URBANO, Humberto, *Investigación de la arquitectura mpls ventajas y servicios,* Tesis Universidad de Los Andes Facultad de Ingeniería Eléctrica y Electrónica, Bogota – Colombia, 2006.

[2] HINOJOSA, Mayra y HERRERA, Fabricio, *Diseño de una red mpls utilizando el protocolo ipv6 para proveedores de servicios de telecomunicaciones,* Tesis *EPN* Facultad de Ingeniería Eléctrica y Electrónica, Quito, julio 2009

[3] BARBERÁ, J., "*Una arquitectura de backbone para la Internet del siglo XXI*", Boletín de RedIRIS, Nº 52. Septiembre 2.000.

[4] CANALIS, María Sol, *MPLS MULTI PROTOCOL LABEL SWITCHING Una Arquitectura de Backbone para la Internet del Siglo XXI,* Trabajo Final de Aplicación, Universidad Nacional del Nordeste Facultad de Ciencias Exactas, Naturales y Agrimensura, Argentina, 2003

[5] BALLESTEROS, Alex y otros, Diseño e Implementación Mediante el Simulador Dynamips de una Red MPLS para la Conexión WAN de una Empresa Mediana con sus Sucursales, ESPOL Facultad de Ingeniería en Electricidad y Computación, Guayaquil – Ecuador, 2007.

[6] http://jedicerocool.blogspot.com/2009/08/mpls.html]

[7] MORALES, Luis, *Investigación de Redes VPN con Tecnología MPLS,* Universidad de las Américas Puebla Escuela de Ingeniería y Ciencias Departamento de Computación, Electrónica, Física e Innovación, Cholula, Puebla- México a 16 de mayo de 2006.

[8] http://dspace.ups.edu.ec/bitstream/123456789/209/3/Capitulo%202.pdf, p. 5.

[9] http://sx-de-tx.wikispaces.com/MPLS-FDDI (grafico cabecera)

[10] JAMOUSSI, B., Otros, "*Constraint-Based LSP Setup using LDP*", RCF 3212. Enero 2.002.

[11] GONZÁLEZ, Agustín, *Multi-Protocol Label Switching,* University of Maryland Dept. of Computer Science.

[12] http://www.slideshare.net/ing.adolfo/gestion-de-redes

[13] DOMINGUEZ, José, *Infraestructura de Gestión de Red,* Universidad de Oregón

[14] CASARES, Diana, Gestión de Red, Octubre, 2001, p 18

[15]http://www.gleijah.com/archivos/9_Admon%20de%20redes.pdf

[16] GARCÍA, Adolfo, *Gestión TMN Telecomunications Management Network,* version 1.0, www.ccapitalia.net/netica

BIBLIOGRAFÍA CAPÍTULO TRES

[1]http://es.scribd.com/doc/53123700/GESTION-Y-MONITOREO PLATAFORMAS- LINUX-WINDOWS-38110

[2] http://www.slideshare.net/magicdrums/presentacion-de-nagios

[3] http://nagios.sourceforge.net/download/contrib/documentation/misc/

Nagios_spanish.pdf

[4]http://www.desarrolloweb.com/de_interes/nagios-completo-servicio-monitoreo-web-4085.html

[5] http://rm-rf.es/cacti-monitorizacion-grafica-de-redes-y-servidores/

[6] http://ws.edu.isoc.org/data/2009/16360680324ac60486606cb/cacti.pdf

[7] http://www.cacti.net

[8] http://forums.cacti.net/

[9] http://ciscosystems.com/

[10] http://www.cisco.com/en/US/products/ps6776/index.html

[11] Cisco 2011, Advanced Services' Cisco Active Network Abstraction (ANA-Operations Training Version 3.7

[12] Cisco 2009, IP Solution Center 5.2 Product Training

[13] http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

BIBLIOGRAFÍA CAPITULO CUATRO

[1] http://www.osiatis.es/

[2] http://www.ieee.org.ar/downloads/2006-hrabinsky-itil.pdf

[3] http://www.cybertesis.cl/tesis/uchile/2006/donoso_f/sources/donoso_f.pdf

[4] http://1180.wikispaces.com/file/view/ITIL+para+FCA+Informatica.pdf

[5] http://www.manageengine.com/products/service-desk/spanish-libro-v2.pdf-

BIBLIOGRAFÍA CAPITULO CINCO

[1] Autores Tesis

ANEXOS

PERDIDA DE PAQUETES POR INTERMITENCIA DE ENLACES

ENLACE

ORIGEN	DESTINO

PROBLEMA:

NODO		RUTA		NODOS INTERMEDIOS	
INTERFAZ FÍSICA		TRANSMISIÓN			
INTERFAZ LÓGICA					

REVISION DE HERRAMIENTAS DE MONITOREO:

☐	CACTI BACKBONE (172.16.19.152)	Novedades	
☐	ANA	Novedades	

REVISIÓN A NIVEL FÍSICO MEDIANTE COMANDOS DE LINEA:

							COMANDO
☐	Ingresar al equipo revisar estado de la interface	Status	UP	☐	Protocol	UP ☐	show interface
			DOWN	☐		DOWN ☐	
		Autonegotation		☐			
		Full Duplex		☐			
		Control de Flujo		☐			
		CRC					
☐	Medir niveles de potencia	Pin			Pout		sh int giga1/1 transceiver
☐	Extraer el log del equipo						show logging
☐	Comprobar Conectividad L2						cdp neighbors

REVISIÓN A NIVEL LÓGICO:

☐	Verificar status del spannig tree	Status	FWD	☐	show spannig-tree mst1
			BLK	☐	
☐	Revisar flaping a nivel mac				show mac-address table
☐	Verificar conexión		Ping WAN	☐	
			Ping VRF	☐	

CONECTIVIDAD LIMITADA O NULA (CLIENTES CORPORATIVOS)

ENLACE

ORIGEN	DESTINO

NOMBRE DEL CLIENTE CORPORATIVO _____

PETICIÓN/# SERVICIO _____

AB CONTRATADO _____

Se dispone de Ingeniería del Cliente — SI ☐ NO ☐

NODO		RUTA		NODOS INTERMEDIOS	
EQUIPO DE UK					
INTERFAZ FÍSICA		TRANSMISIÓN			
INTERFAZ LÓGICA					

REVISION DE HERRAMIENTAS DE MONITOREO:

☐	CACTI BACKBONE (172.16.19.152)	Novedades
☐	CACTI DE ACCESO (10.10.30.14/cacti)	Novedades

REVISIÓN A NIVEL FÍSICO MEDIANTE COMANDOS DE LINEA:

							COMANDO
☐	Ingresar al equipo revisar estado de la interface	Status	UP	☐	Protocol	UP ☐	show interface
			DOWN	☐		DOWN ☐	
		Autonegotation		☐			
		Full Duplex		☐			
		Control de Flujo		☐			
		CRC					
☐	Medir niveles de potencia	Pin			Pout		sh int giga1/1 transceiver
☐	Extraer el log del equipo						show logging
☐	Comprobar Conectividad L2						cdp neighbors

REVISIÓN A NIVEL LÓGICO:

☐	Verificar status del spannig tree	Status	FWD	☐	show spannig-tree mst1
			BLK	☐	
☐	Revisar flaping a nivel mac				show mac-address table
☐	Verificar conexión		Ping WAN	☐	
			Ping VRF	☐	

FALLA DE EQUIPOS DE ACCESO

PROBLEMA:

NOMBRE EQ ACCESO		RUTA		NODOS INTERMEDIOS	
NODO DE INTERCON					
INTERFAZ FÍSICA		TRANSMISIÓN			
INTERFAZ LÓGICA					

REVISION DE HERRAMIENTAS DE MONITOREO:

☐	CACTI BACKBONE (172.16.19.152)	Novedades	
☐	CACTI DE ACCESO (10.10.30.14/cacti)	Novedades	

REVISIÓN A NIVEL FÍSICO MEDIANTE COMANDOS DE LINEA:

							COMANDO
☐	Ingresar al equipo revisar estado de la interface	Status	UP	☐	Protocol	UP	☐ show interface
			DOWN	☐		DOWN	☐
		Autonegotation		☐			
		Full Duplex		☐			
		Control de Flujo		☐			
		CRC					
☐	Medir niveles de potencia	Pin			Pout		sh int giga1/1 transceiver
☐	Extraer el log del equipo						show logging
☐	Comprobar Conectividad L2						cdp neighbors

REVISIÓN A NIVEL LÓGICO:

☐	Verificar status del spannig tree	Status	FWD	☐	show spannig-tree mst1
			BLK	☐	
☐	Revisar fallos a nivel mac				show mac-address table
☐	Verificar conexión		Ping DSLAM	☐	
☐	Revisión VLAN y MTU				show vlan id
☐	Configuración de Puerto		Acceso	☐	show running-interface
			Troncal	☐	

PROBLEMAS DE CONFIGURACIÓN DE PLATAFORMAS

ENLACE

ORIGEN	DESTINO

NODO		RUTA		NODOS INTERMEDIOS	
EQUIPO DE UK					
INTERFAZ FÍSICA		TRANSMISIÓN			
INTERFAZ LÓGICA					

REVISION DE HERRAMIENTAS DE MONITOREO:

☐	CACTI BACKBONE (172.16.19.152)	Novedades	
☐	CACTI DE ACCESO (10.10.30.14/cacti)	Novedades	
☐	CONCURRENCIA CACTI	Novedades	
☐	SALIDAS INTERNACIONALES	Novedades	

REVISIÓN A NIVEL FÍSICO MEDIANTE COMANDOS DE LINEA:							COMANDO
☐ Ingresar al equipo revisar estado de la interface	Status	UP	☐	Protocol	UP	☐	show interface
		DOWN	☐		DOWN	☐	
	Autonegotation		☐				
	Full Duplex		☐				
	Control de Flujo		☐				
	CRC						
☐ Medir niveles de potencia	Pin			Pout			sh int giga1/1 transceiver
☐ Extraer el log del equipo							show logging
☐ Comprobar Conectividad L2							cdp neighbors

REVISIÓN A NIVEL LÓGICO:				
☐ Verificar status del spannig tree	Status	FWD	☐	show spannig-tree mst1
		BLK	☐	
☐ Revisar flaping a nivel mac				show mac-address table
☐ Verificar conexión		Ping WAN	☐	
		Ping VRF	☐	
☐ Revisión VLAN 201 Fast Boy Normal			☐	show vlan id
☐ Revisión VLAN 202 Fast Boy ip fija			☐	show vlan id