PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR
FACULTAD DE INGENIERIA
MAESTRIA EN REDES DE COMUNICACIONES

"DESARROLLO DE PROCEDIMIENTOS PARA UN MODELO DE GESTION DE RENDIMIENTO DE LA RED PARA EL EQUIPAMIENTO DE COMUNICACIONES DE LA PLATAFORMA DE ISP DE LA CNT EP"

CELLERI LOPEZ GERMAN ALBERTO

Trabajo previo a la obtención del Título de
Magister en Redes de Comunicaciones

QUITO, AGOSTO 2015

Contenido

1 CAPÍTULO 1.-SITUACION ACTUAL DE LA RED DE COMUNICACIONES DEL ISP DE LA CNT EP 1
1.1 Arquitectura de Red 1
1.2 Equipos, funciones y especificaciones 7
1.2.1 Equipos 7
1.2.2 Funciones 7
1.2.3 Especificaciones 9
1.3 Redundancia 21
1.4 Necesidad de una Gestión del Rendimiento del ISP 22
2 CAPÍTULO 2: KPI DE RENDIMIENTO DE EQUIPOS DE COMUNICACIONES DEL ISP CNT EP 24
2.1 Modelos de Gestión de Red 24
2.1.1 Modelo de Gestión de Red OSI (ISO) 25
2.1.2 Modelo de Gestión de Red Internet (SNMP) 28
2.2 Herramientas de monitoreo del Rendimiento de Red 32
2.2.1 Características requeridas de una Herramienta de Gestión de Red 34
2.2.2 Herramienta PRTG 35
2.3 Revisión y obtención de los principales indicadores por equipo 43
2.3.1 Indicadores de Rendimiento (Performance) de RED 49
2.4 Definición de los KPI de Rendimiento 68
3 CAPITULO 3: PROCESO DE GESTION DE RENDIMIENTO 78
3.1 INTRODUCCION A PROCESOS 78
3.1.1 Definición de Proceso 78
3.1.2 Descripción del Proceso 79
3.2 Estructura Organizacional de la CNT EP 80
3.3 Definición y elaboración de los procesos 82
4 CAPÍTULO 4: EJERCICIO PRÁCTICO 87
4.1 Obtención de los KPI en el equipo de Borde en tiempo real. 87
4.1.1 KPI LAT (LATENCIA) 89
4.1.2 KPI JIT (JITTER) 91
4.1.3 KPI ABTOT (ANCHO DE BANDA TOTAL, VELOCIDAD) 92
4.1.4 KPI CPU (CARGA DEL CPU) 94
4.1.5 KPI DISP (DISPONIBILIDAD) 95
4.1.6 KPI PDOUT (DESCARTE DE PAQUETES SALIENTES) 96

4.2 Aplicación de los procesos de Gestión de Rendimiento. 98
4.3 Análisis de los resultados obtenidos 103
5 CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES 106
5.1 Conclusiones 106
5.2 Recomendaciones 109
6 BIBLIOGRAFIA 111

1 CAPÍTULO 1.-SITUACION ACTUAL DE LA RED DE COMUNICACIONES DEL ISP DE LA CNT EP

1.1 Arquitectura de Red

El esquema indicado en la Fig.1 fue implementado en el área de ISP de la CNT EP[1]luego de un trabajo en conjunto con las áreas técnicas de operación y mantenimiento e ingeniería, con la finalidad de mejorar la disponibilidad de los servicios y en base a modelos de arquitecturas propuesto por CISCO proveedor de la mayoría del equipamiento de la red de comunicaciones del ISP.

CISCO maneja un modelo jerárquico que consta de 3 capas y para cada una de ellas se definen funciones, permitiendo así poder aplicar de una manera ordenada configuraciones en la red. Cada capa, si bien tiene funciones específicas asignadas, no necesariamente están separadas de manera física sino también de manera lógica, esto permite mantener diferentes equipos en una sola capa o un equipo haciendo las funciones de más de una de las capas.

Para CISCO las funciones de cada capa se resumen de la siguiente manera [7][1] :

- Capa de Acceso: se la conoce también como capa de conmutación (switching), permite la conexión a los equipos finales, controlando la comunicación entre ellos en la red, provee conectividad sin comprometer la integridad de la red. En esta capa de acceso pueden operar equipos como routers, switches o puntos de acceso inalámbrico.

[1] Referencia bibliográfica [7] (CISCO, 2010), ver al final del documento

- Capa de Distribución: Recibe y añade la información que envían los equipos de la capa de acceso antes de trasmitirlos a la capa núcleo, controla el flujo de tráfico en la red (hace más eficiente la utilización del ancho de banda) con el uso de políticas basadas en control del tráfico, facilita ruteo, filtrado, define dominios de broadcast para realizar el enrutamiento entre las VLAN definidas en la capa de acceso.
- Capa Núcleo: se la considera como backbone donde de añade el tráfico de todos los equipos de la capa distribución, maneja gran cantidad de tráfico de manera confiable y veloz. La función principal en esta capa es el conmutar tráfico.

En la Fig. 1.1-1 se muestra el Diagrama de la red de comunicaciones del ISP, el cual tiene un esquema de capas (por temas de seguridad de la información se presenta con nombres genéricos y no se incluye direccionamiento IP),

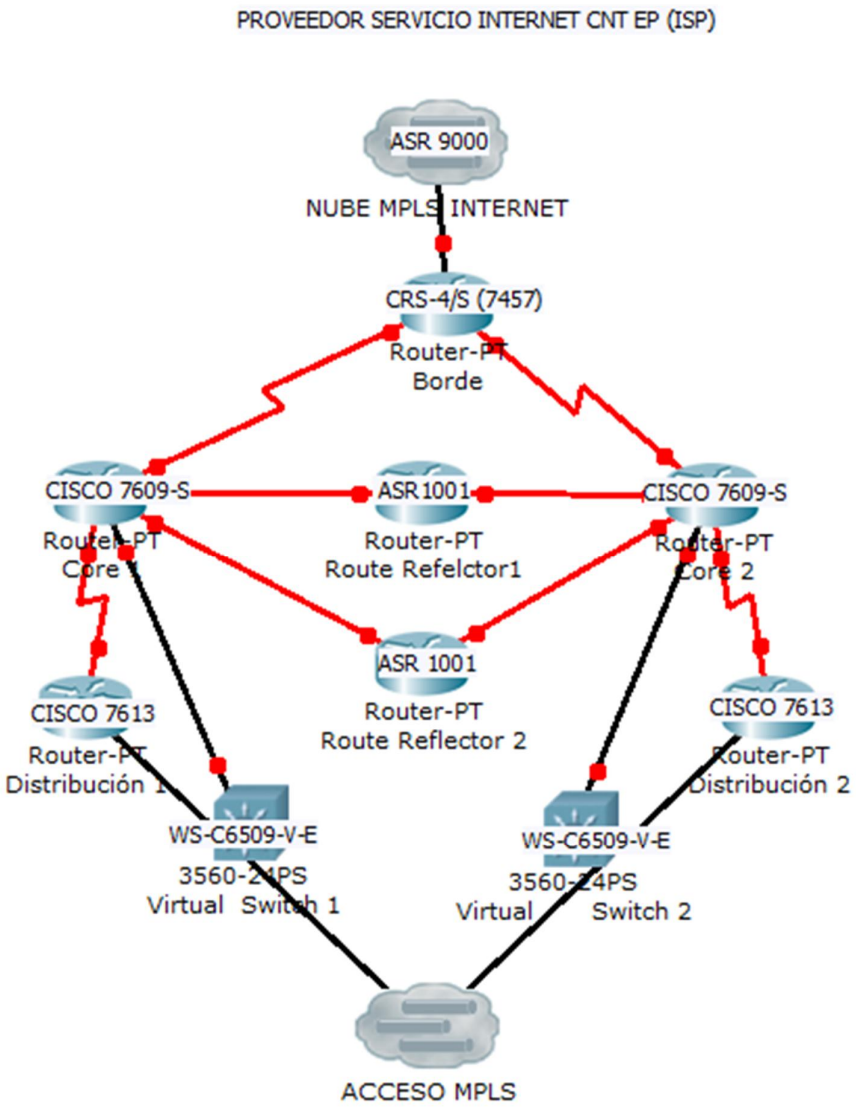

Fig. 1.1-1 Diagrama de la red de comunicaciones del ISP.

Como se puede observar en la gráfica, el ISP de la CNT EP se encuentra operando en un esquema de 3 capas, similar a un esquema de CISCO pero de manera personalizada:

- BORDE: Esta capa se encarga de enviar y recibir el tráfico de Internet hacia el backbone de Internet. Permite interconectar indirectamente al ISP hacia la red Internet de los proveedores denominados Tier1[2], los cuales son proveedores de conectividad hacia el backbone mundial de Internet. En esta capa se configura E-BGP para comunicarse con el sistema autónomo del backbone de Internet.
- CORE: Esta capa concentra todos los servicios que brinda ISP tales como hosting, correo electrónico, internet, caché, DNS. También concentra todo el tráfico de Internet que no se queda en la capa de acceso para el envío hacia la capa de borde. En esta capa se configura I-BGP para comunicarse entre equipos con el sistema autónomo del ISP.
- DISTRIBUCIÓN: esta capa es semejante a la capa de acceso en CISCO, concentra el acceso de las redes de los clientes corporativos y masivos. En esta capa se recibe el tráfico de las denominadas VRF (enrutamiento virtual y reenvío), lo cual permite múltiples instancias de una tabla de enrutamiento para coexistir en el mismo router, debido a que las instancias de enrutamiento son independientes, se pueden utilizar sin entrar en conflicto entre sí, direcciones IP comunes. En esta capa se configura I-BGP para comunicarse entre equipos internos del sistema autónomo del ISP.

[2] En la estructura jerárquica de Internet, es el nivel mas alto de proveedores ISP, disponen de backbone de internet a nivel mundial y se interconectan entre ellos (peering)

Para la comunicación entre los equipos del ISP se utiliza también el protocolo IS- IS , el cual permite ver las loopbacks y wan´s entre los mismos equipos, estableciendo conexiones entre ellos y de esa manera configurar BGP entre los equipos hacia los Router Reflectors y viceversa. Para el balanceo de tráfico se configuran métricas.

El ISP de la CNT EP tiene registrado el sistema autónomo público en LACNIC el cual es exclusivo y permite que pueda ser identificado entre los diferentes sistemas autónomos a nivel mundial. El sistema autónomo sirve también para administración del equipamiento interno del ISP y el tráfico del mismo.

Los denominados sistemas autónomos o AS[3]se interconectan con protocolos de encaminamiento externo como BGPV4[4] anunciando prefijos de red entre AS´s dependiendo de una política de encaminamiento. La política de encaminamiento o "routing policy" es la decisión del AS de anunciar la red a otro AS y es el privilegio del otro AS el aceptar la información de encaminamiento de forma que pueda transitar el flujo de tráfico.

El ISP de la CNT EP maneja una configuración de escalabilidad en BGP la cual se conoce como Reflectores de rutas ó "Route Reflectors", en estos equipos se propagan rutas aprendidas de un I-BGP a un I-BGP vecino reduciendo el número de sesiones BGP TCP en el AS. El reflector de rutas propaga una ruta a todos los equipos internos del ISP independientemente si estos están física o lógicamente conectados.

[3] conjunto de routers con una misma política de enrutamiento dentro de un único dominio administrativo
[4] protocolo de encaminamiento basado en políticas, usa TCP como transporte de mensajes BGP

También dentro de la arquitectura del ISP se tiene un esquema VSS o Virtual Switching System el cual es un sistema en cluster que utiliza dos switches de hardware común que actúan como un solo elemento de red compartiendo la información de control y tráfico de datos. Para lograr que los equipos funcionen como uno solo se configura VSL ó Virtual Switch Link, el cual es un vínculo que lleva el control y tráfico de datos entre los dos switches. El VSL se implementa como un Ether Channel también conocido como un port channel, el cual es un agrupamiento de dos ó más interfaces o enlaces físicos que se combinan para formar un enlace lógico. Las conexiones redundantes entre los dos chasis se realizan usando tarjetas independientes.

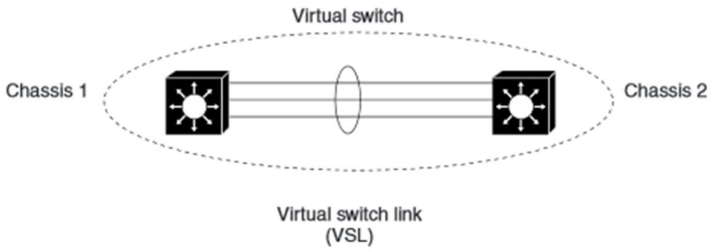

Fig. 1.1-2 VSS y VSL.

En la Fig. 1.1-1 se puede observar también nubes las cuales se detalla a continuación:

- Nube MPLS Internet: esta nube contiene equipos que llevan el tráfico hacia el Backbone de Internet el cual es administrado por el área de TX-MPLS de la CNT EP. A esta nube se interconecta el equipo de BORDER del ISP.

- Acceso MPLS: esta nube hace referencia al conjunto de equipos geográficamente distribuidos a nivel local y nacional, e interconectados mediante una red MPLS para permitir acceso a internet a los clientes masivos y corporativos a los cuales brinda servicio el ISP de la CNT EP.

1.2 Equipos, funciones y especificaciones

1.2.1 Equipos

En la Fig.1.2.1-1 se muestra el listado de los equipos que conforman el diagrama de la Fig. 1.1-1 .

NOMBRE	MODELO	MARCA
Borde	CRS-4/S	CISCO
Core 1	7609-S	CISCO
Core 2	7609-S	CISCO
Route Reflector 1	ASR1001	CISCO
Route Reflector 1	ASR1001	CISCO
Distribución 1	7613	CISCO
Distribución 2	7613	CISCO
Virtual Switch 1	WS-C6509-V-E	CISCO
Virtual Switch 2	WS-C6509-V-E	CISCO

Fig. 1.2.1-1 Listado de equipos de la red de comunicaciones del ISP.

1.2.2 Funciones

En ISP se implementó una ingeniería por capas, en este caso se aplicó un modelo de 3 capas y cada una cumple una función específica. El equipamiento fue colocado en cada una de ellas en base a un estudio de la capacidad de procesamiento, cantidad de interfaces físicas, protocolos que se puede aplicar, volumen de tráfico que soporta cada uno de ellos.

EQUIPO DE BORDE: La función que realiza este equipo dentro del ISP es llevar y

traer el tráfico de internet desde o hacia la nube MPLS Internet a las capas inferiores. En la capa inferior de Core están los servidores de caché que discriminan tráfico de internet local utilizando algoritmos en sus bases de datos,

El equipo de Borde se conecta con otro router en la nube MPLS Internet, éste equipo cumple la función de interconectar el tráfico de Internet que viene del ISP con los equipos de backbone de Internet MPLS los cuales encaminan el tráfico por los diferentes Tier1.a los que se interconecta CNT EP.

EQUIPO DE CORE: La función de este equipo en el ISP es la de concentrar todo el tráfico que viene desde las capas inferiores o los equipos de borde para que de acuerdo a la configuración de los protocolos de enrutamiento BGP e ISIS distribuya el tráfico al borde o a los equipos de distribución de manera balanceada.

Otra de las funciones del equipo del CORE es conectar los servicios que brinda el ISP tales como: Hosting, Correo electrónico, DNS, Monitoreo.

Una función importante del equipo de CORE es la de conectar los enlaces de transmisión que proveen redundancia entre Quito y Guayaquil a nivel del ISP.

EQUIPOS DE DISTRIBUCIÓN: La función de estos equipos es la de concentrar todo el tráfico de Internet de los clientes masivos y corporativos.

En estos equipos se aplican políticas dedicadas a nivel del cliente, por ejemplo bloqueo de puertos. Es una recomendación hacer el bloqueo a nivel más cercano del cliente, para que no afecte el tráfico en las capas superiores de la red.

ROUTE RELECTOR: la función de estos equipos es la aprender y distribuir rutas o redes a través de BGP e ISIS.

VIRTUAL SWITCH: la función de estos equipos es la de conectar directamente los servicios de valor agregado que brinda el ISP, es parte del CORE.

1.2.3 Especificaciones

A continuación se detalla las especificaciones básicas generales de los equipos de borde, core, distribución, route reflector, virtual switch, entre ellas: Versión software, Protocolos que soporta el equipo de acuerdo a la versión de software, tarjetas, puertos, ranuras, memoria, rendimiento, las MIB, interfaces de gestión para el equipo, características de energía que se deben tomar en cuenta para encender este equipo y sus condiciones ambientales.

BORDE CRS-4/S CISCO	
Característica	**Descripción**
Versión software	Cisco IOS XR Software, Version 4.1.2[Default]
Protocolos	• Protocolo de descubrimiento de Cisco
	• IPv4 e IPv6
	• Protocolo de mensajes de control de Internet (ICMP)
	• Border Gateway Protocol versión 4 (BGPv4)
	• Open Shortest Path First versión 2 (OSPFv2)
	• OSPFv3
	• Sistema Intermedio a Sistema Intermedio (IS-IS)
	• Protocolo de administración de grupos de Internet (IGMP) versiones 1, 2 y 3
	• multiprotocolo BGP (MBGP)
	• Multicast Source Discovery Protocol (MSDP)
	• conmutación de etiquetas multiprotocolo (MPLS)
	• MPLS protocolo de distribución de etiquetas (LDP)
	• Protocolo de reserva de recursos (RSVP)
	• Servicios diferenciados (DiffServ) ingeniería de tráfico sea conscientes
	• plano de control MPLS Ingeniería de Tráfico (RFC 2702 y 2430)
	• Enrutamiento de Política Lingüística (RPL)

	• Gestión
	• Simple Network Management Protocol (SNMP)
	• interfaces de programación (lenguaje de marcado extensible [XML])
	• Seguridad
	• Mensaje DigestAlgorithm 5 (MD5)
	• Protocolo (IPsec) de seguridad IP
	• Secure Shell Protocolo (SSHv2)
	• FTP seguro (SFTP)
	• Secure Sockets Layer (SSL)
Tarjetas, puertos y ranuras	2 Management Ethernet
	12 WANPHY controller(s)
	12 TenGigE
	1019k bytes of non-volatile configuration memory.
	34338M bytes of hard disk.
	2053440k bytes of disk0: (Sector size 512 bytes).
Memoria	4 GB
Throughput	1,12 Tbps
MIB QUE SOPORTA EL EQUIPO	SNMP frameworksupport
	• SNMPv1
	• SNMPv2c
	• SNMPv3
	• MIB II, including interface extensions (RFC 1213)
	• SNMP-FRAMEWORK-MIB
	• SNMP-TARGET-MIB
	• SNMP-NOTIFICATION-MIB
	• SNMP-USM-MIB
	• SNMP-VACM-MIB
	Systemmanagement
	• CISCO- BULK-FILE-MIB
	• CISCO-CONFIG-COPY-MIB
	• CISCO-CONFIG-MAN-MIB
	• CISCO-FLASH-MIB
	• CISCO-MEMORY-POOL-MIB
	• Cisco FTP Client MIB
	• Cisco Process MIB
	• Cisco Syslog MIB
	• CISCO-SYSTEM-MIB
	• CISCO-CDP-MIB
	• IF-MIB (RFCs 2233 and 2863)
	Chassis
	• ENTITY-MIB (RFC 2737)

	• CISCO-entity-asset-MIB
	• CISCO-entity-sensor-MIB
	• CISCO-FRU-MIB (Cisco-Entity-FRU-Control-MIB)
	Fabric MIB
	• CISCO-Fabric-HFR-MIB
	• CISCO-Fabric-Mcast-MIB
	• CISCO-Fabric-Mcast-Appl-MIB
	Routingprotocols
	● BGP4-MIB Version 1
	● OSPFv1MIB (RFC 1253)
	• CISCO-IETF-IP-FORWARDING-MIB
	• IP-MIB (was RFC2011-MIB)
	• TCP-MIB (RFC 2012)
	• UDP-MIB
	• CISCO-HSRP-EXT-MIB
	• CISCO-HSRP-MIB
	• CISCO-BGP-POLICY-ACCOUNTING-MIB
	QoS
	• MQC-MIB (Cisco Class-Based QoS MIB)
	• CISCO-PING-MIB
	Traps
	• RFC 1157
	• Authentication
	• Linkup
	• Linkdown
	• Coldstart
Gestión de redes	• Mejora de la CLI
	• Interfaz XML
	• Cisco CIT
	• Soporte SNMP y MIB
Energía	• Consumo máximo de energía cuando el chasis está totalmente configurado con tarjetas de línea con el tráfico de reproducción: 2551W
	• Fuente de alimentación del chasis Capacidad de salida máxima: 4 kW, tanto para la fuente de alimentación de CC y la fuente de alimentación de CA
Condiciones ambientales	Temperatura de almacenamiento: de -40 a 158 ° F (-40 a 70 ° C)
	Temperatura de funcionamiento:
	• Normal: 41 a 104 ° F (5 a 40 ° C)
	• A corto plazo: 23 a (-5 a 50 ° C) 122 ° F
	Humedad relativa:

	• Normal: 5 a 85 por ciento
	• Corto plazo: del 5 al 90 por ciento, pero que no exceda 0,024 kg de agua por kg de aire seco
	Nota: A corto plazo se refiere a un período de no más de 96 horas consecutivas y un total de no más de 15 días a 1 año. (Se refiere a un total de 360 horas en un año determinado, pero no más de 15 apariciones durante ese período de 1 año.)

Fig. 1.2.3-1 1. Especificaciones Básicas del equipo de Borde

CORE 7609-S CISCO	
Característica	
Versión software	Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVIPSERVICESK9-M), Version 15.2(1)S2, RELEASE SOFTWARE (fc1)
Protocolos	CDP
	• IPv4 e IPv6
	• ICMP
	• Border Gateway Protocol versión 4 (BGPv4)
	• Open Shortest Path First versión 2 (OSPFv2)
	• OSPFv3
	• Sistema Intermedio a Sistema Intermedio (IS-IS)
	• Multicast Source Discovery Protocol (MSDP)
	• conmutación de etiquetas multiprotocolo (MPLS)
	• MPLS protocolo de distribución de etiquetas (LDP)
	• Protocolo de reserva de recursos (RSVP)
	• Servicios diferenciados (DiffServ) ingeniería de tráfico sea conscientes
	• plano de control MPLS Ingeniería de Tráfico (RFC 2702 y 2430)
	• Enrutamiento de Política Lingüística (RPL)
	• Gestión
	• Simple Network Management Protocol (SNMP)
	• interfaces de programación (lenguaje de marcado extensible [XML])
	• Seguridad
	• Mensaje DigestAlgorithm 5 (MD5)
	• Protocolo (IPsec) de seguridad IP
	• Secure Shell Protocolo (SSHv2)

	• FTP seguro (SFTP)
	• Secure Sockets Layer (SSL)
Tarjetas, puertos y ranuras	48 CEF720 48 port 1000mb SFP
	48 CEF720 48 port 1000mb SFP
	2 RouteSwitchProcessor 720 (Active)
	2 RouteSwitchProcessor 720 (Hot)
	0 4-subslot SPA Interface Processor-200
	48 CEF720 48 port 10/100/1000mb Ethernet
Memoria	40 Gb
Throughput	720 Gbps
MIB QUE SOPORTA EL EQUIPO	sysUpTime.0
	Interfaces
	Ip
	ipForward
	ipTrafficStats
	mplsLsrStdMIB
	mplsLdpStdMIB
	Ospf
	ospfTrap
	Bgp
	dot1dBridge
	ifMIB
	nhrpMIB
	ipMRouteStdMIB
	igmpStdMIB
	pimMIB
	msdpMIB
	ciscoPingMIB
	ciscoIpSecFlowMonitorMIB
	ciscoIpSecPolMapMIB
	ciscoPimMIB
	ciscoBgp4MIB
	ciscoIfExtensionMIB
	ciscoEigrpMIB
	ciscoCefMIB
	ciscoBridgeDomainMIB
	ciscoNhrpExtMIB
	ciscoIpMRouteMIB
	ciscoIPsecMIB
	mplsLdpMIB
	Cospf

	ciscoExperiment.101
	ciscoIetfIsisMIB
	ciscoIetfBfdMIB
	snmpTrapOID.0
	snmpMIB.1.4.3.0
	snmpTraps.3
	snmpTraps.4
Gestión de redes	• Mejora de la CLI
	• Interfaz XML
	• Cisco CIT
	• Soporte SNMP y MIB
Energía	-208 to 240 VAC (recommended)
	-48 to -60 VDC (4000 WAC supplies require 30A input circuits)
Condiciones ambientales	● Temperatura de funcionamiento : de 32 a 104 ° F (0 a 40 ° C)
	● Temperatura de almacenamiento : -40 a 167 ° F (-40 a 75 ° C)
	● Humedad rela□va: 10 a 90% , sin condensación
	● Cumplimiento de norma□vas

Fig. 1.2.3-2. Especificaciones Básicas del equipo de Core

DISTRIBUCIÓN 7613	
Característica	
Versión software	Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVENTERPRISEK9-M), Version 15.3(1)S, RELEASE SOFTWARE (fc1)
Protocolos	• Protocolo de descubrimiento de Cisco
	• IPv4 e IPv6
	• Protocolo de mensajes de control de Internet (ICMP)
	• Capa 3 protocolos de enrutamiento, incluyendo:
	• Border Gateway Protocol versión 4 (BGPv4)
	• Open Shortest Path First versión 2 (OSPFv2)
	• OSPFv3
	• Sistema Intermedio a Sistema Intermedio (IS-IS)
	• Protocolo de administración de grupos de Internet (IGMP) versiones 1, 2 y 3
	• multiprotocolo BGP (MBGP)
	• Multicast Source Discovery Protocol (MSDP)

	• conmutación de etiquetas multiprotocolo (MPLS)
	• MPLS protocolo de distribución de etiquetas (LDP)
	• Protocolo de reserva de recursos (RSVP)
	• Servicios diferenciados (DiffServ) ingeniería de tráfico sea conscientes
	• plano de control MPLS Ingeniería de Tráfico (RFC 2702 y 2430)
	• GMPLS
	• Enrutamiento de Política Lingüística (RPL)
	• Gestión
	• Simple Network Management Protocol (SNMP)
	• interfaces de programación (lenguaje de marcado extensible [XML])
	• Seguridad
	• Mensaje DigestAlgorithm 5 (MD5)
	• Protocolo (IPsec) de seguridad IP
	• Secure Shell Protocolo (SSHv2)
	• FTP seguro (SFTP)
	• Secure Sockets Layer (SSL)
	• DHCP v6
	• EoMPLS
Memoria	40 GB
Throughput	720 Gbps
MIB QUE SOPORTA EL EQUIPO	sysUpTime.0
	Interfaces
	Ip
	ipForward
	ipTrafficStats
	mplsLsrStdMIB
	mplsLdpStdMIB
	Ospf
	ospfTrap
	Bgp
	dot1dBridge
	ifMIB
	nhrpMIB
	ipMRouteStdMIB
	igmpStdMIB
	ospfv3MIB
	pimMIB
	msdpMIB
	ciscoPingMIB

	ciscoIpSecFlowMonitorMIB
	ciscoIpSecPolMapMIB
	ciscoPimMIB
	ciscoBgp4MIB
	ciscoIfExtensionMIB
	ciscoEigrpMIB
	ciscoCefMIB
	ciscoBridgeDomainMIB
	ciscoNhrpExtMIB
	ciscoIpMRouteMIB
	ciscoIPsecMIB
	mplsLdpMIB
	Cospf
	ciscoExperiment.101
	ciscoIetfIsisMIB
	ciscoIetfBfdMIB
	snmpTrapOID.0
	snmpMIB.1.4.3.0
	snmpTraps.3
	snmpTraps.4
Gestión de redes	CLI
	Interfaz XML
	• Cisco CIT
	• Soporte SNMP y MIB
Energía	Requisitos de Alimentación 208 to 240 VAC recomendado (or –48 to –60 VDC)
Condiciones ambientales	Temperatura de Almacenamiento: –4 to 149°F (–20 to 65°C)
	Temperatura de Operacion: 32 to 104°F (0 to 40°C)
	Humedad Operativo: 10 to 85%
	Humedad de Almacenamiento: 5 to 95%

Fig. 1.2.3-3. Especificaciones Básicas del equipo de Distribución

VSS		
Característica		
Versión software	Cisco IOS Software, s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(33)SXJ2, RELEASE SOFTWARE (fc4)	
Protocolos	IPv4 unicast forwarding, including MPLS VPN	Unidirectional Link Detection (UDLD)

	IPv4 multicast forwarding, including MPLS VPN	Gateway Load Balancing Protocol (GLBP)
	iBGP y eBGP	Hot Standby Routing Protocol (HSRP)
	OSPF	Virtual Router Redundancy Protocol(VRRP)
	EIGRP	UplinkFas
	RIPv1/v2	BackboneFast
	RIPv2	RSTP (802.1w)
	ISIS	PortFast
	Staticrouting	Per VLAN STP (PVSTP)
	Unidirectional link routing (UDLR)	Per VLAN RSTP (PVRSTP)
	IGMPv1, IGMPv2, IGMPv3	MultipleInstance STP (MISTP)
	PIMv1, PIMv2	MSTP (802.1s)
	SSM IGMPv3lite and URD	STP RootGuard
	Stub IP multicastrouting	L2VPN Advanced VPLS (A-VPLS)
	IGMP join	
	IGMP staticgroup	
	Multicastrouting monitor (MRM)	
	Multicast source discovery protocol (MSDP)	
	SSM	
	IPv4 Ping	
	IPv6 Ping	
	LAN Switching:	
	Layer 2 LAN Ports	
	Flex Links	
	EtherChannels	
	mLACP para Servidores de Acceso	
	IEEE 802.1ak MVRP and MRP	
	VLAN TrunkingProtocol (VTP)	
	VLANs	
	PrivateVLANs (PVLANs)	
	Private Hosts	
	IEEE 802.1Q Tunneling	
	Layer 2 ProtocolTunneling	
	STP and MST	
	MultiprotocolLabelSwitching (MPLS)	

	PROTOCOLOS QUE SE ENCUENTRAN CONFIGURADOS:	
	BGP ; AS:14420	
	IS-IS ; ID:1	
Tarjetas, puertos y ranuras	Puertos Gigabit Ethernet GBIC/SFP : 384. Configurado como Virtual SwitchingSystem: 768	
	Puertos 10 GBE XENPAK/X2: 130. Configurado como Virtual SwitchingSystem: 260	
	Puertos10/100/1000 Ethernet: 385. Configurado como Virtual SwitchingSystem: 770	
	Puertos 10 Gigabit Ethernet RJ-45: 128	
	Puertos 40 Gigabit Ethernet RJ-45: 32	
Memoria	40 GB	
Throughput	1,4 Tbps	
MIB QUE SOPORTA EL EQUIPO	ipForward	
	mplsLdpStdMIB	
	dot1dBridge	
	ciscoPingMIB	
	ciscoStpExtensionsMIB	
	ciscoIpSecFlowMonitorMIB	
	ciscoCat6kCrossbarMIB	
	ciscoEigrpMIB	
	ciscoIPsecMIB	
	mplsLdpMIB	
Gestión de redes	• CLI	
	• Interfaz XML	
	• Soporte SNMP y MIB	
Energía	• Cisco Catalyst 6509-V-E chassis soporta alimentación con fuentes AC y DC. Para Fuentes AC: 8700W.Para Fuentes DC: 4000W.	
	• La capacidad máxima de la fuente de alimentación es de hasta 14500W proporcionando la capacidad de soportar configuraciones completamente cargadas de corriente y futuras tarjetas 10 Ethernet Gigabit.	
Condiciones ambientales	Temperatura de almacenamiento: -4 to 149°F (-20 a 65°C)	

	Temperatura de funcionamiento: 32°F a 104°F (0 a 40°C)
	Transición térmica: 0.5 ° C por minuto (caliente a frío) y 0. 33 ° C por minuto (frío a caliente)
	Humedad relativa:
	Ambiente (sin condensación) de funcionamiento: 5% a 90%
	Ambiente (sin condensación) no operativos y de almacenamiento: 5% a 95%

Fig. 1.2.3- 4. Especificaciones Básicas del equipo VSS

ROUTE-REFLECTOR	
Característica	
Versión software	Cisco IOS XE Operating System, which is based on Cisco IOS Software Release 12.2SR
Protocolos	CDP
	• IPv4 e IPv6
	• ICMP
	• Border Gateway Protocol versión 4 (BGPv4)
	• Open Shortest Path First versión 2 (OSPFv2)
	• OSPFv3
	• Sistema Intermedio a Sistema Intermedio (IS-IS)
	• conmutación de etiquetas multiprotocolo (MPLS)
	• MPLS protocolo de distribución de etiquetas (LDP)
	• BGP
	• SNMPv3
	• PPPoX
	• DHCP
	• IPTV
	• Simple Network Management Protocol (SNMP)
	• interfaces de programación (lenguaje de marcado extensible [XML])
	• FTP seguro (SFTP)
	• Secure Sockets Layer (SSL)
	• PPPoX
	• EIGRP
Tarjetas, puertos y ranuras	Management: 1 x 10Base-T/100Base-TX - RJ-45,
	Management: 1 x Console - RJ-45,
	Management: 1 x Auxiliary Input - RJ-45,
	LAN : 4 x SFP (mini-GBIC), USB : 1 x 4 pin USB Type A

Memoria	Instalada 4 GB Máxima hasta 8 GB
Throughput	1,8 Gbps
MIB QUE SOPORTA EL EQUIPO	sysUpTime.0
	Interfaces
	Ip
	ipForward
	ipTrafficStats
	mplsLsrStdMIB
	mplsLdpStdMIB
	Ospf
	ospfTrap
	Bgp
	ifMIB
	nhrpMIB
	ipMRouteStdMIB
	igmpStdMIB
	pimMIB
	msdpMIB
	ciscoPingMIB
	ciscoIpSecFlowMonitorMIB
	ciscoIpSecPolMapMIB
	ciscoPimMIB
	ciscoBgp4MIB
	ciscoIfExtensionMIB
	ciscoEigrpMIB
	ciscoCefMIB
	ciscoNhrpExtMIB
	ciscoGdoiMIB
	ciscoIpMRouteMIB
	ciscoIPsecMIB
	mplsLdpMIB
	ciscoDlcSwitchMIB
	ciscoExperiment.101
	ciscoIetfIsisMIB
	ciscoIetfBfdMIB
	snmpTrapOID.0
	snmpMIB.1.4.3.0
	snmpTraps.3
	snmpTraps.4
Gestión de redes	● Telnet and Secure Shell (SSH) Protocol (command-line interface [CLI])

	● Console port (through the CLI)
	● Simple Network Management Protocol (SNMP)
	● RFC 2665
Energía	● Maximum (DC): 500W
	● Maximum (AC): 471W ● Maximum (out): 400W
Condiciones ambientales	Intervalo de temperatura operativa 0 - 40 °C
	Intervalo de temperatura de almacenaje -40 - 70 °C
	Intervalo de humedad relativa para funcionamiento 5 - 85 %
	Intervalo de humedad relativa durante almacenaje 5 - 95 %
	Altitud de funcionamiento -60 - 4000 m

Fig. 1.2.3-5. Especificaciones Básicas del equipo Route Reflector

1.3 Redundancia

El ISP de la CNT EP maneja redundancia a nivel de los equipos de comunicaciones de dos formas:

- REDUNDANCIA GEOGRAFICA: La estructura de capas y los equipos son el mismo modelo y marca de la Fig. 1.1-1 es decir en Guayaquil a nivel de tráfico y configuraciones soportan de la misma manera que en Quito.
- REDUNDANCIA LOCAL: El ISP mantiene redundancia local a nivel de equipos e interfaces, hay dos equipos VSS, Distribución, Route Reflector yCore cada uno de ellos maneja redundancia de conexiones físicas a nivel de interfaces y comparten la carga pero en el caso de algún incidente en alguno de ellos cualquiera puede soportar el tráfico total. Esta configuración lógica y Física se aplica también en Guayaquil.

A nivel LOCAL el equipo de Borde tiene redundancia de conexión de interfaces con los equipos en la Nube MPLS Internet.

1.4 Necesidad de una Gestión del Rendimiento del ISP

A fin de evitar que los análisis del rendimiento del ISP sean del tipo reactivo, es decir, realizados después de que se detectan los problemas en la red, como congestión de tráfico por enlaces que han alcanzado su máxima capacidad, reducción de la alta disponibilidad que se exige para redes de operadores de servicios, retardos excesivos en la transmisión o recepción de paquetes de datos, entre otros factores, que producen fallas en la red; se hace necesario disponer de procedimientos de gestión del rendimiento de la red del ISP.

Estos procedimientos se basan en los denominados indicadores claves de rendimiento, los cuales nos entregan información del comportamiento real de la red y constituyen la materia prima para realizar los respectivos análisis técnicos y poder prever, por una parte un crecimiento planificado del tráfico en la red evitando congestiones, lo que implica ampliación de capacidad de la red y por otra parte, definir acciones de mejoramiento de red para incrementar la disponibilidad, reducir los retardos y otras mejoras, que en definitiva nos permitan mantener una calidad de servicio dentro de los parámetros predefinidos aceptables para el usuario de los servicios y cumplir con las normativas del ente estatal regulador de los servicios de telecomunicaciones .

Con el presente trabajo de tesis, se pretende aportar al desarrollo de una Gestión del Rendimiento del ISP de la CNT EP, estableciendo los KPI y procedimientos de monitoreo y análisis de los mismos para la red de comunicaciones del ISP.

En el alcance de este trabajo no solamente se contempla el desarrollo teórico de un

modelo de gestión, establecimiento de los KPI y los respectivos procedimientos de monitoreo y análisis, sino también, se incluye una implementación práctica real de obtención de KPI de rendimiento sobre equipos de comunicaciones del ISP, utilizando una herramienta de gestión disponible.

Igualmente los procedimientos a desarrollar están basados sobre una estructura orgánica funcional existente en la CNT EP, de tal manera que los mismos puedan ser implementados en la práctica de así decidirlo CNT.

2 CAPÍTULO 2: KPI DE RENDIMIENTO DE EQUIPOS DE COMUNICACIONES DEL ISP CNT EP

2.1 Modelos de Gestión de Red

Existen varios modelos de gestión de red establecidos con estándares que se utilizan hoy en día, entre los más utilizados se encuentran:

ESTANDAR	PUNTOS FUERTES
OSI/CMIP OSI (Open System Interconnection) adoptado por la ISO (International Standard Organization	Estándar internacional (ISO y OSI)
	Gestión de redes de comunicaciones LAN /WAN
	Conocido por sus 7 niveles o capas
	Muy completo
	Orientado a Objetos
	Bien estructurado
SNMP/Internet	Estándar internacional (IETF)
	Originalmente creado para gestión de internet y luego ampliamente utilizado en redes WAN y sistemas de telecomunicaciones
	Fácil de implementar
	Ampliamente utilizado
TMN	Estándar internacional (UIT)
	Orientado a gestión de redes de telecomunicaciones
	Basado en las capas de OSI
	Completo, gestiona la red y aspectos administrativos
	Basado en eTOM para procesos de negocios y utilizado por NGOSS (Sistemas de soporte a operaciones en redes de próxima generación)
IEEE	Estándar internacional (IEEE)
	Gestiona redes LAN / WAN
	Adopta estándares de OSI
TECNOLOGIAS EMERGENTES	Gestión de empresa basado en WEB (WBEM)
	Extensión de Gestión con Java (JMX)
	Gestión de Red basado en XML
	CORBA (Common Object Request Broker Architecture)

Fig. 2.1-1 Estándares de gestión de Red [5][5]

[5] Referencia bibliográfica [5] (Subramanian, 2012), ver al final del documento

Debido a que la mayoría de los modelos de gestión de red están basados en OSI o toman parte del mismo, es necesario conocer la arquitectura del modelo de Gestión de Red, el cual se encuentra definido por el estándar ISO.

2.1.1 Modelo de Gestión de Red OSI (ISO)

El modelo de gestión de red OSI se divide en 4 componentes denominados [3][6]:

- Modelo Organizacional
- Modelo de Información
- Modelo de Comunicación
- Modelo Funcional

El Modelo Organizacional describe los componentes de un sistema de gestión de red, sus funciones y su infraestructura. También define los términos objeto, agente y gestión.

- Un objeto corresponde a un elemento de red como: host, router, switch, etc.
- Un agente corresponde a un proceso de gestión que corre en el elemento gestionado.
- Un gestor es el que gestiona el elemento, consulta y recibe datos de gestión del elemento (de su agente), los procesa y almacena en su base de datos (MDB).

El modelo de Información trata sobre la estructura y almacenamiento de la información. Este especifica la información base para describir un objeto gestionado y la relación entre objetos.

[6]Referencia bibliográfica [3](EGAS, 2007), ver al final del documento

La sintaxis y la semántica de la información de gestión están especificadas en la denominada SMI (Estructura de información de gestión).

La Base de Información de Gestión (MBI), contiene datos del objeto gestionado y no se limita solo a la parte física (hardware), también puede contener datos de software (programas, algoritmos, protocolos) e información administrativa (contacto, cuenta, etc.).

El modelo OSI organiza los objetos gestionados en base a una estructura tipo árbol denominada Gestión de Información de Árbol (MIT), donde existe un nodo raíz del cual cuelgan otros nodos y estos a su vez se subdividen formando capas o niveles (semejando un árbol con diferentes ramas y hojas). El MIT también es acogido por el Modelo de Gestión de Internet.

Un objeto requiere una representación física para comprender sus características, por ello un objeto gestionado en el modelo OSI es definido por ciertos parámetros, como clase de objeto, atributos, operaciones, etc. Sin embargo y aquí hay una diferencia con el modelo de Gestión de internet donde estos parámetros no son iguales y para este modelo se han definido cinco, los cuales son: Tipo de objeto, Sintaxis, Acceso, Estado, y Descripción, haciéndolo más simple.

El Modelo de Comunicación trata sobre cómo se realiza el intercambio de información de un objeto gestionado entre el gestor y el agente, tiene que ver con los protocolos de transferencia de información.

Mientras que el modelo OSI utiliza protocolos: CMIP (Common Management Information Protocol) / CMIS (Common Management Information Service), el

modelo Internet utiliza SNMP (Simple Network Management Protocol).

Ambos modelos el de Información y el de Comunicación requieren un conjunto de reglas para la estructura y significado del lenguaje de comunicación, lo que se denomina sintaxis y semántica.

UIT e ISO definieron en conjunto un lenguaje de programación para la transferencia de datos entre sistemas y sus capas de aplicación, denominado Abstract Syntax Notation One (ASN.1) [5][7]. Este lenguaje define la terminología, símbolos y convenciones que especifican la sintaxis. El algoritmo mediante el cual se convierte el texto ASN.1 a código de máquina ejecutable se denomina BER (Basic Encoding Rules).

Este lenguaje es utilizado para la definición de los varios tipos de datos y descripción de los objetos en el SMI y en las MIB.

El componente Modelo Funcional cuenta a su vez con los siguientes Procesos y Procedimientos: [3][8]

- Gestión de configuración
- Gestión de fallas
- Gestión de rendimiento (desempeño) de red
- Gestión de seguridades
- Gestión de carga y confiabilidad

[7]Referencia bibliográfica [5] (Subramanian, 2012)
[8]Referencia bibliográfica [3](EGAS, 2007), ver al final del documento

Gestión de Rendimiento, es el conjunto de actividades requeridas para que se evalúe continuamente los principales indicadores del rendimiento de operación de la red para verificar como se mantienen los niveles de servicio.

Gestión de Rendimiento consiste en:

- Colectar datos de la utilización actual de la red, dispositivos y enlaces
- Analizar datos relevantes para visualizar tendencia de alta utilización
- Definir límites de utilización de la red

Gestión de rendimiento se encarga de:

• Monitoreo del desempeño

• Control de gerencia de desempeño

• Manipulación de límites y parámetros de medición

• Medición y gestión de tráfico

• Análisis de desempeño

• Procesamiento y análisis de datos

• Observación de calidad de servicio.

Las principales Funciones de la Gestión de Rendimiento son:

• Definición de indicadores de rendimiento

• Monitoreo del Rendimiento

• Análisis y afinamiento

2.1.2 Modelo de Gestión de Red Internet (SNMP)

Conocido también como Modelo de Gestión SNMP porque está basado en la

arquitectura del protocolo SNMP para la capa de aplicación y utiliza la suite de protocolo TCP/IP con UDP para el transporte.

El componente Organizacional de este modelo es muy simple y consta de dos niveles jerárquicos: el SNMP gestor y el SNMP agente, es equivalente al modelo cliente –servidor en informática.

El protocolo SNMP ha sido diseñado para ser muy simple y versátil, por ello es muy utilizado, su descripción y arquitectura se encuentra definido en la RFC 1157. RFC se refiere a Request for Coments y son documentos que contienen especificaciones técnicas y normas de la IETF (Internet Enginneering Task Force o Grupo de Trabajo de Internet).[6][9]

La comunicación con este protocolo se realiza apenas con cinco mensajes, como se muestra en la figura a continuación:

[9]Referencia bibliográfica [6] (IETF, 2015), ver al final del documento

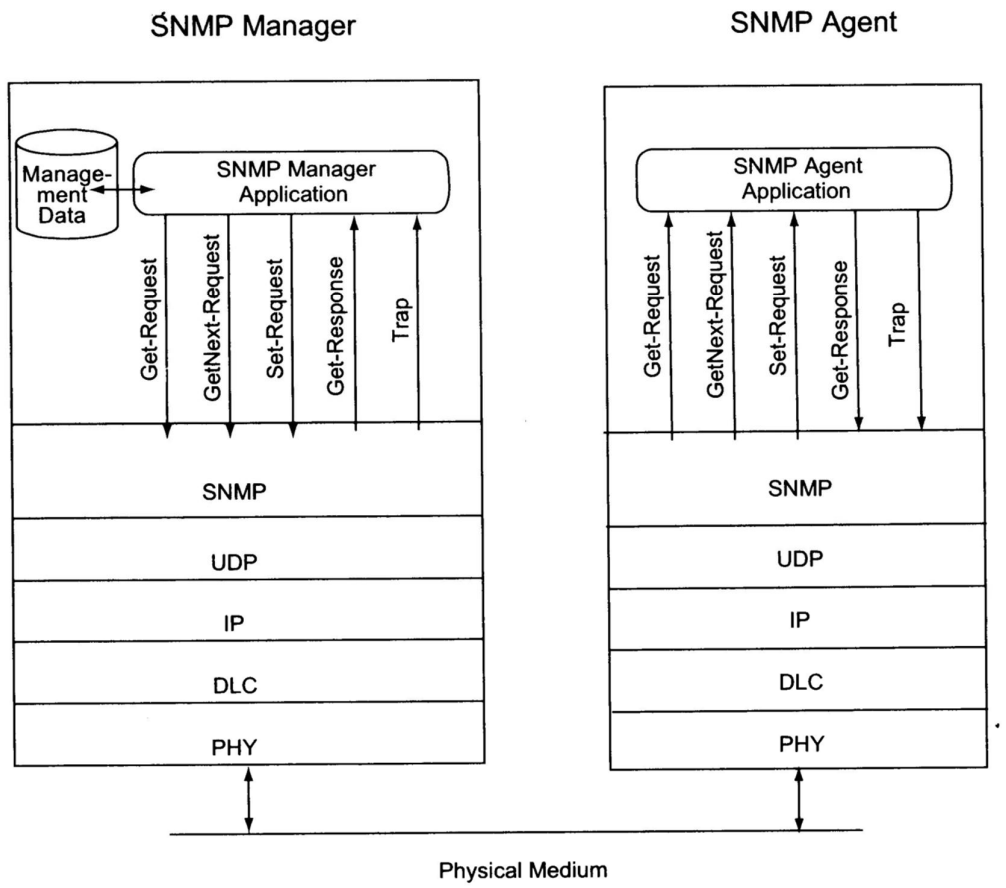

Fig. 2.1.2-1 Arquitectura del modelo de gestión de Red SNMP [5][10]

El componente del Modelo de Información de Internet es similar al de OSI, tiene que ver con la estructura e identificación de la gestión de información (SMI), la cual está definida en la RFC 1155 y la RFC 1156 que describen la base de la información de gestión (MIB), conocida como MIB I (versión inicia). Luego aparecería la RFC 1213 que define la segunda versión de MIB, denominada MIB II, en relación a su antecesora (RFC 1156), se introducen los siguientes cambios:

- Se adicionan definiciones para reflejar nuevos requerimientos operacionales
- Incrementa compatibilidad entre SMI / MIB y el protocolo SNMP

[10]Referencia bibliográfica [5] (Subramanian, 2012)

- Incrementa soporte para entidades multiprotocolo
- Realiza una limpieza de texto en MIB para incrementar claridad y lectura.

Utiliza igualmente el lenguaje ASN.1 y su correspondiente codificador (BER).

A nivel de las MIB II utiliza también estructura tipo árbol y realiza una agrupación de objetos relacionados por Grupos, con su respectivo identificador de objeto (OID), Se han definido 11 grupos: Sistema, interfaces, at (address translation), ip(ip protocol), icmp, tcp, udp, egp(external Gateway protocol), cmot, transmisión y snmp.

A continuación en la figura 2.1.2-2 se muestra un ejemplo del grupo UDP.

ENTIDAD	OID	DESCRIPCION
udpInDatagrams	Udp 1	Número total de datagramas entregadas a los usuarios
udpNoports	udp 2	Número total de datagramas recibidos para los cuales noa hay aplicación
udpInerrors	udp 3	Número de datagramas recibidos con errores

Fig. 2.1.2-2 Grupo UDP [5][11]

El componente del modelo de Comunicación Internet, está definido por las especificaciones del protocolo SNMP, las cuales abarcan los aspectos de: arquitectura, administración (políticas de acceso), SNMP protocolo y SNMP MIB.

A nivel del modelo de administración en SNMP se define la “comunidad”, la cual significa un emparejamiento del SNMP gestor y el SNMP agente, esta tiene un nombre definido por un conjunto de octetos. La comunicación puede establecerse entre entidades que pertenezcan a la misma comunidad; se trata de un esquema de autentificación.

[11]Referencia bibliográfica [5] (Subramanian, 2012)

El protocolo SNMP ha evolucionado, iniciando con la versión SNMP v1, continuando con la V2, cuya principal característica es la de incluir contadores de 64 bits para medir ancho de banda en el orden de los Gbps y la última V3 cuya principal diferencia con V1 y V2 es que mejora la seguridad en el acceso brindando autentificación y cuentas por usuario (V1 y V2 utiliza únicamente autentificación de la llamada comunidad SNMP para todos los usuarios) e incorpora encriptación, aunque esto incrementa el procesamiento del CPU en los gestores y por tanto reduce el número de nodos a monitorear en redes grandes.

El componente Funcional del modelo de Gestión de Internet (SNMP) no tiene una división por áreas funcionales ni un alcance tan completo como en el modelo OSI (configuración, fallas, rendimiento o desempeño, seguridad y cuentas), no dispone de la función de cuentas.

Para la gestión del rendimiento, existen contadores de desempeño definidos en las MIB SNMP, los cuales permiten obtener los datos reales y luego poder procesarlos y realizar el respectivo análisis

Para el alcance de este trabajo de Tesis, nos enfocamos únicamente en los procesos de Gestión de Rendimiento (Desempeño) de red basada en el modelo de Gestión de Internet (SNMP) y en particular al desarrollo de los procesos de Gestión del Rendimiento de los equipos de comunicaciones de la red del ISP de la CNT EP.

2.2 Herramientas de monitoreo del Rendimiento de Red

Existen numerosas herramientas de monitoreo de red, algunas básicas que forman

parte del propio sistema operativo de un sistema como Linux o Windows (entre los más conocidos) que tienen un conjunto de comandos de monitoreo y entre los mas utilizados tenemos:

- ping (packet internet grouping),permite revisar el estado del nodo/host
- Ifconfig(interface configuration), permite configurar y obtener parámetros de una interfaz de red y su estado
- tracert (route trace) permite trazar la ruta a un destino y muestra los tiempos de retardo.

Otras herramientas más completas están implementadas en sistemas independientes, denominados NMS (Network Management System) cuyas funciones incluyen configuración, gestión de fallas, gestión de rendimiento, gestión de cuentas y hoy en día incluyen también el aprovisionamiento de servicios en la red, estos se los conoce como OSS (Operating Support System).

Para el alcance de esta tesis nos referiremos a las herramientas que utilizan SNMP, del tipo software libre (sin costo) como CACTI (de las más utilizadas e igualmente empleada para algunos monitoreos de CNT) y del tipo de software licenciado (con costo) como PRTG utilizada en el ISP de la CNT.

CACTI es una herramienta de monitoreo de red orientada a gráficos, trabajo con una aplicación para manejo de datos denominada RRdTool y esta utiliza la base de datos MySQL. Esto le permite graficar series de datos con bases de tiempo [10][12].

Es muy útil por ejemplo para disponer de gráficos en línea que muestran el consumo de ancho de banda de una interfaz. Sin embargo para redes grandes, su

[12] Referencia bibliográfica [10] (CACTI, 2015)

desempeño disminuye, puede haber saturación y lentitud en el procesamiento. Otro tema es que requiere de recursos dedicados a su mantenimiento y no es muy simple el programar los datos y gráficas requeridas. Utilizarlo como un complemento de otras herramientas representa una mejor opción.

PRTG (Paessler Router Traffic Grapher) es un aplicación para monitoreo de red desarrollada por la compañía alemana Paessler AG, corre sobre el sistema operativo Windows [11][13]Su mejor característica es que es muy fácil de implementar, no requiere de mayor programación, tiene opciones automáticas para descubrimiento y autoconfiguración. Existe una versión sin costo pero limitada en el número de los denominados sensores de prueba.

2.2.1 Características requeridas de una Herramienta de Gestión de Red

Para el modelo de gestión de rendimiento de Internet (SNMP) y las características de equipamiento de la red de comunicaciones del ISP, la herramienta de gestión que permite el monitoreo de los KPI debe reunir al menos los siguientes requisitos:

- Descubrimiento automático de la topología de red
- Gestión de MIBs y protocolo SNMP V1, V2 y V3
- Amplia biblioteca de MIBs y compatibilidad equipos CISCO.
- Monitoreo de tráfico y ancho de banda con datos históricos.
- Monitoreo de QoS , posibilidad de escoger indicadores
- Reportería gráfica con posibilidad de exportar resultados en formatos estándar.
- Interfaz de usuario amigable, gráfica, con procesos automáticos.

[13] Referencia bibliográfica [11] (PAESSLER / PRTG, 2015)

- Disponibilidad de acceso a los datos vía WEB, acceso remoto.
- Gran capacidad de puntos de monitoreo (para redes grandes).
- Facilidad para su implementación, de preferencia Software que puede ser cargado y ejecutarse sobre servidores con sistema operativo Linux o Windows.
- Actualizaciones periódicas on line, con soporte y consultas técnicas
- Incluir seguridad para el acceso
- Acceso simultáneo para múltiples usuarios.
- Perfiles de acceso diferenciados: usuario administrador, usuario de monitoreo, usuario para configuración.
- Incluir opciones de notificaciones (mensajes SMS, correo)

2.2.2 Herramienta PRTG

PRTG es la principal herramienta utilizada en el ISP de CNT para el monitoreo de la red de comunicaciones, de los servidores que proporcionan los diferentes servicios y de clientes corporativos con los cuales se tiene suscrito un SLA, cumple con los características básicas indicadas en el ítem 2.2.1 y por ello utilizaremos esta herramienta para la obtención de los principales indicadores de rendimiento (desempeño) de la red de comunicaciones del ISP. En CNT se utiliza actualmente la versión 15 con todas sus características ya que es licenciada con un costo anual, esto además brinda una ventaja adicional, el disponer de soporte técnico en línea y actualizaciones automáticas de software.

A continuación se presenta una breve descripción de PRTG, sus principales

características y modo de operación. Lo indicado aquí se encuentra con mayor detalle en el manual del usuario de PRTG, el cual puede ser descargado de la página WEB[14]

El software PRTG debe ser descargado del sitio oficial de Paessler (sea que se trate de una versión free, trial o licenciada), posteriormente se procede con su instalación sobre sistema operativo Windows: Microsoft Windows 7, Microsoft Windows 8 o Microsoft Windows server 2008, soporta las dos versiones de OS a 32 o 64 bits.

Es necesario tomar en cuenta los requerimientos de procesamiento de esta aplicación según la cantidad de equipos y sensores que se deseen monitorear, básicamente estos son:

Requerimientos de HARDWARE:

- CPU, computadoras fabricadas desde el año 2007 pueden soportar 1000 sensores, con un Intel core 2 quad (2,6 Gbps) y 8 GB de RAM puede soportar hasta 20.000 sensores con SNMP.
- RAM, mínimo 1 GB , utiliza unos 150KB por sensor
- Hard disk, requiere almacenamiento en disco de 250KB por sensor , por día
- En caso de utilizar sondas remotas (remote probes), requiere una conexión estable entre el denominado Core PRTG y la sonda remota.
- Conexión a internet para activar la licencia.

Requerimientos de navegador (Web browser):

[14]Referencia bibliográfica [11] (PAESSLER / PRTG, 2015)

- Google chrome 38 o posterior
- Mozilla 33 o posterior
- Explorer 10 u 11

Requerimientos para los dispositivos monitoreados:

- Para SNMP que es lo que utilizamos, los dispositivos a ser monitoreados deben tener cargado el agente SNMP v1, v2 o v3 y permitir el acceso a la interfaz SNMP

Una vez instalado el software PRTG, activada la licencia e introducido su usuario y clave (password), se presentará el menú que se muestra en la Figura 2.2.1-1.

Para iniciar se activa el menú de configuración GURU, este es un asistente que mediante cortas preguntas que se deben responder, configurará automáticamente los sensores e iniciará el monitoreo. Luego se puede añadir más sensores y más equipos.

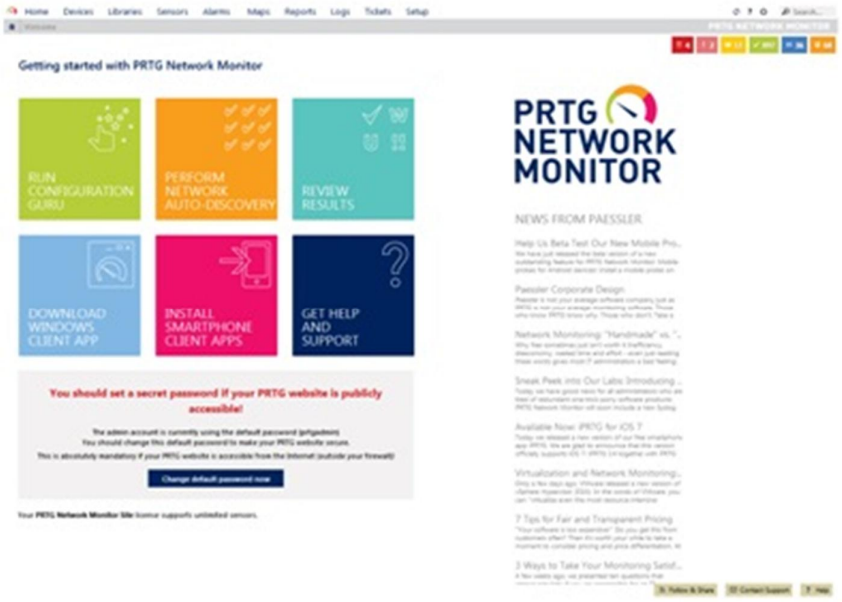

Fig. 2.2.1-1 Pantalla de bienvenida en PRTG[15]

PRTG está conformado básicamente por un core server (servidor de núcleo) que es la parte central y contiene: el almacenamiento de la data, servidor de web, reportería, sistema de notificaciones.

Las sondas son las que realizan el monitoreo en base a los sensores creados en el dispositivo, su configuración está definida en el core server, corre el proceso de monitoreo y entrega los resultados obtenidos al core server. Se crean automáticamente unos pocos sensores predefinidos que pueden mantenerse o no por el usuario.

Las interfaces de usuario principal es la denominada Ajax Web, la cual se utiliza para la configuración de los dispositivos y sensores así como para la revisión de los resultados del monitoreo. También por medio de esta interfaz se realiza la administración del sistema y gestión de los usuarios. PRTG dispone también de

[15]Referencia bibliográfica [11] (PAESSLER / PRTG, 2015)

otras interfaces como la consola de empresa (alternativa a la interface web) que es una aplicación nativa Windows, interfaz móvil optimizada para acceso vía terminales inteligentes móviles.

PRTG presenta los resultados del monitoreo en una estructura tipo árbol como se muestra en la figura 2.2.1-2

- El Root Group contiene todos los objetos, todas las sondas están bajo este grupo
- Una sonda contiene uno o más grupos
- Un grupo contiene uno o más dispositivos
- Un dispositivo representa un elemento de red monitoreado, al cual se accede mediante su dirección IP. Un dispositivo tiene varios sensores.
- Un sensor monitorea un solo aspecto del dispositivo y tiene al menos un canal
- Un canal recibe los resultados del monitoreo y es parte del sensor

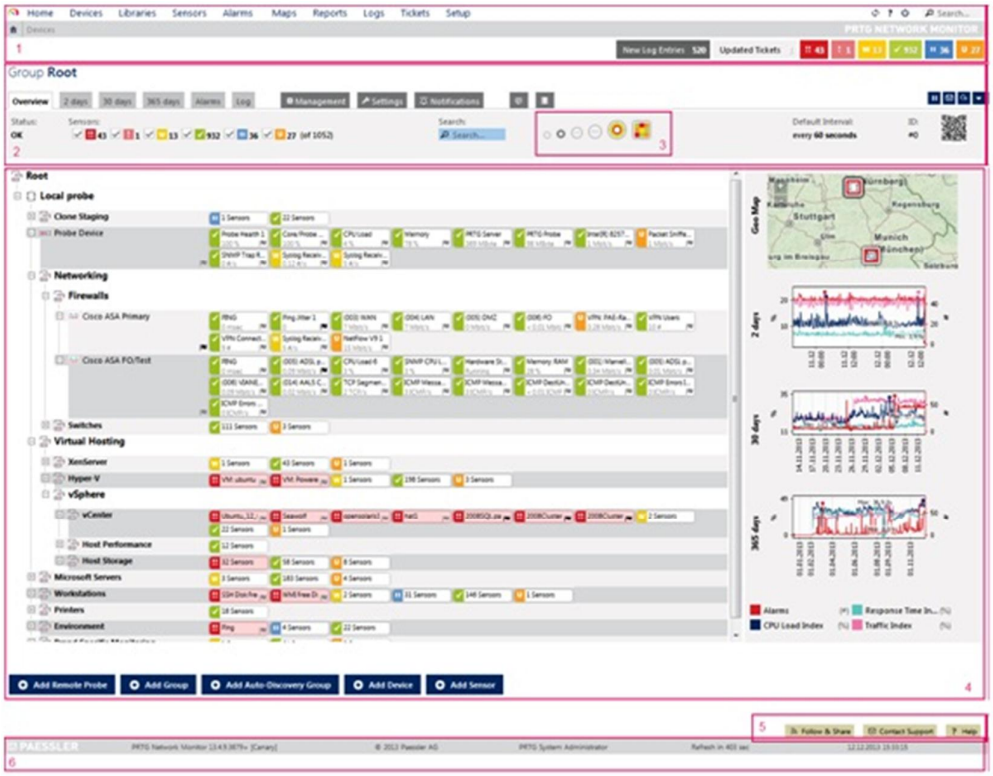

Fig. 2.2.1-2 Presentación de dispositivos en PRTG[16]

SENSORES

PRTG maneja una tabla de sensores con muchas opciones y clasificados como se indica en la figura 2.2.1-3

[16]Referencia bibliográfica [11] (PAESSLER / PRTG, 2015)

Fig. 2.2.1-3 Sensores en PRTG[17]

De esta tabla, a su vez, cada grupo de sensores se subdividen. Así por ejemplo tenemos para Common Sensors, la siguiente figura:

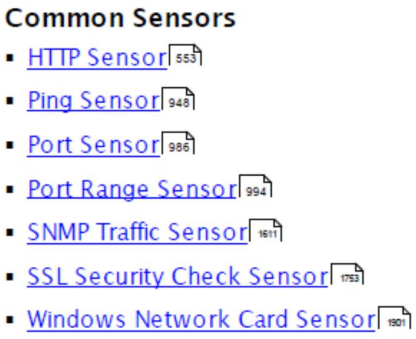

Fig. 2.2.1-4 Common sensors en PRTG

[17]Referencia bibliográfica [11] (PAESSLER / PRTG, 2015)

Finalmente en este grupo, si tomamos por ejemplo “ping sensor” o “snmp traffic sensor” encontraremos las definiciones de los valores que entrega el sensor y su forma de configurarlo.

Para el caso del grupo de sensores de Bandwidth Monitoring, encontramos los indicados en la figura siguiente:

Fig. 2.2.1-5 Grupo de sensores de Bandwidth

A continuación se muestran los sensores correspondientes al grupo SNMP:

Fig. 2.2.1-6 Grupo de sensores PRTG de SNMP[18]

2.3 Revisión y obtención de los principales indicadores por equipo

De acuerdo a lo indicado en el capítulo Uno de este trabajo, los equipos de la Red de comunicaciones (routers) del ISP sobre los cuales obtendremos sus principales indicadores son los denominados: BORDE, CORE y DISTRIBUCION.

Los routers Route Reflector constituyen una configuración que permite la actualización de enrutamientos de manera automática, como se describió en el capítulo 1 y por tanto estos equipos al no cursar tráfico de red no forman parte del análisis de los indicadores de gestión del desempeño para este trabajo.

Igualmente los equipos denominados Virtual Switch que operan en la capa del Core encargados de la interconexión de servidores que brindan servicios de valor agregado del ISP, no son objeto del análisis en este trabajo.

[18]Referencia bibliográfica [11] (PAESSLER / PRTG, 2015)

Los sensores PRTG que contienen el termino flow no podemos utilizarlos, debido a que requieren implementar esta función en los equipos cisco y no esta implementada en el ISP de la CNT EP. Net Flow de Cisco [7][19] se orienta a medir parámetros de tráfico y QoS de las denominadas Clases de servicio (CoS), en las cuales se divide el tráfico en función de su perfil como Datos, Voz, video; lo cual no está implementado en el ISP sino en el backbone MPLS de CNT. A nivel de pruebas anteriormente realizadas en el ISP, esta función incrementa notablemente la carga del CPU.

Como estamos utilizando SNMP, es necesario revisar las respectivas MIB que proporcionen los indicadores de gestión del desempeño.

Las MIB disponibles por cada equipo pueden ser obtenidas de las siguientes maneras:

a) Mediante acceso a la información que proporciona CISCO en su página WEB denominada: http://tools.cisco.com/ITDIT/MIBS/MainServlet, y colocando los datos del equipo y software, como se muestra en la figura 2.3-1

[19]Referencia bibliográfica [7] (CISCO, 2010)

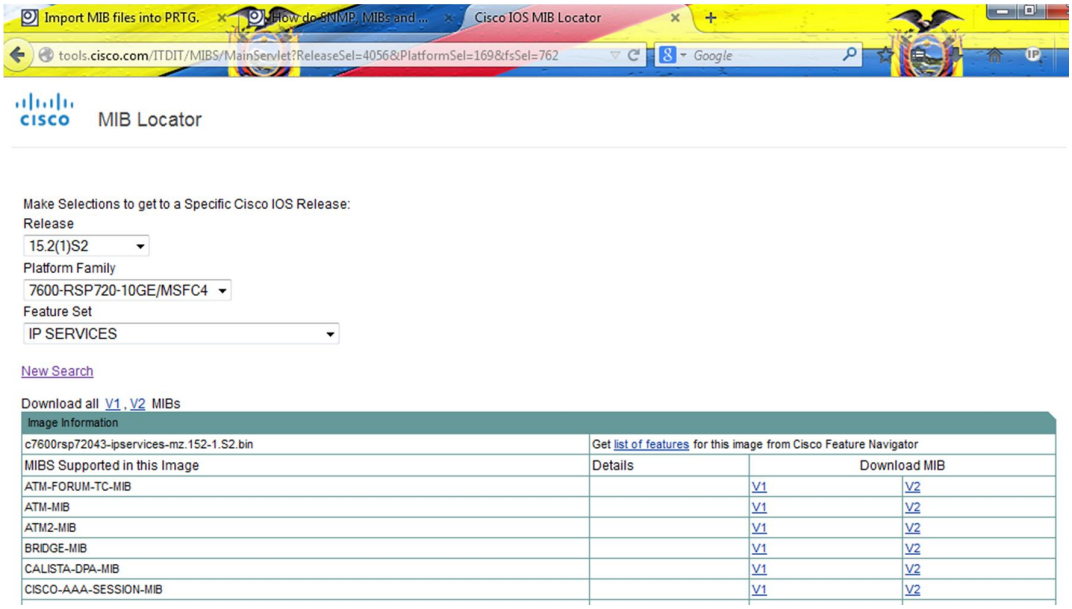

Fig. 2.3-1 Búsqueda de MIB en WEB CISCO

Si ingresamos a una MIB seleccionada (V1 o V2), encontraremos detalles de la MIB como se muestra a continuación:

Fig. 2.3-2 Detalles de MIB seleccionada

Si en esta página Web no se encuentra el equipo, existe también otra WEB de CISCO donde se puede hacer una búsqueda más general de MIB, así como su traducción a un OID (Identificador de Objeto), utilizado por los gestores (Entre ellos PRTG).

La dirección de esta página WEB es: http://tools.cisco.com/Support/SNMP/do/BrowseOID.do y aquí se puede ingresar el OID o texto relacionado a la búsqueda, por ejemplo si estamos interesados en MIBs de Tráfico, ingresamos traffic y obtenemos lo que se muestra en la fig. 2.5

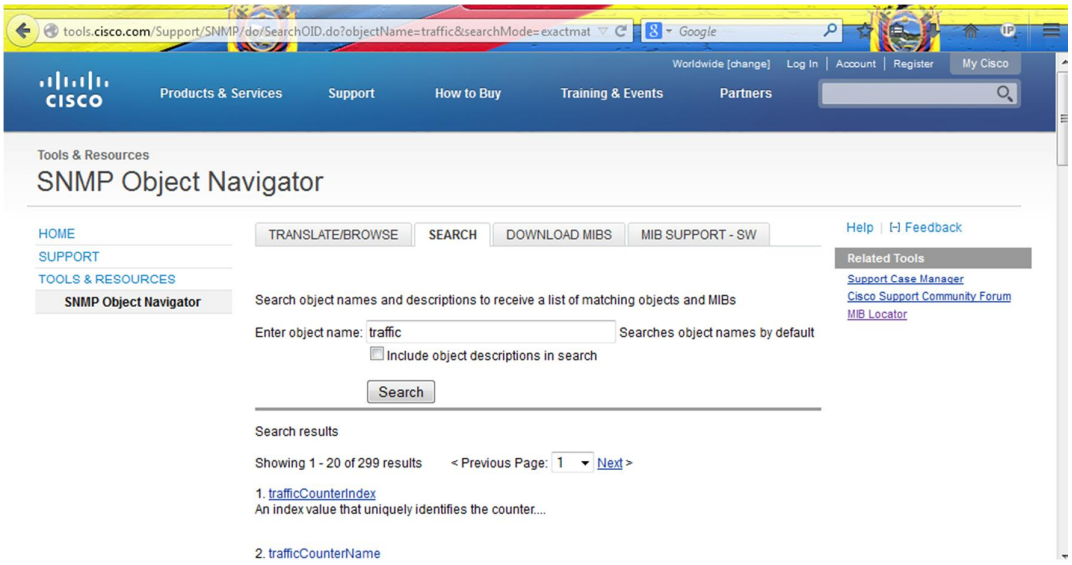

Fig. 2.3-3 Detalles de MIB seleccionada

Si accedemos a la MIB seleccionada obtendremos detalles de la misma (Fig. 2.3-4)

Fig. 2.3-4 Detalles de MIB seleccionada

b) Podemos acceder directamente a los equipos (Routers) utilizando un terminal de consola o una herramienta como PUTTY para acceso remoto y obtener el listado de MIB que dispone el router., como se muestra a continuación en las figuras 2.3-5 y 2.3-6

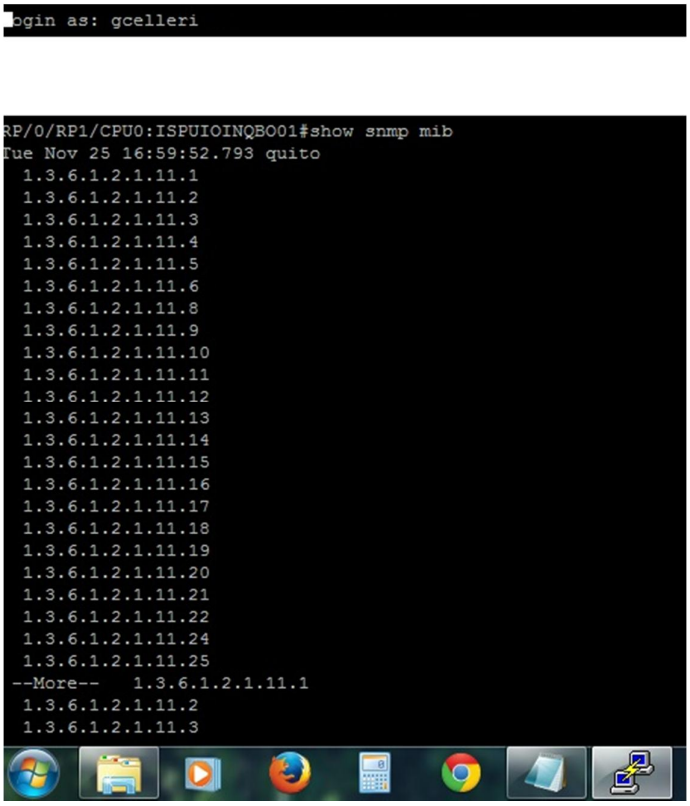

Fig. 2.3-5 Lista de MIB en router (OID)

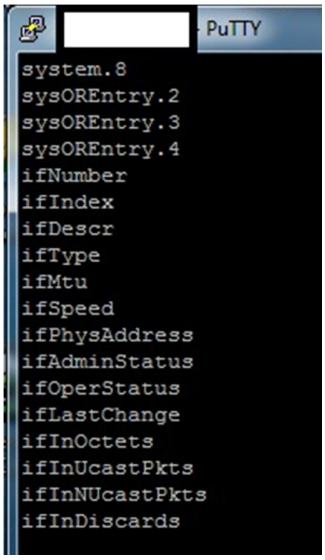

Fig. 2.3-6 Lista de MIB en router (Object name)

c) Podemos utilizar PRTG con su función AUTODISCOVERY, la cual al conectarse con el dispositivo realizará una búsqueda automática de MIB a través de sus sensores preestablecidos.

A esta función se accede a través del menú inicial de PRTG en el ícono denominado Perform Network Autodiscovery. Evidentemente previo a lanzar esta función ya debía haberse configurado PRTG con las credenciales de acceso a los equipos, comunidad SNMP, IP.

PRTG ejecuta las siguientes tareas con esta función:

- Realiza un muestreo (scanning) de los dispositivos del segmento de red utilizando ping.
- Accede al dispositivo detectado en tarea anterior mediante el protocolo configurado, en este caso SNMP.
- Crea un conjunto de sensores que empatan (match) con el tipo de dispositivo detectado en la tarea anterior. (Se recuerda que los sensores de PRTG viene preestablecidos en una biblioteca muy amplia y que incluye equipos CISCO)

2.3.1 Indicadores de Rendimiento (Performance) de RED

A nivel del modelo del sistema de gestión de internet con SNMP que estamos utilizando, la cantidad de MIBs que proporcionan indicadores es enorme, por ello se hace necesario por una parte limitar el número de los mismos escogiendo aquellos indicadores que entregan datos sobre desempeño de la red y por otro lado de estos realizar un filtrado de los que se consideran importantes.

Es necesario recordar lo ya indicado anteriormente, MIB es una base de

información virtual almacenada y los OBJETOS a ser gestionados se acceden vía estas MIB.

Los objetos en las MIB están definidos utilizando el lenguaje ASN.1 y el SMI (Estructura de la gestión de información) define el mecanismo para describir estos objetos, el cual consiste del nombre (Object Descriptor), sintaxis (ASN.1) y codificación (BER).

Los Objetos que están relacionados se agrupan en los denominados Grupos de Objetos (Objects groups), se han definido 11 grupos en MIB II, los cuales se muestran en la figura 2.3.1-1. Cada Objeto en MIB II tiene un OID (object identifier), y definido bajo una estructura tipo árbol (Ejemplo: OID=1.3.1.6.1.2.1.11.5, name= snmpInBadCommunityUses).

GROUP	OID	DESCRIPTION (BRIEF)
system	mib-2 1	System description and administrative information
interfaces	mib-2 2	Interfaces of the entity and associated information
at	mib-2 3	Address translation between IP and physical address
ip	mib-2 4	Information on IP protocol
icmp	mib-2 5	Information on ICMP protocol
tcp	mib-2 6	Information on TCP protocol
udp	mib-2 7	Information on UDP protocol
egp	mib-2 8	Information on EGP protocol
cmot	mib-2 9	Placeholder for OSI protocol
transmission	mib-2 10	Placeholder for transmission information
snmp	mib-2 11	Information on SNMP protocol

Fig. 2.3.1-1 Grupos de Objetos MIB II [5][20]

[20]Referencia bibliográfica [5] (Subramanian, 2012)

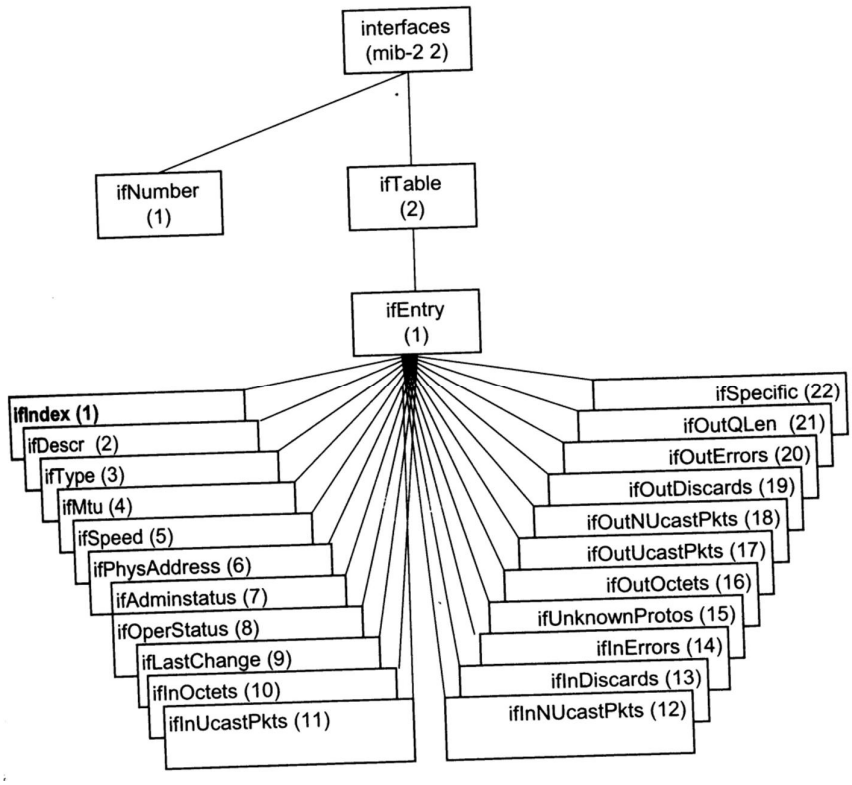

Fig. 2.3.1-2 Grupo Interfaces [5]

El grupo interfaces contiene objetos asociados a las interfaces de los dispositivos (routers) y para cada una de ellas se pueden obtener contadores de velocidad (ifSpeed) y de tráfico (ifInOctets, ifOutOctets). En la figura 2.3.1-2 se muestra la estructura tipo árbol de las MIB asociadas a este grupo.

Al utilizar la función de autodescubrimiento de PRTG, este nos entrega los sensores disponibles para cada equipo, de los cuales escogemos aquellos que nos dan mediciones de tráfico para la gestión del Rendimiento, entonces verificamos que estos contengan los objetos de medición indicados y obtenemos los principales indicadores por cada equipo

La ventaja de revisar con PRTG los sensores que compaginan (match) con los

equipos es que obtenemos aquellos que podemos monitorear y entregan resultados, es decir dependiendo del equipo y del sensor disponible, PRTG indica la factibilidad de entregar o no resultados y esto facilita la gestión, caso contrario tendríamos que ingresar individualmente cada objeto de medición (OID) y esperar a que PRTG nos confirme factibilidad, lo cual conlleva mucho tiempo y no es práctico. De todas maneras en caso de requerirlo, PRTG permite el ingreso manual de un OID específico mediante el código numérico de su respectiva MIB.

Con PRTG ubicamos los siguientes sensores que compaginan con los equipos:

- SNMP Traffic: monitorean ancho de banda y tráfico en las diferentes interfaces del router.
- PING: monitorea conectividad y Latencia utilizando ping
- PING Jitter: Entrega valores estadísticos de Jitter realizando pings al router
- SNMP Cisco SystemHealth: Monitorea la salud (health) del sistema del dispositivo Cisco, esto es Disponibilidad de memoria, carga del CPU
- SNMP Library: permite monitorear un conjunto de MIB de una biblioteca determinada
- SNMP OID: permite monitorear un OID específico.

Existen otros sensores como el SNMP CISCO CBQoS: Monitorea parámetros de red utilizando Cisco Class Bases Quality of Service utilizando SNMP, sin embargo en los routers del ISP no tenemos programada CBQoS dado que el tráfico que por ahí circula básicamente es de internet y no se ha establecido ni implementado clase de servicio (QoS), como sería el caso si por ejemplo por el ISP circulara tráfico de VoIP

(telefonía IP).

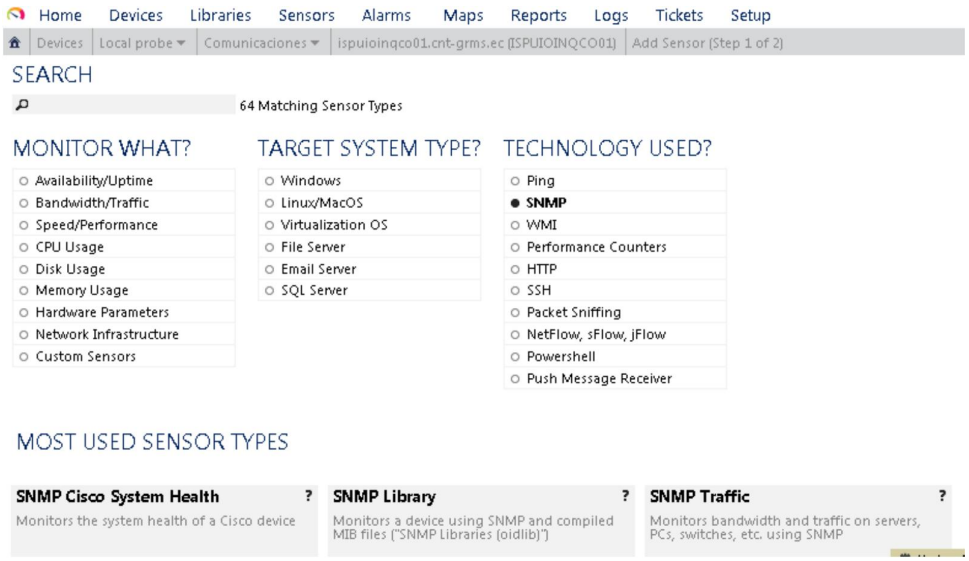

Fig. 2.3.1-3 PRTG Sensores SNMP más utilizados[21]

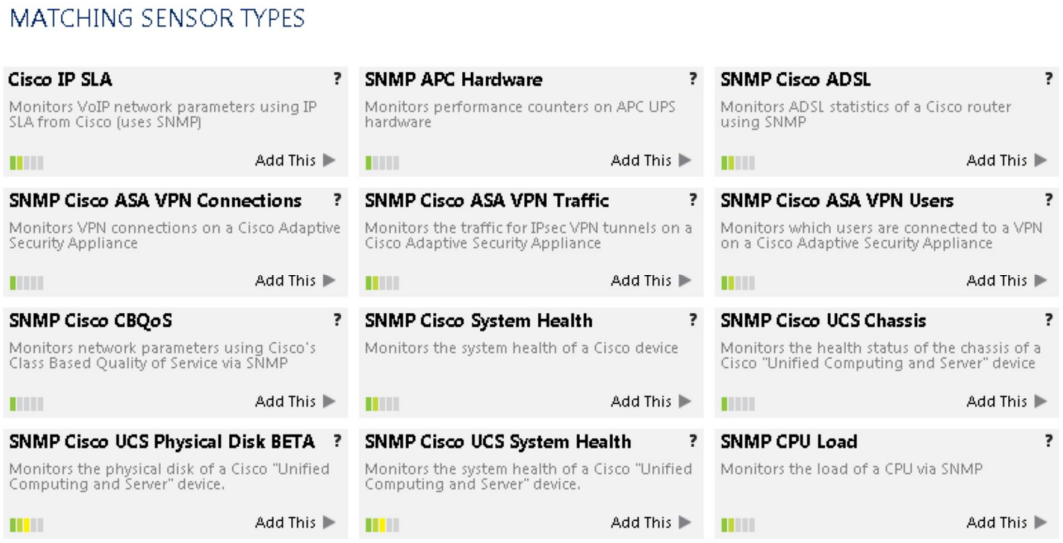

Fig. 2.3.1-4 PRTG Sensores SNMP que concuerdan con el equipo (match)

[21] A partir de esta Fig. los gráficos que se presentan en el resto de figuras de PRTG fueron obtenidos directamente desde el sistema de prueba de PRTG implementado.

Como se había indicado previamente, es necesario realizar un filtrado de estos sensores en función del alcance del presente trabajo orientado a indicadores de rendimiento de red, muchos de estos sensores tienen que ver con otras funcionalidades de los equipos, las cuales no se encuentran implementadas como IP SLA, CBQoS, Flow. Una vez analizados se escogen los denominados: SNMP Library, SNMP Traffic y SNMP Cisco SystemHealth

El Sensor SNMP Library presenta el submenú que se muestra a continuación en la figura 2.3.1-5

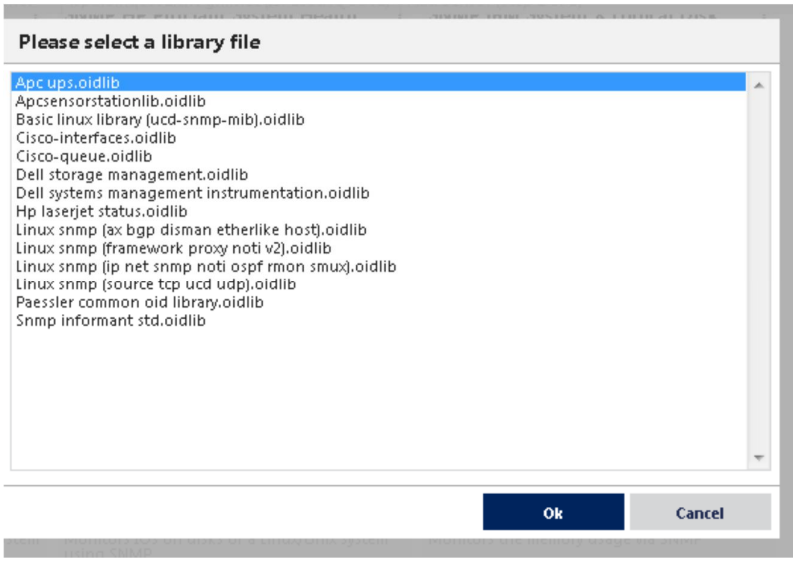

Fig. 2.3.1-5 PRTG Sensores SNMP Library (Biblioteca)

Como se observa el submenú presenta las bibliotecas de OID disponibles, de estas revisamos la Cisco-Interfaces y Cisco-Qeue.

Al marcar en el submenú la biblioteca de Cisco-Interfaces, PRTG nos muestra los objetos de medición disponibles y que podemos escoger (figura 2.3.1-6)

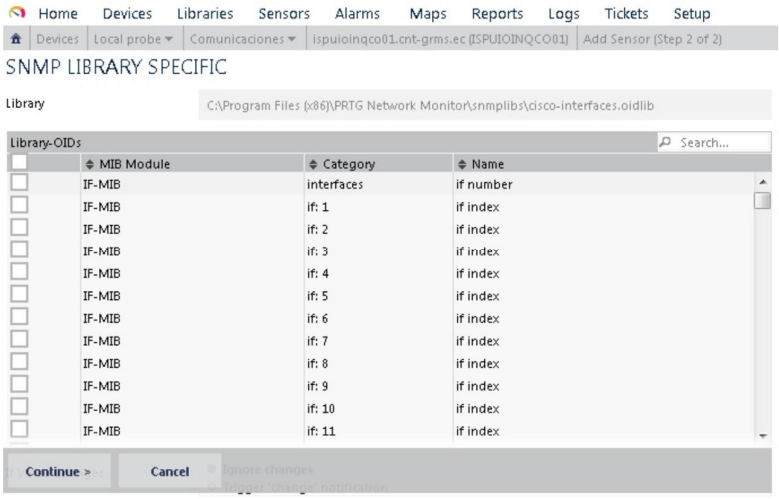

Fig. 2.3.1-6 SNMP Library - Biblioteca Cisco-interfaces

Debido al extenso listado de esta biblioteca de objetos, puesto que se enlistan todas las interfaces del equipo y para cada una diferentes objetos de medición, en la figura se muestra solo una parte, sin embargo se puede observar como la biblioteca de OID de PRTG (En la columna Name de esta figura consta ifnumber, ifindex) coincide con el desglose de Grupo de Objetos denominado Interfaces, mostrado en la figura 2.3.1-2).

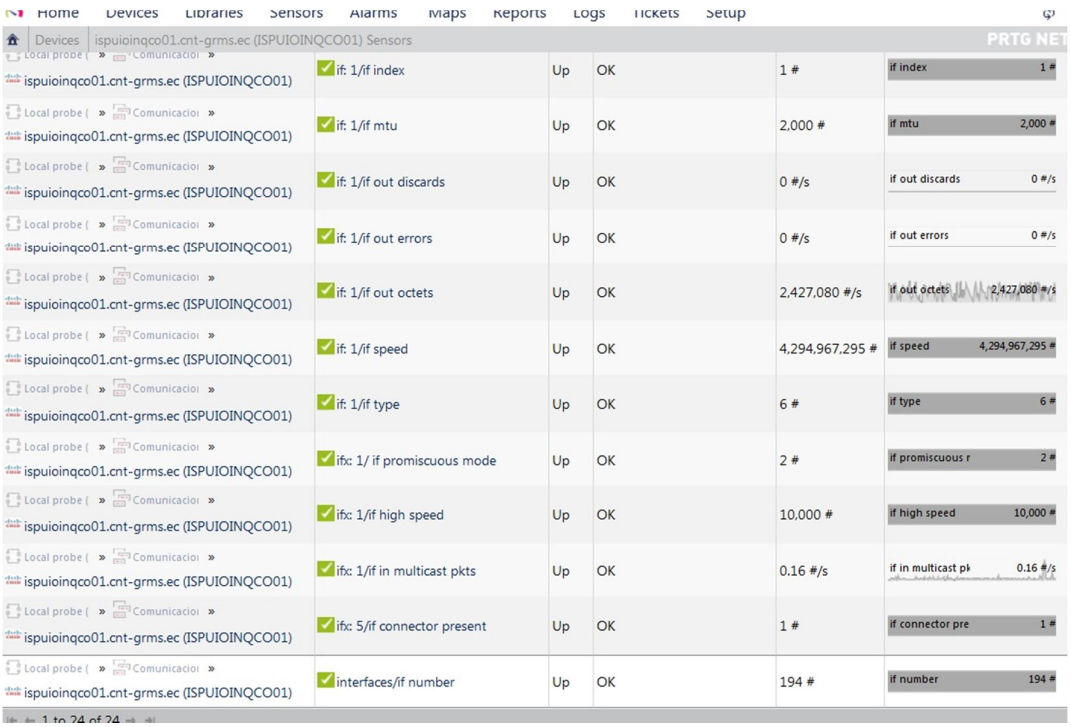

Fig. 2.3.1-7 Resultados sensores Cisco-interfaces

En la figura 2.3.1-7 se muestran los resultados obtenidos con PRTG para el equipo ISPUIOINQC001, a continuación el significado de ellos:

- Ifnumber entrega el número de interfaces por equipo, en este caso 194
- Iftype, el tipo de interfaz de acuerdo al código utilizado por IANA (Internet AssignedNumberAuthority). En este caso corresponde a “6:ethernetCsmacd”
- ifmtu, indica el máximo tamaño del paquete (expresado en octetos) que puede ser enviado o recibido por una interfaz, en esta caso 2000
- ifoutdiscards, entrega el número de paquetes para enviar descartados, en este caso 0
- if in discards, entrega el número de paquetes de entrada descartados, en este caso 0

- if in errors, indica el número de paquetes de entrada con errores y que no serán remitidos a otro nivel.
- If in octets, entrega el número total de octetos recibidos en la interfaz, incluyendo caracteres de trama (en un determinado periodo de tiempo, PRTG realiza gráficos automáticos con escalas apropiadas)
- Ifoutoctets, entrega el número total de octetos enviados por la interfaz, incluyendo caracteres de trama (en un determinado periodo de tiempo)
- Ifoper status, indica el estado operacional de la interfaz (1:up, 2:down,3:test…)
- Ifspeed, entrega un estimado del ancho de banda de la interfaz expresada en bits por segundo. Su valor máximo es 4.294.967.295 y esto significa que esta interfaz soporta mayor ancho de banda pero el indicador muestra solo el máximo.
- Ifhighspeed, muestra un valor estimado n de ancho de banda expresado en unidades de 1.000.000 de bits por segundo o su valor nominal, en este caso el valor de 10.000 representa el valor nominal de una interfaz de 10Gbps
- Ifpromiscuousmode, opera con valores lógicos, 2 (false) significa que la interface solo acepta paquetes direccionados a ese equipo.
- Ifconnectormode, opera con valores lógicos, 1 (verdadero) significa que la interface tiene un conector físico

Del análisis efectuado sobre el significado de cada uno de ellos, los sensores que proporcionarían indicadores claves de rendimiento serían: Ifoutdiscard, if in discard, ifspeed, if in octets, ifoutoctets, sin embargo los sensores de tráfico que

veremos más adelante nos permiten obtener resultados mejor presentados sobre ancho de banda, velocidad y errores o descarte de paquetes que los considerados en este grupo de interfaces.

En cuanto al otro grupo de biblioteca de objetos denominada cisco.queue, PRTG puede monitorear igualmente una lista larga de objetos, una muestra de los mismos se presenta en la figura 2.3.1-8.

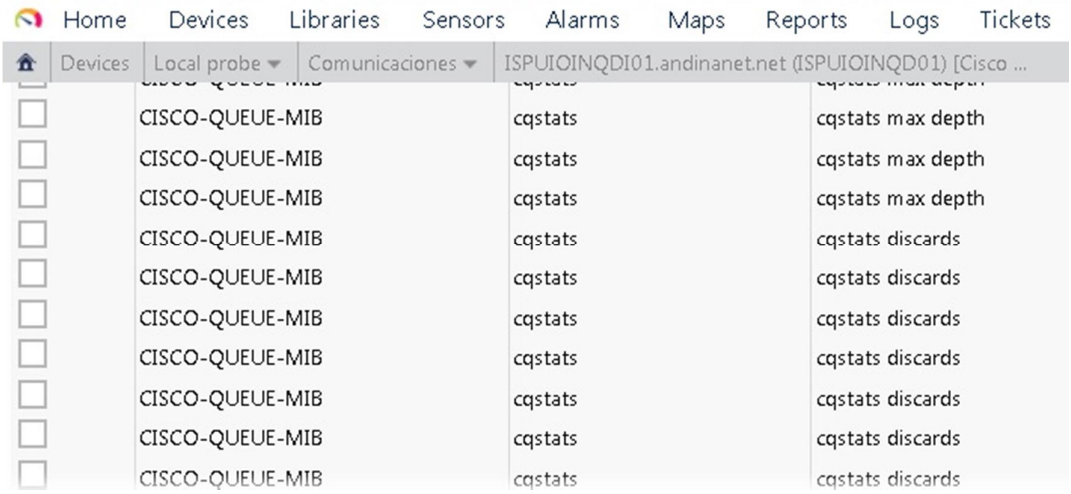

Fig. 2.3.1-8 Sensores Cisco-queue

A continuación el significado de ellos y los resultados obtenidos (figura 2.3.1-9)

- Cqifsubqueues, el número de sub-colas que integran la cola , en este caso es 1 , hay 1 sub-cola
- Cqiftxlimit, el máximo número de mensajes colocados en la cola hardware de transmisión, en este caso 0, no hay mensajes en esta cola.
- Cqifqtype, el tipo de algoritmo que usa la cola, (1=fifo, 2=priority, 3= custom, 4=

Weightedfaired), en este caso 1 es una cola del tipo first in firstout.

- Cqstatsdepth, el número de mensajes en la sub-cola, en este caso 0
- Cqstatsmaxdepth, el máximo número de mensajes permitidos en la sub-cola, en este caso 40
- Cqstatsdiscards, el número de mensajes descartados de la cola, luego que se alcanzó el máximo.

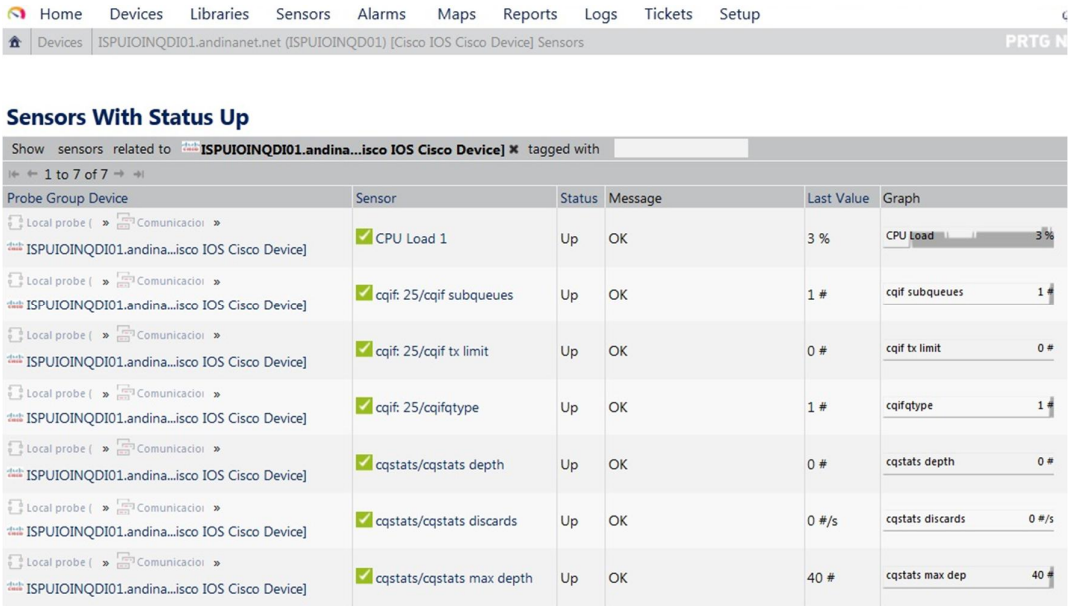

Fig. 2.3.1-9 Resultados sensores Cisco-queue

Sobre el grupo de sensores denominados SNMP Traffic, PRTG nos brinda las opciones que se muestran en la figura 2.3.1-10.

Se obtienen los sensores de tráfico y de velocidad por cada una de las interfaces que automáticamente PRTG detecta, observar también que presenta el estado de cada interfaz (Connected or not Connected) y con ello podemos monitorear únicamente las que presentan tráfico (connected). Se hace notar que estos resultados coinciden con los sensores del grupo Cisco-Interfaces que medían ifspeed, if in octets, ifoutoctets.

En la parte baja de la figura 2.3.1-10 se muestran los denominados canales (channel) adicionales de medición que disponen estos sensores, así tenemos: Errors in/out, Discards In/Out , los cuales también coinciden con los sensores del grupo Interfaces: if in errors, ifouterrors, if in discards, ifoutdiscards.

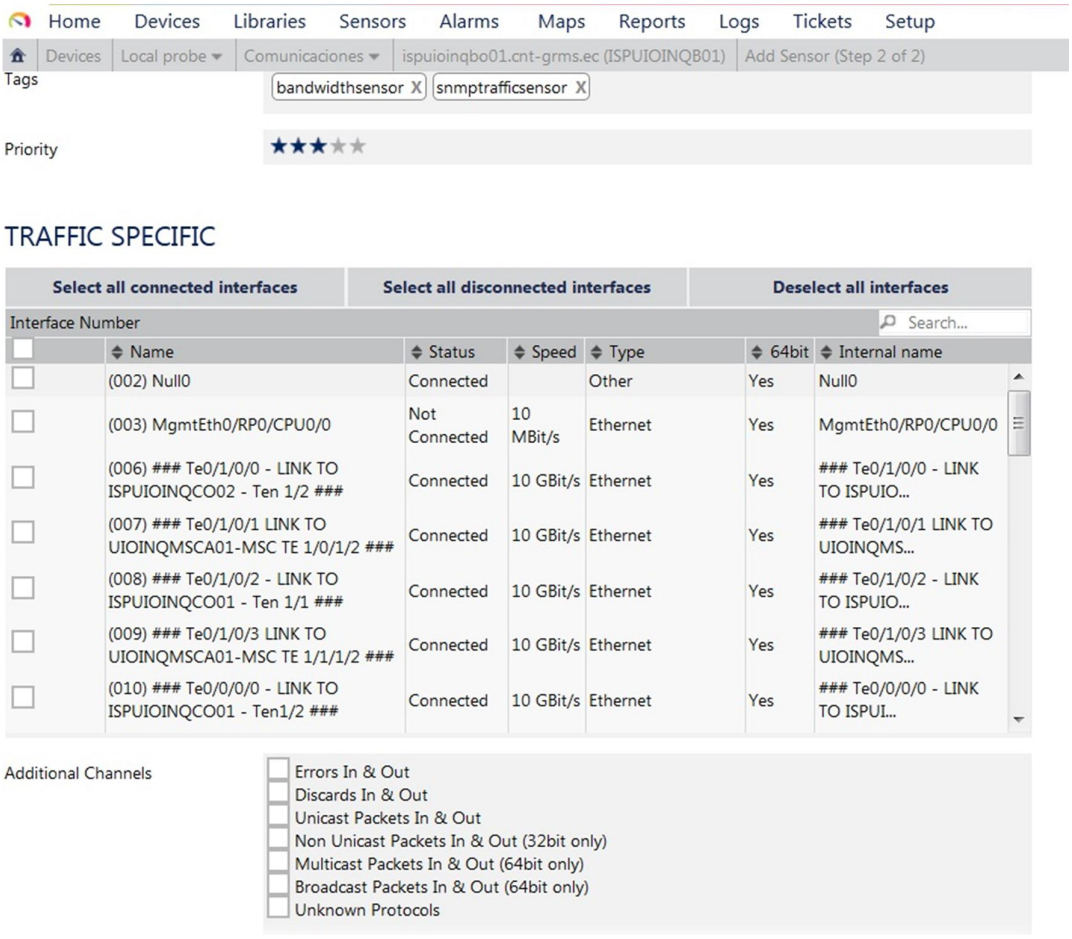

Fig. 2.3.1-10 Sensores snmptraffic

Una vez seleccionadas las opciones de medición, PRTG procesa la información y presenta los resultados de manera gráfica como se indica en la figura 2.3.1-11 o en forma de tabla como se indica en la figura 2.3.1-12.

En los indicadores de tráfico, los gráficos de monitoreo diarios e históricos son los más utilizados para el respectivo análisis, por ejemplo determinar hora pico o visualizar caídas de volumen de tráfico que indican algún tipo de problema. En la figura 2.3.1-13 se presenta una muestra de este tipo de gráfico que entrega PRTG.

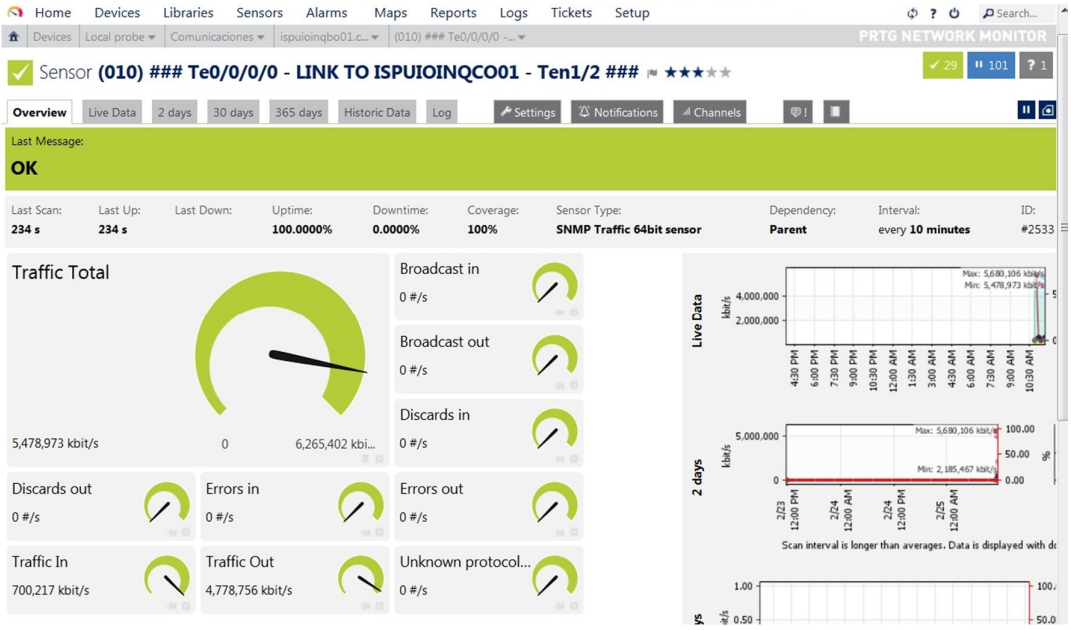

Fig. 2.3.1-11 Resultados Sensores snmptraffic- gráfico

CHANNELS

Channel	ID	Last Value (volume)	Last Value (speed)	Minimum	Maximum	Settings
Broadcast in	8	0 #	0 #/s	0 #/s	0 #/s	
Broadcast out	9	0 #	0 #/s	0 #/s	0 #/s	
Discards in	12	0 #	0 #/s	0 #/s	71,126,107 #/s	
Discards out	13	0 #	0 #/s	0 #/s	0 #/s	
Downtime	-4					
Errors in	10	0 #	0 #/s	0 #/s	0 #/s	
Errors out	11	0 #	0 #/s	0 #/s	0 #/s	
Traffic In	0	51,285,420 KByte	700,217 kbit/s	683,930 kbit/s	700,217 kbit/s	
Traffic Out	1	350,006,551 KByte	4,778,756 kbit/s	4,778,756 kbit/s	4,996,176 kbit/s	
Traffic Total	-1	401,291,971 KByte	5,478,973 kbit/s	0 kbit/s	6,265,402 kbit/s	
Unknown protocols in	14	0 #	0 #/s	0 #/s	0 #/s	

Fig. 2.3.1-12 Resultados Sensores snmptraffic- tabla

En referencia a los sensores denominados snmp cisco systemhealth, PRTG presenta

las opciones de medición como se indica en la figura 2.3.1-14 y los resultados en las figuras 2.3.1-15 y 2.3.1-16.

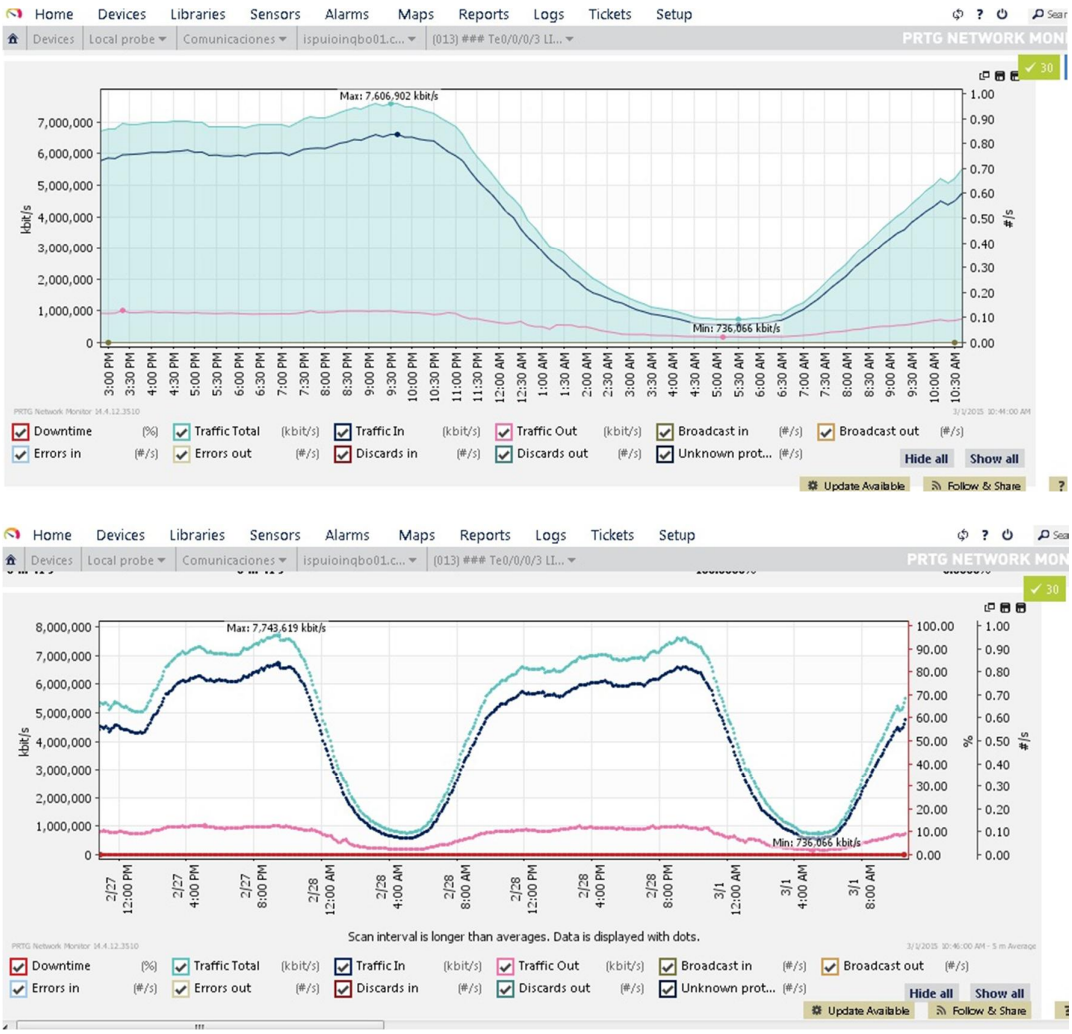

Fig. 2.3.1-13 Gráficos PRTG Tráfico por horas y por días

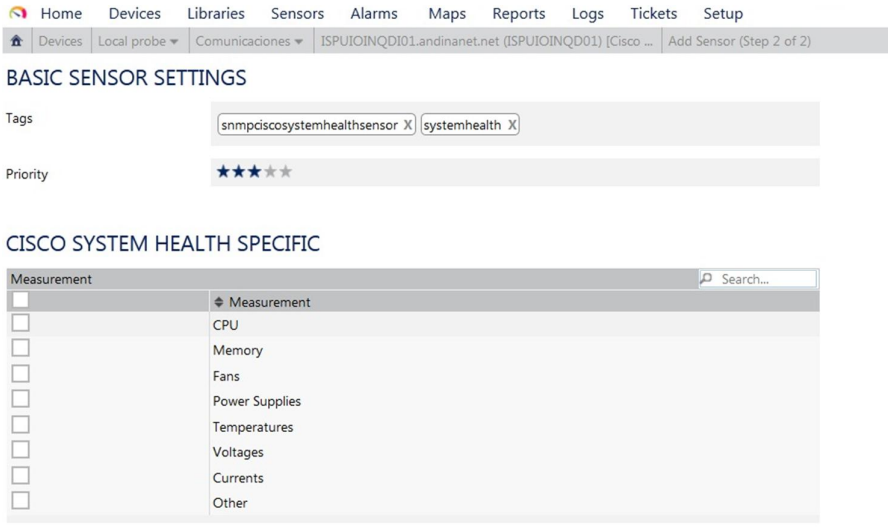

Fig. 2.3.1-14 Sensores snmp cisco system health

Fig. 2.3.1-15Resultados de Sensores snmp cisco systemhealth CPU

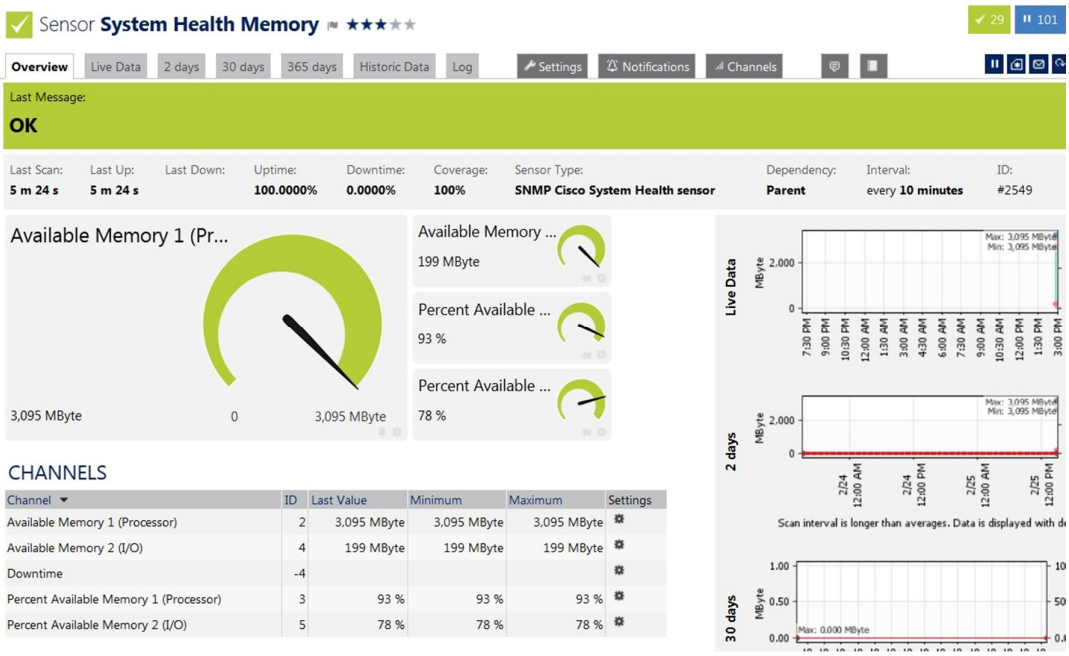

Fig. 2.3.1-16 Resultados de Sensores snmp cisco system health Memory

PRTG también dispone de un sensor denominado Ping Jitter el cual mide la variación de la latencia entre paquetes (interpaquet delay variance), entendiéndose por latencia el retardo o tiempo de tránsito extremo a extremo del paquete en un flujo, también se conoce como la variabilidad del tiempo de ejecución de los paquetes, como se describe en la RFC1889 [6], la cual utiliza PRTG para su cálculo.

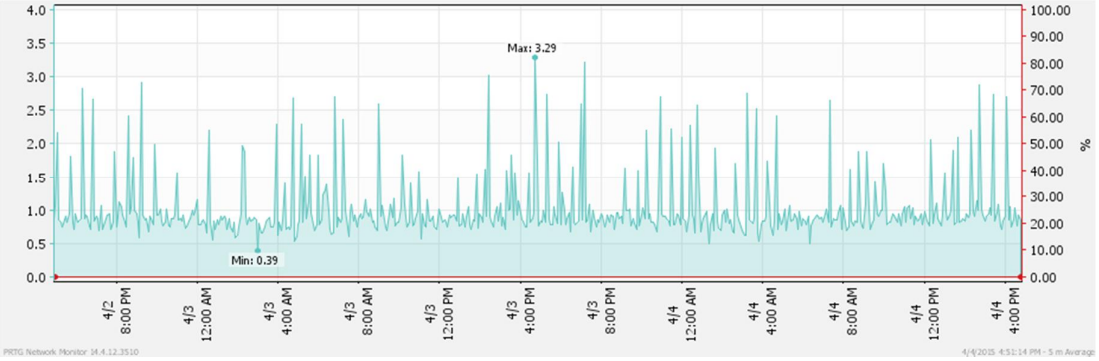

Fig. 2.3.1-17 Resultados Sensor Ping Jitter

En la figura 2.3.1-17 se muestran los resultados obtenidos de la medición de Jitter, el máximo valor obtenido es de 3,29mseg. Lo cual indicaría que está dentro de los valores aceptables para VoIP si el equipo manejara ese tráfico y QoS.

De acuerdo a lo revisado en esta sección y experimentado con PRTG, entonces los principales indicadores de desempeño que podemos obtener para los equipos de comunicaciones del ISP se indican a continuación:

INDICADOR	MIDE	Unidad	Periodo	Forma de obtención	Donde se mide
Tráfico IN diario (Tr.in)	Volumen de tráfico de entrada	Kbyte	Cada 5 minutos	PRTG sensoressnmp-traffic in (volume)	En cada interfaz del router
Tráfico OUT diario (Tr.out)	Volumen de tráfico de salida	Kbyte	Cada 5 minutos	PRTG sensoressnmp-traffic out (volume)	En cada interfaz del router
Velocidad de bajada (V.down)	Cantidad de bits por segundo de entrada	Kbit/seg	Cada 5 minutos	PRTG sensoressnmp-traffic in (speed)	En cada interfaz del router
Velocidad de subida (V.up)	Cantidad de bits por segundo de salida	Kbit/seg	Cada 5 minutos	PRTG sensoressnmp-traffic out (speed)	En cada interfaz del router
Paquetes unicast Out (Pqu.out)	Cantidad (#) de paquetes por segundo Transmitidos	#/seg	Cada 5 minutos	PRTG sensoressnmp-traffic unicast out	En cada interfaz del router
Paquetes unicast In (Pqu.in)	Cantidad (#) de paquetes por segundo Recibidos	#/seg	Cada 5 minutos	PRTG sensoressnmp-traffic unicast in	En cada interfaz del router
Paquetes descartados (Pd.in y Pd.out)	Cantidad (#) de paquetes que descarta el equipo In/Out	#/seg	Cada 5 minutos.	PRTG sensoressnmp-traffic Discards In y out	En cada interfaz del router
Errores (Er.in y Er.out)	Cantidad (#) de paquetes In/Out no tramitados	#/seg	Cada 5 minutos	PRTG sensoressnmp-traffic Errors In y Out	En cada interfaz del router
Jitter (Jit)	Variación de latencia de paquetes	mseg	Cada 5 minutos	PRTG sensor ping jitter	En el router
Latencia (Lat)	Tiempo medio que tardan en llegar los paquetes	mseg	Cada 5 minutos	PRTG sensor ping	En el router
Disponibilidad (Disp)	Tiempo sin servicio del equipo	mseg	Cada 5 minutos	PRTG sensor ping	En el router
Carga CPU (Cpu)	Carga de procesamiento del CPU	%	Cada 5 minutos	PRTG sensor cisco system health	En cada CPU del router
MTU (Mtu)	Máximo tamaño del paquete IN/OUT	bytes	Cada 5 minutos	PRTG sensor de Library cisco interface ifmtu	En cada interfaz del router
Profundidad de cola (Pq)	# mensajes en la subcola	#	Cada 5 minutos	PRTG sensor de Library cisco queueCqstatsdepth	En las colas definidas del router
Mensajes descartados de cola (Mjdq)	el número de mensajes descartadosde la cola, luego que se alcanzó el máximo	#	Cada 5 minutos	PRTG sensor de Library cisco queueCqstatsmaxdepth	En las colas definidas del router

Fig. 2.3.1-18 Principales Indicadores de rendimiento para equipos de comunicaciones (router) del ISP

Los indicadores obtenidos corresponden a aquellos que son útiles para evaluar el rendimiento de los equipos de comunicaciones del ISP y que pueden ser monitoreados por la herramienta PRTG.

Estos indicadores abarcan los principales aspectos que reflejan el rendimiento de la red, esto es: tráfico, ancho de banda, disponibilidad, latencia, QoS, carga del equipo.

2.4 Definición de los KPI de Rendimiento

KPI (siglas en inglés Key performance Indicator) son siglas comúnmente utilizadas en el lenguaje de un Operador o Proveedor de Servicios y en español significan Indicador Clave de Rendimiento (o Desempeño).

Estos indicadores permiten a un operador como CNT monitorear el rendimiento de su red y constituyen la información de entrada para la ejecución de los procesos de gestión de rendimiento, cuyos resultados generarán las acciones correspondientes para mantener una adecuada disponibilidad y calidad de servicio en su red, lo que a su vez, permite al Operador la provisión de los servicios de acuerdo a las normas y estándares de calidad definidos.

EL alcance del presente trabajo de tesis abarca la red de comunicaciones (routers) del ISP de la CNT mediante el cual se brinda el servicio de internet.

Recordemos unas reglas básicas, que indican como escoger estos KPI [8][22]

- Relevancia : deben valorar una actividad importante
- Adherencia: Estar directamente relacionados con el concepto a evaluar

[22] Referencia bibliográfica [8] (Sanchez, 2007)

- Cuantificable: Los resultados se pueden cuantificar con un dato numérico o un valor de clasificación
- Rentable: El beneficio de su uso supera el coste de obtenerlo
- Disponibilidad: Los resultados deben estar disponible a tiempo para la oportuna toma de decisiones
- Comparable: Debe permitir representar la evolución temporal del concepto a evaluar
- Fiable: Proporcionan confianza sobre la validez de medidas sucesivas (exactitud y precisión).

Sobre la cantidad de KPI monitoreados en un sistema de gestión de rendimiento se aconseja (en base a experiencia del operador) que esta no sea extensa, facilitando de esta manera el monitoreo (no sobrecarga capacidad de procesamiento de los equipos) y presentación de los mismos (para control, seguimiento y análisis) con la finalidad de obtener tiempos rápidos de respuesta en caso de decisiones que deben tomarse sobre la red.

Si es necesario, luego del primer análisis de los KPI, se podrán monitorear otros indicadores más específicos como parte ya de un proceso de investigación sobre un evento particular.

En la prestación del servicio de internet por la red de comunicaciones del ISP actualmente no se maneja QoS[23] (entendida como al establecimiento de parámetros que permitan diferenciar el tipo de tráfico que transportan los paquetes IP) ya que todo el tráfico corresponde al servicio de internet, evidentemente como

[23] Quality of Service

parte del tráfico de internet puede existir tráfico multimedia (voz y video), sin embargo este tráfico no está diferenciado en el ISP y por ello no se implementa QoS. Donde si se implementa QoS es en el backbone MPLS por donde pasa todo tipo de tráfico que brinda el Operador, incluyendo Internet, IPTV, Telefonía IP, Móvil y es necesario diferenciarlo para cumplir con los parámetros de calidad de los diferentes servicios que se ofrecen.

Para monitorear el rendimiento de la red de comunicaciones del ISP se toman en cuenta los siguientes parámetros:

- Velocidad de los paquetes (Ancho de banda) que permite verificar la capacidad de ancho de banda asignada a cada interfaz de los equipos (routers).
- Volumen de tráfico, permite establecer la cantidad de tráfico que pasa por la red.
- Latencia, tiempo medio que tardan en llegar los paquetes, ayuda a verificar congestión de red o problemas e enrutamientos.
- Jitter, varianza de la fluctuación que provoca el retardo, importante si se aplica QoS
- Descarte de paquetes (o dropeo), permite verificar la capacidad de procesamiento de paquetes y optimizar el buffer y colas del router.
- Carga del procesador (CPU) del equipo, permite verificar la capacidad del procesamiento central del router y si este soporta el tráfico requerido de paquetes.
- Disponibilidad, permite medir el tiempo que el equipo permanece operando, es

decir cumpliendo su función básica que es la de transmitir y recibir paquetes IP en la red (cursar tráfico).

De acuerdo a lo analizado, revisamos los principales indicadores de desempeño obtenidos con PRTG (que se muestran en la figura 2.3.1-18) y se confirma que aquellos incluyen las mediciones de los parámetros de gestión de rendimiento aquí señalados y de entre ellos escogemos los indicadores claves de rendimiento (KPI) que se presentan a continuación y que se aplicarían para cada router que conforma la red de comunicaciones del ISP.

Los valores límites definidos para cada KPI se basan en estándares internacionales, utilizados por otros operadores internacionales, regulaciones nacionales sobre calidad de servicio y a los acuerdos de niveles de servicio denominados SLA que cada proveedor ofrece a sus usuarios en un entorno competitivo.

KPI	Indicadores Utilizados	MIDE	Unidad	Cálculo	Valores límites
PARA CADA INTERFAZ DEL ROUTER					
AB TOT (Ancho de banda Total)	V.down V.up	Cantidad de bits por segundo totales en una interfaz	Kbits/seg	AB TOT = 100 * (V.down + V.up) /AB	<= 80% AB = ancho de banda máximo de la interfaz
PQD OUT (Paquetes descartados salientes)	Pd.out Pqu.out	Relación (%) entre #paquetesdescartados y # paquetes transmitidos	%	PQD OUT= 100 * (Pd.out / Pqu.out)	<= 3%
PARA CADA ROUTER					
LAT (LATENCIA)	Lat	Suma de retardos temporales en el equipo que retrasan los paquetes	mseg	LAT = Lat (Directo sin cálculo)	<=2,4 mseg
DISP (Disponibilidad)	Disp	Tiempo que el equipo permanece operativo	%	DISP = 100% - Disp	>= 99,99%
JIT (JITTER)	Jit	Variación de latencia de paquetes	mseg	Jit (Directo sin cálculo)	<= 1,2mseg
CPU (Carga CPU)	Cpu	Carga de procesamiento del CPU	%	Cpu (Directo sin cálculo)	<= 80%

Fig. 2.4-1 KPI de rendimiento para equipos de red de comunicaciones del ISP

Con la finalidad de obtener referencias de parámetros internacionales para los KPI definidos, a continuación se presentan KPI que disponen operadores internacionales como Verizon[24] y NTT[25].

NTT también publica en su sitio WEB,la tasa de pérdida de paquetes que ofrece un máximo de 0,3% y para Jitter un máximo de 10 mseg.

[24] www.verizonenterprise.com/about/network/latency
[25] www.ntt.net/english/service/sla_ts.html

Verizon Enterprise Solutions Latency Statistics for Country Specific Metrics (ms)												
	2015		2014									
	February	January	December	November	October	September	August	July	June	May	April	March
Hong Kong to US (230.000)	166.209	159.445	152.159	152.100	152.194	155.080	168.440	167.816	168.204	167.334	168.110	166.528
Singapore to US (260.000)	182.582	178.739	182.881	180.743	181.859	175.581	173.547	175.399	172.131	177.268	174.881	177.441
Australia to US (210.000)	154.623	154.578	154.576	154.575	154.799	154.332	153.758	153.779	153.759	153.774	153.805	153.731
Argentina to US (160.000)	124.785	124.489	124.606	124.467	127.916	132.293	134.318	133.827	135.369	131.978	132.171	126.272
Brazil to US (130)	115.511	115.205	116.079	116.327	115.870	115.891	114.529	108.632	108.602	113.185	115.981	116.201
Chile to US (150.000)	98.488	99.093	98.321	99.078	97.730	98.636	98.627	98.768	98.834	98.631	98.856	122.395
Colombia to US (95.000)	57.209	57.531	57.187	57.973	58.582	58.500	58.064	59.518	58.039	58.735	58.528	58.169
Panama to US (60.000)	46.771	45.859	45.854	46.340	46.267	46.231	48.758	49.254	49.253	49.246	49.258	49.264
Venezuela to US (110.000)	54.416	50.249	50.894	50.325	50.141	50.135	50.119	50.043	58.111	49.999	50.017	49.989
NA to India (380.000)	252.008	253.387	266.727	293.393	285.620	253.937	279.740	289.906	273.684	276.699	288.691	285.906
NA to Intra EMEA (110.000)	87.624	89.164	87.983	88.067	88.046	88.827	88.836	88.464	88.789	88.385	88.731	89.079
NA to Korea (200.000)	139.181	139.011	138.163	139.051	139.348	139.289	139.583	139.509	144.864	139.922	139.939	139.006
NA to Taiwan (220.000)	143.291	144.054	143.598	143.373	143.766	143.740	143.817	143.673	145.132	146.655	143.685	143.711

Fig. 2.4-2 valores estadísticos de latencia (latency) que ofrece Verizon

NTT Communications

Region	Reference value (Latency)
Intra-Japan	25ms
Intra-Asia	95ms
Intra-US	60ms
Intra-Europe	35ms
Trans-Atlantic	90ms
Japan-US	130ms
Japan-Europe	300ms

Month	Intra-Japan (25ms)	Intra-Asia (95ms)	Intra-US (60ms)	Intra-Europe (35ms)	Trans-Atlantic (90ms)	Japan-US (130ms)	Japan-Europe (300ms)
Dec 2014	9.90	56.25	42.57	21.76	71.87	90.35	202.36
Jan 2015	9.79	57.37	41.80	21.86	71.95	87.63	212.43
Feb 2015	10.02	57.18	41.70	21.57	70.51	88.79	205.32

Fig. 2.4-3 valores estadísticos de latencia (latency) que ofrece NTT

Estas referencias nos permiten ubicar valores de los KPI que guarden relación con el

entorno competitivo, aclarando que estos grandes operadores internacionales se encuentran en el denominado nivel de Tier1 que manejan el backbone mundial de internet (por el cual circula todo tipo de tráfico), mientras que CNT EP a través de la NAP en Miami se interconecta con estos Tier1. La latencia depende de algunos factores, entre ellos de cuantos saltos (equipos routers) atraviese el enlace y por ello que no es una medida única ni constante y tiene variaciones.

Cuando el operador aplica un SLA predeterminado entonces lo que configura es QoS en su backbone para establecer una ruta que priorice este tráfico (paquetes de alta prioridad) y evitar muchos saltos, reduciendo la latencia.

En la red de CNT EP a nivel de su backbone MPLS nacional, también existe la posibilidad de ofrecer SLA específicos para enlaces de datos de clientes corporativos, aplicar priorización de tráfico para servicios de telefonía fija o móvil, mediante la implementación de QoS. A nivel del servicio de internet para el segmento masivo los valores de latencia varían dependiendo de los equipos de acceso, ruta del backbone nacional y priorización del tráfico.

A continuación se muestra una medida de latencia de la red de de internet de CNT EP (incluye acceso, backbone e ISP) medida obtenida con el aplicativo de prueba de velocidad que CNT EP dispone en su página web[26], de libre acceso para sus usuarios.

[26] http://speedtest.cnt-grms.com.ec/

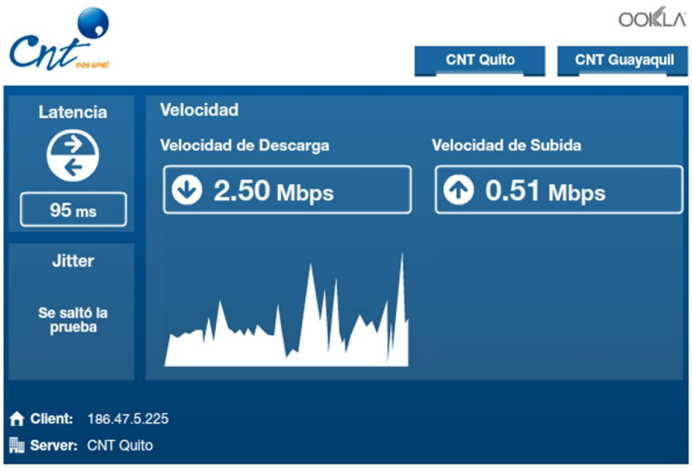

Fig. 2.4-4 Medición de velocidad y latencia en operador CNT (usuario internet masivo)

Por lo indicado, siendo el ISP una parte de la red de CNT EP y considerando que estos valores de Latencia engloban toda la red, para los equipos de la red de comunicaciones del ISP, se hace necesario establecer un valor máximo de latencia.

Este valor se lo puede definir, tomando en cuenta los datos de mediciones históricas y que han venido funcionando con un buen desempeño de la red, así si tomamos el indicador de latencia durante un tiempo de tres meses que hemos monitoreado en PRTG, tenemos que puede establecerse en 2,4 mseg, como se muestra en la siguiente figura.

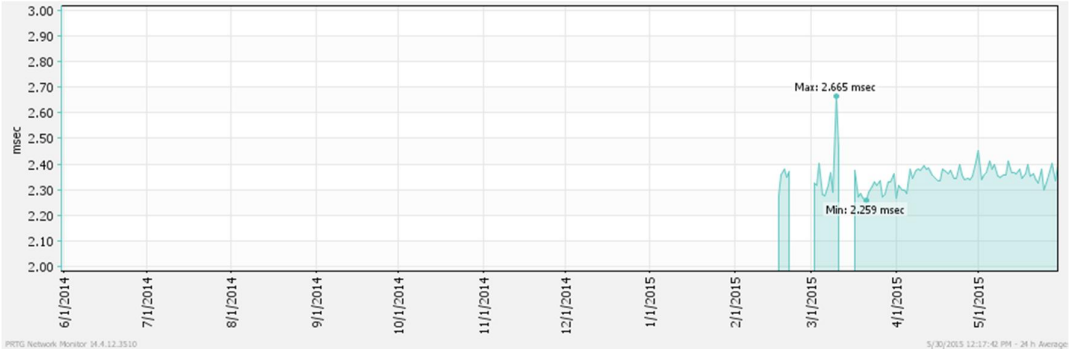

Fig. 2.4-5 Valores históricos de latencia en router de borde

Similarmente para el KPI de JITTER, es necesario definir un valor para el ISP y por ello se toman también valores históricos que se obtienen de PRTG.

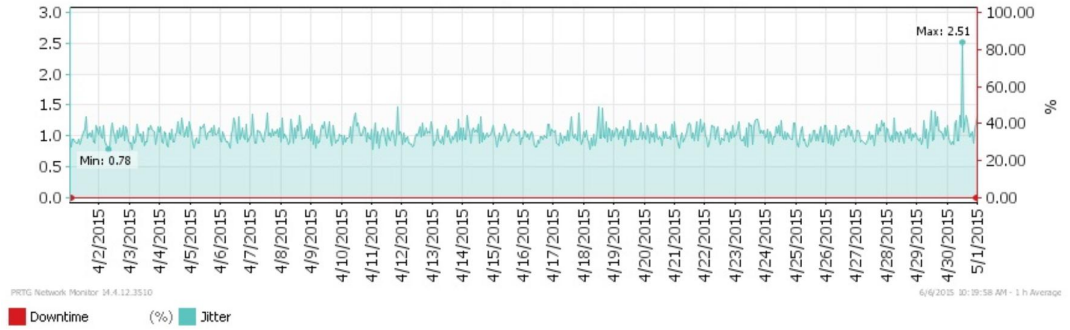

Fig. 2.4-6 Valores históricos de Jitter en router de borde

Como se observa en la Fig. 2.4-6, un valor de Jitter que podemos asignar es el de 1,2mseg.

Hay que tomar en cuenta que la sonda de PRTG está instalada en un servidor que se conecta a los routers del ISP por medio del VSS de acuerdo al esquema de conexión

que se muestra a continuación.

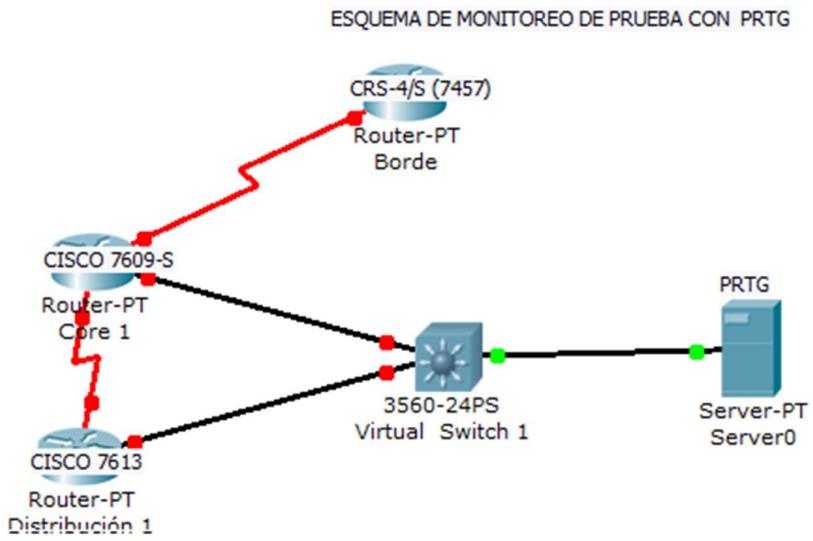

Fig. 2.4-7 Esquema de conexión de monitoreo con PRTG

Los KPI indicados en la figura 2.4.1 cumplen con los principales requerimientos de una gestión del rendimiento siendo estos:

- Monitoreo del tráfico y ancho de banda utilizado en los equipos de comunicaciones del ISP.
- Monitoreo de Disponibilidad de los equipos.
- Monitoreo de QoS (latencia, pérdida de paquetes, Jitter)
- Monitoreo de la capacidad de procesamiento de los equipos (carga CPU)

3 CAPITULO 3: PROCESO DE GESTION DE RENDIMIENTO

3.1 INTRODUCCION A PROCESOS

3.1.1 Definición de Proceso

Se toma como referencia lo definido en la Norma ISO 9001 -2008 [9][27], la cual promueve la adopción de la gestión de la calidad enfocada en procesos y lo define así:

"Una actividad o un conjunto de actividades que utiliza recursos, y que se gestiona con el fin de permitir que los elementos de entrada se transformen en resultados, se puede considerar como un proceso".

La norma enfatiza la importancia de:

a) la comprensión y el cumplimiento de los requisitos,

b) la necesidad de considerar los procesos en términos que aporten valor,

c) la obtención de resultados del desempeño y eficacia del proceso, y

d) la mejora continua de los procesos con base en mediciones objetivas

En la figura 3.1 a continuación se representa gráficamente un proceso y sus actividades, si bien está orientada a procesos generales en una empresa, es aplicable también a los procesos de gestión del rendimiento que queremos desarrollar.

[27] Referencia bibliográfica [9] (ISO, 2008)

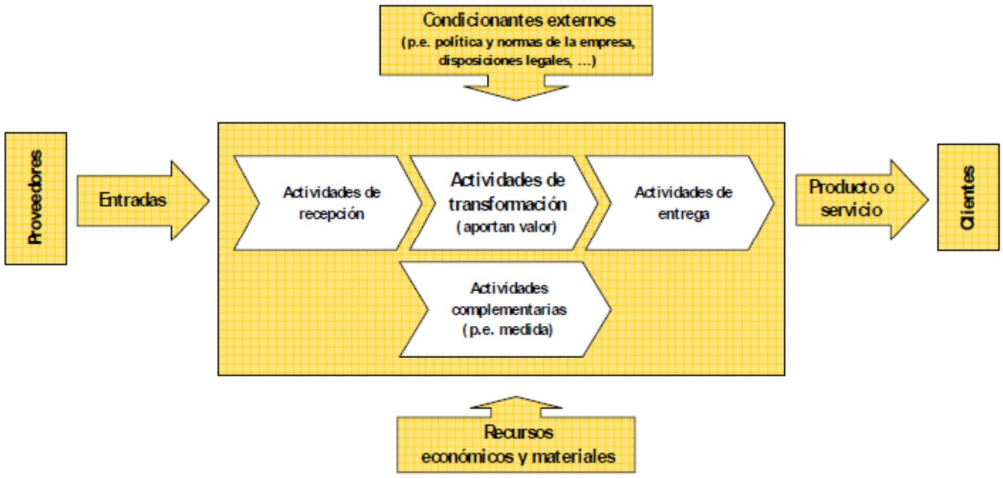

Fig. 3.1 Representación gráfica de un proceso [8] [28]

3.1.2 Descripción del Proceso

Un proceso se describe por lo siguiente [8] [29]:

Misión: Propósito o razón de ser del proceso (debe generar valor)

Propietario: Responsable de la administración del proceso y sus resultados

Entrada: Lo que debe ser transformado en el proceso (Puede ser la salida de otro proceso)

Salida: Producto, servicio o información generada en el proceso (Puede ser la entrada de otro proceso)

Cliente: Receptor de la salida del proceso, pueden ser internos o externos

Proveedor: Aporta el producto, servicio o información necesaria para el proceso

Actividades: Conjunto de tareas secuenciales y recurrentes para transformar la entrada en salida o para el control interno del proceso.

[28] Referencia bibliográfica [8] (Sanchez, 2007)
[29] Referencia bibliográfica [8] (Sanchez, 2007)

Recursos: Medios materiales y económicos disponibles

Condicionantes

Externos: Reglamentan, limitan o establecen la forma en que pueden desarrollarse las actividades.

Indicadores: Datos o conjunto de datos que ayudan a medir objetivamente la evolución del proceso.

Para el presente trabajo, los indicadores que servirán de base para la definición de los procesos son los denominados KPI de rendimiento (desempeño) de la red de comunicaciones (routers) del ISP, los cuales han sido ya definidos y constan en la figura 2.4-1 del Capítulo II.

3.2 Estructura Organizacional de la CNT EP

Con la finalidad de establecer quién será el propietario del proceso y cuáles serán los clientes internos que utilicen la información generada en el proceso, se revisa la estructura orgánica funcional de CNT EP [1] [30].

La Corporación Nacional de Telecomunicaciones en lo que se refiere al área Técnica está estructurada como se muestra en la figura 3.2-1.

En esta estructura se ha colocado las aéreas funcionales que se encargan del ISP, así tenemos:

[30] Referencia bibliográfica [1] (CNT, 2014)

- OyM ISP, se encarga de las actividades de operación y mantenimiento del ISP, adicionalmente de configurar y mantener operativa la herramienta de gestión PRTG.
- GD ISP, se encarga de la Gestión del Desempeño del ISP, esta área es la que recolecta la información de los KPI de desempeño(rendimiento) del ISP y genera los respectivos reportes a OyM e Ingeniería
- OyM TX MPLS, se encarga de la operación y mantenimiento del backbone de MPLS, al cual se conecta la red de comunicaciones del ISP.
- ING ISP, se encarga de analizar los reportes del KPI del ISP y en base a ellos , definir si se requieren procesos de mejoramiento(optimización) o ampliación de Red, diseñar, adquirir (procesos de compra) e implementar las ampliaciones de red del ISP.

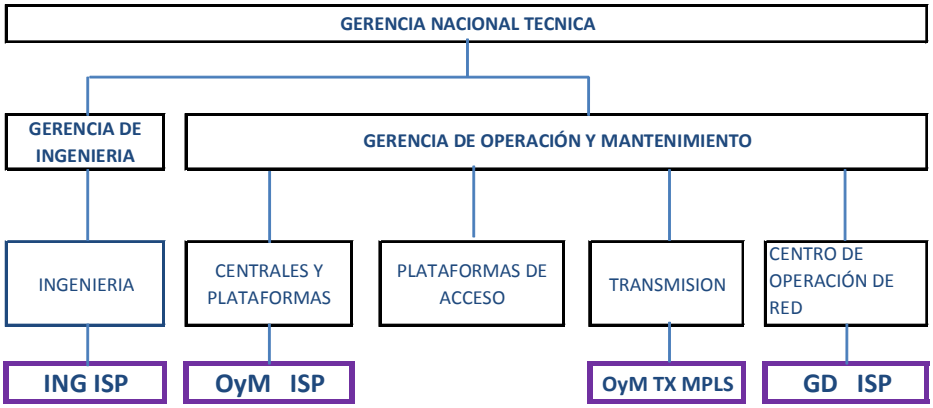

Figura 3.2-1 Estructura organizacional área técnica CNT EP

3.3 Definición y elaboración de los procesos

En la figura 3.3-1 se muestra la definición del proceso general que aplica a todos los KPI de rendimiento del ISP, luego se procede a elaborar los diagramas de flujo para los procesos particularizados por cada KPI.

Para el presente trabajo los indicadores que servirán de base para la definición de los procesos son los denominados KPI de rendimiento (desempeño) de la red de comunicaciones (routers) del ISP, los cuales han sido ya definidos y constan en la figura 2.4-1 del Capítulo II.

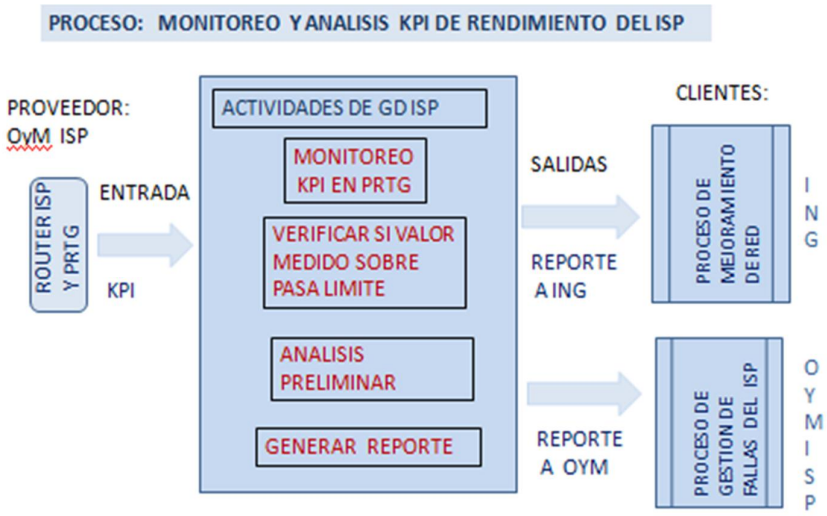

Figura 3.3-1 Proceso monitoreo y análisis KPI de rendimiento del ISP

Los procesos están orientados hacia el área funcional GD ISP (Gestión del Desempeño de la CNT EP) la cual, de acuerdo a la estructura forma parte de Operación y Mantenimiento y como tal está encargada del monitoreo de los KPI de

rendimiento y generación de reportes del estado de la Red del ISP.

Los reportes generados por GD ISP hacia el área de Ingeniería, son analizados en conjunto con otros reportes de toda la red de CNT EP, los procesos de Ingeniería formarían parte de otro análisis más amplio, considerando otros KPI de los demás componentes de la red, como Backbone MPLS, Red de Acceso, Red del Core Fijo-Móvil se considera no están dentro del alcance de este trabajo.

Los diagramas de flujo constituyen una herramienta muy utilizada para describir los procesos, ya que permiten explicar de mejor manera las actividades y las áreas involucradas, en CNT EP se los utiliza y son registrados oficialmente en su base de información (MAI) de procesos, cumpliendo con la norma de calidad.

Los diagramas de flujo tienen símbolos estandarizados para explicar las actividades y no entraremos en detalles explicativos de los mismos, asumimos que son conocidos por la mayoría de empresas u organizaciones. Un software que permite su elaboración en computadora y facilita su diseño se denomina Visio (viene en el paquete de office de Microsoft) y es el que se utiliza para su elaboración.

A continuación se presentan los diagramas de flujo de los procesos definidos para cada KPI.

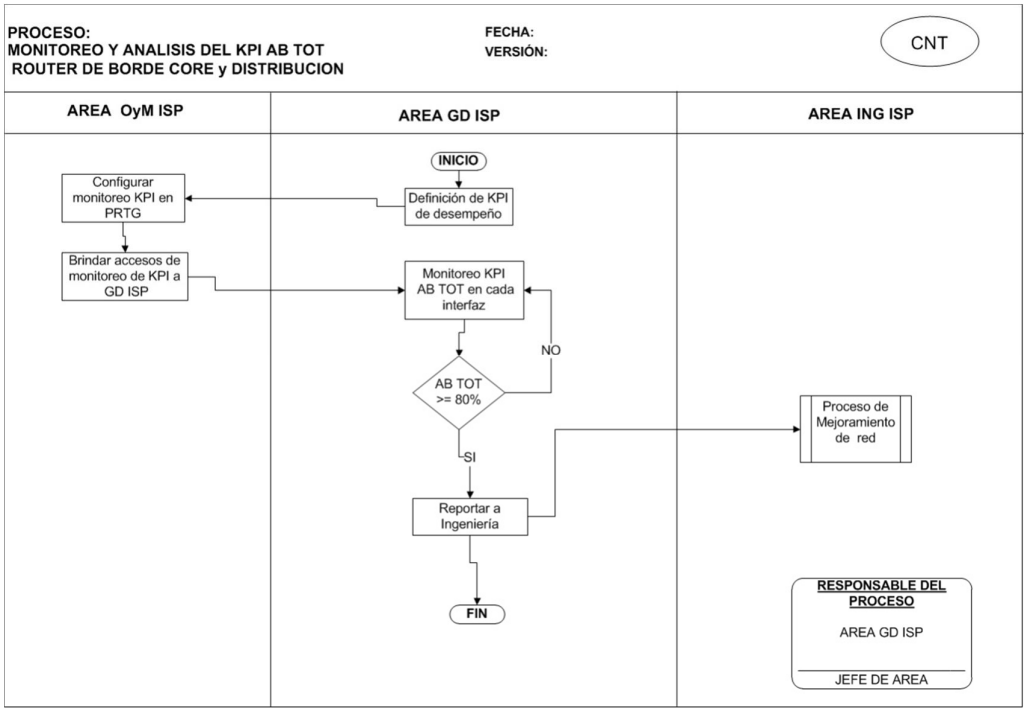

Figura 3.3-2 Proceso monitoreo y análisis KPI AB TOT

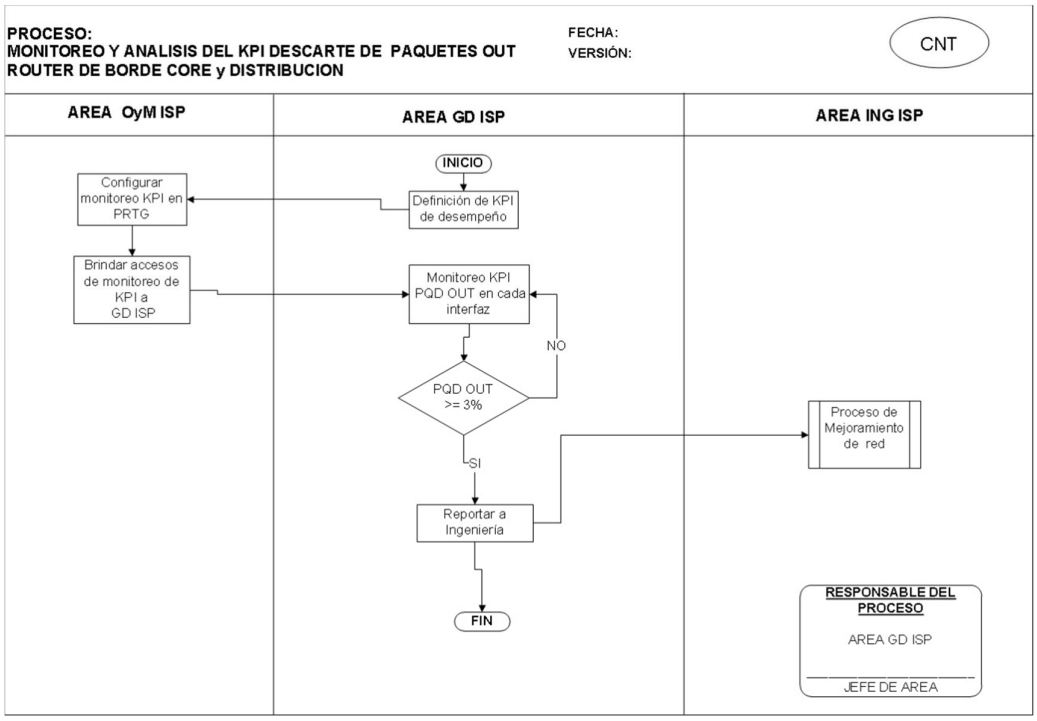

Figura 3.3-3 Proceso monitoreo y análisis KPI PQD OUT

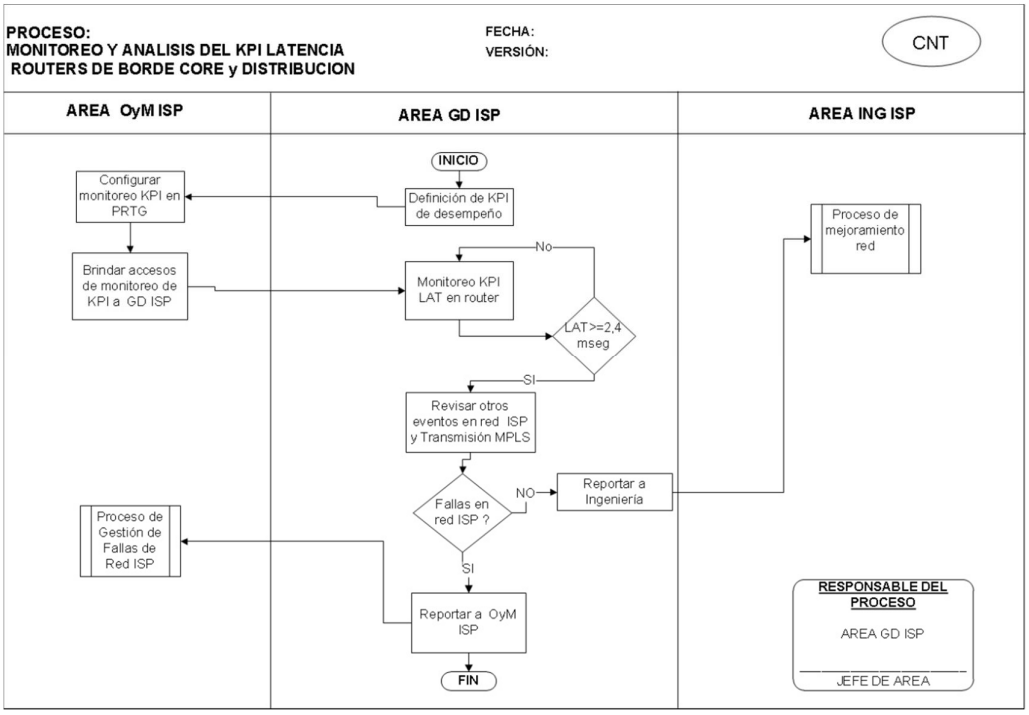

Figura 3.3-4 Proceso monitoreo y análisis KPI LATENCIA

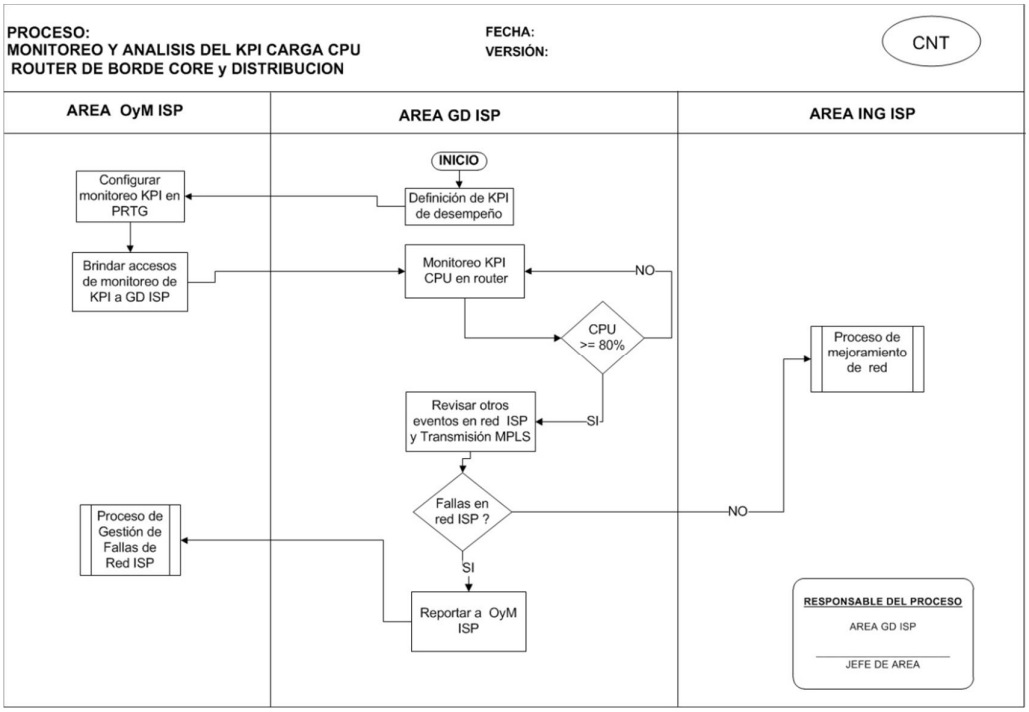

Figura 3.3-5 Proceso monitoreo y análisis KPI CPU

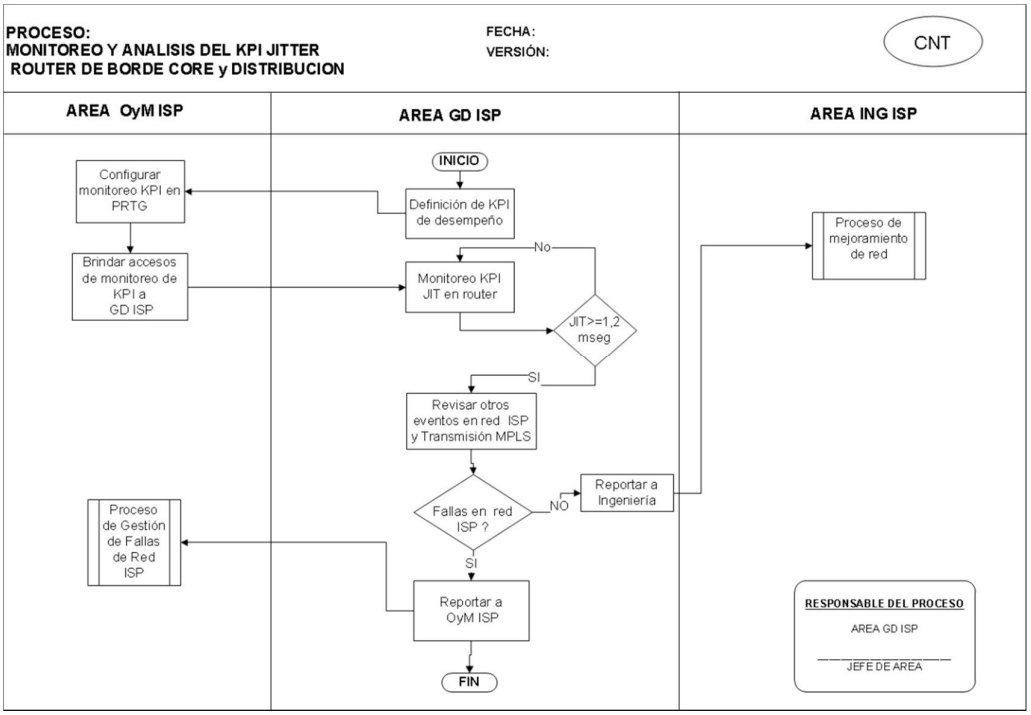

Figura 3.3-6 Proceso monitoreo y análisis KPI JITTER

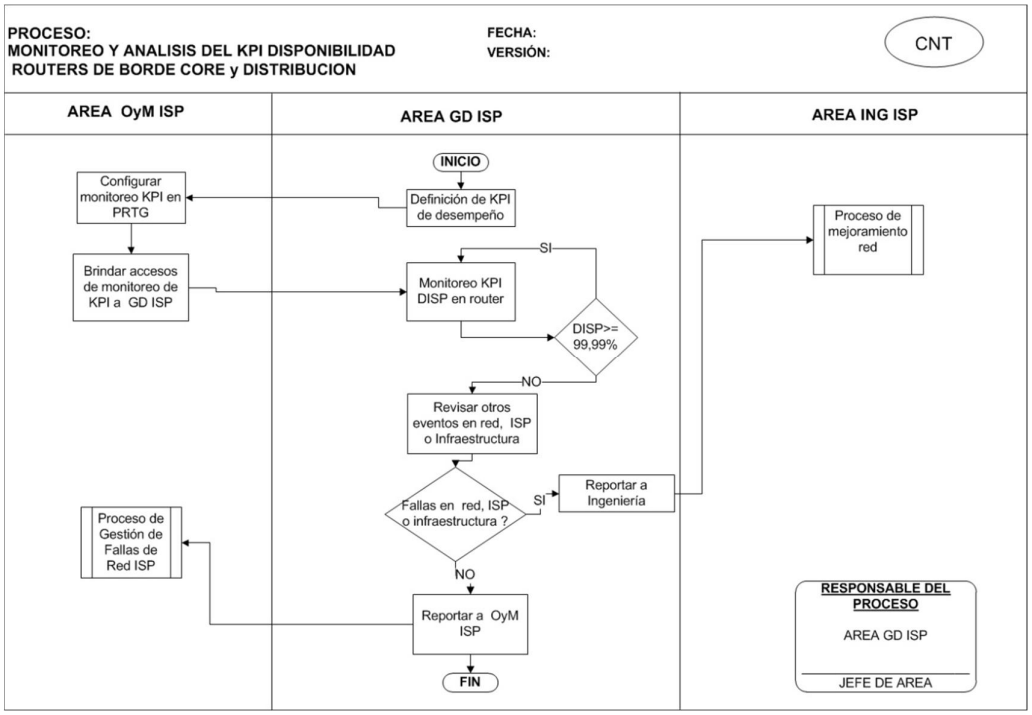

Figura 3.3-7 Proceso monitoreo y análisis KPI DISP

4 CAPÍTULO 4: EJERCICIO PRÁCTICO

4.1 Obtención de los KPI en el equipo de Borde en tiempo real.

Previo a obtener las mediciones de los KPI de los equipos de comunicaciones del ISP se verifica que el software de monitoreo PRTG se encuentre operativo y configurado.

Se utiliza un computador (laptop) con sistema operativo windows 7, un explorador (motzila), una VPN (Cisco) para disponer de un acceso seguro y los permisos respectivos de acceso a PRTG.

Para este ejercicio práctico se utiliza un servidor de pruebas con el respectivo software de monitoreo PRTG. Esto nos permite realizar configuraciones de monitoreo y experimentar con los sensores de PRTG sin afectar al monitoreo en producción que utiliza CNT EP.

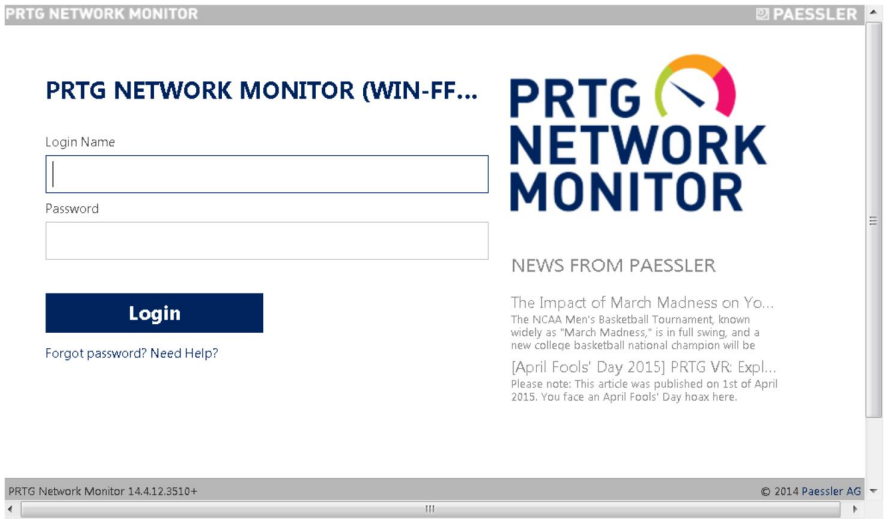

Fig. 4.1-1 Acceso a PRTG[31]

[31] Los gráficos presentados en este capítulo corresponden a capturas de pantalla del PRTG implementado

A continuación se introduce usuario, clave y accedemos a la pantalla inicial preconfigurada.

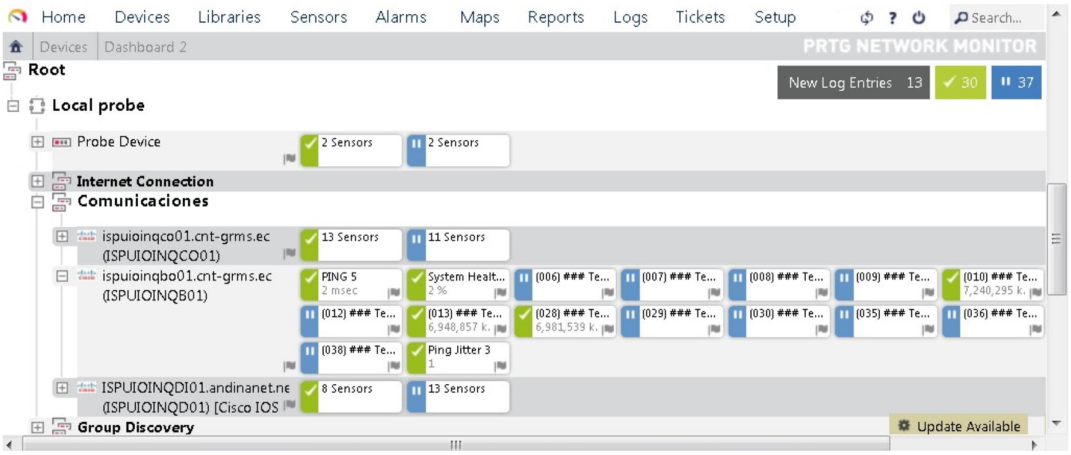

Fig. 4.1-2 Pantalla inicial de monitoreo PRTG de equipos de comunicación ISP

En esta pantalla inicial se ha configurado el grupo denominado Comunicaciones, en el cual se incluyen tres equipos de comunicaciones del ISP, el router denominado ISPUIOINQC001 que corresponde a equipamiento del CORE, el router ISPUIOINQB01 que corresponde al equipamiento de BORDE y el router ISPUIOINQD01 que corresponde a equipamiento de DISTRIBUCION.

Cada equipo tiene configurado ciertos sensores que monitorean los KPI que se han predefinido y otros adicionales de pruebas. Los sensores en color verde significan que están activos y los de color azul están pausados o detenidos temporalmente.

En esta pantalla podemos observar que los sensores en color verde indican actividad, es decir están operando normalmente, PRTG los pondrá

automáticamente en otro color si detecta alguna anomalía de su estado, esto es, se pondrán en color tomate si existe una advertencia (warning) de alguna intermitencia o en rojo si existe alguna falla (sensor down).

También PRTG permite configurar una opción de envío de mensajes de correo electrónico a cuentas de usuarios preconfiguradas, cuando existen alarmas o sensores que sobrepasan los umbrales predefinidos. En este caso por ejemplo se podrían configurar mensajes notificadores a ciertos usuarios cuando la medición de un indicador sobrepase un valor límite predefinido. Esta opción se configura preferentemente para la gestión de fallas.

Para este ejercicio se toman las mediciones del equipo de BORDE, por ello apuntamos con el cursor sobre el sensor que nos interese, dentro del grupo de sensores asociados a cada equipo cuyo nombre aparece en la pantalla de PRTG (Fig 4.1-2) y pulsamos la tecla enter.

4.1.1 KPI LAT (LATENCIA)

Para obtener mediciones del KPI LAT (latencia) ingresamos al sensor PING, el cual nos presenta el indicador de latencia Lat definido en el capítulo 2 de este trabajo (Fig. 2.3.1-18) y su KPI asociado LAT (Fig. 2.4-1) que en este caso es directo, es decir no hace falta más cálculos.

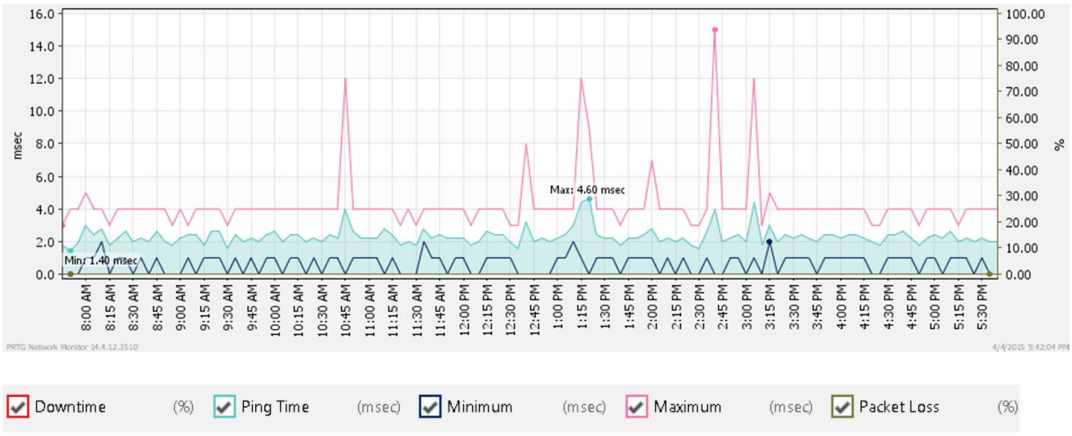

Fig. 4.1.1-1 Valores diarios del KPI LAT

PRTG muestra gráficos y tablas para mayor detalle, sin embargo la forma preferente de monitoreo son los gráficos que permiten una mejor visualización. Para los valores históricos se pueden configurar diferentes periodos de medición, en este caso se han configurado para 2 días ,30 días y 100 dìas.

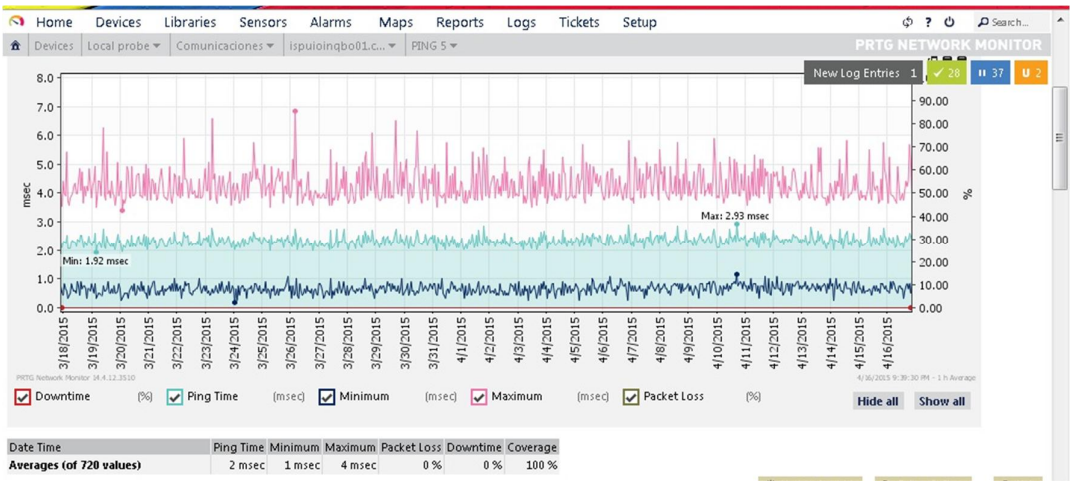

Fig. 4.1.1-2 Valores de 30 días del KPI LAT

PRTG presenta las mediciones como se indican en la figura 4.1.1-2, la gráfica de color celeste corresponde al Ping Time y es el valor promedio de latencia que se debe tomar. Adicionalmente PRTG también muestra los valores máximos y mínimos que corresponden a las gráficas de color rojo y azul respectivamente. Es importante destacar que en razón de que la latencia medida como tiempo de respuesta a un PING depende de algunos factores como tiempo de procesamiento del router, tiempo en colas, saltos en equipos intermedios, en caso de alto tráfico manejo de prioridad de paquetes, sus valores son variables y por ello se calcula un tiempo promedio.

Del monitoreo se obtiene entonces que LAT (Latencia) para este router de Borde se mantiene en un valor promedio (average) de 2mseg, sin sobrepasar el valor límite establecido de 2, 4 mseg, para este KPI (ver Fig.2.4-1).

Existen ciertos valores picos ocasionales como el que aparece en la Fig.4.1.1-1 que alcanza los 4,6 mseg, que no afectan mayormente al promedio, estos deberán analizarse si se vuelven muy repetitivos.

4.1.2 KPI JIT (JITTER)

Para obtener las mediciones de este KPI de Jitter ingresamos en el sensor denominado Ping Jitter, el cual nos entrega el indicador Jit directamente.

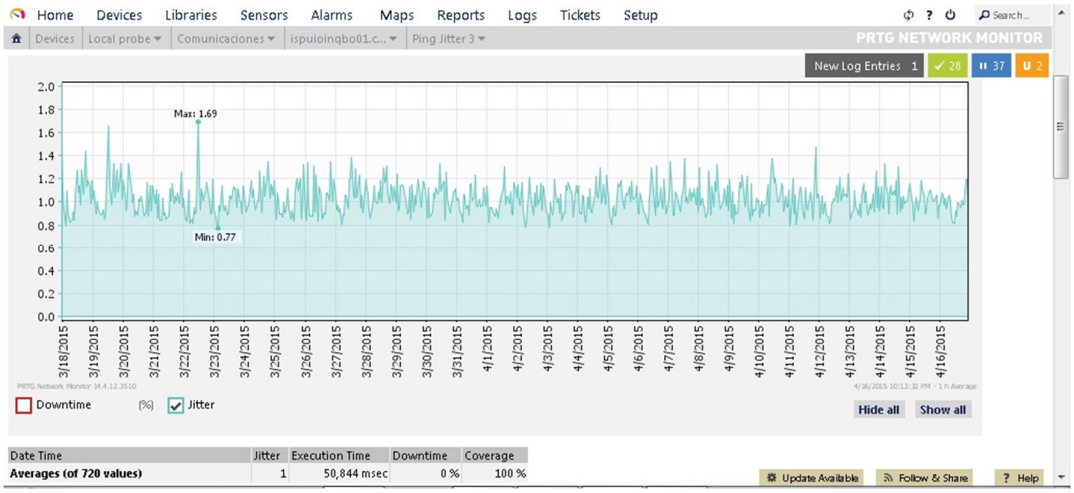

Fig. 4.1.2-1 Valores de 30 días del KPI JIT (Jitter)

El KPI JIT mantiene un promedio de 1mseg, por debajo del valor límite preestablecido para este KPI que es de 1,2 mseg, se observa que ocasionalmente alcanza valores picos de 1,4 y 1,69 mseg, los cuales deberán analizarse si se presentan repetitivamente.

4.1.3 KPI ABTOT (ANCHO DE BANDA TOTAL, VELOCIDAD)

Para obtener este KPI ingresamos al sensor de snmp-traffic de una de las interfaces y observamos los siguientes gráficos que se muestran a continuación.

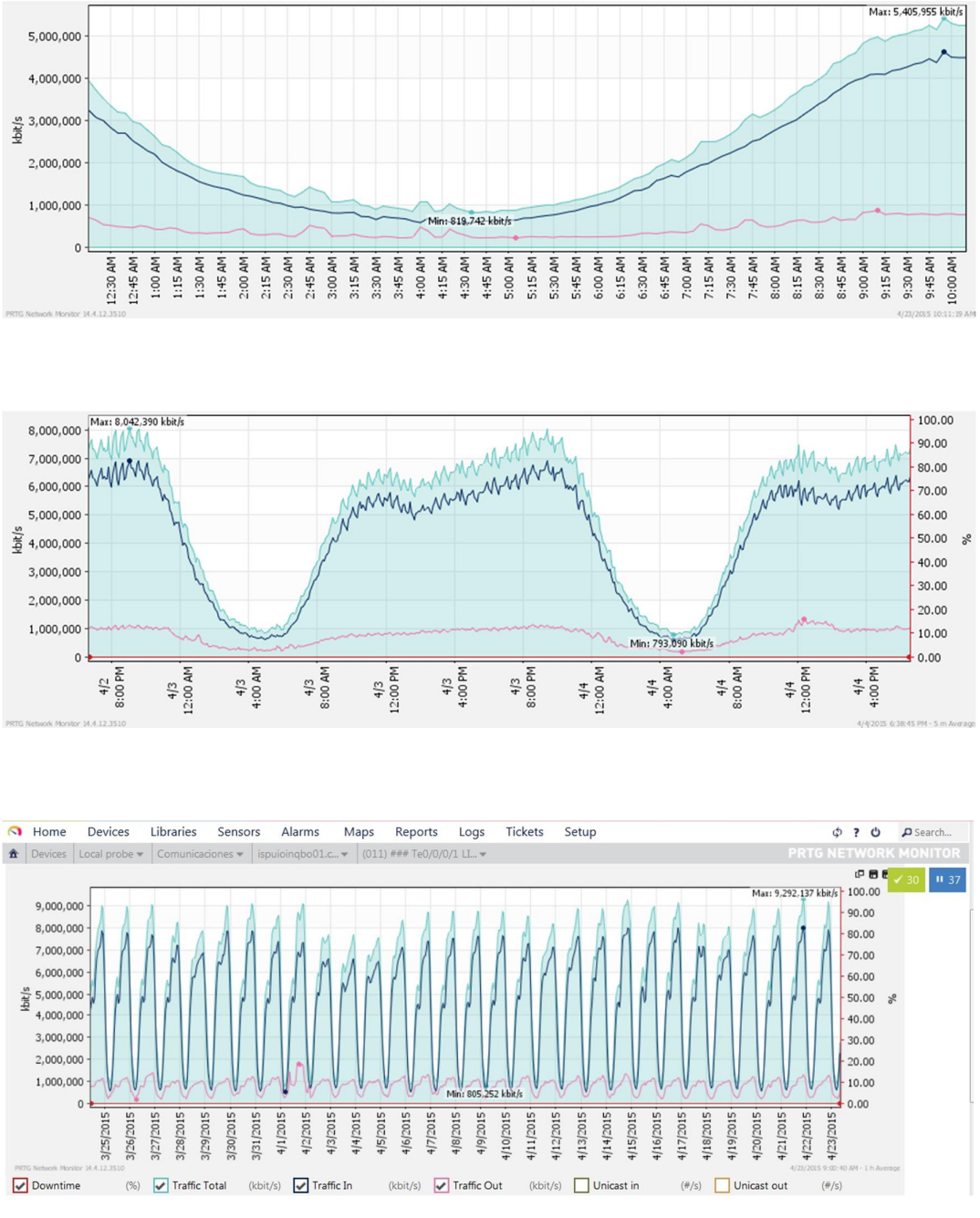

Figura 4.1.3-1 Valores diarios, de 2días y 30 días del KPI AB TOT

El gráfico en PRTG puede mostrar todas las mediciones que contiene este sensor

con sus diferentes canales (channels), por ello es necesario marcar con un visto únicamente aquellas que nos interesan para este KPI, esto es Tráfico Total, Trafico In (entrante), Tráfico Out (Saliente), expresado en Kbits/seg, es decir mide el ancho de banda consumido o velocidad.

Recordemos que el KPI AB TOT se obtiene (ver figura 2.4-1 del capítulo 2):

AB TOT = 100* (Vout + Vin)) / AB

De acuerdo a la figura 4.1.3-1 la suma de Vout (TrafficOut) + Vin (Traffic In) se la obtiene directamente en la curva de color celeste (TrafficTotal), la cual en algunos días alcanza un pico de 9 Gbps .

Entonces,

AB TOT = 100* (9 Gbps/10 Gbps) = 90%

El valor de KPI AB TOT sobrepasa su valor límite predefinido del 80%.

PRTG también entrega directamente este %, si observamos al lado derecho de la figura 4.1.3-1, existe una escala que marca el porcentaje, ya que PRTG automáticamente conoce la capacidad de AB de la interfaz, la cual es de 10 Gbps.

4.1.4 KPI CPU (CARGA DEL CPU)

Para acceder al KPI CPU que mide la carga del CPU en el router se selecciona el sensor Healthsystem y obtenemos el siguiente gráfico.

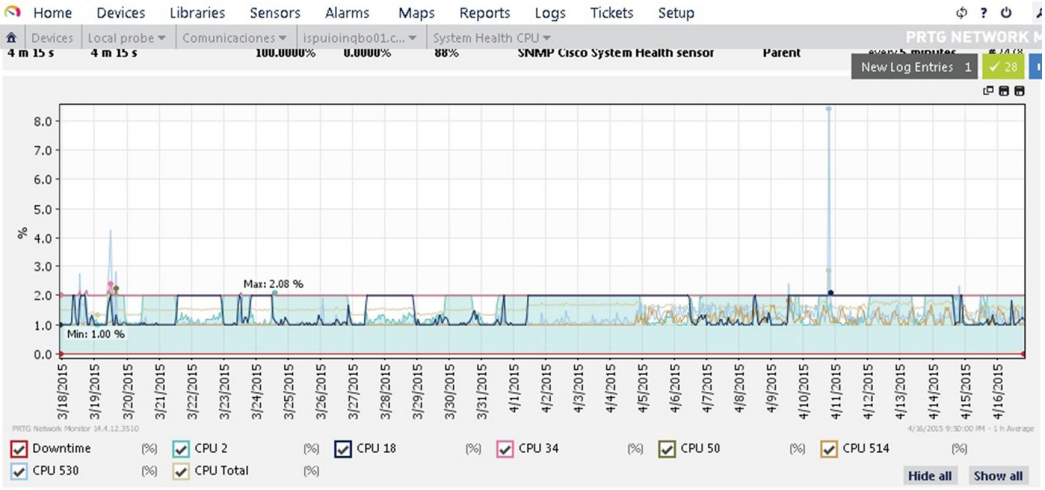

Fig. 4.1.4-1 Valores de 30 días del KPI CPU

Como se observa en el gráfico de la Figura 4.1.4-1, la carga de los CPU alcanza un valor promedio del 2% en este router, muy por debajo del valor límite establecido para este KPI del 80%.

PRTG nos entrega las mediciones de carga para cada CPU del router y un valor promedio total. En este gráfico se refleja un pico de carga máximo medido para el CPU2 que llegó al 8%, valor ocasional y único de este periodo, de repetirse con más frecuencia, habría que investigar las causas que lo provocaron.

4.1.5 KPI DISP (DISPONIBILIDAD)

Para el monitoreo del KPI de disponibilidad utilizamos el mismo sensor Ping que para latencia, por lo que para observar su valor, se lo hace en el mismo gráfico del KPI de latencia. Para mayor claridad del gráfico, marcamos (con un visto bueno) únicamente en el valor de disponibilidad (Downtime) y obtenemos el siguiente

gráfico.

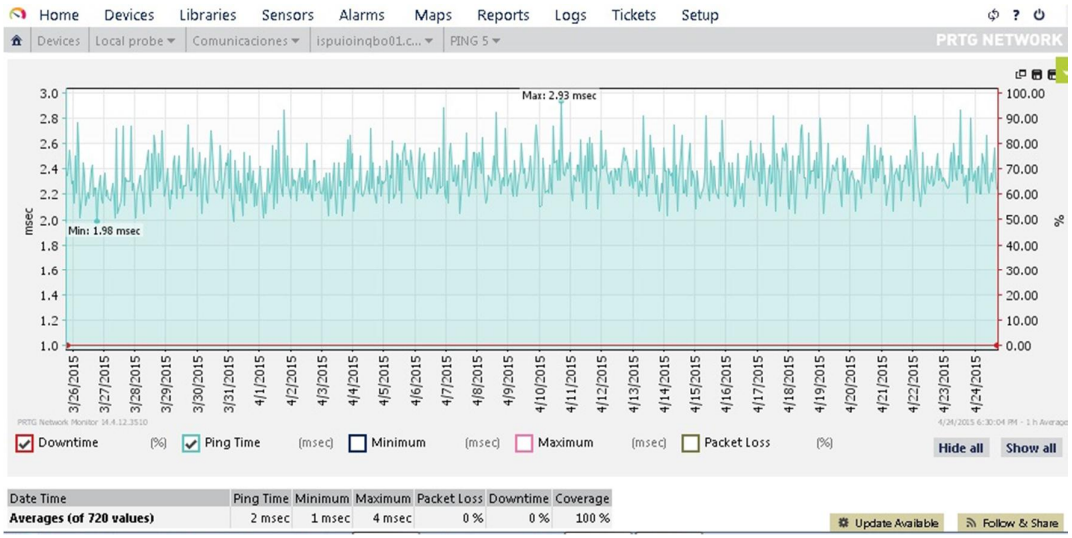

Fig. 4.1.5-1 Valores de 30 días del KPI DISP

En este gráfico observamos la línea roja que representa el casillero marcado como Downtime, este indicador nos da en porcentaje, el tiempo en que el router no estuvo disponible sobre el tiempo de medición, en este caso de 30 días.

El valor obtenido es de 0%, es decir el router estuvo disponible (en servicio) el 100% del tiempo en este monitoreo de 30 días. Este KPI por tanto cumple por encima de su valor límite mínimo predefinido que es del 99,99%.

4.1.6 KPI PDOUT (DESCARTE DE PAQUETES SALIENTES)

Para monitorear este KPI utilizamos el mismo sensor de tráfico, el cual por uno de sus denominados canales (channels) nos entrega la medición del indicador Pqu.out

(cantidad de paquetes unicast transmitidos) y por otro mide el indicador Pd.out (cantidad de paquetes descartados, no transmitidos).

Para visualizar estos indicadores, utilizamos el mismo gráfico que entrega el sensor de tráfico y marcamos con un visto los casilleros denominados Unicastout y Discardsout, como se presenta en la figura 4.1.6-1.

El KPI PDOUT se calcula de acuerdo a lo indicado en la figura 2.4-1:

PQD OUT= 100 * (Pd.out / Pqu.out)

Fig. 4.1.6-1 Valores de 10 días del KPI PDOUT

En este gráfico, tomamos un dato en el mismo instante de tiempo para los dos indicadores (pico del día 30/03/15) y el valor que obtenemos para Pd.out (Discardsout) es de 0 paquetes/seg y para Pqu.out (Unicastout) obtenemos 900.000 paquetes/seg, lo cual nos da un valor para el KPI PQD OUT de 0%.

Este valor está por debajo del límite máximo establecido para este KPI que es del 3%, es decir esta dentro de lo esperado como comportamiento normal del router.

4.2 Aplicación de los procesos de Gestión de Rendimiento.

Con este ejercicio lo que se pretende es verificar la lógica de los procesos definidos para la Gestión del Rendimiento del ISP. Es decir se hace un seguimiento a los flujos de actividades de cada proceso desarrollado en el capítulo 3 y representados mediante sus correspondientes diagramas de flujo, tomando una muestra que la hemos obtenido del monitoreo de los KPI para el router de Borde.

Para el proceso Monitoreo y análisis del KPI ABTOT cuyo diagrama de flujo se muestra en la figura 3.3-2, tenemos:

- Definición del KPI del desempeño: Los KPI fueron definidos en el capítulo 2 (ver figura 2.4-1). Se aplicarían estas definiciones para el ISP de la CNT EP
- Configurar monitoreo KPI en PRTG: Se ha configurado en PRTG (servidor de prueba) el monitoreo de los indicadores que utilizan los KPI (ver figura 1.4-2). En el ISP de la CNT EP se deberá configurar en el servidor (en producción) de PRTG de monitoreo.
- Brindar los accesos de PRTG a la unidad GD ISP: Para este ejercicio se han configurado los accesos a una PC-laptop desde la cual se han obtenido las mediciones. En la ejecución práctica en CNT EP, la unidad de OyM ISP que opera PRTG otorgará los accesos en función del usuario y perfil autorizado a la unidad GD ISP.
- Monitoreo KPI AB TOT en cada interfaz de cada router: Para este trabajo hemos implementado el monitoreo de algunas interfaces. En CNT EP se deberá implementar para todas las interfaces y todos los routers (ver figura 1.1-1). Para

esto es importante tener en cuenta la capacidad de sensores que dispone PRTG.

- Toma de decisión :El valor del KPI AB TOT es mayor o igual a 80%?
    - NO, es decir es menor, se considera normal y se continúa monitoreando.
    - SI, se debe reportar a Ingeniería a la unidad ING ISP. En este caso se ha obtenido para el router de borde un valor superior al 80% y por ello en la ejecución práctica en CNT EP se deberá reportar a la unidad de Ingeniería del ISP.
- La unidad de ING ISP: ejecutará su proceso de ampliación de red, dado que la capacidad de esta interfaz ha llegado a su límite. Este proceso en CNT EP incluye un análisis de la demanda del servicio actual y proyectada con el fin de dimensionar la capacidad necesaria y realizar un proceso de ampliación de capacidad del equipo, si este lo permite o adquirir más equipos. Podría también incluir un rediseño de la configuración del ISP. Este proceso no se incluye en el alcance de este trabajo.

Para los otros procesos que tienen actividades similares, revisamos únicamente el nivel de decisión.

Para el proceso Monitoreo y análisis del KPI PQD OUT cuyo diagrama de flujo se muestra en la figura 3.3-3, tenemos:

- Toma de decisión : El valor obtenido del KPI PQD OUT es mayor o igual al 3%?.
    - NO (es decir es menor), se considera normal y se continúa monitoreando.
    - SI, se debe reportar a Ingeniería a la unidad ING ISP. En este caso se ha

obtenido para el router de borde un valor inferior al 3% y por ello en la ejecución práctica en CNT EP se lo considera normal y deberá continuar monitoreando.

Para el proceso Monitoreo y análisis del KPI LAT cuyo diagrama de flujo se muestra en la figura 3.3-4, tenemos:

- Toma de decisión: El valor del KPI LAT es mayor o igual a 2,4 mseg?
    - NO, es decir es menor, se considera normal y se continúa monitoreando. En este caso se obtuvo 2 mseg, en consecuencia se seguiría monitoreando.
    - SI es mayor o igual a 2,4 mseg, se ejecuta la siguiente actividad.
- Revisar otros eventos de Red ISP o MPLS: La latencia depende de otros recursos de red como el comportamiento de otros routers del ISP o MPLS , por lo que un incremento de la misma no siempre está ligada al router al cual se envía el ping. Por ello es necesario revisar si existieron otros eventos de red que puedan afectarla.
- Toma de decisión: Existieron fallas en red, ISP?.
    - NO, entonces reportar a Ingeniería para proceso de mejoramiento de red. Al no encontrar fallas en la red que pudieron provocar incremento de la Latencia, Ingeniería deberá revisar la configuración de red para implementar mejoras.
    - SI, entonces reportar a OyM ISP para que ejecute el proceso de gestión de fallas.

Para el proceso Monitoreo y análisis del KPI CPU cuyo diagrama de flujo se muestra en la figura 3.3-5, tenemos:

- Toma de decisión: El valor del KPI CPU es mayor o igual a 80%?
    - NO, es decir es menor, se considera normal y se continúa monitoreando. En este caso se obtuvo 2%, en consecuencia se seguiría monitoreando.
    - SI, es mayor y se ejecuta la siguiente actividad.
- Toma de decisión: Existieron fallas en red, ISP?.
    - NO, entonces reportar a Ingeniería para proceso de mejoramiento de red. Al no encontrar fallas en la red que pudieron provocar incremento de la carga del CPU, Ingeniería deberá revisar la capacidad de procesamiento del router para ampliarlo o migrar a un equipo de mayor capacidad.
    - SI, entonces reportar a OyM ISP para que ejecute el proceso de gestión de fallas.

Para el proceso Monitoreo y análisis del KPI JIT cuyo diagrama de flujo se muestra en la figura 3.3-6, tenemos:

- Toma de decisión: El valor del KPI JIT es mayor o igual a 1,2 mseg?
    - NO, es decir es menor, se considera normal y se continúa monitoreando. En este caso se obtuvo 1 mseg, en consecuencia se seguiría monitoreando.
    - SI es mayor o igual a 1,2 mseg, se ejecuta la siguiente actividad.

- Revisar otros eventos de Red ISP o MPLS: El Jitter depende de otros recursos de red como el comportamiento de otros routers del ISP o MPLS , por lo que un incremento del mismo no siempre está ligado al router al cual se monitorea. Por ello es necesario revisar si existieron otros eventos de red que puedan afectar.
- Toma de decisión: Existieron fallas en red, ISP?.
    - NO, entonces reportar a Ingeniería para proceso de mejoramiento de red. Al no encontrar fallas en la red que pudieron provocar incremento, Ingeniería deberá revisar la configuración de red para implementar mejoras.
    - SI, entonces reportar a OyM ISP para que ejecute el proceso de gestión de fallas.

Para el proceso Monitoreo y análisis del KPI DISP cuyo diagrama de flujo se muestra en la figura 3.3-7, tenemos:

- Toma de decisión: El valor del KPI DISP es mayor o igual a 99,99%?
    - SI, se considera normal y se continúa monitoreando. En este caso se obtuvo 100%, en consecuencia se seguiría monitoreando.
    - NO, se ejecuta la siguiente actividad.
- Revisar otros eventos de Red, ISP o Infraestructura: La disponibilidad la estamos midiendo en base al ping, cuya respuesta no solo depende del router sino también de la ruta y si existen otros routers en ella, por ello se verifica si existieron otros eventos en la red que pudieran afectar el resultado. Igualmente también se debe verificar eventos de infraestructura de energía, aire

acondicionado del ISP que pudieron causar indisponibilidad del router.

- Toma de decisión: Existieron fallas en red, ISP o infraestructura?.
    - NO, entonces reportar a Ingeniería para proceso de mejoramiento de red. Al encontrar fallas en la red, ISP o infraestructura (energía, aire acondicionado, racks, del ISP), que pudieron provocar indisponibilidad del router, Ingeniería deberá revisar la red e infraestructura para implementar mejoras.
    - SI, entonces reportar a OyM ISP para que ejecute el proceso de gestión de fallas.

4.3 Análisis de los resultados obtenidos

Los valores obtenidos en este ejercicio práctico para los KPI de rendimiento del equipo de comunicaciones del ISP, denominado router de Borde y utilizando PRTG, se resumen a continuación:

KPI	VALOR OBTENIDO	VALOR LIMITE
AB TOT	9 Gbps	8 Gbps
PQD OUT	0 %	3%
LAT	2mseg	2,4 mseg
CPU	2%	80%
JIT	1 mseg	1,2 mseg
DISP	100%	99,99%

Fig. 4.3-1 Resultados obtenidos para los KPI de rendimiento

Los resultados nos muestran que el rendimiento de este equipo en la red es

satisfactorio y cumple con los principales parámetros que nos aseguran una buena calidad de servicio de internet.

Sin embargo, pudimos observar que el KPI AB TOT medido sobre una de las interfaces del router, sobrepasa su valor límite y sería necesario realizar los estudios de ingeniería respectivos para implementar mejoras en la red como por ejemplo una redistribución de tráfico o una ampliación de capacidad en esa ruta.

AL verificar el flujo lógico de los procesos definidos, se pudo comprobar que estos están correctamente definidos, así fue que al verificar el proceso de Monitoreo y análisis del KPI ABTOT (cuyo diagrama de flujo se muestra en la figura 3.3-2), encontramos que debía reportarse al área de Ingeniería de la CNT EP para que realicen el proceso de mejoramiento de red (referirse al ítem 4.2).

Adicionalmente, de las mediciones efectuadas de tráfico sobre una de las interfaces del router de Borde (figura 4.1.3-1) para obtener el KPI AB TOT, se puede observar que el tráfico de internet, tiene un comportamiento típico en la red, es decir, se asemeja a una figura sinusoidal con valores máximos y mínimos según las horas del día.

Esto refleja también el comportamiento del usuario de internet, existe menos consumo de internet aproximadamente desde las 12 am a las 8 am

También podemos observar otro comportamiento típico del tráfico de internet, la cantidades de paquetes recibidos o entrantes (Traffic In) es mucho mayor que la cantidad de paquetes transmitidos o salientes (Trafficout), aproximadamente se tiene una relación de 10 a 1.

Sobre el KPI LAT (latencia), el método de Ping como lo señala el manual del PRTG es una opción de medición, la otra más precisa, es utilizar el sensor denominado IP SLA, el cual utiliza parámetros de QoS (calidad de servicio), sin embargo esta debe estar implementada en el router y como ya se ha mencionado anteriormente, actualmente no se ha implementado QoS en los equipos de comunicaciones del ISP.

Los resultados obtenidos de latencia nos dieron un promedio de 2 mseg, lo cual permite corroborar el hecho de que los equipos de comunicación (routers) del ISP al ser equipos del Core de la red de internet (de gran capacidad y velocidad de procesamiento de paquetes), no deben agregar grandes retardos que incrementen la latencia.

Sobre los KPI JIT y PQD OUT, si bien su objetivo es asegurar QoS cuando esta se encuentra implementada, sus valores obtenidos para jitter de 1 mseg y Pérdida (o descarte) de paquetes salientes del 0%, nos sirven de referencia para asegurar que la red de comunicaciones del ISP esta lista para implementar QoS cuando así se lo requiera.

El KPI JIT es importante cuando existe tráfico de Telefonía (VoIP), el cual actualmente no cursa el ISP, sin embargo su valor es aceptable para aplicaciones de internet que utilizan VoIP.

5 CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

En base a la revisión de los modelos de Gestión de Red realizado en el capítulo 2, de algunas de las herramientas de monitoreo de red existentes en el mercado, la factibilidad de disponer de una de ellas, la arquitectura de red del ISP basada en IP (indicada en el capítulo 1) y el alcance del presente trabajo (Gestión del rendimiento de equipos de comunicaciones del ISP), se escogió el modelo de Gestión de Red SNMP/Internet y la herramienta PRTG.

Existen Modelos de Gestión de Red mucho más completos como los basados en TMN (estándares de la UIT), denominados NGOSS (Sistemas de soporte a Operaciones en redes de próxima generación o simplemente OSS) que abarcan todos los módulos funcionales de un modelo de gestión y las diferentes tecnologías de red que dispone un operador como CNT EP (no únicamente de internet/ IP).

SI bien existe estandarización para las MIB, estas son bastante numerosas, cada fabricante escoge cuales de ellas las implementa o no en sus equipos y por ello es necesario revisar tanto en documentación del fabricante, como en los equipos del ISP aquellas que están disponibles y son efectivas para obtener los indicadores de rendimiento. Igualmente es necesario verificar que la herramienta de monitoreo (en este caso PRTG) posee en su biblioteca de MIB las requeridas.

Uno de los aspectos fundamentales de la gestión del rendimiento es el establecer los denominados KPI (Indicadores Claves de desempeño), los cuales deben ser muy objetivos y permitir con ellos disponer de una visualización del desempeño de una

red. Es decir tanto los equipos como la herramienta de monitoreo nos pueden entregar muchos indicadores de rendimiento y de ellos se deben escoger los KPI más representativos. En el presente trabajo se identificaron 15 indicadores de rendimiento y de ellos se establecieron 6 KPI (ver figura 2.4-1).

Los KPI para un Operador permiten optimización de recursos como: personal de monitoreo, licencias (software) de la herramienta, servidores de gestión (almacenan información diaria e histórica de los KPI), no sobrecarga de procesamiento de los routers u otros equipos monitoreados.

Para este trabajo se implementó un servidor de pruebas equipado con la herramienta PRTG, lo cual permite experimentar con indicadores de rendimiento sin afectar al monitoreo en producción que CNT EP dispone.

Los resultados obtenidos para los KPI de rendimiento en el capítulo 4 y que se muestran en la figura 4.3-1 nos muestran que el rendimiento de este equipo en la red es satisfactorio y cumple con los principales parámetros que nos aseguran una buena calidad de servicio de internet.

En el capítulo 2 se muestran en las figuras 2.4-2 y 2.4-3, valores de los principales parámetros que utilizan operadores internacionales para indicar que su red tiene buena calidad de servicio, los valores obtenidos en la red de comunicaciones del ISP son comparables con ellos en lo que respecta a latencia, jitter, perdida de paquetes y disponibilidad.

Es necesario recordar que los valores de KPI obtenidos corresponden según el alcance del presente trabajo únicamente a la red de comunicaciones del ISP y no a

la red completa, es decir no está incluida la red de acceso y backbone MPLS.

La red de comunicaciones del ISP actualmente no maneja QoS pues, por ahí circula únicamente tráfico de internet, sin embargo se podría implementarla de así requerirlo, ya que los valores de KPI obtenidos, indican que el ISP soportaría aplicaciones de internet que demandan QoS, como VoIP o streamming de video. Al implementar QoS, será necesario añadir otros KPI de rendimiento.

La herramienta PRTG presenta una limitación en cuanto a que no se puede disponer de una visión integral de la red, existen otras herramientas (evidentemente mucho mas costosas) que pueden monitorear la red en su conjunto y disponer de indicadores de extremo a extremo (end to end) y el servicio asociado a cada cliente; también existen otras menos costosas como CACTI (de libre uso),que permiten graficar la red.

Sobre los procesos definidos en el capítulo 3, estos se corresponden con la estructura organizacional de CNT EP y contienen actividades para cada unidad administrativa involucrada con el ISP. Se toma en cuenta a la unidad de Gestión del Desempeño (GD- ISP) de red del ISP como la dueña del proceso y hacia ella se orientan estos procesos.

Los procesos están relacionados con la norma de calidad ISO 9001, la cual enfatiza en que los procesos deben entregar un valor añadido, medir su desempeño, eficacia y una mejora continua de los mismos.

Los procesos aquí definidos para la gestión del rendimiento de los equipos del ISP constituyen una base inicial y su aplicación deberá estar sujeta a una mejora

continua y adaptación a los continuos cambios que la tecnología y las redes exigen.

Los resultados obtenidos con el presente trabajo de tesis, cumplen con los objetivos de la Gestión del rendimiento: Definición de los indicadores de rendimiento, monitoreo del rendimiento y análisis y afinamiento.

Igualmente se han cumplido con los objetivos específicos planteados para el desarrollo del proyecto de tesis: Definir los KPI de rendimiento para el ISP de la CNT EP, monitoreo en tiempo real, análisis de las mediciones obtenidas y elaboración de los procedimientos de gestión del rendimiento para CNT EP.

Finalmente, los resultados obtenidos con el presente trabajo de Tesis, como son: Los KPI de Rendimiento, los procesos para una Gestión del Rendimiento de los equipos de comunicaciones del ISP de la CNT EP y la implementación práctica con la herramienta PRTG disponible, permitirán a la CNT EP contar a corto plazo con una Gestión del Rendimiento para el ISP brindando de esta manera la posibilidad de realizar acciones proactivas para optimizar o ampliar la red, evitando asi depender de acciones reactivas frente a las fallas de red o pérdida de calidad de servicio.

5.2 Recomendaciones

Dado que para esta investigación se implementó PRTG en un servidor de pruebas, este debería mantenerse operativo en CNT para que sirva de plataforma de experimentación para obtener otros indicadores que pueden ser útiles en la mejora continua de la calidad de servicio de la red del ISP.

Implementar los procedimientos aquí definidos en CNT EP y poder obtener los

beneficios esperados de: Mejorar la disponibilidad de la red del ISP, optimización de recursos, mejoramiento del cumplimiento de los SLA y crear una cultura de calidad con procesos.

Ampliar la cobertura de la gestión del rendimiento del ISP a las otras partes constitutivas de la red, como son el acceso y el backbone MPLS.

Adquirir y utilizar otras herramientas de monitoreo mas completas que permitan no solamente el monitoreo de los KPI de rendimiento de la red sino también el monitoreo de los parámetros de calidad de un servicio extremo a extremo (end to end).

6 BIBLIOGRAFIA

[1] http://corporativo.cnt.gob.ec/wp-content/uploads/2014/11/a_Estructura_Organizacional_CNT_EP-2014.pdf (www.cnt.gob.ec, 2014)

[2] www.cisco.com(CISCO, 2015)

[3] GESTION DE REDES .Pr(EGAS, 2007)

[4] INTERNETWORKING WITH TCP/IP, Douglas E. Comer, 2014 (Comer, 2014)

[5] Network Management: Principles and Practices (2nd Edition), Mani Subramanian, 2012(Subramanian, 2012)

[6] IETF página WEB oficial https://www.ietf.org/rfc/(IETF, 2015)

[7] Designing Cisco Network Service Architectures Vol 3, v2.1 2010, Lesson 2(CISCO, 2010)

[8] Presentación sobre Indicadores de Calidad y Rendimiento de Procesos Zaragosa BEHR – F Sanchez, 2007 (http://www.aec.es/c/document_library/get_file?uuid=785ee585-d742-4db1-aea3-5b511a1d7617&groupId=10128)(Sanchez, 2007)
BEHR: empresa fabricante con procesos de calidad
www.aec.es es la página Web oficial de la Asociación española para la calidad (QAEC)

[9] Norma ISO9001:2008 (http://www.iso.org)(ISO, 2008)

[10] Página WEB de CACTI (http://www.cacti.net) (CACTI, 2015)

[11] Página WEB de Paessler/PRTG (http://www.es.paessler.com) (PAESSLER / PRTG, 2015)