UNIVERSIDAD RICARDO PALMA

FACULTAD DE INGENIERÍA

PROGRAMA DE TITULACIÓN POR TESIS

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

APLICACIÓN DE PROTOCOLOS SNMP Y NETFLOW PARA OPERAR UNA LAN DE 4 SEDES DE LA EMPRESA DETCOM LIMA 2020

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:

Bach. Dett Sotelo, Bryan Alexis

Bach. Vega Santiago, Edwin Cesar

Asesor: Ing. Cuadrado Lerma, Luis Alberto

LIMA-PERÚ

2020

DEDICATORIA

En memoria de mi tío Oscar Sotelo por su constante motivación que siempre me brindo. También dedicado a mi papá Víctor y mamá Maria, tíos, Pancho y en especial a mi madre Ana por su amor y sacrificios en todos estos años gracias a ustedes todo esto es posible; a Tassiane por ser mi principal motivo de alcanzar mis metas.

Bryan Alexis Dett Sotelo

Principalmente a Dios, por ser mi fuerza de fe y mi paz. A mis padres por su esfuerzo en brindarme una educación e inculcarme los valores que son la base principal en mi vida profesional, los quiero mucho. A mi esposa y mis hijos por su apoyo incondicional y por ser mi mayor inspiración, los amo eternamente. A mis hermanos por brindarme siempre su ayuda y confianza.

Edwin Cesar Vega Santiago

AGRADECIMIENTO

Nuestro agradecimiento a los docentes de la carrera de ingeniería electrónica y a nuestra alma mater por los conocimientos brindados en esta maravillosa carrera.

Al Ing. Luis Cuadrado y a la Dra. Margarita Murillo, nuestros asesores, quienes con su apoyo se logró culminar la presente tesis.

A nuestros padres, a nuestras familias que siempre nos brindaron su ayuda y confianza para alcanzar nuestras metas.

Y finalmente a todas las personas, amigos e instituciones que nos brindaron su apoyo para poder lograr los objetivos planteados en la presente tesis.

Bryan Alexis Dett Sotelo y
Edwin Cesar Vega Santiago

INDICE GENERAL

DEDICATORIA ii
AGRADECIMIENTO iii
RESUMEN xiv
ABSTRACT xv
INTRODUCCIÓN 1
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 3
1.1 Descripción del problema 3
1.2 Formulación del problema 4
1.2.1 Problema general 4
1.2.2 Problemas específicos 4
1.3 Importancia y justificación del estudio 4
1.3.1 Importancia 4
1.3.2 Justificación 5
1.4 Delimitación del estudio: 5
1.5 Limitación del estudio: 6
1.6 Objetivos de la investigación 6
1.6.1 Objetivo General 6
1.6.2 Objetivos Específicos 6
CAPÍTULO II: MARCO TEÓRICO 7
2.1 Marco histórico 7
2.2 Investigaciones relacionadas con el tema: 10
2.2.1 Antecedentes Internacionales 10
2.2.2 Antecedentes Nacionales 12
2.3 Estructura teórica y científica que sustenta el estudio 14
2.3.1 Protocolo SNMP (Simple Network Management Protocol) 14
2.3.2 Protocolo NETFLOW 21
2.3.3 LAN (Local Area Network) 25
2.4 Definición de términos básicos 37
2.5 Variables 43
CAPÍTULO III: METODOLOGÍA DEL ESTUDIO 45
3.1 Tipo de investigación 45
3.2 Método de investigación 45
CAPÍTULO IV: DISEÑO DE INGENIERÍA 46

4.1 Diseño 46
4.1.1 Presentación del escenario de trabajo 46
4.1.2 Opciones de herramientas de monitoreo y gestión 48
4.1.3 Selección de la herramienta de monitoreo y gestión 54
4.2 Emulación de redes 56
4.2.1 Escenario de emulación 56
4.2.2 Topología propuesta en GNS3 68
4.2.3 Desarrollo de la emulación 74
4.2.4 Desarrollo de emulación del SNMP 100
4.2.5 Desarrollo de emulación del NETFLOW 117
4.3 Escenario de pruebas y análisis de resultados 132
CAPITULO V: ASPECTOS ADMINISTRATIVOS 158
5.1 Recursos humanos 158
5.2 Materiales 159
5.3 Presupuesto 160
5.4 Cronograma de actividades 163
CONCLUSIONES 165
RECOMENDACIONES 167
REFERENCIAS BIBLIOGRÁFICAS 168
ANEXOS 173
Anexo N°1: Matriz de consistencia interna 173
Anexo N°2: Matriz de operacionalización de variables 174
Anexo N°3: Cuadro de Incidencias – Empresa DETCOM 176
Anexo N°4: Hoja de datos del software OpManager 178
Anexo N°5: Formato de autorización 183

ÍNDICE DE TABLAS

Tabla 1: Cuadro de Estándares 28
Tabla 2: Cuadro de Dimensiones de cada variable 44
Tabla 3: Tabla de servicio 47
Tabla 4: Cuadro de comparación – Solarwind vs ManageEngine vs PRTG 50
Tabla 5: Cuadro de Funcionalidades – OpManager Professional Edition 57
Tabla 6: Recursos de Servidor 58
Tabla 7: Sistemas Operativos 58
Tabla 8: Segmento de red entre los router P, PE1 y PE2 69
Tabla 9: Segmento de red entre los router PE1 – CE1 y PE2 – CE2 70
Tabla 10: Segmento de red entre los routers CE1 – ISP1 y CE2 – ISP2 71
Tabla 11: Segmento de la red LAN 72
Tabla 12: Comandos SNMP 106
Tabla 13: Comandos NETFLOW 123
Tabla 14: Cuadro de Incidencias emuladas 132
Tabla 15: Horas hombre por mes para la emulación 158
Tabla 16: Implementación de la solución por días 159
Tabla 17: Equipos utilizados 159
Tabla 18: Aplicaciones utilizadas 160
Tabla 19: Costo CAPEX del proyecto 161
Tabla 20: Costo OPEX del proyecto 161
Tabla 21: Costo de inversión 162
Tabla 22: Flujo de caja de TI 162
Tabla 23: Tabla de rentabilidad 163
Tabla 24: Cuadro saturación de ancho de banda Enero – Marzo 176
Tabla 25: Cuadro incidencias de saturación de CPU Enero – Marzo 176
Tabla 26: Cuadro incidencias de saturación de memoria Enero – Marzo 176
Tabla 27: Cuadro incidencias de intermitencias en el servicio Enero - Marzo 177
Tabla 28: Cuadro total de incidencias Enero – Marzo 177

ÍNDICE DE FIGURAS

Figura N° 1: Elementos del SNMP 15
Figura N° 2: Esquema de comunicación SNMP 17
Figura N° 3: Diagrama del árbol MIB 19
Figura N° 4: Gestión de capas de Ethernet 29
Figura N° 5: LAN Ethernet básica 30
Figura N° 6: Comparación entre los modelos OSI y TCP/IP 31
Figura N° 7: Niveles de referencia de LAN respecto al modelo OSI 31
Figura N° 8: Trama Ethernet 802.3 33
Figura N° 9: Transmisión a través del medio físico 33
Figura N° 10: Red topológica de la empresa DETCOM 47
Figura N° 11: Puertos usados por la Aplicación y Base de Datos 59
Figura N° 12: Puertos usados para el Monitoreo 59
Figura N° 13: Puertos Complementarios 60
Figura N° 14: Página del GNS3 62
Figura N° 15: Ingresando con una cuenta de GNS3 62
Figura N° 16: Seleccionando la opción de Software 63
Figura N° 17: Seleccionando la opción de descarga del software 63
Figura N° 18: Descarga del software GNS3 64
Figura N° 19: Archivo de instalación del GNS3 64
Figura N° 20: Proceso de instalación del GNS3 64
Figura N° 21: Aplicación GNS3 65
Figura N° 22: Área de trabajo del GNS3 65
Figura N° 23: IOS del router C7200 66
Figura N° 24: IOS del router C2691 66
Figura N° 25: IOS del router C2691 66
Figura N° 26: IOS del switch C3725 67
Figura N° 27: VirtualBox 67
Figura N° 28: Topología a emular 68
Figura N° 29: Segmentos entre los router PE1 – P – PE2 69
Figura N° 30: Segmento entre los router PE1 – CE1 y PE2 – CE2 70
Figura N° 31: Segmento entre los routers CE1 – ISP1 y CE2 – ISP2 71
Figura N° 32: Segmento oficina principal 73

Figura N° 33: Segmento oficina sucursal 73
Figura N° 34: IGP- OSPF del router P 75
Figura N° 35: IGP- OSPF del router PE1 76
Figura N° 36: IGP- OSPF del router PE2 77
Figura N° 37: Adyacencias en el router P 78
Figura N° 38: Configuración del LDP y MPLS en el router P 78
Figura N° 39: Configuración del LDP y MPLS en el router PE1 79
Figura N° 40: Configuración del LDP y MPLS en el router PE2 79
Figura N° 41: Etiquetas y Tablas MPLS – Router P 80
Figura N° 42: Etiquetas y Tablas MPLS – Routers PE1 y PE2 80
Figura N° 43: Configuración VRF en el router PE1 81
Figura N° 44: Configuración VRF en el router PE2 81
Figura N° 45: Tabla VRF en el router PE1 81
Figura N° 46: Tabla VRF en el router PE2 82
Figura N° 47: Configuración del BGP y VPNV4 en el router PE1 82
Figura N° 48: Configuración del BGP y VPNV4 en el router PE2 83
Figura N° 49: Configuración del BGP y VPNV4 en el router CE1 83
Figura N° 50: Configuración del BGP y VPNV4 en el router CE2 84
Figura N° 51: Tablas de BGP y VPNV4 en el router PE1 84
Figura N° 52: Tablas de BGP y VPNV4 en el router PE2 85
Figura N° 53: Enlace entre el CE1 y el Core1 85
Figura N° 54: Enlace entre el CE1 y el Core1 86
Figura N° 55: Interfaz VLAN 10 - Core1 86
Figura N° 56: Interfaz VLAN 20 – Core2 87
Figura N° 57: Enlace ISP1 – Oficina Principal 87
Figura N° 58: Enlace ISP2 – Sucursal 88
Figura N° 59: RIP – Oficina Principal 88
Figura N° 60: RIP – Sucursal 89
Figura N° 61: Acceso a Internet - ISP1 89
Figura N° 62: Acceso a Internet – ISP2 90
Figura N° 63: VPCS – PC del GNS3 91
Figura N° 64: Asignación de IP - PC1 91
Figura N° 65: Máquinas Virtuales – Virtual Box 92
Figura N° 66: Asignación de VM – GNS3 92

Figura N° 67: Asignación de IP – PC2 92
Figura N° 68: Ping entre PC1 - WinXP 93
Figura N° 69: Ping entre PC1 – WinXP – Win2012 94
Figura N° 70: Ping hacia Internet – PC1 95
Figura N° 71: Ping hacia Internet – WinXP 95
Figura N° 72: Ping hacia Internet – Win2012 96
Figura N° 73: Ping entre PC1 y PC2 97
Figura N° 74: Ping entre PC2 y el servidor Win2012 97
Figura N° 75: Trace entre el Core1 y el Core2 98
Figura N° 76: Tabla del IP CEF de los routers Ce1 y CE2 99
Figura N° 77: Ping hacia Internet – PC2 100
Figura N° 78: Ping hacia Internet – PC2 101
Figura N° 79: Archivo ejecutable del OpManager. 101
Figura N° 80: Instalación del OpManager. 101
Figura N° 81: Validación del espacio de almacenamiento. 102
Figura N° 82: Designación de puertos. 102
Figura N° 83: Designación de la base de datos. 103
Figura N° 84: Inicialización del software. 103
Figura N° 85: Browser del OpManager. 104
Figura N° 86: Ingreso al OpManager. 104
Figura N° 87: Configuración SNMP – CE1 y Core1 105
Figura N° 88: Configuración SNMP – CE2 y Core2 106
Figura N° 89: Muestra del estado del SNMP 107
Figura N° 90: Inventory – Devices – Agregación automática de equipos. 108
Figura N° 91: Inventory – Devices – Agregación manual de equipos. 108
Figura N° 92: Inventory – Devices – Agregación manual de equipos. 109
Figura N° 93: Inventory – Devices – Agregación manual de equipos. 109
Figura N° 94: Inventory – Devices – Agregación manual de equipos. 110
Figura N° 95:Inventory – Devices – Agregación manual de equipos. 110
Figura N° 96: Agregación manual de equipos. 111
Figura N° 97: Filtro por alerta – Sort by severity – Alertas activas 111
Figura N° 98: Filtro por alerta – Sort by severity – alarmas critical activas de la red. 112
Figura N° 99: Filtro por tipo – Interfaces 112
Figura N° 100: Menu dashboard - configuración 113

Figura N° 101- Menu dashboard - Mapa 113
Figura N° 102: Menu dashboard – Business view 114
Figura N° 103: Menu dashboard – HeatMap 115
Figura N° 104:Menu dashboard – Monitores – Devices by CPU utilization 115
Figura N° 105: Menu dashboard – Monitores – Devices by Memory Utilization 116
Figura N° 106: Menu dashboard – Monitores – Devices Down 116
Figura N° 107: Menu dashboard – Monitores – Interfaces by traffic 117
Figura N° 108: Configuración Netflow – CE1 118
Figura N° 109: Configuración Netflow – CE2 119
Figura N° 110: Configuración Interfaces a monitorear – CE1 120
Figura N° 111: Configuración Interfaces a monitorear – CE2 120
Figura N° 112: Configuración versión del NETFLOW – CE1 121
Figura N° 113: Configuración versión del NETFLOW – CE2 121
Figura N° 114: Show flow exporter – CE1 121
Figura N° 115: Show flow monitor – CE1 122
Figura N° 116: Show ip cache verbose Flow – CE1 122
Figura N° 117: NETWORK – NETFLOW 128
Figura N° 118: NETWORK-NETFLOW 128
Figura N° 119: NETWORK – NETFLOW 129
Figura N° 120: NETWORK – NETFLOW 129
Figura N° 121:NETWORK – NETFLOW 129
Figura N° 122: NETWORK –Flow analysis – Device traffic 130
Figura N° 123: NETWORK –Flow analysis – Application 130
Figura N° 124: NETWORK –Flow analysis – Protocol 131
Figura N° 125: NETWORK –Flow analysis – Source 131
Figura N° 126: NETWORK - Flow analysis - Destination 131
Figura N° 127: NETWORK –Flow analysis – Conversation 132
Figura N° 128: Escenario 1 – Tráfico hacia internet CE2 134
Figura N° 129: Escenario 1 – Tráfico hacia internet CE2 134
Figura N° 130: Escenario 1 – Tráfico hacia internet CE1 135
Figura N° 131: Escenario 1 – Utilización del ancho de banda de internet CE1 135
Figura N° 132: Escenario 1 – Utilización de aplicativos CE1 136
Figura N° 133: Escenario 1 – Conversación de IP origen – destino en la red CE1 136
Figura N° 134: Escenario 1 – Utilización del ancho de banda de internet 137

Figura N° 135: Escenario 2 – Tráfico LAN CE2 - SERVIDOR 137
Figura N° 136: Escenario 2 – Tráfico LAN CE2 - SERVIDOR 138
Figura N° 137: Escenario 2 – Tráfico LAN CE2 - SERVIDOR 139
Figura N° 138: Escenario 2 – Tráfico LAN CE2 - SERVIDOR 139
Figura N° 139: Escenario 2 – Tráfico LAN CE2 - SERVIDOR 140
Figura N° 140: Escenario 2 – Tráfico LAN CE1 - SERVIDOR 140
Figura N° 141: Escenario 2 – Tráfico LAN CE1 - SERVIDOR 141
Figura N° 142: Escenario 2 – Tráfico LAN CE1 - SERVIDOR 141
Figura N° 143: Escenario 3 – Core1 Visualización de salud de equipos – CPU Dispositivo 142
Figura N° 144: Escenario 3 – Core1 Visualización de salud de equipos - CPU Opmanager 142
Figura N° 145Escenario 3 – Core1 Visualización de salud de equipos – CPU Opmanager 143
Figura N° 146: Escenario 3 – Core1 Visualización de salud de equipos – Memoria Dispositivo 143
Figura N° 147: Escenario 3 – Core1 Visualización de salud de equipos - Memoria Opmanager 144
Figura N° 148: Escenario 3 – Core1 Visualización de salud de equipos – Memoria Opmanager 144
Figura N° 149: Escenario 3 – CE1 Visualización de salud de equipos – CPU Dispositivo 145
Figura N° 150: Escenario 3 – CE1 Visualización de salud de equipos – CPU Opmanager 145
Figura N° 151 : Escenario 3 – CE1 Visualización de salud de equipos – Memoria Dispositivo 146
Figura N° 152: Escenario 3 – CE1 Visualización de salud de equipos – Memoria Opmanager 146
Figura N° 153: Escenario 4 – CE1 Envió de protocolo ICMP para la visualización de latencia y perdida de paquetes - Dispositivo 147
Figura N° 154: Escenario 4 – CE1 Envió de protocolo ICMP para la visualización de latencia y perdida de paquetes - Opmanager 148
Figura N° 155: Escenario 4 – Core2 Envió de protocolo ICMP para la visualización de latencia y perdida de paquetes - Dispositivo 149

Figura N° 156: Escenario 4 – Core2 Envió de protocolo ICMP para la visualización de latencia y perdida de paquetes - Opmanager 149
Figura N° 157: Escenario 5 – Core2 Apagado y desconexión de equipos router y switch en la red - Dispositivo 150
Figura N° 158: Escenario 5 – Core2 Apagado y desconexión de equipos router y switch en la red - Opmanager 150
Figura N° 159: Escenario 5 – Core2 Apagado y desconexión de equipos router y switch en la red - Opmanager 151
Figura N° 160: Escenario 5 – Core2 Apagado y desconexión de equipos router y switch en la red - Opmanager 151
Figura N° 161: Escenario 5 – Core2-CE2 Apagado y desconexión de equipos router y switch en la red - Dispositivo 152
Figura N° 162: Escenario 5 – Core2-CE2 Apagado y desconexión de equipos router y switch en la red - Dispositivo 152
Figura N° 163: Escenario 5 – Core2-CE2 Apagado y desconexión de equipos router y switch en la red - Dispositivo 153
Figura N° 164: Escenario 5 – Core2-CE2 Apagado y desconexión de equipos router y switch en la red - Opmanager 153
Figura N° 165: Escenario 6 – MPLS- Caída de la red MPLS - Red 154
Figura N° 166: Escenario 6 – MPLS- Caída de la red MPLS - Opmanager 154
Figura N° 167: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Dispositivo 155
Figura N° 168: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager 155
Figura N° 169: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager 156
Figura N° 170: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager 156
Figura N° 171: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager 157
Figura N° 172: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager 157
Figura N° 173: Cronograma de actividades 163
Figura N° 174: Cronograma de actividades 164

Figura N° 175: Cronograma de actividades 164
Figura N° 176: Datasheet - Opmanager 178
Figura N° 177- Datasheet Opmanager 179
Figura N° 178- Datasheet Opmanager 180
Figura N° 179- Datasheet Opmanager 181
Figura N° 180: Datasheet Opmanager 182

RESUMEN

La presente investigación de tesis, se desarrolló en un entorno emulado en el cual se implementó una herramienta de monitoreo y gestión utilizando para ello los protocolos SNMP y NETFLOW replicando la topología de la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima en el año 2020.

El propósito de la investigación consistió en explicar las variables independientes, definidas por los protocolos SNMP y NETFLOW, y la variable dependiente, definida por la LAN.

De esta manera y siguiendo la técnica y el método de investigación, acompañado de las bases teóricas de cada una de las variables, sus procesos de implementación y configuración; Se logró alcanzar los resultados esperados, cumpliendo con los objetivos especifico y general de la presente tesis, obteniendo de esta manera información en tiempo real o cuando sea solicitado de la LAN.

Los resultados obtenidos de la emulación realizada permitieron dar un panorama de la importancia que hoy en día aporta una herramienta de monitoreo y gestión aplicando los protocolos SNMP y NETFLOW sobre la LAN, podemos concluir que con una buena gestión de los recursos se pudo mejorar la accesibilidad a los servicios de Internet y por ende controlar el ancho de banda, el monitorear en tiempo real a los dispositivos mejoro el rendimiento de la LAN con el cual el administrador de TI pudo anticiparse a eventos que puedan degradar la red y el tener una red gestionada logró controlar las incidencias mejorando los tiempos de atención y resolución de problemas.

Palabras Clave: Protocolo SNMP, protocolo NETFLOW, LAN, monitoreo y gestión, ancho de banda, rendimiento e incidencias.

ABSTRACT

The present thesis research was developed in an emulated environment in which a monitoring and management tool was implemented using SNMP and NETFLOW protocols, replicating the LAN topology for 4 offices of DETCOM company in Lima city in the year 2020.

The purpose of the research was to explain the independent variables, defined by the SNMP and NETFLOW protocols, and the dependent variable, defined by the LAN.

In this way and following the technique and the research method, accompanied by the theoretical basis of each variable, the implementation and configuration processes. The expected results were obtained, complying with the specific and general objectives of this thesis, thus obtaining information in real time or when requested from the LAN.

The results obtained from the executed emulation allowed us to give an overview of the importance that today a monitoring and management tool contribute by applying the SNMP and NETFLOW protocols over the LAN, we can conclude that with a good management of resources it was possible to improve accessibility to Internet services and therefore control the bandwidth, Monitoring the devices in real time improved the performance of the LAN with which the IT administrator could anticipate events that could degrade the network and having a managed network managed to control incidents by improving service time and problem solutions.

Keywords: SNMP protocol, NETFLOW protocol, LAN, monitoring and management, bandwidth, performance and incidents.

INTRODUCCIÓN

Hoy en día las comunicaciones de redes en toda empresa y/o organismo gubernamental son pieza clave y sensible en la operación diaria de sus actividades, A medida que una empresa va creciendo y posicionándose en el tiempo como es el caso de la empresa DETCOM, es necesario contar con una herramienta de monitoreo y gestión que ayude al administrador de red a tener una red gestionada, controlada y confiable. Para el desarrollo de la presente investigación referida a la "Aplicación de protocolos SNMP y NETFLOW para operar una LAN de 4 sedes de la empresa DETCOM", se consideró los siguientes antecedentes: Becerra, E. (2016), Implementación de monitoreo de red utilizando los protocolos ICMP y SNMP; así como también a Juanes, P (2015), *Analysis of possibilities to use information from NetFlow protocol for improvement of performance of Wide Area Network*; también la investigación de Zambrano, D. (2015), Propuesta de utilización de herramientas de telemetría, para identificar técnicas de ciberdelitos como watering hole, en redes de infraestructura (caso de estudio NETFLOW de cisco); también mencionamos a Fernandez, O. (2019), Implementación de un servidor como gestión y monitoreo de servicios para la red de datos en la UGEL Huamanga; también a Quispe, J. (2019), Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce; finalmente la investigación de Ramirez, E. (2019), Alternativas de configuración con el uso de los protocolos Syslog y SNMP para la gestión de red de redes avanzadas.

La empresa DETCOM al contar con oficinas instaladas en diferentes distritos de la capital, cada una de ellas presentan problemas en la conectividad y en los accesos al servicio de Internet, y al no tener una visualización real del entorno o dispositivos que integran la red se formuló el problema general de la siguiente manera: ¿Cómo aplicar los protocolos SNMP y NETFLOW para operar una LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima?, interrogante que a través de la investigación se ha podido dar respuesta.

Esta investigación se justifica en las variables independientes, protocolos SNMP y NETFLOW como medidas de optimización para la solución a los problemas de administración y control presentado en la variable dependiente LAN y como pueden

impactar en ella. Así mismo los resultados obtenidos en la investigación servirán de base para incentivar en mejorar el diseño e implementar nuevos sistemas basados en otros requerimientos que ayuden a mejorar la LAN.

Es así como el objetivo principal de esta tesis de investigación es aplicar protocolos SNMP y NETFLOW para operar una LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima.

Siendo así, la estructura seguida para la presente investigación la podemos detallar de la siguiente manera.

CAPITULO I: Planteamiento del problema, se presenta la descripción del problema que aqueja a la empresa DETCOM, el problema general y sus específicos, con el cual pasamos a la importancia y justificación del estudio, mencionamos las delimitaciones, así como las limitaciones encontradas y finalmente se plantea el objetivo general y sus específicos para dar solución al problema encontrado.

CAPITULO II: Marco Teórico, presentamos el marco teórico correspondiente en base a nuestras variables independientes, así como también en la variable dependiente, se presentan los antecedentes internacionales como nacionales utilizados que nos sirvieron de base en la presente investigación y para finalizar presentamos el cuadro de nuestras variables.

CAPITULO III: Metodología del Estudio, mencionamos el tipo de investigación empleada, la cual para nuestro caso fue la aplicada dado que no empleamos hipótesis y la técnica utilizada que es este caso fue la explicativa porque no variamos ningún dato si no que la interpretamos, analizamos y en base a ese análisis se toman las correctas decisiones para mejorar la gestión y rendimiento de la LAN.

CAPITULO IV: Diseño de Ingeniería, presentamos el diseño de ingeniería, la implementación, configuración y el análisis de los resultados con el cual se logran alcanzar los objetivos propuestos en la solución del problema planteado.

CAPITULO V: Aspectos Administrativos, se presentan los aspectos administrativos que involucran al tiempo del personal involucrado en la implementación y configuración del sistema tanto en la parte de la emulación, como en la instalación en sitio, lo costos de licencias del software en base a los dispositivos e interfaces, los costos de CAPEX y OPEX, finalmente mencionamos los materiales utilizados tanto en la emulación de la solución como en la instalación de este.

Para finalizar, se presentan las conclusiones que responden a los objetivos planteados, recomendaciones para seguir mejorando el diseño e implementación de la LAN.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del problema

En los últimos años y en la actualidad grandes empresas e incluso pequeñas tienen la necesidad de tener todas sus oficinas comunicadas entre sí, transmitiendo información entre sedes a grandes capacidades, en tiempo real y/o permanente. Esto, gracias al avance de las tecnologías en el mundo de las Redes y Telecomunicaciones es posible mediante la solución MPLS (*MultiProtocol Label Switching*) la cual permite comunicar e intercambiar información de forma segura entre todas sus sedes.

Basados en esta tecnología se puede describir la situación de la Empresa DETCOM que cuenta con una oficina central, una sucursal y dos tiendas, toda esta red ubicada en la ciudad de Lima. La empresa cuenta con switches de conmutación de capa 3 en la oficina principal, así como también en la sucursal y tiendas, las cuales se enlazan con un router hacia la red MPLS adquirida, estos equipos al no tener un control centralizado de cambios o no tener visibilidad de consumo del ancho de banda no se pueden gestionar de manera óptima y a esto se suman los problemas que se presentan para detectar la congestión del ancho de banda en cada oficina.

En la actualidad en la empresa DETCOM específicamente en el área de Tecnología de la Información (TI) enfrenta diversos problemas al no tener recursos o herramientas que le permitan una correcta administración y gestión en los equipos de la LAN (Local Area Network) este detalle se evidencia en la tabla de incidentes (véase Anexo N°3 - Tabla 27), donde se observa que el 10.91% de los incidentes son debido a una saturación del ancho de banda, ocasionado por el uso inadecuado de acceso a internet generando alta latencia y/o lentitud en el uso del servicio. Adicionalmente, se presenta un 47.27% en total de los incidentes ocasionadas por problemas de salud de equipo; saturación de CPU, memoria e intermitencia en su servicio (véase Anexo N°3- Tabla 25 - 27), generando alta latencia, problemas de acceso a los servidores de aplicación e incluso reinicio constante de estos equipos. Finalmente, las incidencias que presenta la LAN tienen una demora en el análisis y solución generando una indisponibilidad del servicio afectando los indicadores claves de rendimiento (KPI) los cuales representan un 48% de incidencias no

solucionadas a tiempo (véase Anexo N°3- Tabla 28) esto genera una insatisfacción por parte del cliente interno ante el servicio ya que este no es óptimo. En consecuencia, al operar en estas condiciones seguirán en incumplimientos constantes de KPI.

Una solución de mejora ante los problemas que aquejan a la empresa DETCOM serían las herramientas de monitoreo y gestión que ayudarían en gran medida a superar estos inconvenientes actuales, ya que frente a eventos que aparezcan en la LAN tendríamos resultados óptimos en atención o resolución de estos, así como también podríamos evaluar de forma correcta el ancho de banda necesario que requiere la empresa; todo esto se verá reflejado en satisfacción de los usuarios y cumplimientos de KPI.

1.2 Formulación del problema

1.2.1 Problema general

¿Cómo aplicar los protocolos SNMP y NETFLOW para operar una LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima - 2020?

1.2.2 Problemas específicos

a) ¿Cómo aplicar los protocolos SNMP y NETFLOW para la visibilidad y análisis del ancho de banda en la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima?
b) ¿Cómo aplicar los protocolos SNMP y NETFLOW para el análisis de rendimiento de la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima?
c) ¿Cómo aplicar los protocolos SNMP y NETFLOW para la administración de incidencias en la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima?

1.3 Importancia y justificación del estudio

1.3.1 Importancia

Esta investigación se orienta a mejorar la gestión de los equipos de networking y a tener un mejor control del ancho de banda de la red de datos de la empresa, lo cual conlleva a tener un mejor desempeño ante una solución de incidentes, diagnosticando y/o detectando problemas en los enlaces contratados ya sean físicos o lógicos, de allí la importancia de tener un centro de control de redes orientado a tener una LAN controlada, actualizada y escalable.

La utilización de las herramientas necesarias de gestión de red ayudara a la empresa DETCOM a tener mayor accesibilidad a sus servidores, tiempos más rápidos de solución de problemas y contar con una red escalable en el tiempo que vendría a ser pieza clave en su desarrollo empresarial.

1.3.2 Justificación

Esta investigación se justifica en los protocolos simple network managment protocol (SNMP) y NETFLOW como medidas de optimización para la solución a los problemas de administración y control de los enlaces de red. Desde el punto de vista técnico ante la problemática analizada en la Empresa DETCOM, la presente investigación pretende dar una solución aplicando los protocolos SNMP y NETFLOW por ende al personal de TI se le dotará de visibilidad de los equipos de red de cualquier sede, podrá anticiparse a eventos de saturación de ancho de banda, realizar cambios y tener alertas de problemas tanto en la parte física de los equipos como en la parte lógica de la red. Se podrá tener una mejor eficiencia de gestión de la red actual, se mejorará el planeamiento de recursos de ancho de banda en cada oficina, se mejorará los costos de soporte e inversión.

Finalmente, en la parte económica al tener un centro de gestión centralizado el área de TI podrá disponer de un presupuesto más acorde a su red, además contará con personal capacitado en la administración de la LAN, operará su red de una forma eficiente y bajará los tiempos de atención de incidentes en el soporte de mesa de ayuda de las oficinas remotas.

1.4 Delimitación del estudio:

Teórica: Las áreas de conocimiento que se abordan en la presente investigación están comprendidas en la gestión de una LAN mediante protocolos SNMP y NETFLOW de acuerdo con la bibliografía utilizada para los protocolos mencionados anteriormente.

Espacial: Se focaliza en la emulación de una oficina central, una sucursal y dos tiendas en la ciudad de Lima de la Empresa DETCOM.

Temporal: La presente investigación está siendo diseñado y emulado en el software GNS3 en un periodo de tiempo de setiembre a octubre del 2020.

Muestra: Toma de muestras de la emulación de red en el flujo de datos, incidentes, cambios y monitoreo de los equipos de red de la LAN y al router de enlace hacia la red MPLS.

1.5 Limitación del estudio:

Debido a la coyuntura actual referido a la pandemia del COVID-19, se encontraron restricciones para poder ingresar a las oficinas de la Empresa DETCOM, además de la limitación del transporte público para el traslado hacia las oficinas por un lado y la seguridad fueron complicaciones que no se tenían previstas, esto trae por consecuencia que la investigación sea emulada bajo la plataforma de software GNS3, por un periodo de 3 meses. El alcance de la investigación y diseño abarca a equipos de la red LAN del cliente y al router de enlace hacia la red MPLS del Operador.

1.6 Objetivos de la investigación

1.6.1 Objetivo General

Aplicar protocolos SNMP y NETFLOW para operar una LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima.

1.6.2 Objetivos Específicos

a) Aplicar los protocolos SNMP y NETFLOW para la visibilidad y análisis del ancho de banda en la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima.
b) Emplear los protocolos SNMP y NETFLOW para el análisis de rendimiento de la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima.
c) Aplicar los protocolos SNMP y NETFLOW para la administración de incidencias en la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima.

CAPÍTULO II: MARCO TEÓRICO

2.1 Marco histórico

Los inicios de la LAN se dan con el inicio de la tecnología ETHERNET, según (James & Keith, 2017).

> Esto fue a mediados de la década de 1970 por Bob Metcalfe y David Boggs. La LAN Ethernet original utilizaba un bus coaxial para interconectar los nodos. Las topologías de bus para Ethernet consiguieron mantenerse durante la década de 1980 y hasta mediados de la década de 1990. Ethernet con una topología de bus es una LAN de difusión (todas las tramas transmitidas viajan hasta todos los adaptadores conectados al bus y son procesadas en ellos). A finales de la década de 1990 la mayor parte de las empresas y universidades habían reemplazado sus redes LAN por instalaciones Ethernet utilizando topologías en estrella basadas en concentradores (hubs). En ese tipo de instalación, los hosts (y los router) están directamente conectados a un concentrador mediante un cable de cobre de par trenzado. Un concentrador es un dispositivo de la capa física que actúa sobre los bits individuales en lugar de sobre las tramas. Cuando un bit, que representa un cero o un uno, llega procedente de una interfaz, el concentrador simplemente vuelve a crear el bit, incrementa su intensidad de energía y lo transmite a todas las demás interfaces. Por tanto, Ethernet con una topología de estrella basada en concentrador es también una red LAN de difusión (cuando un concentrador recibe un bit por una de sus interfaces, envía una copia al resto de sus interfaces). En particular, si un concentrador recibe tramas procedentes de dos interfaces distintas al mismo tiempo, se produce una colisión y los nodos que crean las tramas tendrán que retransmitirlas (p. 393).

También. a finales de la década de los 80’s llegan los inicios del software de gestión de redes, donde se define que el software de gestión son unos de los principales elementos que ayudará al ingeniero TI a tener una respuesta rápida frente a un evento, está detectarán de forma oportuna la fallas en la red y/o visualizarán el comportamiento mediante el análisis de tráfico de los equipos que conforman esta.

Uno de los elementos de un software de gestión es el protocolo SNMP (Protocolo de Simple Gestión de Red). En 1,987 se crea el protocolo SGMP de acuerdo con el RFC 1028 (Davin, Case, Fedor, & Schoffstall, 1987) “Este protocolo permitía administrar la red en constante crecimiento” (p. 1). Según el (Davin, J., M., & M., 1988) “RFC 1067 hace referencia que este protocolo en 1,988 se desarrolla el SNMP.V.1 el cual determina la estrategia de gestión en el modelo TCP/IP” (p. 1); este protocolo esta descrito también en los documentos RFC 1155,1157,1212 y 12123.

El SNMP se desarrolla por la necesidad de tener una forma simple y estándar de poder gestionar y monitorear la red, sin hacer uso del ancho de banda. En 1996 el protocolo SNMP evoluciona llegando a su versión SNMP.V2 basado en el RFC 1901 (Case, McCloghrie, Rose, & Waldbusser, 1996) “esta nueva versión agrega una mejora en la seguridad, operación de traps empleando un formato de mensaje distinto y reemplazando los traps de la versión SNMP.V1” (p. 3).

En 1997, se hace una breve descripción del SNMP.V3 en los RFC 1902-1908 y 2271-2275 presentando unas mejoras en la seguridad como la cuenta de usuario, autenticación y autentificación. Sin embargo, tenemos en el RFC 3410 (Case, Mundy, Partain, & Stewart, 2002) “que en el 2002 se define el SNMP.V3 como un estándar completo agregando principalmente capacidad de seguridad y configuración remota a SNMP” (pp. 3-4).

La evolución del software de gestión de redes también ha sido complementada con la llegada de protocolos Flow. Como indica (Auvik.com, 2019)

> Exactamente el NETFLOW generado por CISCO se introduce por primera vez en 1995 como la técnica basada en software para su uso exclusivamente LAN, ya que presentaba problemas en uso de gran ancho de banda. Es recién en 1996 esta característica se introduce como hardware dentro de los router CISCO para solucionar el problema principal y poder capturar flujos en mayor ancho de banda es así como da origen al NETFLOW.V1 (párr. 4-5).

En el 2004 en el RFC 3954 (Claise, 2004) se lanza el “NETFLOW.V9 el cual es la versión más común y utilizada al igual que la versión base NETFLOW.V5. Hasta el momento

con mayor diversidad de compatibilidad con otras marcas de router como Juniper, Mikrotik, Palo Alto, Riverbed, otros" (pp. 2-3).

Teniendo en cuenta que ambos protocolos no fueron creados al mismo tiempo y tampoco para trabajar juntos, en la siguiente publicación nos dan un concepto de cada protocolo y como estos pueden trabajar conjuntamente en una red; (Noction.com, 2019):

> SNMP y NETFLOW ofrecen dos enfoques diferentes para el monitoreo de la red. La amplia adaptación del proveedor, las características en tiempo real y el bajo consumo de recursos (en su mayoría las versiones anteriores de SNMP 1 y 2 sin autenticación y cifrado) hablan del uso de SNMP siempre que sea posible. Además, SNMP juega un papel clave en la gestión de fallas, donde puede detectar o incluso prevenir fallas de hardware. Todo esto nos permite suponer que SNMP se utilizará en los próximos años a pesar de sus limitaciones obvias. Por otro lado, SNMP carece de la precisión proporcionada por NETFLOW, por lo que no puede calificar en el análisis de tráfico. Por lo tanto, si corresponde, combine ambos métodos para el monitoreo de la red. SNMP para la gestión de fallas y una visión general rápida del rendimiento de la red, mientras que NETFLOW para la precisión en la estimación de los parámetros de tráfico de la red (párr. 11).

Como se vio en la línea de tiempo estos protocolos no se crearon a la vez y tampoco para trabajar conjuntamente es por esto que podemos observar las diferencias que existen entre estos protocolos según (Zhu., 2018) manifiesta que:

NetFlow surge como un protocolo más compacto que SNMP el cual escala mejor para la recopilación de rendimiento y la gestión del tráfico de red. Un par de grandes diferencias entre SNMP y NetFlow son:

-SNMP se puede utilizar para tiempo real (es decir, cada segundo) y, aunque NetFlow proporciona horas de inicio y finalización para cada flujo, no es tan real como SNMP.

-NetFlow le dice quién y con qué está consumiendo el ancho de banda, también es mucho más detallado que SNMP y, por lo tanto, las exportaciones de NetFlow consumen mucho más espacio en disco para la información histórica.

-SNMP se puede utilizar para recopilar la utilización de la CPU y la memoria y eso todavía no está disponible con NetFlow. (párr. 7)

Adicionalmente según (Bhardwaj, 2019) nos indica:

-SNMP utiliza un ancho de banda con respecto al envió de la información a través de la WAN menos del 1% aproximadamente, en cambio NETFLOW utiliza entre 2-5% para el envío de su información.

-SNMP utiliza la tecnología PULL debido a los traps de eventos que envía al servidor y NETFLOW utiliza tecnología PUSH cuando se realiza la consulta.

-El protocolo SNMP en la mayoría se encuentra en todos los equipos de red y NETFLOW esta limitad por la marca CISCO y algunas otras marcas.

-SNMP es usado principalmente para alarmas de equipos y notificaciones incluyendo sus interfaces y NETFLOW es usado para el ancho de banda, aplicaciones y origen/destino de IP (párr. 5).

2.2 Investigaciones relacionadas con el tema:

2.2.1 Antecedentes Internacionales

Se encontró la investigación de tesis de (Becerra, 2016) que lleva por título la implementación de monitoreo de red utilizando los protocolos ICMP y SNMP; para obtener el título de Ingeniería en Electrónica y Telecomunicaciones en la Universidad Estatal Península de Santa Elena, La Libertad - Ecuador, en donde:

> Se implementa un servidor con el que se van a monitorear los dispositivos y servidores de la Universidad Estatal Península de Santa Elena, con el propósito de poder brindar a las personas a cargo de la supervisión, una mejor gestión y control del consumo de los recursos de la red. Para este efecto se debe tomar en consideración que actualmente todo el caudal de información primordial de la institución viene en formatos sea de voz, datos y video en tiempo real, con una creciente demanda de disponibilidad y eficiencia de las comunicaciones en tales circunstancias. Con el cual concluye que el tema propuesto resalta la importancia de implementar este tipo de gestión, utilizando un servidor con características robustas y software comprobado, donde se utilicen recursos y protocolos cada vez más eficientes y amigables con sus usuarios y el entorno, el presente trabajo de investigación aplica métodos Hipotético, Deductivo, Analítico, Sintético, alcanzando los objetivos propuestos (p. 5).

En el presente antecedente citado, observamos la importancia del protocolo NETFLOW en un enlace, el cual puede ayudar a optimizar y resolver los problemas

del ancho de banda en una WAN según (Juane, 2015) en su tesis de investigación titulada *Analysis of possibilities to use information from NETFLOW protocol for improvement of performance of Wide Area Network*; para obtener su Licenciatura de fin de carrera en la Escuela Politécnica Superior Universidad Autónoma de Madrid manifiesta que:

> El principal objetivo de esta investigación es analizar la información relacionada con las conexiones que las Redes de Área Extensa (WAN) realizan con la red de la Universidad AGH de Cracovia, en Polonia, y de ahí obtener posibilidades de optimización. Es por ello que, mediante análisis de los registros de las conexiones, recogeremos las características de nuestra red, y de este análisis intentaremos averiguar cómo resolver los problemas que estas conexiones sufren. Este documento contiene los resultados obtenidos de un profundo análisis del tráfico producido en una WAN y a lo largo de ella (red del campus), y también los métodos y herramientas usadas durante el desarrollo de este (p. 10).

Adicionalmente, observamos que el protocolo NETFLOW aplicado en los router nos permite analizar el tráfico frente a un comportamiento anómalo que puede afectar el ancho de banda según lo citado por (Zambrano, 2015) en su investigación titulada Propuesta de utilización de herramientas de telemetría, indica que para:

> Identificar técnicas de Ciberdelitos como *Watering Hole*, en redes de infraestructura (caso de estudio NETFLOW de Cisco); para obtener el título de Máster en Redes de Comunicación en la Universidad Pontificia Universidad Católica del Ecuador expuso la propuesta de utilización de herramientas de telemetría, para identificar técnicas de ciberdelitos como *watering hole* en redes de infraestructura, caso de estudio NETFLOW de cisco. Para simular este ciberataque se diseñó una red de infraestructura con la herramienta GNS3, en este caso una topología vulnerable que consta de dos redes LAN, conectadas entre sí a través del internet. El área LAN de los clientes será denomina como LNCL y el área de los servidores como LNSR. El área atacada fue la de los servidores donde se explotaron las vulnerabilidades de los navegadores y de la base de Datos utilizando la herramienta Kali Linux. Para realizar el monitoreo de nuestra red se utilizó la herramienta Solarwinds Real-time NETFLOW Analyzer misma que permitió capturar flujos de datos de los routers previamente configurados con

NETFLOW, para luego mostrar gráficamente el tráfico de nuestra red una manera rápida y sencilla (p. 3).

2.2.2 Antecedentes Nacionales

Para este antecedente citado, vemos como el protocolo SNMP es aplicado para poder diagnosticar problemas de latencia y congestión en una red LAN según lo expuesto (Fernández, 2019) en su investigación titulada Implementación de un servidor como gestión y monitoreo de servicios para la red de datos en la UGEL Huamanga; para obtener el título profesional de Ingeniero de Sistemas de la Universidad Nacional de San Cristóbal de Huamanga expuso lo siguiente:

> En la UGEL Huamanga a medida que va creciendo la red de datos la carga de información que viaja a través de la red va disminuyendo, lo cual produce una gran congestión en el tráfico de tal manera que satura el ancho de banda, haciendo que el servicio sea de calidad baja y poco satisfactoria para el uso de los trabajadores que requieren una conexión eficiente. El objetivo de la presente investigación es implementar un servidor como gestión y monitoreo de dispositivos y servicios, mediante el protocolo SNMP, tecnologías de virtualización, Sistema Operativo Centos 7, Nethserver, herramientas Open Source como Ntopng, Suricata y Zabbix con la finalidad de monitorear el consumo del ancho de banda, análisis de todo el tráfico en el firewall en busca de ataques y anomalías conocidos y verificar el correcto funcionamiento de elementos de hardware y software para la red de datos. A partir de la implementación, el administrador de red podrá obtener la interfaz de graficas de la carga del CPU, el tráfico que atraviesa la red, que servicios son los que más usan el CPU, monitorización de los recursos de un host (carga del procesador, usos de los discos, logs del sistema) en varios sistemas operativos como son los que utilizan los servidores, controlar el consumo del ancho de banda a través de túneles SSL cifrados o SSH, chequeo de servicios paralizados, reportes y estadísticas del estado cronológico de disponibilidad de servicios y hosts (p. 9).

En el presente antecedente se ve la importancia del protocolo SNMP el cual permite al administrador recibir alertas ante cualquier evento anómalo de la red y de la salud de sus equipos según lo aplicado (Quispe, 2019). en su tesis titulada Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales

utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce; para obtener el título de Ing. de Telecomunicaciones en la UNMSM determina en los siguiente:

> Desarrollar e implementar un prototipo que permita monitorear en tiempo real los dispositivos de comunicación (router, switches, acces point) y los usuarios finales (laptop, computadoras personales, impresoras, fotocopiadoras) utilizando el protocolo Simple Network Management Protocol-SNMP y software libre para una empresa dedicada a la compra, venta y distribución de productos y servicios a través de Internet (e-commerce) con el fin de mejorar su productividad. El prototipo propuesto permite que el especialista en el área de Redes y Comunicaciones (Seguridad Perimetral) tenga el control a través de las alertas y reporte de eventos de los diferentes equipos de comunicación cuando presente fallas o alguna anomalía en el funcionamiento normal de dichos dispositivos y por consecuencia los diferentes eventos presentados en la topología de red serán presentados a través de un reporte gráfico donde indica la disponibilidad de los equipos, con ello se tomará las decisiones inmediatas para la continuidad del negocio (p. 5).

Finalmente observamos en este último antecedente como trabajar con dos protocolos para gestionar una red, mediante los cuales podremos monitorear la salud de equipos y recolectar los log de eventos para un análisis más detallado según lo citado por (Ramirez, 2019) en su tesis titulada Alternativas de configuración con el uso de los protocolos SYSLOG y SNMP para la gestión de red de redes avanzadas; para obtener el título de Ing. en Informática y Sistemas expone lo siguiente:

> Este estudio identifica a dos protocolos comúnmente utilizados para la gestión de red, con amplia difusión y disponibilidad en los dispositivos propios de una red avanzada; con el objetivo de determinar la mejor alternativa de configuración en un entorno emulado de la gestión de una red avanzada considerando la configuración de los protocolos en los equipos, el uso de recursos, la seguridad que presentan y los servicios disponibles. Debido a que la Red Académica Peruana se encuentra inactiva, como primera fase de este trabajo de investigación se realizó la propuesta de una topología con el fin de reinsertar a la Red Académica Peruana a la Red CLARA, además de usarlo como escenario para la emulación que es parte del estudio. La segunda fase consistió en la emulación de los

protocolos Syslog, SNMP v2c y v3 cada uno configurado en la misma topología, pero en escenarios distintos para realizar pruebas independientes de cada protocolo. Las pruebas realizadas demostraron que Syslog y SNMPv3 poseen capacidades propias cada una de ellas, pero que pueden complementarse configurándose de forma paralela; SNMPv3 se cataloga como una configuración "compleja" frente a SNMPv2c y Syslog que se considera entre "regular" y "simple"; además de presentar mayor consumo de recursos computacionales sobreponiéndose en el uso del CPU, memoria y ancho de banda (3.10%, 0.6KB, 0.23kbps) versus un Syslog más ligero consumiendo CPU, memoria y ancho de banda (0.5%, 0.3 KB, 0.07kbps); pero también se determinó que el nivel de seguridad authpriv del protocolo SNMPv3 presenta un nivel de seguridad "alto" por encima de SNMPv2c y Syslog, esto explica el mayor consumo de recursos e incluso el nivel de complejidad en la configuración. El protocolo que presenta mayores indicios favorables de los servicios disponibles para cada mensaje es Syslog, porque aporta mayor disponibilidad de información (p. 10).

2.3 Estructura teórica y científica que sustenta el estudio

2.3.1 Protocolo SNMP (Simple Network Management Protocol)

(ManageEngine, 2020) Define el SNMP como: Uno de los protocolos ampliamente aceptados para administrar y monitorizar elementos de red. La mayoría de los elementos de red de nivel profesional vienen con un agente SNMP incluido. Estos agentes deben estar habilitados y configurados para comunicarse con el sistema de administración de red (NMS).

Por otra parte, (Ford & Lew, 1998) define al protocolo SNMP como:

> Ideal para manejar y monitorear dispositivos y servicios de redes, este se basa en paquetes UDP, protocolo de la capa de transporte, basado en IP, compatible con SMNP. UDP es un protocolo sin conexión que no garantiza la entrega del paquete, por lo tanto, SMNP es un protocolo no orientado a la conexión y utiliza los puertos 161 y 162. El protocolo SNMP corresponde a la capa de aplicación del modelo de referencia OSI. El utilizar UDP implica que no se establece una sesión entre el NMS y los agentes, lo cual hace que las transmisiones sean más rápidas y que la red no se sobrecargue, pero también implica que el que envía los mensajes debe, por algún medio, asegurar que este ha sido recibido, en el caso del sondeo el NMS

> puede esperar un tipo por la respuesta y, en caso no está reciba, se puede reenviar el paquete (p. 63).

Entonces podemos decir que el SNMP es un protocolo importante correspondiente a la capa de aplicación del modelo OSI, que nos permitirá gestionar y monitorear la salud de mis equipos de red sin utilizar altos recursos del ancho de banda; gracias a la comunicación entre administrador y agente podremos recolectar información para gestionar y monitorear sus agentes.

Adicionalmente, según bases teóricas sabemos que es un protocolo de administración de red simple (SNMP) que como indica (Odom, 2017):

> Es de capa de aplicación que a su vez proporciona un formato de mensaje para la comunicación entre lo que se denomina administradores y agentes. Un administrador SNMP es una aplicación de administración de red que se ejecuta en una PC o servidor, y ese host se suele llamar estación de administración de red (NMS). Existen muchos agentes SNMP en la red, uno por dispositivo que está administrado. El agente SNMP funciona con software dentro de cada dispositivo (enrutador, conmutador, etc.), con conocimiento de todas las variables en ese dispositivo que describen la configuración, el estado y los contadores del dispositivo. El administrador SNMP utiliza los protocolos SNMP para comunicarse con cada agente SNMP (p. 418), como se observa en la Figura N° 1.

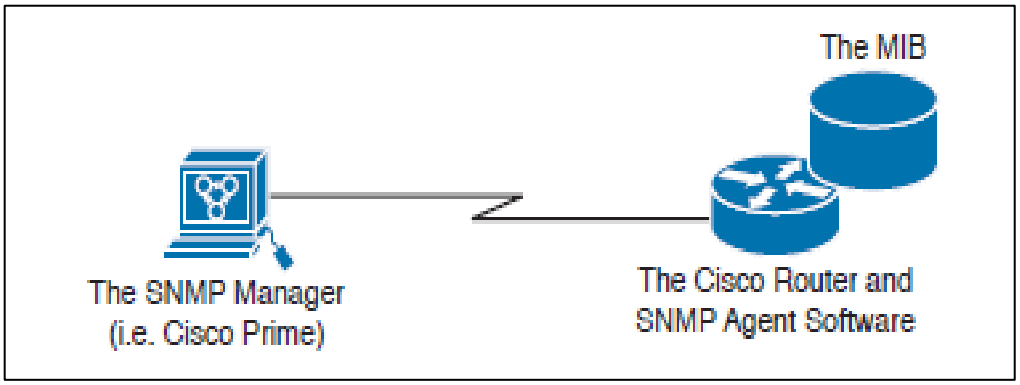


Figura N° 1: Elementos del SNMP
Fuente: Odom, W. (2017)

Con respecto a la arquitectura y funcionalidades del SNMP: Los componentes de la arquitectura del SNMP mencionados por (ManageEngine, 2020) son:

Administrador SNMP: Un administrador o sistema de administración es una entidad separada responsable de comunicarse con los dispositivos de red implementados por el agente SNMP. Normalmente es un equipo que se utiliza para ejecutar uno o más sistemas de administración de red.

Funciones clave del administrador SNMP: presenta lo siguiente: agentes de consultas, obtiene respuestas de agentes, establece variables en agentes y finalmente reconoce eventos asincrónicos de agentes.

Dispositivos administrados: Un dispositivo administrado o el elemento de red es una parte de la red que requiere algún tipo de monitorización y administración, por ejemplo, enrutadores, conmutadores, servidores, estaciones de trabajo, impresoras, UPS, etc. (párr. 8).

Agente SNMP: El agente es un programa que está empaquetado dentro del elemento de red. La habilitación del agente le permite recopilar la base de datos de información de administración del dispositivo localmente y la pone a disposición del administrador SNMP, cuando se le solicita. Estos agentes pueden ser estándar (por ejemplo, Net-SNMP) o específicos de un proveedor (por ejemplo, HP Insight Agent) (párr. 9).

Funciones clave del agente SNMP: presenta lo siguiente: recopila información de administración sobre su entorno local, almacena y recupera información de gestión según se define en la MIB, señala un evento al administrador y finalmente actúa como proxy para algunos nodos de red administrables que no son SNMP (párr. 10), como se observa en la Figura N° 2.

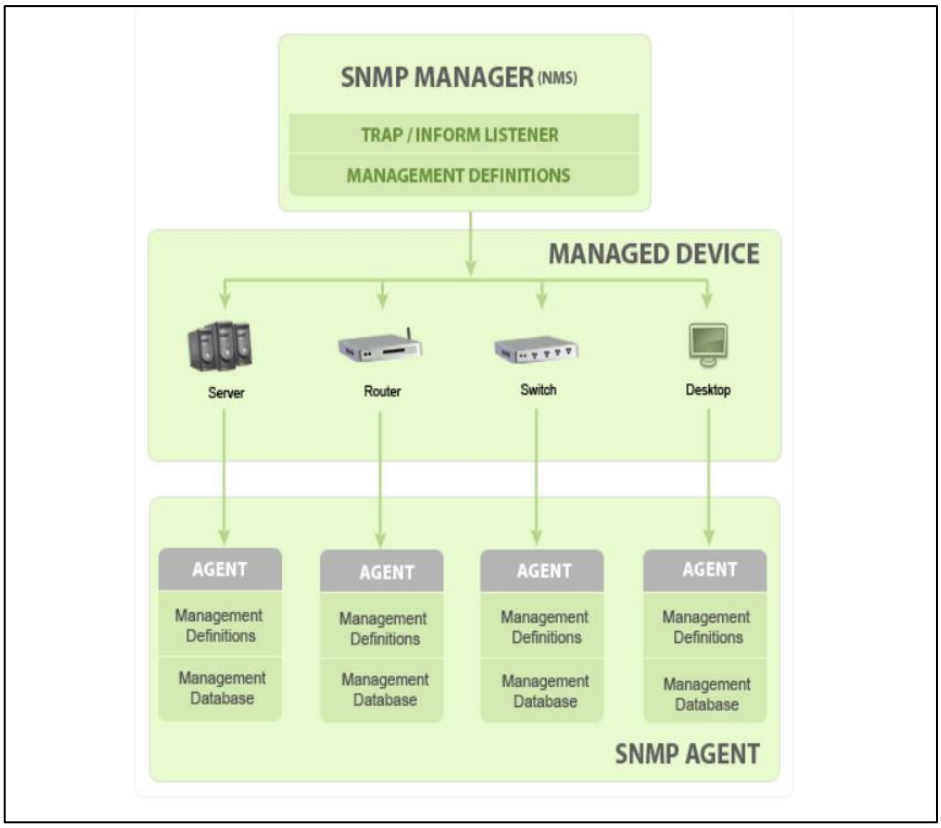


Figura N° 2: Esquema de comunicación SNMP
Fuente: ManageEngine (2020)

Base de datos de información de administración o Base de información de administración (MIB): Cada agente SNMP mantiene una base de datos de información que describe los parámetros del dispositivo administrado. El administrador SNMP usa esta base de datos para solicitar al agente información específica y traduce aún más la información según sea necesario para el Sistema de administración de red (NMS). Esta base de datos comúnmente compartida entre el Agente y el Administrador se denomina Base de información de administración (MIB) (párr. 11).

Por lo general, estas MIB contienen un conjunto estándar de valores estadísticos y de control definidos para nodos de hardware de una red. SNMP también permite la extensión de estos valores estándar con valores específicos para un agente en particular mediante el uso de MIB privadas (párr. 12).

En resumen, los archivos MIB son el conjunto de preguntas que un administrador SNMP puede hacerle al agente. El agente recopila estos datos localmente y los almacena, según se define en la MIB. Por lo tanto, el administrador de SNMP debe conocer estas preguntas estándar y privadas para cada tipo de agente (párr. 13).

Estructura de MIB e identificador de objeto (ID de objeto u OID): La Base de información de administración (MIB) es una recopilación de información para administrar el elemento de red. Las MIB se componen de objetos administrados identificados mediante el nombre Identificador de objeto (ID de objeto u OID) (párr. 15).

Cada identificador es único y señala características específicas de un dispositivo administrado. Cuando se lo consulta, el valor de retorno de cada identificador puede ser diferente, por ejemplo, Texto, Número, Contador, etc. (párr. 16).

Hay dos tipos de objeto administrado o ID de objeto: Escalar y tabular. Podrían entenderse mejor con un ejemplo (párr. 17).

Escalar: Nombre del proveedor del dispositivo, el resultado solo puede ser uno. (Como dice la definición: "Objeto escalar define una instancia de objeto única") (párr. 18).

Tabular: El uso de la CPU de un procesador cuádruple, esto me daría un resultado para cada CPU por separado, lo que significa que habrá 4 resultados para esa ID de objeto en particular. (Como dice la definición: "El objeto tabular define varias instancias de objetos relacionados que se agrupan en tablas MIB") (párr. 19).

Cada ID de objeto se organiza jerárquicamente en MIB. La jerarquía de MIB se puede representar en una estructura de árbol con un identificador de variable individual (párr. 20).

Un ID de objeto normal será una lista punteada de enteros. Por ejemplo, el OID en RFC1213 para "sysDescr" es .1.3.6.1.2.1.1.1. En la siguiente Figura N° 3 podemos observar el diagrama del árbol MIB (párr. 21):

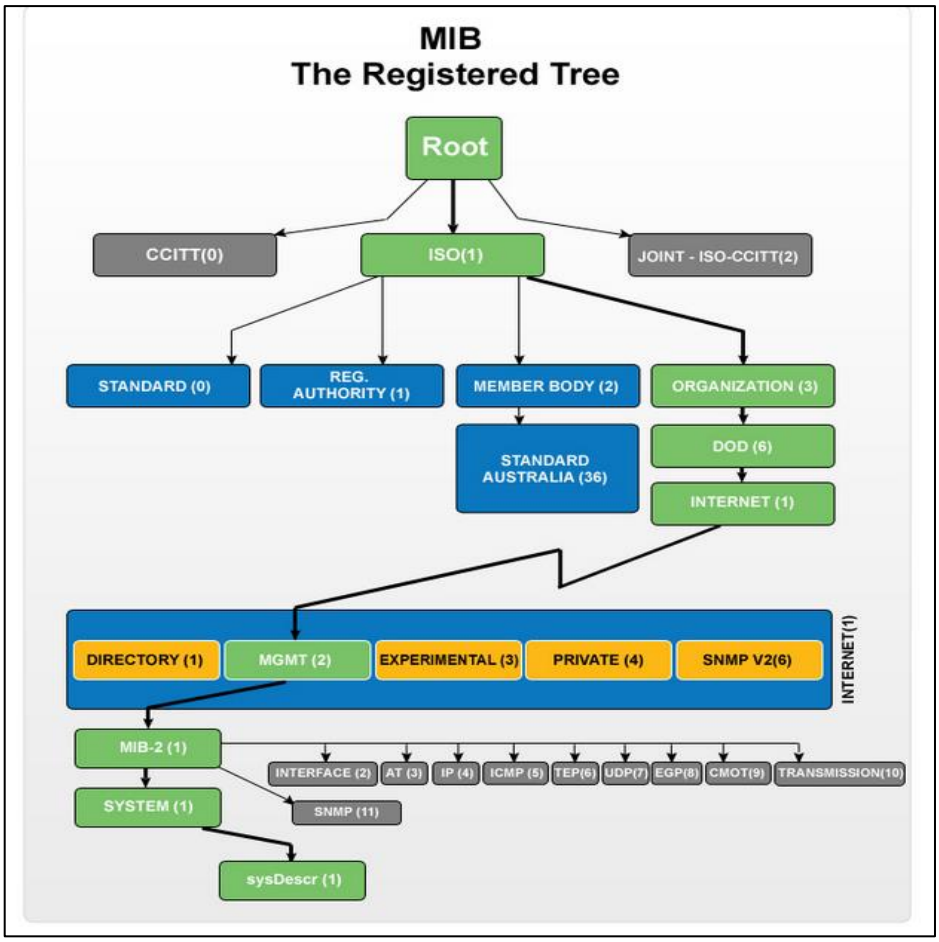


Figura N° 3: Diagrama del árbol MIB
Fuente: ManageEngine (2020)

Con el tiempo este protocolo SNMP ha ido evolucionando en distintas versiones y con los RFC como documentación que acompaña a cada versión nos da un mayor alcance de este protocolo, es así que ManageEngine (2020) nos menciona lo siguiente:

El SNMP v1 y v2c son las versiones más implementadas de SNMP. La compatibilidad con el protocolo SNMP v3 ha comenzado a ponerse al día recientemente, ya que es más segura en comparación con sus versiones anteriores, pero aún no ha alcanzado una cuota de mercado considerable (párr. 27).

SNMPv1: Esta es la primera versión del protocolo SNMP, que se define en RFC 1155 y 1157 (párr. 28).

SNMPv2c: Este es el protocolo revisado, que incluye mejoras de SNMPv1 en las áreas de tipos de paquetes de protocolo, asignaciones de transporte y elementos de estructura MIB, pero usando la estructura de administración SNMPv1 existente ("basada en la comunidad" y, por lo tanto, SNMPv2c). Se define en RFC 1901, RFC 1905, RFC 1906, RFC 2578 (párr. 29).

SNMPv3: SNMPv3 define la versión segura de SNMP. El protocolo SNMPv3 también facilita la configuración remota de las entidades SNMP. Se define mediante RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415 (párr. 30).

En la presente investigación hemos utilizado el siguiente dimensionamiento para el protocolo SNMP:

Dimensión 1: Monitoreo de salud de equipos:

También conocida como la gestión del rendimiento según lo que indica (Romero, 2013) que consiste en monitorizar la red para conocer su estado de salud, esto nos ayudará a conocer la red para saber si es posible añadir nuevos servicios y adelantarnos a los futuros problemas de red, asegurando la disponibilidad del servicio y niveles óptimos de red (párr. 7).

El monitoreo de salud de equipos también se relaciona con la administración de fallos dado que el monitoreo constante de todos los elementos de la red permite detectar errores que se presenten tanto en el hardware como en la parte lógica del equipo. De este modo podemos citar a (Becerra, 2016) quien explica el monitorear un servidor y las partes a monitorear.

> Monitorear un servidor de red significa que el administrador conocerá si uno o todos sus servicios están caídos. La monitorización del servidor puede ser interna o externa. Durante el monitoreo se verifican características como el uso del CPU, usos de memoria, rendimiento de red y el espacio libre en disco e incluso las aplicaciones instaladas (pág. 17).

También (Becerra, 2016) menciona los métodos de monitoreo de la red los cuales se basan en: "Monitoreo Activo: Este tipo de monitoreo se realiza introduciendo paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones y midiendo sus tiempos de repuesta". Y "Monitoreo Pasivo: Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red", utilizando para esto equipos como router, switches o computadoras equipos que deben tener el agente SNMP como base primordial".

Esta recopilación de información que se puede obtener de los dispositivos administrados es muy valiosa y se puede ser muy proactivo al momento de gestionar la LAN y ver en el tiempo las renovaciones de aquellos equipos que necesiten algún tipo de actualización de hardware o lógico.

Dimensión 2: Gestión de red:

Según (Romero, 2013) consiste en detectar, aislar y resolver los problemas de red, es el proceso donde los problemas son descubiertos y corregidos. Es obligatorio ser pro - activos para minimizar los tiempos medios de reparación (MTTR) y maximizar los tiempos medios entre fallo (MTBF), para ello se utilizan mecanismos de notificación como SNMP que permiten medir y controlar el estado actual de la infraestructura de red (párr. 4).

Bajo este concepto podemos mencionar también lo indicado por (Quispe, 2019) en el modelo de gestión de redes de datos:

> La gestión de red se refiere a la supervisión, organización y control de los servicios de comunicación de red, así como el estado de los dispositivos de red. El objetivo es garantizar que la red informática tenga un funcionamiento normal. La gestión de los recursos puede ser asistido mediante el uso de un marco de gestión de red (pág. 37).

La gestión de red es la base primordial en toda empresa y viene a ser parte fundamental en el éxito del mismo. El más pequeño problema que se pueda presentar en la red puede traer consigo resultado que afecten la productividad de la empresa, por ello la herramienta asociada a la gestión de la red debe ser fácil de implementar y usar, además que se pueda ir mejorando o desarrollando de forma gradual, mejor dicho, que sea una solución escalable. Desde este punto podemos citar a (Ramirez, 2019), en el cual manifiesta en su tesis "que la gestión de red consiste en realizar 4 actividades básicas que son: El monitoreo, configuración, actualización y resolución de problemas de los recursos de la red" (pág. 18).

El administrador de red debe contar con una herramienta que le pueda proporcionar visibilidad de su entorno de red y poder actuar en base a la información que va recopilando, mediante obtención de reportes de una manera fácil y sencilla que ayude a optimizar su red, a tener menos fallas de equipos en el tiempo y que las incidencias sean manejadas de una forma ágil y rápida, teniendo un control total de los dispositivos que integran la red LAN.

2.3.2 Protocolo NETFLOW

Según (Claise, 2004) lo define como un protocolo que sirve para recopilar información sobre el tráfico de la red, este flujo se define como una secuencia unidireccional de paquetes con algunas propiedades comunes que pasan a través de

un dispositivo de red. Estos flujos recopilados se exportan a un dispositivo externo, el recopilador NETFLOW. Los flujos de red son altamente granulares; por ejemplo, los registros de flujo incluyen detalles como direcciones IP, conteos de paquetes y bytes, marcas de tiempo, Tipo de Servicio (ToS), puertos de aplicación, interfaces de entrada y salida, etc. (p. 2).

También tenemos a (ManageEngineBlog, 2019) que indica:

El NETFLOW se puede definir de muchas maneras. Cisco NetFlow v5, el estándar, define un flujo como la secuencia unidireccional de paquetes que comparten los siguientes valores:

Dirección IP de origen

Dirección de destino

Protocolo IP

Puerto de origen para UDP o TCP

Puerto de destino para UDP o TCP, tipo y código para ICMP

Tipo de servicio de IP Cisco también ofrece NetFlow v7, v9 y v10, que amplían la definición de v5 agregando más campos (párr. 1-2).

Basados en esto, podemos definir que el protocolo NETFLOW nos servirá para monitorear y analizar el flujo de red, ya que podremos supervisar todos los paquetes que viajan en la red de forma granulada desde la dirección IP origen, dirección IP destino, puertos UPD y/o TCP, otros.

Adicionalmente, según bases teóricas sabemos según (PaesslerAg, 2020) que el NETFLOW es:

> Un protocolo para recopilar, agregar y registrar datos de flujo de tráfico en una red. Los datos de NetFlow proporcionan una vista más granular de cómo se utilizan el ancho de banda y el tráfico de red que otras soluciones de monitoreo, como SNMP (párr. 1).
>
> NetFlow fue desarrollado por Cisco y está integrado en el software IOS de Cisco en los enrutadores y conmutadores de la compañía, y ha sido compatible con casi todos los dispositivos Cisco desde el tren 11.1 del software Cisco IOS. Muchos otros fabricantes de hardware admiten NetFlow o utilizan tecnologías de flujo alternativas, como jFlow o sFlow (párr. 2).

Con respecto a las versiones de NETFLOW, (PaesslerAg, 2020) indica que:

> Técnicamente, hay diez versiones diferentes de NetFlow. Sin embargo, varias versiones se lanzaron solo internamente o nunca se implementaron ampliamente más allá del hardware específico.
>
> La versión 5 todavía se usa comúnmente hoy en día, debido a una gran base de instalación existente de enrutadores y conmutadores Cisco lanzados mientras era la versión estándar.
>
> La versión 9 es la versión actual y está basada en plantillas. Como tal, permite un soporte ampliado sin necesidad de cambiar el formato de registro de flujo. Se prefiere esta versión para IETF IP Information Export (IPFIX) WG y IETF Pack Sampling WG (PSAMP) y funciona tanto con IPv4 como con IPv6 (párr. 3-7).

Otras versiones de Flow (flujo de red) según (ManageEngineBlog, 2019) tenemos las siguientes versiones que trataron de imitar o asemejarse a la funcionalidad del NETFLOW (párr. 3-4):

IPFIX
sFlow
J-Flow
AppFlow
NetStream
Cflowd

En esta investigación hemos utilizado el siguiente dimensionamiento para el protocolo NETFLOW:

Dimensión 1: Monitoreo del flujo de red

Según la definición de (ManageEngineOpManager, 2020) permite visualizar los patrones de tráfico de la red y el uso del ancho de banda, con soporte de flujo para NetFlow, sFlow, j-Flow, IPFIX, etc. Permite monitorear el ancho de banda en tiempo real con informes de tráfico detallados para identificar los problemas de ancho de banda antes de que afecten a los usuarios finales (párr. 1).

Dado esta definición al haber tráfico de red en una empresa el objetivo de analizarlo y poder monitorearlo es parte fundamental del administrador de TI, según (Juane,

2015) se puede decir que los primeros pasos fueron desarrollar enfoques de monitoreo de redes divididos en dos categorías:

Monitoreo Activo: Inyecta tráfico a la red para realizar diferentes tipos de medidas como los conocidos comandos PING y TRACEROUTER.

Monitoreo Pasivo: Observar el tráfico existente a medida que pasa por un punto de medición y, por tanto, observar el tráfico generado por el usuario (p. 21).

(Juane, 2015) también complementa lo siguiente en cuanto al monitoreo del flujo de red:

> El objetivo de monitorear el tráfico en las redes de alta velocidad ha aumentado el monitoreo del flujo, convirtiéndolo en un método predominante. Antes de que el monitoreo basado en flujo tomara la importancia que tiene hoy en día, el conocido análisis basado en paquetes solía ser el más utilizado, pero las redes de alta velocidad (hasta 100Gbps) requieren hardware costoso y una gran infraestructura para asignar y analizar posteriormente los paquetes. Debido a esto un enfoque más escalable para su uso en redes de alta velocidad es la exportación de flujo, en el que los paquetes se agregan en flujos y se exportan para su almacenamiento y análisis (pág. 21).

Dimensión 2: Análisis de flujo de red

Según (ManageEngineNetFlowAnalyzer, 2020) el analizador de tráfico de red basado en la web utiliza datos de flujo como NetFlow de dispositivos Cisco, sFlow, J-Flow, IP FIX y más y los almacena para analizar y generar informes de tráfico. En términos simples, NetFlow Analyzer recopila información de flujo, los correlaciona y presenta las estadísticas de tráfico en una forma más representable y comprensible. Ofrece gráficos e informes de tráfico en tiempo real para conocer su comportamiento y uso del tráfico por parte de las aplicaciones, los usuarios y sus conversaciones (párr. 1).

En el análisis del flujo de red (Juane, 2015) hace referencia a tres áreas que se relacionan con el análisis de una red.

> Análisis e informes de flujo, se utiliza para verificar como los usuarios utilizan su red, simplemente navegando y filtrando los datos de flujo, verificando estadísticas como los que más hablan, las subredes que intercambian más tráfico, el uso del ancho de banda y también la posibilidad de informar y alertar cuando se supere alguna de estas situaciones, simplemente configurando un umbral de tráfico. Con

la ayuda de unos gráficos podemos comprobar los momentos en los que el tráfico se comporta diferente, debido a que puede ser malicioso o confiable.

La detección confiable, podemos distinguir entre dos tipos de uso: Los datos de flujo se pueden usar únicamente para analizar que host se ha comunicado con que host, incluyendo resúmenes de la cantidad de paquetes y bytes involucrados, la cantidad de conexiones, etc. El segundo utiliza la definición de un flujo para analizar ciertos tipos de amenazas, lo que permite modelar las amenazas en términos del comportamiento de la red.

Monitoreo de desempeño, que tiene como objetivo observar el estado de los servicios que se ejecutan en la red. Podemos distinguir entre la posibilidad de realizar el exportador y el recolector de alguna manera para poder obtener mejores flujos para analizar, verificar los efectos de la resolución del reloj o desarrollar algunos métodos para la elaboración de perfiles de exportadores. El rendimiento de las aplicaciones de análisis de datos generalmente se mide por medio de la capacidad de respuesta de la interfaz. Las métricas más comunes que se utilizan para realizar informes de aplicaciones de análisis de datos incluyen el tiempo de ida y vuelta (RTT), el retraso, la fluctuación, el tiempo de respuesta, la perdida de paquetes y el uso del ancho de banda (p. 23).

2.3.3 LAN (Local Area Network)

Podemos comenzar a definir la LAN con el concepto de (Stallings, 2004) quien manifiesta lo siguiente; “Al igual que las redes WAN, una LAN es una red de comunicaciones que interconecta varios dispositivos y proporciona un medio para el intercambio de información entre ellos.” (p. 17).

Asimismo, (Perez, 2018) manifiesta:

El modo de operar de estas se basa en Ethernet, definido en el estándar IEEE 802.3, el cual establece los protocolos y tecnologías necesarios a aplicar tanto en capa física como en enlace de datos para que dicha comunicación pueda ser llevada a cabo entre todos los miembros de la red (p. 18).

Adicionalmente, según bases teóricas el concepto de LAN (*Local Area Network*) definido por (Alcócer, 2000) :

Se inicia con el desarrollo del procesamiento distribuido en la década del 70. El primer paso fue interconectar dos computadoras idénticas punto a punto. Una vez

vistas las ventajas del procesamiento distribuido, las redes de computadoras se desarrollaron rápidamente. Una de las primeras redes fue ARPANET, del Departamento de Defensa de los Estados Unidos (DoD), a fines de los años 60. Durante la siguiente década, las computadoras personales versátiles y relativamente baratas se establecieron firmemente y surgió entre los usuarios de programas de aplicación la necesidad de:

Compartir programas, archivos (*files*).

Compartir periféricos (impresoras).

Compartir memoria de masa (discos duros), etc.

Entonces se inició el desarrollo de una LAN comercial en el Centro de Investigación de Xerox en Palo Alto California, en 1972. En 1979 salió al mercado la red Ethernet, gracias a los esfuerzos corporativos de Digital Equipment Corporation (DEC), Intel y Xerox. Sus especificaciones vinieron a ser la norma de facto de las redes LAN. (p. 116).

(Alcócer, 2000) también nos menciona que:

El comité IEEE Proyecto 802, que fue encargado de establecer las normas de estas redes, de aquí en adelante nos referiremos a la red de área local como LAN. Esta se diferencia de otros tipos de redes en lo siguiente:

Sus comunicaciones están confinadas a un área geográfica moderada, tal como un solo edificio, un almacén o un campus universitario.

Opera a velocidades moderadas y altas (10, 100, 1000Mbps) con bajo porcentaje de errores.

Permite a las estaciones comunicarse directamente, empleando un medio físico común sobre enlace punto a punto sin requerir de ningún nodo de conmutación intermedio. Por ello, requiere una subcapa de acceso que administre el acceso al medio compartido

Posibilita la compatibilidad entre equipos de diferentes fabricantes, posibilitando las comunicaciones con un mínimo esfuerzo de los usuarios.

Es operada por una sola organización. Esto contrasta con las redes de área amplia (*Wide Area Network – WAN*), las que interconectan equipos de comunicación de datos de distintas organizaciones y en diferentes partes de un país, pudiendo brindar un servicio público.

> Son diferentes de otras redes tales como los buses planos, que se usan para interconectar dispositivos de una computadora personal o componentes dentro de una sola pieza de equipo (p. 116).

Características de una LAN ideal: Una LAN ideal debe ser fácil de usar y administrar, es decir, no presentar complicaciones en su operación. Sus características según lo expuesto por (Alcócer, 2000) son:
-Instalación de una sola vez.
-Acceso ampliamente distribuido.
-Independencia de aplicación.
-Exceso de capacidad (caudal).
-Fácil mantenimiento y administración (p. 117).

Aplicaciones: La LAN se puede aplicar en muchos sitios, como, por ejemplo: Universidades, colegios, fábricas, hospitales, automatizando fábricas, corporaciones, centro de datos, etc.

Dada estas definiciones, podemos mencionar lo que respecta a topologías de red, las cuales se indican a continuación (Varela, 2010): “Bus, Anillo, Doble anillo, Estrella, Estrella extendida. Árbol, Malla y Mixta”.

Estándares de la LAN: Vamos a comenzar citando lo expuesto por (Perez, 2018):

> Manifiesta que la LAN dispone de diferentes variantes, adaptadas a cada medio y velocidad, de tal manera que el estándar necesario para una LAN de 10Mbps no coincide con el aplicado sobre otra de 100Mbps. El primero en aparecer fue 802.3i, el cual define una red de 10Mbps utilizando como medio de transporte cableado de cobre. A raíz del mismo, y en relación con la aparición de nuevas tecnologías resulto necesaria la adaptación del estándar a estas, dando lugar al desarrollo de diferentes versiones (p. 18).

En el siguiente cuadro se mencionan las más comunes según (Perez, 2018) y (Alcócer, 2000):

Tabla 1: Cuadro de Estándares

Nombre común	Estándar IEEE	Nombre alternativo	Velocidad	Medio físico
Ethernet	802.3	10Base5	10Mbps	Coaxial, 500m
Thin Ethernet	802.3a	100Base2	10Mbps	Coaxial, 185m
Ethernet	802.3i	10Base-T	10Mbps	Cobre, 100m, cat 3,5,5e y 6
Ethernet	802.3j	10Base-FL	10Mbps	FO MM 850nm, 2000m
Fast Ethernet	802.3u	100Base-TX	100Mbps	Cobre, 100m, cat 5,5e y 6
		100Base-FX	100Mbps	FO MM 1300nm
Gigabit Ethernet	802.3z	1000Base-LX 1000Base-SX 1000Base-CX	1000Mbps	Fibra, 550m 850nm (SX), 5km (LX) 1300nm
Gigabit Ethernet	802.3ab	1000Base-T	1000Mbps	Cobre, 100m, cat. 5 o superior
10Gigabit Ethernet	802.3ae	10GBase-SR 10GBase-LR 10GBase-T	10Gbps	FO y Cobre
40Gigabit Ethernet	802.3ba	----------	40Gbps 100Gbps	40: Cobre más 10m. FO MM 100m 100: Cobre 10m. FO MM 100m. FO SM 40km

Fuente: Elaboración propia

(Perez, 2018) explica que todas ellas comparten la misma finalidad, basadas en ejecutar las funciones necesarias en capa 1 y 2 para que la transmisión de datos concluya con éxito.

En capa 1 se define las señales, cadenas de bits componentes físicos y distintas topologías de red. Mientras en enlace de datos, cada una de las subcapas ejecutara funciones específicas. En este aspecto, LLC aplica el estándar 802.2, encargándose de: establecer la conexión con capas superiores, crear la trama en capa 2, identificar el protocolo aplicado en capa 3.

Mientras, MAC hace uso de 802.3, siendo sus funciones: encapsulado de datos, lo que incluye delimitación de tramas, direccionamiento físico y detección de errores; control de acceso al medio.

De tal manera como se observa en la siguiente Figura N°4 - gestión de capas de ethernet:

-

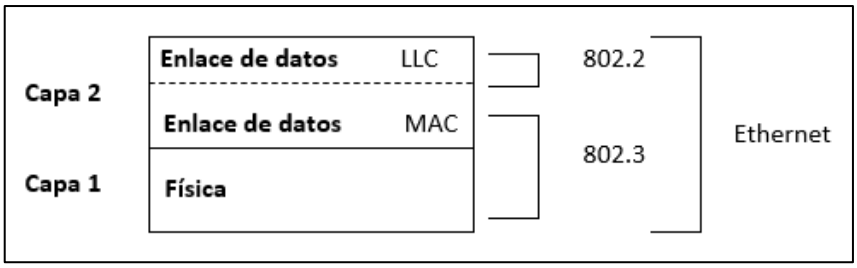


Figura N° 4: Gestión de capas de Ethernet
Fuente: Perez, D. (2018)

Ethernet realmente ejecuta ambos, pero el primero (LLC) nunca varia, es decir, realiza siempre las mismas funciones de la misma manera sin importar el medio físico al que esté conectado. Sin embargo, la subcapa MAC y la capa 1 sí que necesitan variar las técnicas aplicadas dependiendo de los componentes físicos (p. 19).

Actualmente, la creación de una LAN domestica consta de un procedimiento bastante sencillo como se observa en la Figura N°5 – la LAN ethernet básica, donde tan solo bastarían 3 elementos (p. 20): Una tarjeta de red (NIC) en cada uno de las Pc´s, un Hub o switch ethernet y un cableado UTP para establecer la conexión entre los Pc´s y el hub o switch.

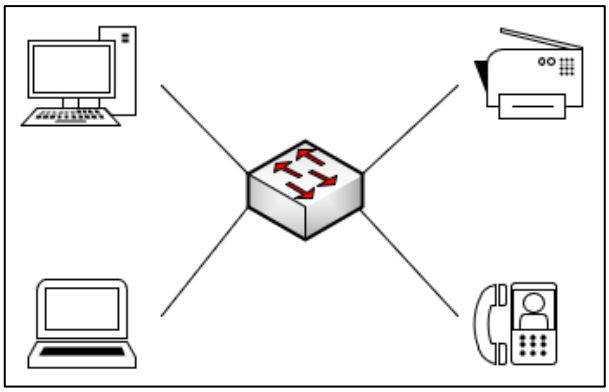


Figura N° 5: LAN Ethernet básica
Fuente: Perez, D. (2018)

Comparación entre el modelo OSI y TCP/IP: En esta parte (Perez, 2018), explica: La mayor diferencia entre ambos modelos simplemente radica en el número de capas, OSI hace uso de 7, mientras que TCP/IP de 4. Sin embargo, el procedimiento llevado a cabo para establecer, mantener y transportar la comunicación entre dispositivos resulta prácticamente el mismo. Ello debido a que tanto OSI como TCP/IP hacen uso de protocolos ya existentes, como HTTP, SNMP, etc., en aplicación. TCP o UDP para transporte. IP en capa de red, etc. Estos son los que realmente manipulan los datos, por lo tanto, los procesos llevados a cabo en ambos modelos coinciden. OSI además tiene la peculiaridad que, al ser dividido en más capas, cada una de ellas está muy bien definida, mientras que TCP/IP al englobas funcionalidades, en ocasiones resulta más tedioso (p. 17).

La comparación entre los estándares indicados la tenemos con mayor detalle en la Figura N°6:

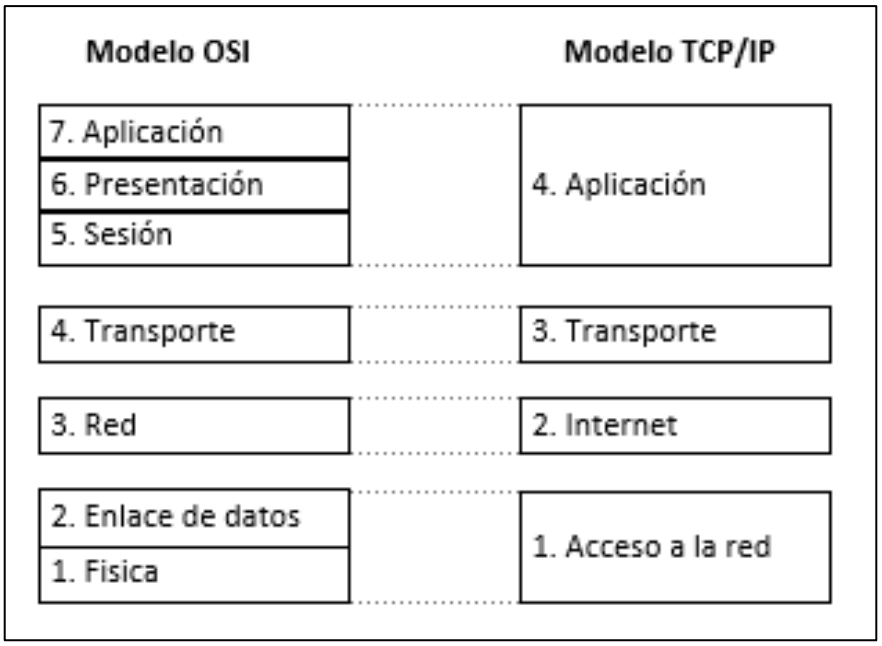


Figura N° 6: Comparación entre los modelos OSI y TCP/IP
Fuente: Perez, D. (2018)

En la Figuran N°7 se muestran los niveles de referencia LAN respecto al modelo OSI:

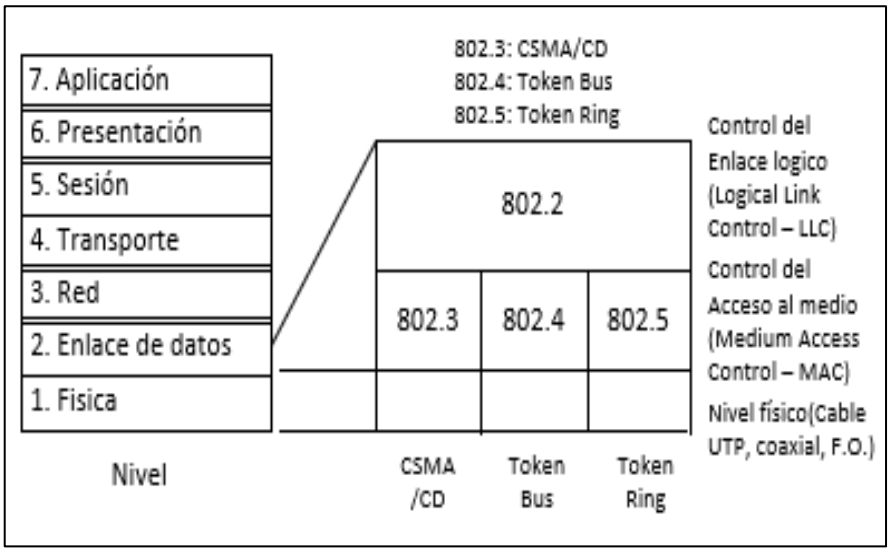


Figura N° 7: Niveles de referencia de LAN respecto al modelo OSI
Fuente: Alcócer, C. (2000)

CAPA 2 – Enlace de Datos: (Perez, 2018), conceptualiza lo siguiente:

Una vez concluido el proceso de encapsulación en capa 3 el paquete es enviado a capa 2, que desarrolla dos funciones principales: primero, aplica el protocolo necesario en relación con el medio físico disponible, y segundo, ejecuta las técnicas necesarias de control de acceso al medio. Para ello divide su modo de operar en dos subcapas, LLC y MAC.

LLC (*Logical Link Control*): su misión consiste en identificar el protocolo aplicado en capa 3 y convertir el paquete en trama.

MAC (Media Access Control): agrega las direcciones físicas del origen y destino de la comunicación (direcciones MAC), controla el acceso al medio mediante diferentes técnicas y dispone funciones de control de flujo y detección de errores.

El control de acceso al medio se encarga de examinar el medio físico antes de proceder al envió de datos, con el objetivo de que no se produzcan colisiones y la transmisión resulte fiable. Para lograrlo se puede hacer uso de dos técnicas, CSMA/CD o CSMA/CA.

En CSMA/CD el dispositivo monitoriza el medio físico en busca de una señal de datos. Si no la detecta significa que está libre, por lo tanto, comienza a transmitir. Sin embargo, aun así, es posible que se produzcan colisiones. En estos casos todos los dispositivos detienen el envío para volverlo a intentar pasado un tiempo aleatorio definido por cada uno de ellos. Esta técnica es la aplicada mayormente en redes Ethernet.

CSMA/CA resulta bastante similar en cuanto a modo de operar, pero agrega una pequeña característica, que consiste en el envío de una notificación antes de transmitir datos. Es decir, primero se examina el medio en busca de alguna señal, y si está libre, envía una notificación informando al resto de dispositivos su intención de utilizarlo. Esta técnica es la aplicada generalmente en tecnologías inalámbricas 802.11.

Tanto CSMA/CD como CSMA/CA se aplican en medios compartidos como Ethernet o inalámbricos. Estas conexiones pueden ser de dos tipos, half-duplex o full-dúplex.

Por último, la trama creada incluirá una nueva cabecera y tráiler, y con ella queda definido el formato final de los datos que serán transmitidos, el cual varía en función del protocolo aplicado, que a su vez depende del medio físico. Los más comunes son:

IEEE 802.3 (Ethernet)

IEEE 802.5 (Token Ring)

IEEE 802.11 (Wireless)

ITU Q.922 (Frame Relay)

ITU Q.921 (ISDN)

ITU HDCL (Control de enlace de datos de alto nivel)

La gran mayoría de protocolos de enlace de datos, incluido Ethernet, permiten un máximo de 1500 bytes recibidos desde capa 3. Este tamaño es denominado MTU (*Maximun trasmission unit*) (pp. 14-16), en la siguiente Figura N°8 observamos la trama Ethernet.

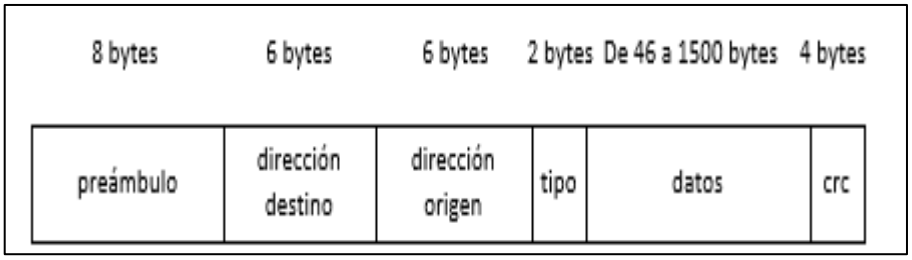


Figura N° 8: Trama Ethernet 802.3
Fuente: Elaboración propia.

CAPA 1 – Física: Para la capa 1 (Perez, 2018) indica que:

Es aquella que conecta directamente con los medios para realizar el envío de datos, desarrollando principalmente tres funciones: identificación de componentes físicos, codificación y señalización.

La identificación de componentes hace referencia al tipo de cableado, conectores, circuitos, señales inalámbricas, etc. En definitiva, el medio disponible para transportar los bits que conforman la trama desde el origen hasta el destino.

La codificación es la técnica aplicada para transformar los datos en bits. Este hecho resulta importante, ya que la capa física no transporta tramas, ni paquetes, simplemente transfiere bits.

Una vez codificados los datos, deben ser señalizados. Esta tarea consiste en representar los bits “0” y “1” en el medio físico, aplicando para ello diferentes estándares como NRZ o Manchester (p. 16). De tal manera se tiene la Figura N°9 se observa un esquema referencial de una transmisión a través del medio físico.

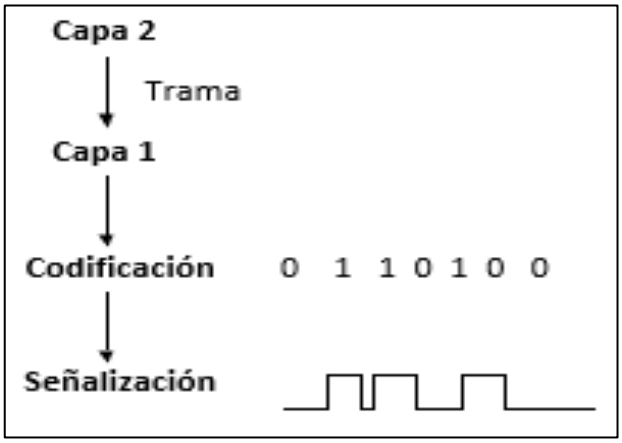


Figura N° 9: Transmisión a través del medio físico
Fuente: Perez, D. (2018)

Dependiendo del medio físico disponible la transferencia podrá llevarse a cabo a diferentes velocidades. Esta puede ser medida con relación a tres conceptos:

El ancho de banda se refiere a la capacidad total que posee un medio para transportar datos.

El rendimiento es la velocidad real de transferencia. Generalmente no coincide con el ancho de banda debido a diferentes factores entre los que se encuentran el volumen, el tipo de tráfico que atraviesa la red o la cantidad de dispositivos conectados a ella.

La capacidad de transferencia útil puede ser entendida como la medida y velocidad de transferencia de los datos generados en la capa de aplicación (eliminando la sobrecarga del tráfico generado por las encapsulaciones, acuses de recibo, establecimiento de sesiones, etc.) durante un periodo de tiempo determinado (pp. 16-17).

La función principal de Ethernet consiste en transformar los datos para que de esta manera poder adaptarlos al medio físico, es por ello que se asocia directamente con el estándar 802.3 (pp. 19-20).

Bajo esta premisa podemos citar (Stallings, 2004).

Todo el sistema de comunicación es lo suficientemente complejo como para ser diseñado y utilizado sin más, es decir, se necesitan funcionalidades de gestión de red para configurar el sistema, monitorizar su estado, reaccionar ante fallos y sobrecargas y planificar con acierto los crecimientos futuros (p. 13).

En esta investigación hemos utilizado el siguiente dimensionamiento para la variable dependiente LAN:

Dimensión 1: Visibilidad y análisis del ancho de banda

Esta dimensión se basa en la visibilidad y análisis del ancho de banda, por lo cual citaremos a (Lewis, 2009).

"El proceso de medir el uso del ancho de banda en una red y el análisis de los datos son los objetivos de ajustar el rendimiento, planificar la capacidad y tomar las decisiones necesarias para la mejora del hardware" (p. 18). Todo este proceso se realiza utilizando un software idóneo de acuerdo a la red y a lo que se quiera medir.

Así podemos también definir que si las demandas de cada segmento de red en la LAN se incrementase y el ancho de banda interno se viese afectado, la carga de red total aumentara y por consecuencia el tiempo de respuesta de toda la red entrara en un deterioro ya que al no tener un análisis real de la red, el incrementar dispositivos y

oficinas trae estos problemas y el no saber por dónde comenzar a encontrar la solución presenta un nuevo problema en tiempos de solución a los incidentes. El poder contar con un software que permita obtener reportes y visualización del tráfico en tiempo real ayuda a determinar si la red está bien configurada, si los segmentos asignados son los correctos, si los dispositivos ya sean switches, controladores o repetidores tienen configurados la velocidad correcta o si el cableado es el idóneo para los servicios que se tienen implementado pudiendo observar broadcast, latencias, perdidas de paquetes, etc. Con una visualización del tráfico de red se puede determinar si hay equipos que están ocasionado estos inconvenientes como por ejemplo las cámaras de videovigilancia o las impresoras, las cuales puede repercutir en el rendimiento de la LAN.

Como complemento (Lewis, 2009), manifiesta lo siguiente:

> Todos los datos de la red contribuyen al tráfico, independientemente de su propósito u origen. El análisis de las distintas fuentes de tráfico y su impacto en la red permiten un ajuste más fino de la misma y actualizarla para conseguir el mejor rendimiento posible. El flujo de datos puede emplearse para determinar hasta cuando puede seguir usándose el hardware de red existente antes de que tenga sentido actualizarlo para acomodarlo a los requisitos de ancho de banda (p. 18).

Dimensión 2: Administración de incidencias

En su forma resumida podemos indicar que es detectar, aislar, notificar, y corregir los incidentes que se presenten en la red. Como mejores prácticas (Cisco, 2018) menciona lo siguiente:

El objetivo de la administración de fallas es detectar, registrar, notifica a los usuarios de, y (en la medida de lo posible) fije automáticamente los problemas de red para guardar la red el ejecutarse con eficacia. Porque los incidentes pueden causar el tiempo muerto o la degradación de red inaceptable (párr. 9).

Dado que hoy en día la gestión de incidencias ha alcanzo un punto importante en todo centro de datos a consecuencia del crecimiento de las redes, la tecnología y las comunicaciones citamos a (Gómez Beas, 2016) el cual manifiesta lo siguiente:

Si se realiza una mala gestión, hay un aumento de tiempo y costes, algo importante para toda empresa. Pero algo que no hay que dejar de lado es la imagen que se da en una mala resolución de cualquier evento. La mala imagen de cualquier empresa puede llegar a ser lapidaria.

Para ello se utiliza la gestión de incidencias, en la que se trabaja con una metodología o un manual de buenas prácticas en concreto. Todos los pasos que se describen en la metodología son importantes. Por ello hay que tener en cuenta que ningún paso se debe saltar ni dedicarle menos atención, porque puede ocurrir que todo el método falle. Tienen que estar todas las actividades descritas:

Identificación.

Registro.

Clasificación.

Priorización.

Diagnóstico inicial.

Escalado.

Investigación y diagnóstico.

Resolución y recuperación.

Cierre.

Para ello, se llevará una base de datos en la que todos estos elementos queden registrados (p. 58).

Dimensión 3: Análisis del rendimiento

En análisis del rendimiento podemos citar a (Calvo, 2016) quien explica lo siguiente:

> El gran crecimiento de las redes IP y el aumento de la velocidad en las conexiones ha hecho que surjan nuevos servicios y aplicaciones que requieren de grandes prestaciones. Para garantizar los requerimientos de esas nuevas tecnologías se desarrollan herramientas de monitorización que aportan la información necesaria sobre la utilización de los recursos de la red. Es necesario conocer cómo responde la red a los requerimientos que se le exige. Hasta ahora se ha visto cómo se podía recoger esa información, una vez recogida se puede pasar a analizarla (p. 227).

Toda empresa mediana o grande se basa hoy en día en niveles de servicio o acuerdo de niveles de servicio (SLA), los cuales pueden ir de la mano con el rendimiento de los equipos como los router, switches, servidores, etc., que tengan que ver en el funcionamiento de la LAN, así tenemos a (Cisco, 2018) que manifiesta lo siguiente:

> En el nivel del dispositivo, las mediciones de rendimiento pueden incluir la utilización de CPU, la asignación de memoria intermedia y la asignación de memoria. El funcionamiento de ciertos protocolos de red se relaciona directamente con la disponibilidad del búfer en los dispositivos de red. Las estadísticas de

> medición del funcionamiento del dispositivo-nivel son críticas en la optimización del funcionamiento de los protocolos de mayor nivel (p. 14).

En base a este análisis respecto al hardware de los equipos es muy importante las operaciones de mantenimiento en este caso ser muy proactivos en la revisión de la salud de los equipos y tener un esquema de trabajo en base al rendimiento y funcionamiento de estos. En la parte lógica el rendimiento en la red es muy importante, contar con herramientas con el cual se pueda monitorizar el tráfico y mantener la LAN aceptable en cuanto a tiempos de respuestas y poder prever cualquier evento que pueda afectar el rendimiento de la red, el tener una visualización e información conlleva a poder contar con una red bien gestionada.

2.4 Definición de términos básicos

A continuación, se presentan las definiciones principales:

Análisis de red: Existen distintas categorías de análisis de red que representan los diferentes enfoques históricos en cuanto al registro y la lectura de datos de las operaciones, que se presentan mediante registros, informes o gráficos por medio de utilidades informáticas. Estos informes proporcionan a los administradores imágenes con periodicidad horaria, diaria, mensual y anual de los eventos que se producen en una red determinada, o pueden basarse en la actividad de los usuarios y los dispositivos. (VMware, 2020, párr. 2).

Ancho de Banda: El concepto de ancho de banda se popularizó en las últimas décadas a partir de la masificación del uso de Internet. En la Informática, se conoce como ancho de banda a la cantidad de datos que pueden enviarse y recibirse en el marco de una comunicación. Dicho ancho de banda suele expresarse en bits por segundo o en múltiplos de esta unidad (Porto & Merino, 2017, párr. 1).

Averías: El concepto de avería puede utilizarse de múltiples maneras, en el lenguaje coloquial, se conoce como avería a un fallo, un inconveniente o un daño que afecta el uso normal de algo (Porto & Gardey, 2016, párr. 1).

BGP (*Borde Gateway Protocol*): Es un protocolo de enrutamiento moderno diseñado para ser escalable y poder utilizarse en grandes redes creando rutas estables entre las organizaciones (Ariganello & Barrientos, p. 193).

CEF (*Cisco Express Forwarding*): Es una característica avanzada de Cisco IOS que permite un modo de conmutación de capa 3 más rápido y eficiente en los routers y switchs multicapa Cisco (Ariganello & Barrientos, p. 45).

Ciberdelitos: Se refiere a cualquier actividad ilegal llevada a cabo mediante el uso de tecnología. Los responsables pueden ser personas aisladas, grupos organizados o facciones con patrocinio estatal, y utilizan técnicas como el phishing, la ingeniería social y el malware de todo tipo para cumplir sus siniestros planes (Nica, 2020, párr. 1).

CSMA/CA: Acceso múltiple con detección de portador y prevención de colisiones. Resulta bastante similar al CSMA/CD en cuanto al modo de operar, pero agrega una pequeña característica, que cosiste en el envío de una notificación antes de transmitir datos, es decir, primero se examina el medio en busca de alguna señal, y si está libre, envía una notificación informando al resto de dispositivos su intención de utilizarlo (Perez, p. 15).

CSMA/CD: Acceso múltiple con detección de portadora y detección de colisiones. En la práctica, esto significa que varios puestos pueden tener acceso al medio y que, para que un puesto acceder a dicho medio, deberá detectar la portadora para asegurarse de que ningún otro puesto esté utilizándolo (Ariganello, p. 51).

Emulación de red: A diferencia de los simuladores de red que brindan limitadas funcionalidades, según la implementación realizada por cada programador, un emulador permite cargar la imagen de uno o más sistemas operativos en una PC o servidor, lo cual brinda la posibilidad de implementar casi todas las funcionalidades de un equipo real en un entorno de laboratorio (Ocampo Zuñiga, párr. 1).

Estado Óptimo: Generalmente, la palabra se emplea a instancias de alguna actividad que se desarrolló o de una tarea terminada y cuyos resultados fueron muy beneficiosos para quienes la llevaron a cabo. Por tanto, el término óptimo es una palabra que la solemos

encontrar en diferentes ámbitos y claro, siempre asociada como decíamos a una actividad, a una acción que se realiza (Ucha, 2010, párr. 2).
Basados en esto, para esta investigación, vamos a definir como estado óptimo a un estado ideal o el esperado en las mejores circunstancias.

Gestión de red: Un sistema de gestión de red es un conjunto de herramientas para monitorizar y controlar la red. Existe una única interfaz de operador con un potente, pero sencillo para el usuario conjunto de órdenes para llevar a cabo la mayoría de las tareas de gestión de red. Se requiere una cantidad mínima de equipo adicional, la mayor parte de software y hardware requerido para la gestión de red se incorpora en el equipo de usuario existente (Stallings, 2004, p. 795).

HTTP (*Hypertext Transfer Protocol*): Soporta el intercambio de páginas web que constan de texto, imágenes gráficas, sonido, video y otros archivos multimedia en la web (Vachon, p. 645).

HTTPS (*Hypertext Transfer Protocol Secure):* El protocolo de transferencia es el lenguaje en el que el cliente web (generalmente el navegador) y el servidor web se comunican entre sí. HTTPS es una versión del protocolo de transferencia que utiliza u cifrado seguro para la comunicación (IONOS, párr. 3).

ICMP: Protocolo de mensajes de control de Internet, suministra capacidades de control y envió de mensajes. Herramientas tales como PING y tracert utilizan ICMP para poder funcionar, enviando un paquete a la dirección destino específica y esperando una respuesta (Ariganello & Barrientos, 2016, p. 43).

IGP (*Interior Gateway Protocol*): Se usan para intercambiar información de enrutamiento dentro de un sistema autónomo (Ariganello, p. 167).

ISP (*Internet Service Provider*): Es el termino con el que se identifica a las compañías que proporcionan acceso a Internet, tanto a los hogares como a las empresas. Además del acceso a Internet, los ISP ofrecen una variedad de servicios a sus clientes como líneas telefónicas o televisión por cable (Garcia Calvache, párr. 1-19).

Latencia: La latencia es el tiempo requerido para que un paquete viaje desde su origen hasta el destino. Algunas aplicaciones tales como Voz sobre IP (VoIP), son sensibles a la latencia, lo que significa que no funcionarán satisfactoriamente si la latencia es demasiado alta. La latencia es un factor en el cálculo del producto ancho de banda-retardo (Ariganello & Barrientos, 2016, p. 44).

LLC (*Logical Link Control*): Su misión consiste en identificar el protocolo aplicado en capa 3 y convertir el paquete en trama (Perez, p. 15).

MAC (*Media Access Control*): Agrega las direcciones físicas del origen y destino de la comunicación (direcciones MAC), controla el acceso al medio mediante diferentes técnicas y dispone funciones de control de flujo y detección de errores (Perez, p. 15).

Máquinas Virtuales: Es aquella que emula a un ordenador completo, es un software que puede hacerse pasar por otro dispositivo como una PC, de tal modo que puedes ejecutar otro sistema operativo en su interior (Ramirez I. , párr. 5).

MIB: Esta organizada de una forma jerárquica, creando una estructura de árbol. De hecho, toda la MIB es realmente una colección de variables que se almacenan de forma granular en otras MIB individuales, que forman las ramas del árbol (Ariganello & Barrientos, p.353).

Monitoreo: Dentro del ámbito de la administración de redes, se conoce con el nombre de monitoreo de red a un sistema que realiza un control constante de una red de ordenadores, intentando detectar defectos y anomalías; en caso de encontrar algún desperfecto, envía un informe a los administradores (Porto & Gardey, párr. 7).

MPLS (*MultiProtocol Label Switching*): Los servicios VPN de MPLS siguen un modelo familiar de WAN privado, con un cliente conectando los sitios a una nube MPLS, y la nube enviando datos a todos los sitios de ese cliente conectados a la nube. Para mantener los datos privados, como es habitual, para dos clientes A y B no relacionados, MPLS se compromete a no reenviar los datos de A hacia los enrutadores de B y viceversa. Básicamente, para el cliente, la red MPLS actúa como una red IP, enrutando los paquetes IP de los clientes entre sitios (Odom, 2017, p. 459).

NAT (*Network Address Traslation*): Permite acceder a Internet traduciendo las direcciones privadas en direcciones IP registradas. Incrementan la seguridad y la privacidad de la red local al traducir el direccionamiento interno a uno externo (Ariganello & Barrientos, p.367).

OSPF (*Open Shortest Path First*): Es un protocolo de enrutamiento estándar definido en la RFC 2328. Utiliza el algoritmo SPF (*Shortest Path First*) para encontrar las mejores rutas hacia los diferentes destinos y es capaz de converger muy rápidamente (Ariganello & Barrientos, p. 137).

PING: Es considerada la herramienta por excelencia necesaria para realizar testeos de conectividad de extremo a extremo en capa 3. Su modo de operar se basa en el protocolo ICMP, donde el emisor envía un paquete "IP ICMP echo request" al destino, y este, al recibirlo, responde con un "IP ICMP echo replay". Si la comunicación concluye con éxito significa que existe conectividad entre ambos (Ariganello & Barrientos, p. 267).

POP (*Point of Presence*): El punto de presencia consiste en un lugar físico donde un proveedor de servicios tiene equipamiento, la función del POP recibir las señales digitales o análogas, convertirlas y enrutarlas hacia Internet. (Perez, p. 425).

PostgreSQL: Es un potente sistema de base de datos relacional de objetos de código abierto que utiliza y amplia el lenguaje SQL combinado con muchas características que almacenan y escalan de forma segura las cargas de trabajo de datos más complicadas. (Grupo de desarrollo global de PostgreSQL, párr. 1).

Protocolos: "Los protocolos son mecanismos por los cuales la información de enrutamiento se intercambia entre enrutadores para que se puedan tomar decisiones de enrutamiento" (Medhi & Ramasamy, 2017, p. 65).

RIPv2 (*Routing Information Protocol versión 2*): Es un protocolo sin clase que admite CIDR, VLSM, resumen de rutas y seguridad mediante texto simple y autenticación MD5 (Ariganello & Barrientos, p. 92).

SNMP Agent: Es un proceso que se ejecuta en el dispositivo de red que se está monitorizando. Diferentes tipos de datos son recogidos por el propio dispositivo y son almacenados en una base de datos local (Ariganello & Barrientos, p. 353).

Software libre: Es un programa informático donde el usuario propietario del programa tiene la libertad de copiarlo, modificarlo, redistribuirlo y distribuirlo para el beneficio de una comunidad (Significados.com, 2017, párr. 1).

Syslog: Es un protocolo encargado de recopilar y almacenar de manera centralizada los logs generados por los distintos dispositivos ubicados en la red, facilitando gracias a ello su lectura y análisis (Perez, 2018, p. 536).

TCP: Protocolo de control de transmisión, es básicamente el más utilizado, tiene control de flujo, reensamblado de paquetes y acuse de recibo. Es un protocolo orientado a conexión muy seguro que utiliza un saludo de tres vías antes del envió de los datos (Ariganello, p. 42).

Telemetría: Se conoce como telemetría al sistema que permite la monitorización, mediación y/o rastreamiento de magnitudes físicas o químicas a través de datos que son transferidos a una central de control. Etimológicamente, la palabra telemetría es de origen griego “tele" que significa “distancia” y “metría” que expresa “medida” (Significados.com, Telemetría, 2015, párr. 1-6).

Topología de red: En el contexto de una red de comunicaciones, el termino topología se refiere a la forma según la cual se interconectan entre si los puntos finales, o estaciones, conectados a la red (Stallings, p. 484).

Traps: Consiste en alertar al mánager cuando ocurre alguna incidencia y sin necesidad de que este lo haya solicitado previamente. Entes proceso se lleva a cabo mediante mensajes SNMP Traps, que son aquellos generados y enviados automáticamente por el protocolo cuando algún elemento presenta errores (Perez, 2018, p. 540).

UDP: Protocolo de datagrama de usuario, es un protocolo poco fiable, no orientado a la conexión donde solo se establece un saludo de dos vías antes de enviar los datos, carece

de la numeración de secuencia tamaño de ventana y es mucho más pequeña que un encabezado TCP (Ariganello & Barrientos, p. 42).

WAN: Es aquella que abarca una distancia geográfica tan amplia que resulta prácticamente ilimitada, siendo capaz de interconectar dispositivos ubicados en cualquier parte del mundo. Ello es posible gracias a la implementación de medios físicos y protocolos específicos en capa 1 y 2 (Perez, 2018, p. 421).

Watering Hole: Hace referencia a una táctica empleada durante la realización de campañas de ataques dirigidos donde la distribución del APT se realiza a través de una web de confianza que suele ser visitada por los empleados de la empresa o entidad objetivo (Fernandez, 2016, párr. 1).

2.5 Variables

Las variables que intervienen en la presente investigación las mencionamos a continuación.

Variable Independiente: Se implementará el monitoreo y análisis de red mediante los siguientes protocolos.
-Protocolo SNMP
-Protocolo NETFLOW

Variable Dependiente: Se mejorará la gestión y monitoreo de eventos que serán aplicados a la red de la empresa DETCOM.
-LAN

Las dimensiones de cada variable son presentadas en la siguiente Tabla:

Tabla 2: Cuadro de Dimensiones de cada variable

APLICACIÓN DE PROTOCOLOS SNMP Y NETFLOW PARA OPERAR UNA LAN DE 4 SEDES DE LA EMPRESA DETCOM - LIMA 2020		
Variable Independiente	Dimensión	Indicador
SNMP	Monitoreo de salud de equipos	Alarmas en tiempo real frente anomalías que puedan afectar la salud del equipo.
	Gestión de red	Evaluación semanal de cumplimiento de KPI.
NETFLOW	Monitoreo del flujo de red	Alarmas en tiempo real frente anomalías que puedan el flujo de red.
	Análisis de flujo de red	Evaluación semanal de protocolos más utilizados en la LAN.
Variable Dependiente	Dimensión	Indicador
LAN	Visibilidad y análisis del ancho de banda.	Evaluación de los reportes de consumo de ancho de banda
	Administración de incidencias.	Evaluación de disponibilidad de los equipos en red
	Análisis del rendimiento.	Evaluación y análisis de los recursos de red.

Fuente: Elaboración propia

CAPÍTULO III: METODOLOGÍA DEL ESTUDIO

3.1 Tipo de investigación

Los tipos de investigación se pueden definir en base a su propósito, en este sentido tenemos la básica y por otro lado la aplicada, si bien es cierto cada una tiene objetivos diferentes en nuestro caso se elegirá la investigación aplicada dado que este tipo de investigación se caracteriza porque busca la aplicación o utilización de los conocimientos que se adquieren. Es el estudio y aplicación de la investigación a problema concretos, en circunstancias y características concretas. (Behar, 2008, p. 20).

3.2 Método de investigación

En cuanto a los métodos de investigación (Sampieri, 2014), los conceptualiza de la siguiente forma:

> Explorativos: Investigan problemas poco estudiados, indagan desde una perspectiva innovadora, ayudan a identificar conceptos promisorios y preparan el terreno para nuevos estudios (p. 122).
>
> Descriptivos: Consideran al fenómeno estudiado y sus componentes, miden conceptos y definen variables (p. 122).
>
> Correlacionales: Asocian conceptos o variables, permiten predicciones y cuantifican relaciones entre conceptos o variables (p. 122).
>
> Explicativos: Determinan las causas de los fenómenos, generan un sentido de entendimiento y son sumamente estructurados (p. 122).

Por lo tanto, la presente investigación se trabaja con el método de investigación explicativa.

CAPÍTULO IV: DISEÑO DE INGENIERÍA

4.1 Diseño

4.1.1 Presentación del escenario de trabajo

a) Descripción de la empresa DETCOM

La empresa DETCOM opera en el Perú por medio de su casa matriz ubicada en Lima en el distrito de Ate y cuenta con tres sucursales instaladas en los distritos de Ate, La Victoria y Carabayllo. La empresa ya tiene 14 años en el rubro automotriz e industrial, muy aparte de ser un habitual proveedor de empresas fabricantes de reguladores de gas (aplicables en cocinas, estufas, etc.), industria farmacéutica, autopartes, hidráulicas y neumáticas, entre otras.

Ante el crecimiento en sus operaciones debido a la demanda de sus productos, la empresa abrió sucursales estratégicamente ubicadas en la ciudad de Lima, y con ello también aumento el tema de equipos a gestionar para mantener las sucursales en producción y con un grado de operatividad aceptable que conlleva al continuo crecimiento de la empresa.

b) Topología de red

La topología de red de la empresa DETCOM está conformada por una oficina principal y tres sucursales, cada una de ellas cuenta con una salida a Internet que va de entre 10Mb a 5 Mb, este servicio se otorga a través de los router ubicados en cada oficina que a través de una de sus interfaces otorga la salida a Internet y utiliza otra interface que da la facilidad de la red MPLS para la comunicación con las demás oficinas.

En el siguiente diagrama (véase Figura N° 10) observamos la red topológica de la empresa.

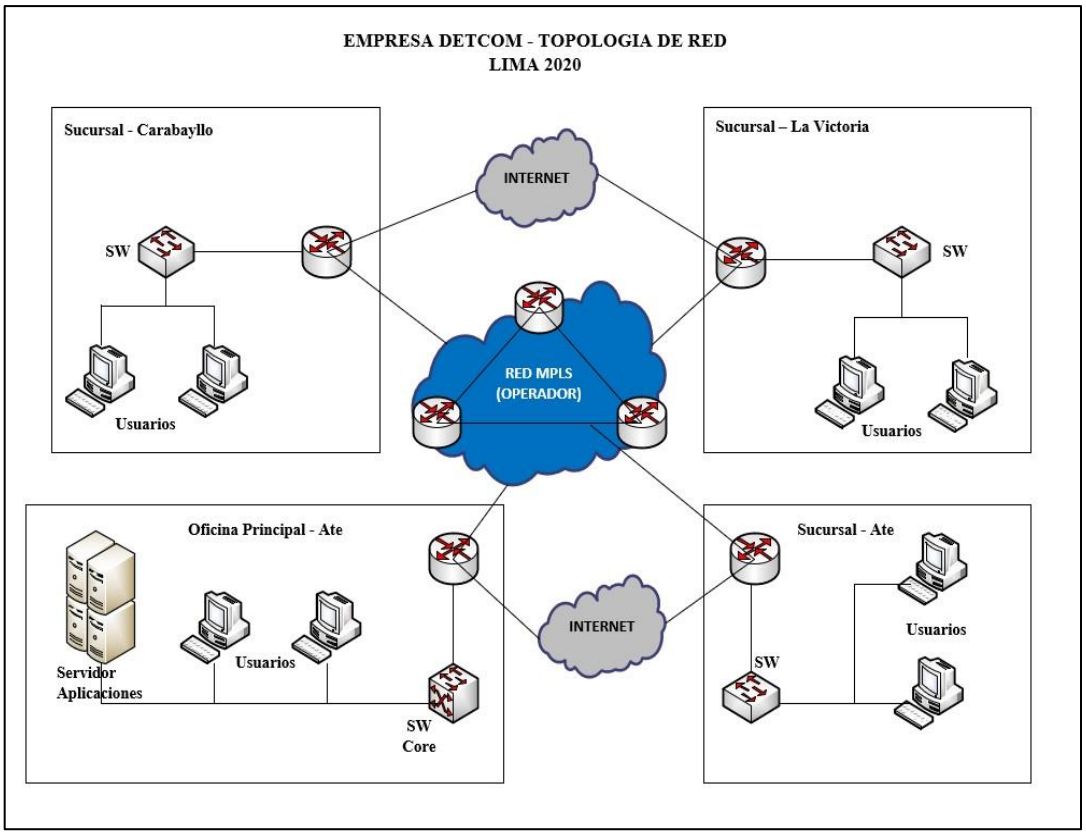


Figura N° 10: Red topológica de la empresa DETCOM
Fuente: Elaboración propia

La red está conformada por los siguientes equipos:

Router de Enlace e Internet

Cada sede cuenta con un router Cisco modelo 1921/K9, el cual se enlaza a la red MPLS y a su vez, a través de otra interfaz, da salida a Internet mediante su proveedor de servicio. En el siguiente detalle se observa el tipo de servicio (véase Tabla 3).

Tabla 3: Tabla de servicio

SEDE \ SERVICIO	MPLS- VPN(Mb)	INTERNET(Mb)
Oficina Principal – Ate	15	10
Sucursal – Carabayllo	5	5
Sucursal - La Victoria	5	5
Sucursal - Ate	5	5

Fuente: Elaboración propia

Switch Core

La sede principal y las sucursales poseen un switch Cisco de capa 3, en la cual encontramos las configuraciones de su red LAN.

Servidor de Aplicaciones

La empresa DETCOM, cuenta con servidor de correos, de archivos, de aplicación contable, de ventas y otros. A esto se adiciono un servidor de gestión y monitoreo en el cual se instaló la herramienta que cumplió la función recopilar los datos para su respectivo análisis.

Red Interna

La empresa DETCOM cuenta con 45 usuarios en total, los cuales se distribuyen entre computadoras, laptop, impresoras multifuncionales y cámaras de seguridad.

4.1.2 Opciones de herramientas de monitoreo y gestión

En este subcapítulo se analizó tres soluciones de herramientas de monitoreo y gestión, para saber cuál sería la herramienta más factible de utilizar en base a los problemas que aquejan al área de TI – DETCOM. Teniendo como resultado las siguiente:

a) Solarwinds:

Encontramos que es uno de los sistemas de monitoreo más asequible y sólido de redes que por el cual se puede detectar, analizar y resolver fallas de una manera rápida. Este sistema cuenta con las siguientes características:

-Monitoreo de fallas, desempeño y disponibilidad en la red.
-Análisis salto por salto en rutas críticas.
-Alertas inteligentes y personalizadas.
-Asignación y detección de redes inalámbricas y cableadas dinámicas.
-Previsión, alertas e informes de capacidad automatizados.
-Monitoreo exhaustivo de la familia de productos F5 BIG-IP.
-Administración y monitoreo de redes.
-Implementación de monitores.
-Generación de tableros, vistas y cuadros personalizables.
-Monitoreo del estado del hardware.

-Informes personalizables de desempeño y disponibilidad.
-Cuadros de desempeño de la red.

b) ManageEngine:

Con el ManageEngine se observó que presenta productos para la gestión y monitoreo de redes de una manera fácil y asequible de usar. En caso de fallas se puede detectar de manera rápida, ya que se tiene una visibilidad y control de toda la red permitiendo tener una alta disponibilidad. Este sistema de monitoreo cuenta con las siguientes características:

-Monitoreo de los dispositivos de red.
-Monitoreo de servidores virtuales.
-Monitoreo de hardware.
-Alertas y notificaciones.
-Automatización de workflows.
-Dashboards personalizados y específicos por usuario.
-Vistas de negocio.
-Mapeo de redes
-Monitoreo de WAN RTT
-Gestión de configuración
-Análisis de tráfico de red.
-Monitoreo y Análisis de netflow y paquetes Flow.
-Monitoreo de IP SLA.
-Monitoreo de jitter.

c) PRTG Network Monitor:

Este sistema de monitoreo permite supervisar todos los sistemas, dispositivos, tráfico y aplicaciones de la red TI. A continuación, se brinda las características del sistema:

-Alertas flexibles
-Interfaces de usuario
-Mapas y dashboards.
-Monitorización distribuida.
-Informes detallados.
-Detección de paquetes.
-Supervisión de jflow, sflow y netflow.

-Supervisión de IPSLA.

-Supervisión de jitter.

-Optimización y monitoreo de red.

Observamos que cada sistema tiene funcionalidades equivalentes, es por eso por lo que se elaboró la siguiente tabla de comparación (véase la Tabla 4), el cual nos permitió elegir la opción más correcta en base a nuestras necesidades y problemáticas encontradas en la red.

Tabla 4: Cuadro de comparación – Solarwind vs ManageEngine vs PRTG

		Solarwind	ManageEngine	PRTG Network Monitor
Características	Parámetros	Factibilidad	Factibilidad	Factibilidad
		61	77	74
Descripción general	Monitoreo de red y servidor	SI	SI	SI
	Análisis de ancho de banda	SI	SI	SI
	Log firewall mgmt	NO	SI	NO
	Configuración mgmt por NCM	NO	SI	NO
	Automatización workflow	NO	SI	NO
	SNMP (trap processing, windows evento log monitoring, syslog monitoring, network performance reporting)	NO	SI	SI
	Integración de dashboard	SI	SI	SI
	Reporte de tráfico en tiempo real	SI	SI	SI

NMS				
Inventario	Tipo	SI	SI	SI
	OS	SI	SI	SI
	CPU	SI	SI	SI
	RAM	NO	SI	SI
	Estado de interface	NO	SI	SI
	Energía	NO	SI	SI
	Fan	SI	SI	SI
	Temperatura	NO	SI	SI
Interface	Ancho de banda	SI	SI	SI
	RX-TX power	SI	SI	SI
	Packet (Unicast / Multicast / Broadcast / Non-Unicast Reate)	SI	SI	SI
Routing	Tabla ARP	SI	SI	SI
	Tabla forwarding	SI	SI	SI
	Tabla routing	SI	SI	SI
IP SLA	Tiempo de respuesta	NO	SI	SI
	Configuración SLA	SI	SI	SI
	Packet loss	SI	SI	SI
	Jitter	SI	SI	SI
Gestión de fallos				
Alertas	Color	SI	SI	SI
	Predicciones estadísticas	SI	SI	SI
	Voz	SI	SI	SI
	Syslog	SI	SI	SI
	Email	SI	SI	SI
	SMS	NO	SI	SI
	Estado	SI	SI	SI
	Threshold	NO	SI	NO

	IPSLA			
Informes	Type Table	SI	SI	SI
	IPSLA	SI	SI	SI
	Tipo de gráfico	SI	SI	SI
	Estadística	SI	SI	SI
	Informe Top N	SI	SI	SI
	Informes programados	SI	SI	SI
	Informe de planificación de capacidad	SI	SI	SI
	Informes filtrados	SI	SI	SI
	Exportación de informe para PDF, Exel, CSV	SI	SI	SI
Gráficos	Easy to view	SI	SI	SI
	95th percentile	**	**	**
	Cambio de color	SI	SI	SI
	Tiempo real	SI	SI	SI
	Tráfico total	SI	SI	SI
Weather Map	Easy to view	SI	SI	SI
	Auto discover	SI	SI	SI
	Custom Color	**	NO	NO
	Graph URL link	**	SI	SI
Overview	Web based	SI	SI	SI
	iPhone app	SI	SI	SI
	Android app	SI	SI	SI
	windows Phone app	NO	SI	SI
Tipo de clientes	Freelancers	NO	NO	NO
	Small Businesses	NO	SI	SI
	Mid-size Business	SI	SI	SI
	Enterprise	SI	SI	SI
Soporte	Por llamada	NO	SI	SI
	Soporte Online	SI	SI	SI
	Base knowledge	SI	SI	SI
	Video tutoriales	SI	SI	SI
Netflow Analyzer				

Display	Good-loSIing	SI	SI	SI
	Type 3D Pie	NO	SI	SI
	Type Chart	SI	SI	SI
	Type Table	SI	SI	SI
Monitor Parameters	Tráfico de origen	SI	SI	SI
	Tráfico de destino	SI	SI	SI
	Aplicación	SI	SI	SI
	AS Number	SI	SI	SI
	País o lugar	SI	SI	SI
Informes	Top N	SI	SI	SI
	Formato csv, excel, xml, html	SI	SI	SI
	Formato pdf	SI	SI	SI
	Programados por horario	SI	SI	SI
	Type Table	SI	SI	SI
	Type Chart	SI	SI	SI
	NCM - Network Configuration Manager			
Parámetros	Acceso de control y administración por NCM	SI	SI	SI
	Programación de horarios para aplicar cambios.	NO	SI	SI

Fuente: Elaboración propia

4.1.3 Selección de la herramienta de monitoreo y gestión

Basados en el punto 4.1.2 – tabla de comparación; obtuvimos a ManageEngine como mejor opción de software para aplicar en la red, el cual nos ofreció productos de gestión y monitoreo de red y servidores, estos productos ayudaron a tener visibilidad de la red lo cual mediante el análisis se pudo optimizar y mejorar el rendimiento. En la investigación realizada se trabajó con dos productos del ManageEngine:

a) OpManager:

Como se vió en el cuadro de comparación este producto nos permitió contar con un monitoreo completo de la red y servidores en su actividad, en su funcionamiento 24x7 y tiempo real. Adicionalmente pudimos realizar un análisis granulado de los datos de router, switches, servidores y equipos de la red por SNMP. Al tener mayor visibilidad de la red pudimos tener un mejor control de esta, este producto nos brindó las siguientes funciones:

Administración de redes:

-Monitoreo de desempeño de Router/Switchs: Por el cual se pudo monitorear la salud de los equipos (CPU, memoria, errores y descartes, aciertos y desaciertos del búfer, otros).

-Monitoreo de disponibilidad de la red, tiempo de respuesta y pérdida de paquetes del dispositivo 24*7.

-Estado de los puertos del equipo, así como los cambios de configuración.

Monitoreo de interfaz:

-Avanzado, identificando los principales usuarios y aplicaciones que hicieron uso del ancho de banda, por medio de paquetes Flow o netflow.

-Políticas QoS para regular el ancho de banda de las aplicaciones críticas para el negocio.

-Monitoreo del tráfico, errores, descartes y uso de Tx/Rx por medio del SNMP

-Activación/ desactivación administrativa de una interfaz.

Monitoreo de ancho de banda:

-Identificación de las principales conversaciones, aplicaciones, protocolos y QoS por ancho de banda.

-Informes detallados de las aplicaciones por tráfico de ENTRADA y SALIDA.

-Principales orígenes y destinos por tráfico de ENTRADA y SALIDA.

-Monitoreo de ancho de banda por aplicación y forma del tráfico.

-Análisis granulado y análisis de seguridad de red.

Administración de direcciones IP

-Análisis de sub-redes IPv4 e IPv6 para identificar ip disponibles.

-Recepción de alertas para saber si cambio el estado de una dirección IP.

Administración de fallas:

-Alarmas y notificaciones, se crean alarmas y eventos para indicar fallas encontradas.

-Se organizan las alarmas por gravedad.

-Notificación de las alarmas por medio de correo electrónico, SMS.

-Alarmas aceptadas/ no aceptadas.

-Comentar en las alarmas para suministrar más información.

Traps y syslogs:

-Recolección de traps y syslogs para detectar fallar en la red.

-Creación de perfiles para filtrar traps y syslogs.

Dashboards y widgets:

-Creación de multiples dashboards personalizados.

-Vista NOC de los dashboard personalizados.

-Rendimiento de toda la red en un vistazo.

-Navegación desde el widget a la página para un análisis detallado.

Vistas de negocio:

-Creación de vistas lógicas en su red y vea su rendimiento.

-Identificación del rendimiento de los dispositivos y los enlaces mediante códigos de color.

-Vistas en la pantalla de NOC para ver el rendimiento de un vistazo.

Informes:

-Generación de informes fácil de usar, teniendo un total de 108 informes de rendimiento predefinidos.

-Programación de informes por email.

-Informes personalizados con información de elección.

-Exportación de informes a XLS y PDF.

b) Netflow Analyzer:

Producto que nos permitió realizar el análisis del tráfico que pasaba por el ancho de banda, teniendo una visibilidad en tiempo real del rendimiento de este. Adicionalmente, se pudo observar de forma granulada y detallada el uso del ancho de banda, alertándonos de forma temprana lo cual nos permitió aplicar una resolución de problemas ante averías por saturación y/o anomalías. Este producto cuenta con las siguientes funcionalidades:

Monitoreo y Análisis en tiempo real

-De aplicaciones y protocolos que viajan por el ancho de banda.

-Reportes en tiempo real de las aplicaciones y protocolos con mayor consumo.

Vista de dashboard:

-Conversación entre la IP de origen y destino de la red.

-Creación de dashboard personalizado de consumo de tráfico.

Análisis de reporte de tráfico:

-Identificación de usuarios, aplicaciones y protocolos que más usan el ancho de banda.

-Generación de reportes personalizados.

Monitoreo forense del tráfico del ancho de banda:

-Monitoreo del ancho de banda por interfaz en tiempo real.

-Obtención en detalle de la saturación del ancho de banda.

Monitoreo de tráfico por aplicación.

-Visibilidad de tráfico en tiempo real.

4.2 Emulación de redes

4.2.1 Escenario de emulación

a) Especificaciones técnicas de hardware y software

Las especificaciones técnicas de hardware y software se basaron en la cantidad de equipos a monitorear, interfaces, syslog, traps, etc.

También tiene que ver la versión implementada, ManageEngine cuenta con tres tipos de versiones de OpManager los cuales detallamos a continuación: OpManager Standard Edition, OpManager Professional Edition y OpManager Enterprise Edition.

De las tres versiones mencionadas, se eligió el OpManager Professional Edition, el cual es ideal para pequeñas y medianas empresas, en el presente cuadro (véase Tabla N° 5) se destacan las principales funcionalidades de esta versión.

Tabla 5: Cuadro de Funcionalidades – OpManager Professional Edition

Professional
Destacados:
- Monitoreo de Servidores
- Monitoreo del estado del hardware de los servidores
- Monitoreo de UPS, impresoras
- Monitoreo de Router
- Monitoreo de Switches
- Gráfico en tiempo real del rendimiento de cualquier monitor a sensar
- Configuración de detección automática de redes
- Configuración de plantillas de dispositivos
- Panel de control personalizable y mapas de red
- Monitoreo de Syslog
- Monitoreo de traps de SNMP
Complementos:
- NCM
- Netflow

Fuente: Elaboración propia

En cuanto al recurso mínimo disponible recomendado por ManageEngine que debe tener el servidor para alojar el software OpManager Professional Edition y tener un buen rendimiento acorde a su funcionalidad son (véase Tabla N°6):

Tabla 6: Recursos de Servidor

Recursos del Servidor	Descripción
Procesador	Intel Xeon Quad Core, 2.5Ghz
Memoria	16 Gb
Disco Duro	40 Gb
Equipos	1000 dispositivos

Fuente:https://download.manageengine.com/networkmonitoring/opmanager_datasheet.pdf

El OpManager Professional Edition soporta ser instalado en un servidor físico o en un entorno virtual, siempre y cuando se dispongan de los recursos necesarios de acuerdo con la cantidad de dispositivos a gestionar y monitorear. En la presente investigación el cliente posee un servidor Power Edge R630 -Dell que cuenta con doble fuente de energía redundante de 750watts AC, el software no altera la capacidad de consumo de energía del servidor, este solamente se basa en los recursos indicados en la Tabla 6.

Los sistemas operativos en las cuales puede residir la herramienta del ManageEngine se muestran en la siguiente Tabla N° 7:

Tabla 7: Sistemas Operativos

Software	Evaluación	Producción
SO Windows	Windows 10/8/7 o Windows Server 2019/2016/2012 R2/2012/2008	Windows Server 2019/2016/2012 R2/2012/2008
SO Linux	Ubuntu/Suse/Red Hat Enterprise Linux (hasta la versión8) /Fedora/Centos/Mandriva (Mandrake Linux)	Red Hat/64-bit Linux flavors
Database	MSSQL 2008, 2012, 2014 y 2016 OpManager bundled PostgreSQL	MSSQL 2008, 2012, 2014, 2016, 20017 OpManager bundled PostgreSQL
Browser	Chrome/Firefox/Edge/IE11	Chrome (de preferencia) /Firefox/Edge/IE11

Fuente: Elaboración propia

Los puertos requeridos tanto para la parte de aplicación, monitoreo y gestión se mencionan en las siguientes imágenes (véase Figuras N°:11 – 13)

Ports used by the application

Port	Protocol	Port Type	Usage	Remarks
13306	TCP	Static (PostgreSQL)	Database Port	Can be changed in **conf/database_params.conf** file.
1433	TCP	Static (MS SQL)	Database Port	Can be changed in **conf/database_params.conf** file/ **dbconfiguration.bat** file.
23	TCP	Static	SSH Port	
8060	TCP	Static	Web Server Port	Can be configured using **ChangeWebServerPort.bat**.
7275	TCP	Static	Remote Desktop Port (RDP)	Can be configured using **gateway.conf** (Under <opmanager_home>\conf folder)

Figura N° 11: Puertos usados por la Aplicación y Base de Datos
Fuentes: https://www.manageengine.com/network-monitoring/help/hardware-and-software-requirements.html

Puertos usados para el monitoreo:

Ports used for monitoring

Port	Protocol	Port Type	Usage	Remarks
161	UDP	Static	SNMP	
135	TCP	Static	WMI	
445	TCP	Static	WMI	
5000 to 6000	TCP	Dynamic	WMI	
49152 to 65535	TCP	Dynamic	WMI	Windows 2008R2 and higher
56328	TCP	Dynamic	ShutDown Listener Port	
162	UDP	Static	SNMP Trap Receiver Port	
514	UDP	Static	SYSLOG Receiver Port	SYSLOG Receiver Port can be changed via WebClient

Figura N° 12: Puertos usados para el Monitoreo
Fuentes: https://www.manageengine.com/network-monitoring/help/hardware-and-software-requirements.html

Puertos complementarios:

Ports used by add-ons

Central Server

Port	Protocol	Port Type	Usage	Remarks
69	UDP	Static	TFTP Port [NCM]	
1514	UDP	Static	Firewall Log Receiver [FWA]	Firewall Receiver Port can be changed via WebClient
9996	TCP		NetFlow Listener Port [NFA]	NetFlow Listener Port can be changed via WebClient

Figura N° 13: Puertos Complementarios
Fuentes: https://www.manageengine.com/network-monitoring/help/hardware-and-software-requirements.html

Para el tema de la base de datos, está ya vino incluida en el software del OpManager, el cual trabaja con el PostgreSQL. En caso se tenga otra base de datos se recomienda el Microsoft SQL el cual soporta las siguientes versiones:

-SQL 2017

-SQL 2016

-SQL 2014

-SQL 2012

-SQL 2008

Los puertos usados para el plugin son los siguientes:

-HTTP – 9090

-HTTPS - 8443

b) Software GNS3

Aplicación del GNS3

GNS3 es un software *free* de código abierto utilizado para emular, configurar y replicar topologías, el cual nos ayudó a encontrar soluciones a problemas presentados en redes físicas.

En el siguiente enlace: https://www.gns3.com, nos sirvió como soporte en actualizaciones y consultas que se presentaron en la emulación, gracias al aporte que

realiza la comunidad y a la actualización constante que tiene el software se pudieron levantarlas las observaciones que se presentaron.

El GNS3 soporta equipos tanto emulados como simulados:

Emulación: Imita o emula el hardware de un dispositivo como un router o un switch mediante imágenes reales que pueden ser instalados en el software y utilizados en la topología que se va a replicar.

Simulación: Simula las características y funcionalidades de un dispositivo como un switch de capa 2, en este caso no se ejecuta un sistema operativo de una imagen de cisco sino uno desarrollado por el propio software GNS3.

Por lo tanto, a través del GNS3 pudimos emular parte de la red de la Empresa DETCOM y se desarrolló las configuraciones pertinentes en la demostración de la operatividad del software de monitoreo y gestión. Adicionalmente, se dio una visualización en el aporte de análisis de datos que se obtuvieron y mostraron en un entorno emulado.

Instalación del GNS3

El software GNS3 se instaló en un sistema operativo Windows 10 de 64bits con 16Gb de memoria RAM, la versión más reciente que se utilizó fue: 2.2.12. Los pasos de instalación que seguimos fueron:

Paso 1: Se ingreso a la siguiente página web: https://www.gns3.com y en la opción de *Sing in* (véase Figura N° 14*)*, se dio doble click con el botón izquierdo del mouse para poder ingresar el usuario y contraseña.

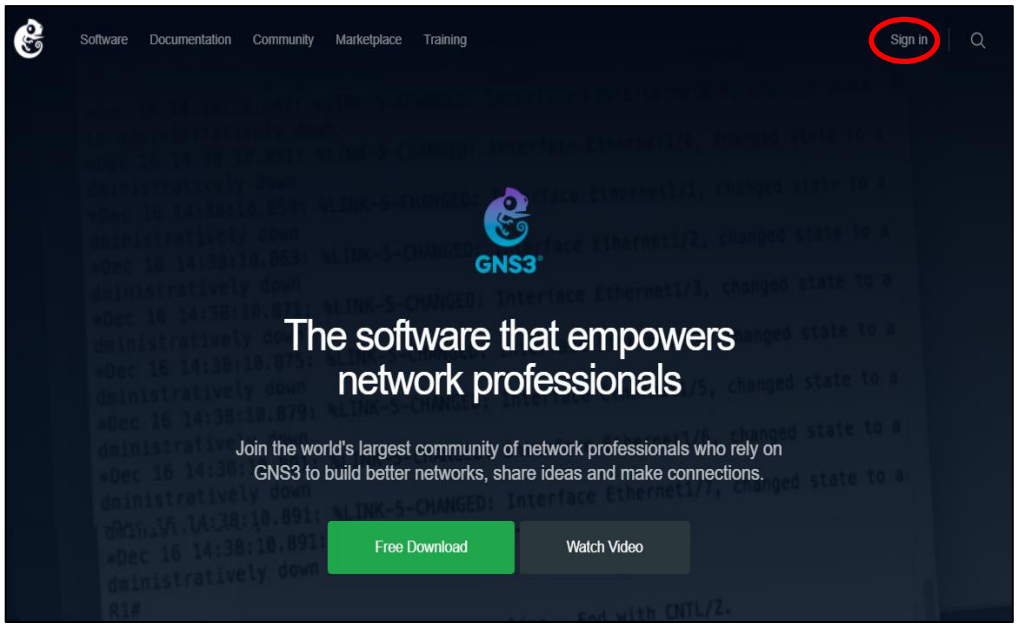


Figura N° 14: Página del GNS3
Fuente: https://www.gns3.com/

Paso 2: ´Se creo una cuenta en el GNS3, en la siguiente Figura N° 15 mostramos los campos para ingresar el usuario y contraseña.

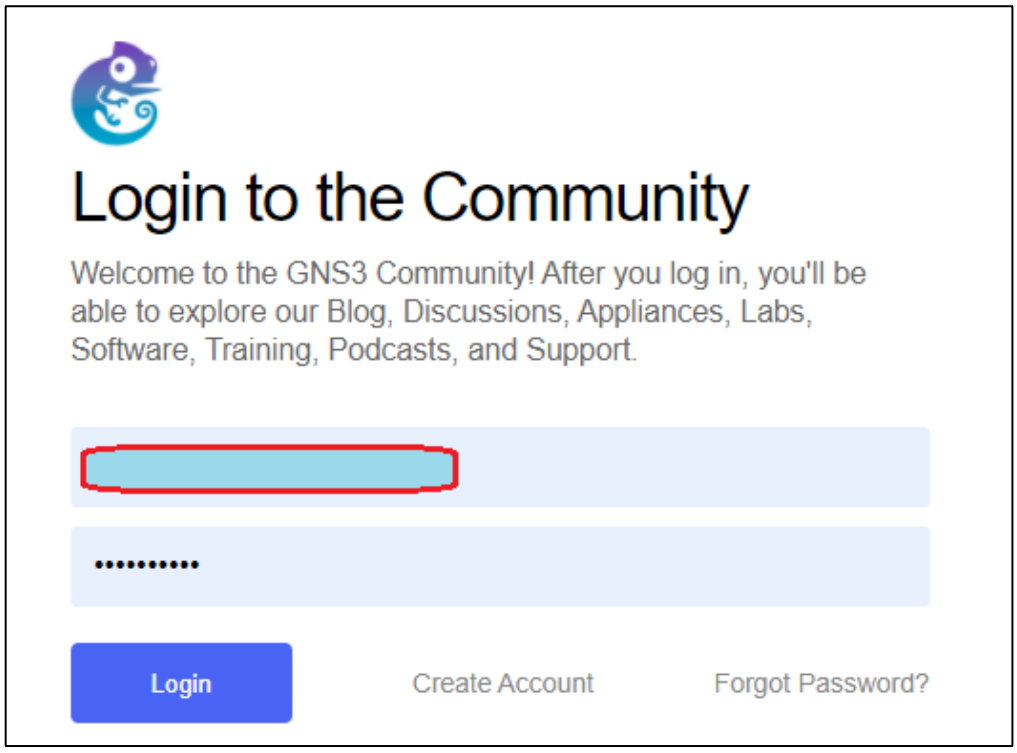


Figura N° 15: Ingresando con una cuenta de GNS3
Fuente: https://www.gns3.com/

Paso 3: Una vez ingresado visualizamos un menú de opciones, para nuestro caso se escogió la opción de Software y a continuación se procedió a dar click con el botón izquierdo del mouse (véase Figura N° 16):

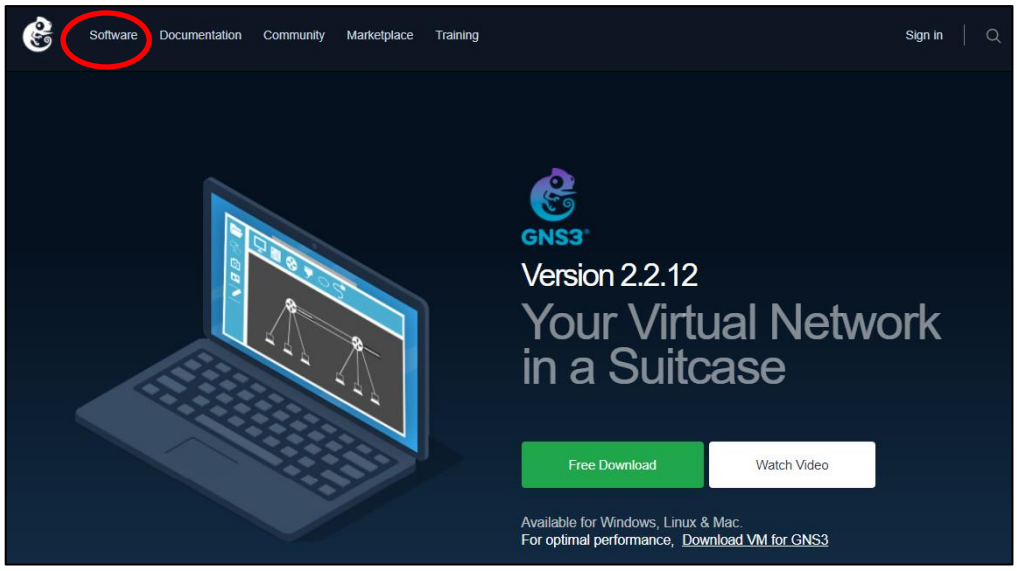


Figura N° 16: Seleccionando la opción de Software
Fuente: https://www.gns3.com/

Paso 4: Seguidamente se seleccionó la opción de *Free Download*, y nos mostró las opciones de descarga según el sistema operativo (véase Figura N° 17).

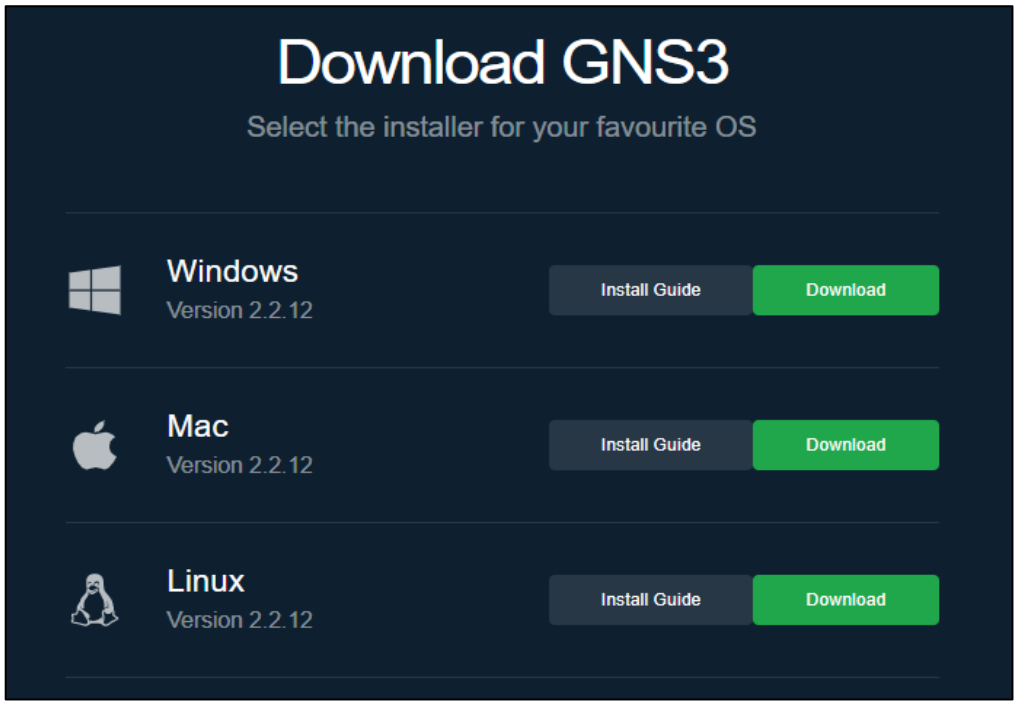


Figura N° 17: Seleccionando la opción de descarga del software
Fuente: https://www.gns3.com/

Paso 5: Se seleccionó la opción para el sistema operativo Windows, se muestra la versión del GNS3 a descargar: versión 2.2.12. Luego seleccionamos la opción de Download para que inicie la descarga de 87 Mb aprox. (véase Figura N° 18).

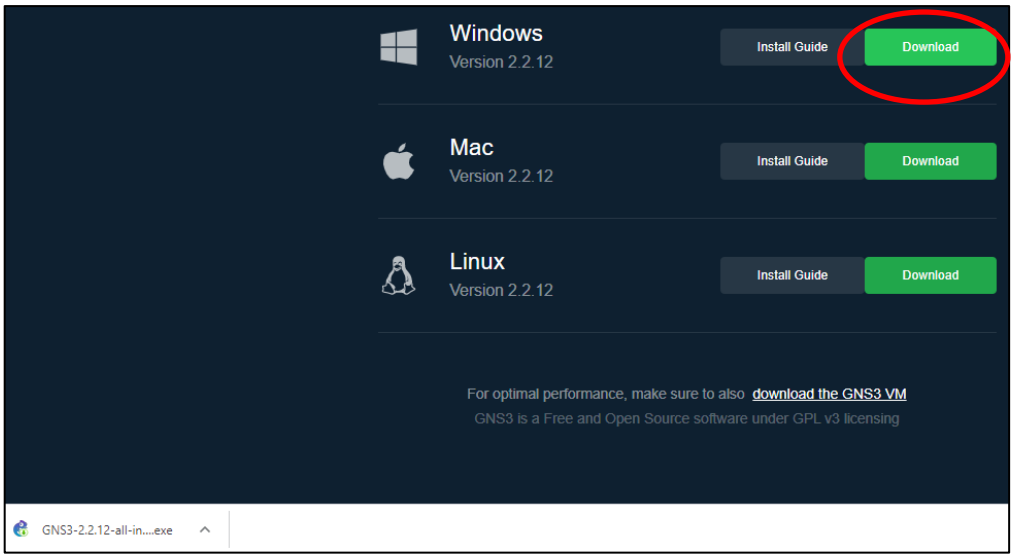


Figura N° 18: Descarga del software GNS3
Fuente: https://www.gns3.com/

Paso 6: Una vez finalizada la descarga de la aplicación, se procedió a la instalación (véase Figura N° 19).

Figura N° 19: Archivo de instalación del GNS3
Fuente: Elaboración propia

Paso 7: En el proceso de instalación, solicito especificar la ubicación de la carpeta de los archivos de arranque de la aplicación. Se procedió a descargar e instalar los complementos de Wireshack, Putty, etc, necesarios para poder simular o emular la topología de red que se configuro. En la siguiente Figura N° 20, se muestra el proceso de instalación.

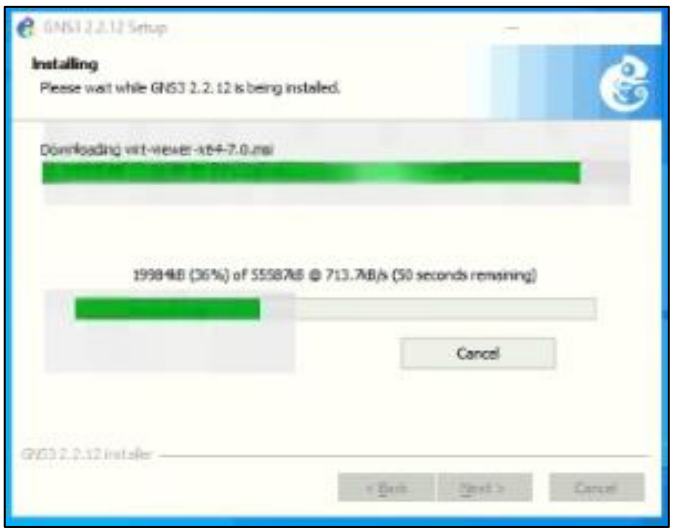


Figura N° 20: Proceso de instalación del GNS3
Fuente: Elaboración propia

Paso 8: Una vez finalizado el proceso de instalación, la aplicación ya está lista para trabajar tal como se observa en la siguiente Figura N° 21.

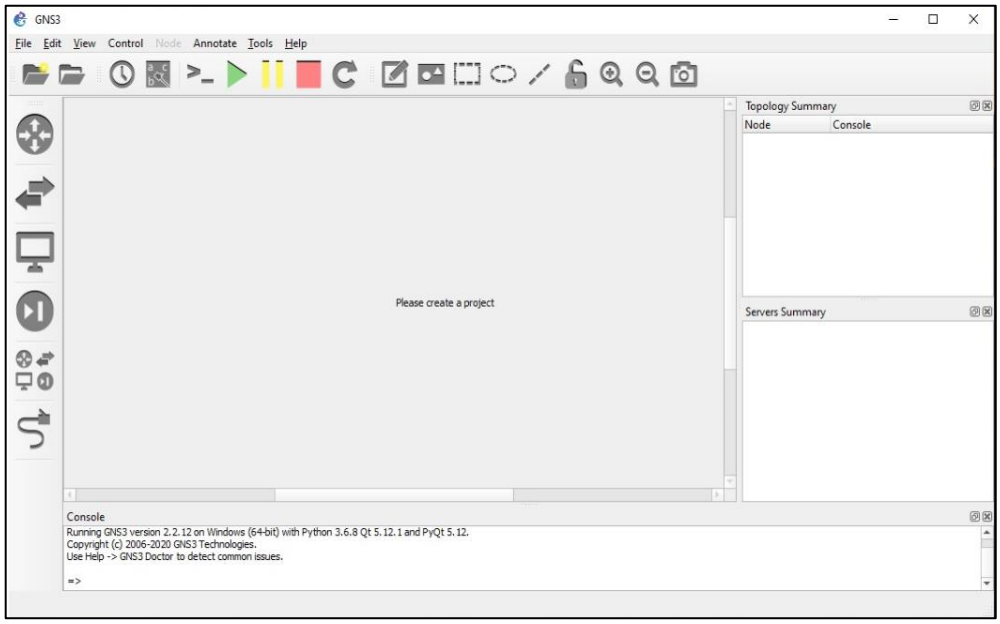


Figura N° 21: Aplicación GNS3
Fuente: Elaboración propia

Paso 9: En esta parte del proceso, ya se puede iniciar a construir y configurar la topología a emular, en las ventanas del lado derecho superior se puede visualizar los elementos que se están utilizando y en la parte inferior el recurso utilizado del CPU y RAM de la computadora donde se está ejecutando la aplicación del GNS3 (véase Figura N° 22):

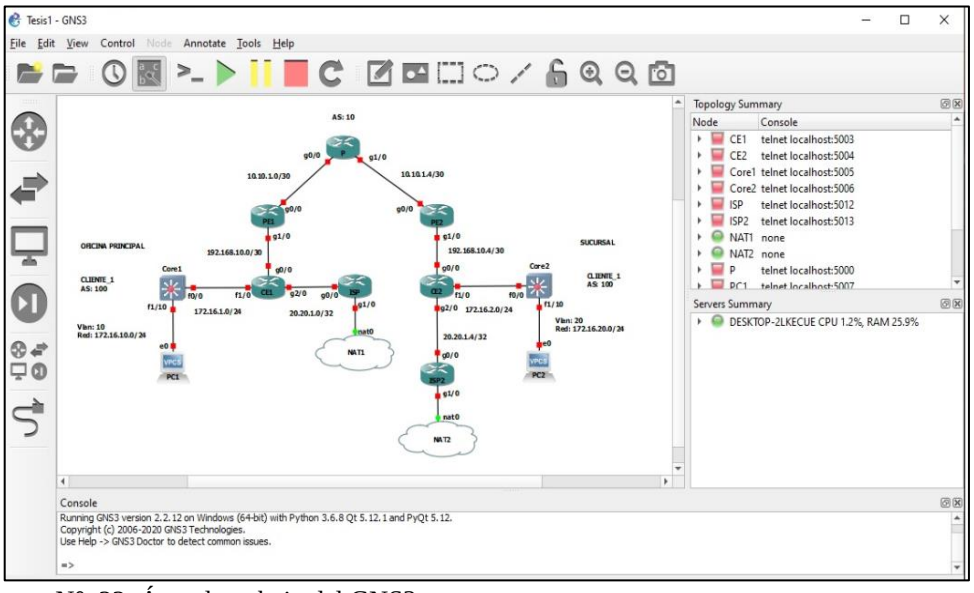


Figura N° 22: Área de trabajo del GNS3
Fuente: Elaboración propia

c) Router Cisco

El modelo del router cisco utilizado para la emulación de la red MPLS fue el c7200, así como también el IOS del software, esto lo podemos apreciar en la siguiente Figura N° 23:

```
P#show hardware
Cisco IOS Software, 7200 Software (C7200-ADVIPSERVICESK9-M), Version 12.4(9)T1, REL
EASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 30-Aug-06 20:48 by prod_rel_team
```

Figura N° 23: IOS del router C7200
Fuente: Elaboración propia

Para la parte que corresponde al router que van en el lado del usuario se utilizó el modelo c2691, así como también el IOS del software, esto lo podemos apreciar en la siguiente Figura N° 24:

```
CE1#show hardware
Cisco IOS Software, 2600 Software (C2691-ADVIPSERVICESK9-M), Version 12.4(15)T6, RELEASE SOFTWAR
E (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 07-Jul-08 04:30 by prod_rel_team
```

Figura N° 24: IOS del router C2691
Fuente: Elaboración propia

El modelo de router utilizado para emular el acceso a Internet fue el c2691, así como también el IOS del software, esto lo podemos apreciar en la siguiente Figura N° 25:

```
ISP1#show hardware
Cisco IOS Software, 2600 Software (C2691-ADVIPSERVICESK9-M), Version 12.4(15)T6, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Mon 07-Jul-08 04:30 by prod_rel_team
```

Figura N° 25: IOS del router C2691
Fuente: Elaboración propia

Los IOS de software que se muestran para los modelos de routers utilizados fueron obtenidos de la página del fabricante de Cisco.

d) Switch Cisco L3

Para la emulación del switch de capa 3 tanto en la oficina principal como en la sucursal se utilizó el modelo c3725, así como también el IOS del software, esto lo podemos apreciar en la siguiente Figura N° 26:

```
Core1#show hardware
Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(15)T14, RELEASE SOFTWA
RE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 17-Aug-10 12:08 by prod_rel_team
```

Figura N° 26: IOS del switch C3725
Fuente: Elaboración propia

e) Software de Virtualización

Para la emulación de las máquinas virtuales se trabajó bajo la plataforma del Oracle VM VirtualBox, aplicación la cual permite correr sistemas operativos como Windows y Linux los cuales son los más utilizados actualmente, esta aplicación es un software libre de código abierto que actualmente es desarrollado por Oracle Corporation. La versión utilizada fue la 6.1.14 la cual se puede observar en la siguiente Figura N° 27:

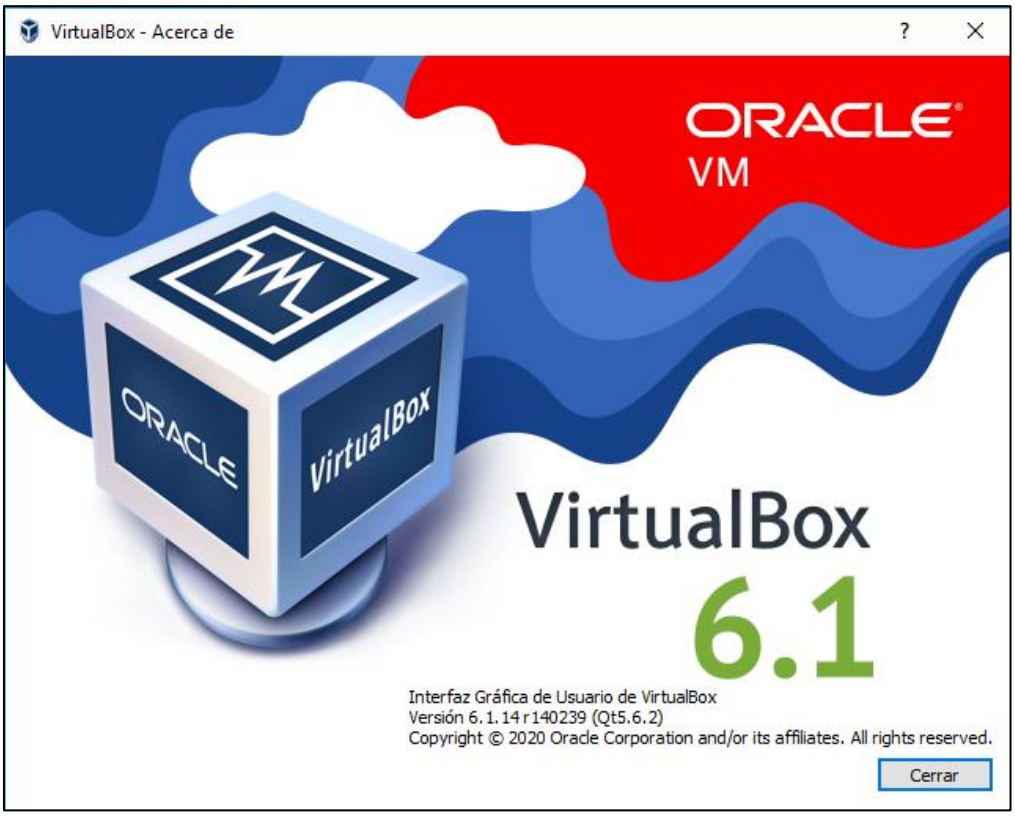


Figura N° 27: VirtualBox
Fuente: Elaboración propia

Bajo esta plataforma se instalaron dos máquinas virtuales, el primero fue un Windows XP el cual emula el tráfico que realiza un usuario dentro de la red LAN y el otro sistema operativo fue un Windows 2012 R2 que emula al servidor donde se instaló el software del OpManager, el cual realizo la captura de los datos enviados por los equipos: router, switches y servidores.

4.2.2 Topología propuesta en GNS3

a) Topología a emular

La topología que se configuro para emular un entorno de red de la empresa DETCOM consistió en dos oficinas, las oficinas elegidas fueron la oficina principal y una sucursal, en este aspecto las oficinas se enlazan a través de una red MPLS por el cual los usuarios que pertenecen a la sucursal pueden llegar a los servidores de aplicación que están instaladas en la oficina principal.

Los equipos que se tienen desplegados en la red LAN tanto en la oficina principal como en la sucursal consistieron en un router CE de enlace hacia la red MPLS el cual a su vez también brinda el acceso a internet independiente para cada una de ellas. Cada oficina tiene asignado un switch de capa 3 en el cual se conectan los equipos de los usuarios de acuerdo con la VLAN que le corresponde. La descripción indicada es mostrada en la siguiente Figura N° 28:

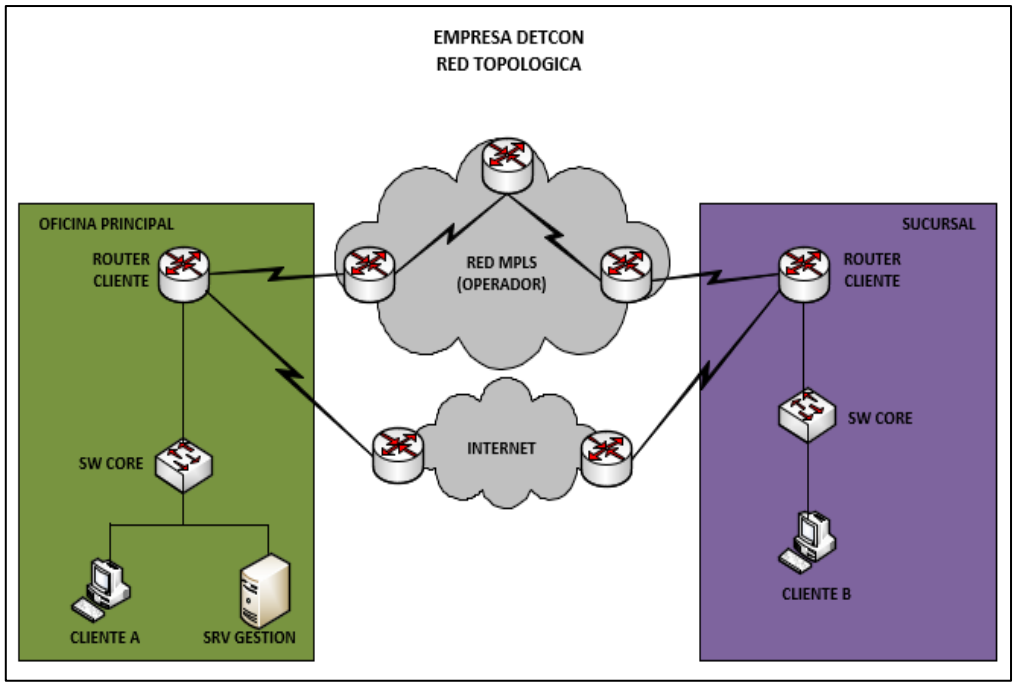


Figura N° 28: Topología a emular
Fuente: Elaboración propia

Es en base a este diagrama se procedió a elaborar la configuración respectiva en la aplicación del GNS3, seleccionando los modelos de los router para cada caso, el modelo del switch, así como también los terminales virtuales con el cual se procedió a realizar el tráfico de red respectivo y la parte de monitoreo y análisis de la data recopilada.

b) Segmentos de red a utilizar

Se desarrolló y configuró en base a la topología indicada en la Figura N° 28 donde se asignó diferentes segmentos de red tanto para los enlaces de la red MPLS como también para la red LAN, VLAN y acceso a internet con el cual cuentan en cada oficina, a continuación, detallamos el direccionamiento otorgado:

Red MPLS:

Los segmentos utilizados en el enlace entre los routers P, PE1 y PE2, así como las direcciones IP asignadas a cada interfaz son mostradas en la siguiente Tabla N° 8:

Tabla 8: Segmento de red entre los router P, PE1 y PE2

Enlace	Segmento	Mascara	Rango
P – PE1	10.10.1.0	255.255.255.252	10.10.1.1 – 10.10.1.2
Equipo	Dirección IP	Mascara	Interfaz
Router P	10.10.1.1	255.255.255.252	Gi Eth 0/0
Router PE1	10.10.1.2	255.255.255.252	Gi Eth 0/0
Enlace	**Segmento**	**Mascara**	**Rango**
P – PE2	10.10.1.4	255.255.255.252	10.10.1.5 – 10.10.1.6
Equipo	Dirección IP	Mascara	Interfaz
Router P	10.10.1.5	255.255.255.252	Gi Eth 1/0
Router PE2	10.10.1.6	255.255.255.252	Gi Eth 1/0

Fuente: Elaboración propia

En la siguiente Figura N° 29, se muestra en forma gráfica el direccionamiento asignado:

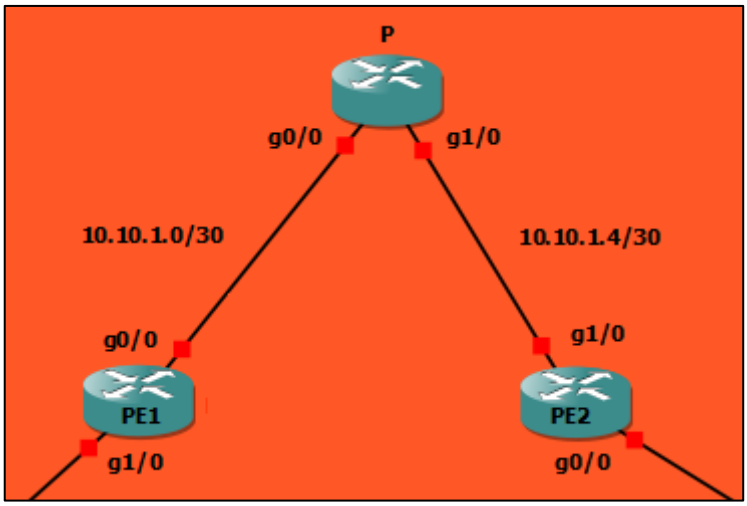


Figura N° 29: Segmentos entre los router PE1 – P – PE2
Fuente: Elaboración propia

Los segmentos utilizados entre los routers PE1 y CE1, así como también entre los routers PE2 y CE2, y sus direcciones IP asignadas a cada interfaz son mostradas en la siguiente Tabla N° 9:

Tabla 9: Segmento de red entre los router PE1 – CE1 y PE2 – CE2

Enlace	Segmento	Mascara	Rango
PE1 – CE1	192.168.10.0	255.255.255.252	192.168.10.1 – 192.168.10.2
Equipo	Dirección IP	Mascara	Interfaz
Router PE1	192.168.10.1	255.255.255.252	Gi Eth 1/0
Router CE1	192.168.10.2	255.255.255.252	Fa Eth 0/0
Enlace	**Segmento**	**Mascara**	**Rango**
PE2 – CE2	192.168.10.4	255.255.255.252	192.168.10.5 – 192.168.10.6
Equipo	Dirección IP	Mascara	Interfaz
Router PE2	192.168.10.5	255.255.255.252	Gi Eth 0/0
Router CE2	192.168.10.6	255.255.255.252	Fa Eth 0/0

Fuente: Elaboración propia

En la siguiente Figura N° 30, se muestra en forma gráfica el direccionamiento asignado:

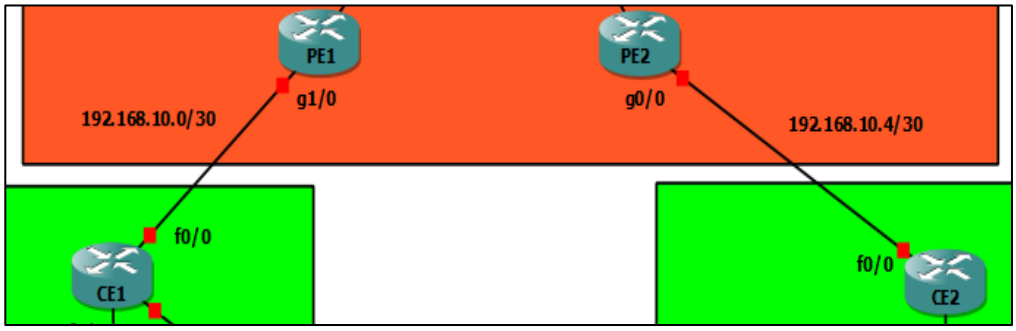


Figura N° 30: Segmento entre los router PE1 – CE1 y PE2 – CE2
Fuente: Elaboración propia

Acceso a Internet:

El acceso a internet se da a través de los router CE1 y CE2, los cuales se enlazan con los routers ISP1 e ISP2 y estos equipos a su vez se conectan vía la facilidad de conexión nat para obtener una dirección dinámica del puerto de ethernet de la computadora para el acceso a Internet.

El segmento y sus direcciones IP asignadas a cada interfaz de los respectivos equipos mencionado son mostradas en la siguiente Tabla N° 10:

Tabla 10: Segmento de red entre los routers CE1 – ISP1 y CE2 – ISP2

Enlace	Segmento	Mascara	Rango
CE1 – ISP1	20.20.1.0	255.255.255.252	20.20.1.1 – 20.20.1.2
Equipo	Dirección IP	Mascara	Interfaz
Router CE1	20.20.1.2	255.255.255.252	Fa Eth 1/0
Router ISP1	20.20.1.1	255.255.255.252	Fa Eth 0/0
Enlace	**Segmento**	**Mascara**	**Rango**
CE2 – ISP2	20.20.1.4	255.255.255.252	20.20.1.5 – 20.20.1.6
Equipo	Dirección IP	Mascara	Interfaz
Router CE2	20.20.1.6	255.255.255.252	Fa Eth 1/0
Router ISP2	20.20.1.5	255.255.255.252	Fa Eth 0/0
Enlace	**Segmento**	**Mascara**	**Rango**
ISP1 - Internet	192.168.106.0	255.255.255.0	192.168.106.1 – 192.168.106.254
Equipo	Dirección IP	Mascara	Interfaz
ISP1	DHCP	255.255.255.0	Fa Eth 0/1
Enlace	**Segmento**	**Mascara**	**Rango**
ISP2 - Internet	192.168.106.0	255.255.255.0	192.168.106.1 – 192.168.106.254
Equipo	Dirección IP	Mascara	Interfaz
ISP2	DHCP	255.255.255.0	Fa Eth 0/1

Fuente: Elaboración propia

En la siguiente Figura N° 31, se muestra en forma gráfica el direccionamiento asignado:

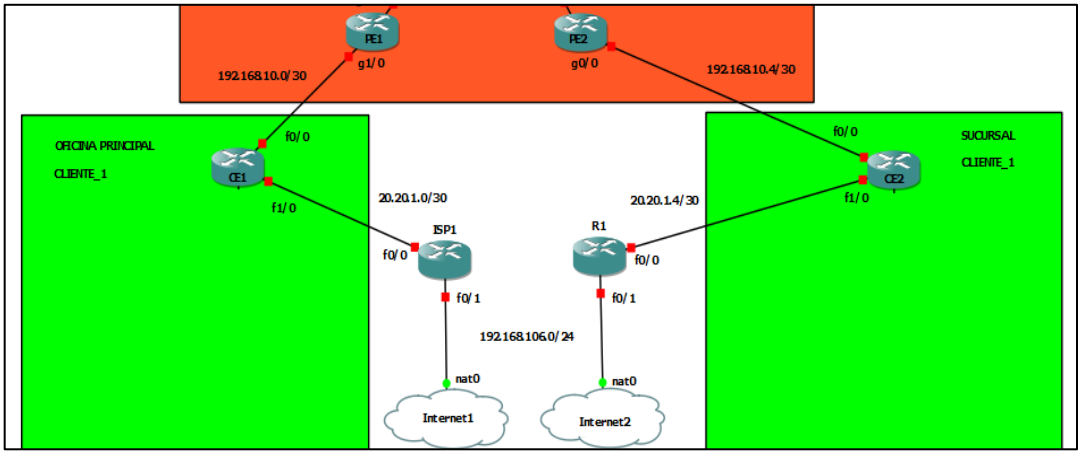


Figura N° 31: Segmento entre los routers CE1 – ISP1 y CE2 – ISP2
Fuente: Elaboración propia

LAN:

Se asigno un segmento para el enlace entre los routers CE y los Core, y un segmento para la vlan´s en cada oficina, de esta manera cada oficina manejo su propio direccionamiento de acuerdo con las áreas desplegadas en cada una de ellas, se manejó un direccionamiento estático en base al esquema actual.

El segmento y sus direcciones IP asignadas a cada interfaz de los respectivos equipos indicados en la LAN son mostradas en la siguiente Tabla N° 11, así como también al servidor y computadoras configuradas:

Tabla 11: Segmento de la red LAN

OFICINA PRINCIPAL			
Enlace	**Segmento**	**Mascara**	**Rango**
CE1 – Core1	172.16.1.0	255.255.255.0	172.16.1.1 – 172.16.1.254
Equipo	Dirección IP	Mascara	Interfaz
Router CE1	172.16.1.1	255.255.255.0	Fa Eth 0/1
Core 1	172.16.1.2	255.255.255.0	Fa Eth 0/0
LAN	**Segmento**	**Mascara**	**IP**
VLAN 10	172.16.10.0	255.255.255.0	172.16.10.1
Equipo	Dirección IP	Mascara	Puerto Core 1
PC1	172.16.10.10	255.255.255.0	Fa Eth 1/10
Windows XP	172.16.10.11	255.255.255.0	Fa Eth 1/11
Serv. Win 2012	172.16.10.12	255.255.255.0	Fa Eth 1/12
OFICINA SUCURSAL			
Enlace	**Segmento**	**Mascara**	**Rango**
CE2 – Core2	172.16.2.0	255.255.255.0	172.16.2.1 – 172.16.2.254
Equipo	Dirección IP	Mascara	Interfaz
Router CE2	172.16.2.1	255.255.255.0	Fa Eth 0/1
Core 2	172.16.2.2	255.255.255.0	Fa Eth 0/0
LAN	**Segmento**	**Mascara**	**IP**
VLAN 20	172.16.20.0	255.255.255.0	172.16.20.1
Equipo	Dirección IP	Mascara	Interfaz
PC2	172.16.20.10	255.255.255.0	Fa Eth 1/10
Windows XP	172.16.20.11	255.255.255.0	Fa Eth 1/11

Fuente: Elaboración propia

En la siguiente Figuras N° 32-33, se muestra de forma gráfica el direccionamiento indicado:

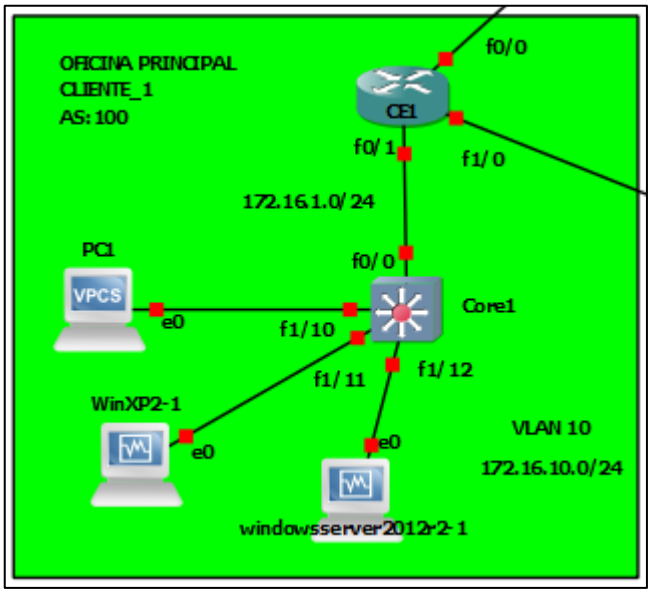


Figura N° 32: Segmento oficina principal
Fuente: Elaboración propia

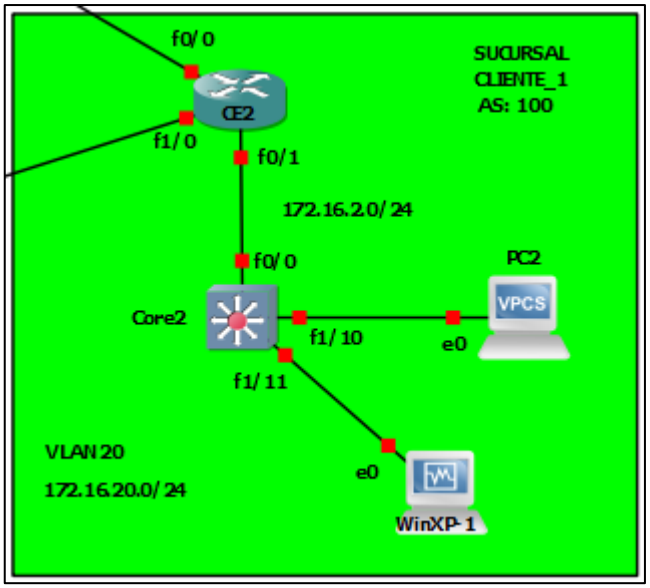


Figura N° 33: Segmento oficina sucursal
Fuente: Elaboración propia

En base al direccionamiento definido para cada área, enlace y/o conexión asignado a la oficina principal como a la sucursal, se procedió a realizar las configuraciones respectivas de cada enlace de red, los cuales abarcan la red MPLS, la red LAN y el acceso a Internet. De tal manera que una vez culminado las configuraciones indicadas se realizó el despliegue de los protocolos SNMP en los routers CE1, CE2, Core1 y Core2, paso seguido se desplego el protocolo Netflow en los routers CE1 y CE2, de

acuerdo con las interfaces que dan el acceso a Internet y de esta manera tener una mejor gestión de la red LAN y mejorar su rendimiento, así como los accesos hacia la WAN dando una mejor velocidad y disponibilidad del recurso adquirido.

4.2.3 Desarrollo de la emulación

a) Configuración de la red MPLS

La red MPLS, es un mecanismo de conmutación el cual ejecuta un proceso de conmutación de paquetes MPLS incluyendo el análisis de la etiqueta, aquí también se dan los principios básicos de enrutamiento y soportan múltiples protocolos. El mecanismo de MPLS en los routers Cisco está basado en CEF (*Cisco Express Forwarding*) mecanismo necesario para el funcionamiento de las mismas.

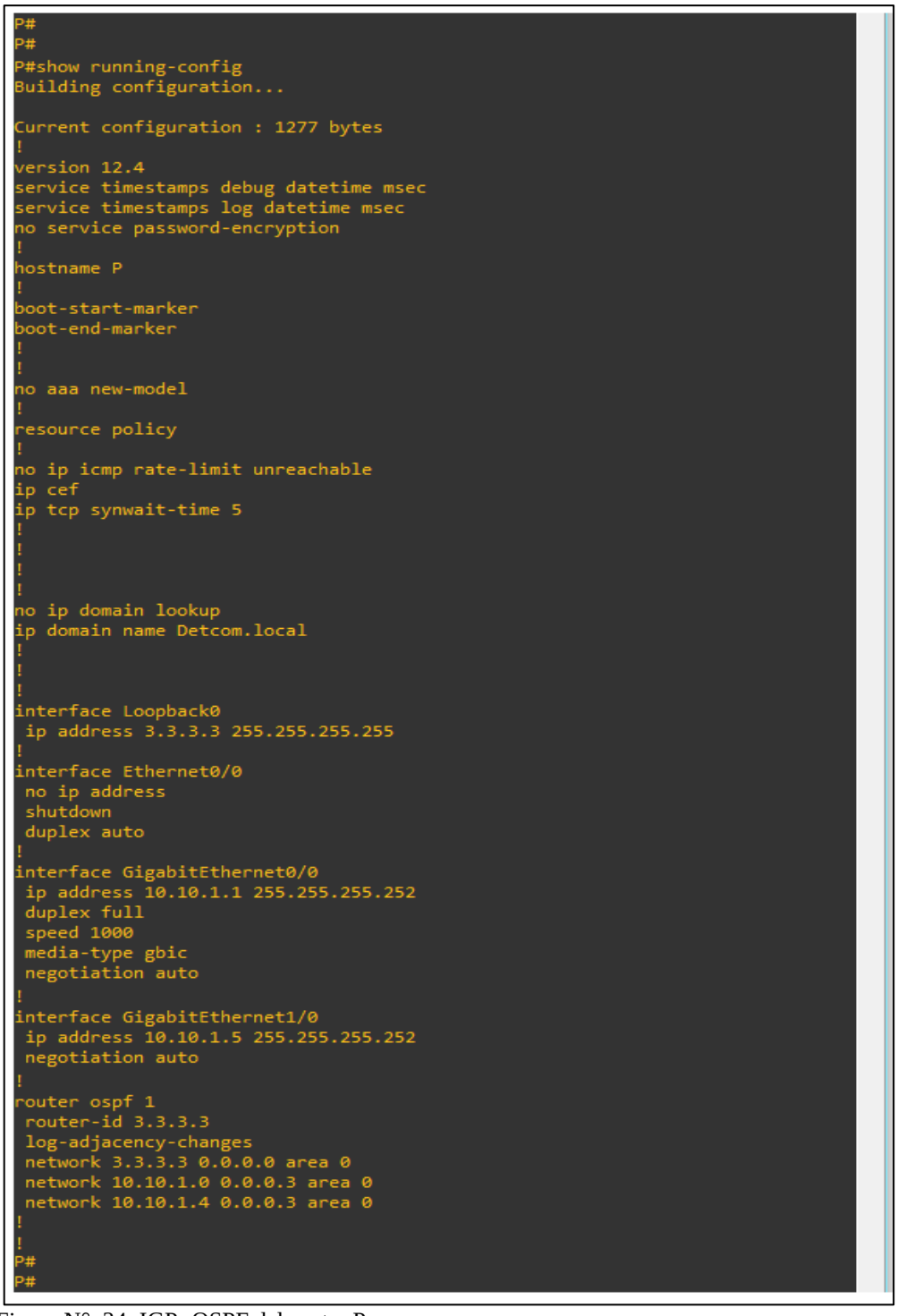
Bajo esta premisa podemos indicar los roles de los equipos que conforman una red MPLS:

- CE (*Customer Equipment*): Es el router que se encuentra fuera de la red MPLS, ubicado en la oficina del cliente, este equipo no utiliza el sistema de etiquetado del protocolo MPLS. Este equipo también es capaz de proporcionar salida a Internet a través de otra interfaz de red.
- PE (*Provider Edge*): Este equipo si pertenece a la red MPLS, es un equipo de borde, se enlaza con el router CE del cliente y realiza las funciones de POP, también introduce el VRF (*Virtual Route Forwarding*)
- P (*Provider Core*): Esta ubicado dentro de la red MPLS, y es el enrutador interno de esta red.

Como primer paso en la construcción de la red MPLS, se procedió a la creación de los Loopback en cada router P y PE, configuración de las direcciones IP de las interfaces a enlazar y a la creación del enrutamiento OSPF para lograr las adyacencias entre los router. Por último, se habilito el CEF en cada router mencionado.

Paso 1: IGP - OSPF: Los routers P, PE1 y PE2 trabajan en modo de conmutación de etiquetas llamados comúnmente LSR (*Label Switch Routers*), para la asociación de dichas etiquetas con las IP´s, en este sentido las tablas de ruteo se computan en un IGP (Interior Gateway Protocol) y el protocolo de ruteo utilizado fue el OSPF (*Open Shortest Path First*).

En las siguientes Figuras N° 34-37, se muestra las configuraciones de los routers P, PE1 y PE2:



```
P#
P#
P#show running-config
Building configuration...

Current configuration : 1277 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
ip domain name Detcom.local
!
!
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 10.10.1.1 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface GigabitEthernet1/0
 ip address 10.10.1.5 255.255.255.252
 negotiation auto
!
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 3.3.3.3 0.0.0.0 area 0
 network 10.10.1.0 0.0.0.3 area 0
 network 10.10.1.4 0.0.0.3 area 0
!
!
P#
P#
```

Figura N° 34: IGP- OSPF del router P
Fuente: Elaboración propia

```
PE1#
PE1#
PE1#
PE1#show running-config
Building configuration...

Current configuration : 1789 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
ip domain name Detcom.local
!
!
!
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 10.10.1.2 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
!
interface GigabitEthernet1/0
 no ip address
 shutdown
 duplex auto
!
router ospf 1
 router-id 2.2.2.2
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.10.1.0 0.0.0.3 area 0
!
PE1#
PE1#
PE1#
```

Figura N° 35: IGP- OSPF del router PE1
Fuente: Elaboración propia

```
PE2#
PE2#
PE2#show running-config
Building configuration...

Current configuration : 1789 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
ip domain name Detcom.local
!
!
!
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet1/0
 ip address 10.10.1.6 255.255.255.252
 negotiation auto
!
router ospf 1
 router-id 4.4.4.4
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 10.10.1.4 0.0.0.3 area 0
!
PE2#
PE2#
```

Figura N° 36: IGP- OSPF del router PE2
Fuente: Elaboración propia

En la siguiente Figura N° 37, se muestran las adyacencias.

```
P#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4           1   FULL/DR         00:00:38    10.10.1.6       GigabitEthernet1/0
2.2.2.2           1   FULL/BDR        00:00:35    10.10.1.2       GigabitEthernet0/0
P#
P#show ip ospf database

            OSPF Router with ID (3.3.3.3) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
2.2.2.2         2.2.2.2         439         0x80000008 0x0031A4 2
3.3.3.3         3.3.3.3         485         0x80000009 0x008202 3
4.4.4.4         4.4.4.4         499         0x80000008 0x00A70D 2

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.10.1.1       3.3.3.3         485         0x80000007 0x00E11F
10.10.1.6       4.4.4.4         499         0x80000007 0x00E50A
P#
P#show ip route ospf
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 10.10.1.2, 03:29:26, GigabitEthernet0/0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/2] via 10.10.1.6, 03:29:26, GigabitEthernet1/0
P#
P#
```

Figura N° 37: Adyacencias en el router P
Fuente: Elaboración propia

Paso 2: MPLS - LDP: El LDP (*Label Distribution Protocol*), es el que anuncia las vinculaciones entre rutas y etiquetas, en esta parte también se activa el parámetro "mpls ip" en cada interfaz de los elementos que constituyen la red MPLS.

En las siguientes Figuras N° 38-40, se muestra las configuraciones respectivas.

```
!
interface GigabitEthernet0/0
 ip address 10.10.1.1 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls ip
!
interface GigabitEthernet1/0
 ip address 10.10.1.5 255.255.255.252
 negotiation auto
 mpls ip
!
```

```
!
mpls ldp router-id Loopback0
!
control-plane
```

Figura N° 38: Configuración del LDP y MPLS en el router P
Fuente: Elaboración propia

```
!
interface GigabitEthernet0/0
 ip address 10.10.1.2 255.255.255.252
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 mpls ip
!

!
mpls ldp router-id Loopback0
!
control-plane
!
```

Figura N° 39: Configuración del LDP y MPLS en el router PE1
Fuente: Elaboración propia

```
!
interface GigabitEthernet1/0
 ip address 10.10.1.6 255.255.255.252
 negotiation auto
 mpls ip
!

!
mpls ldp router-id Loopback0
!
control-plane
!
```

Figura N° 40: Configuración del LDP y MPLS en el router PE2
Fuente: Elaboración propia

En las siguientes Figuras N° 41 y 42, se muestran las tablas MPLS:

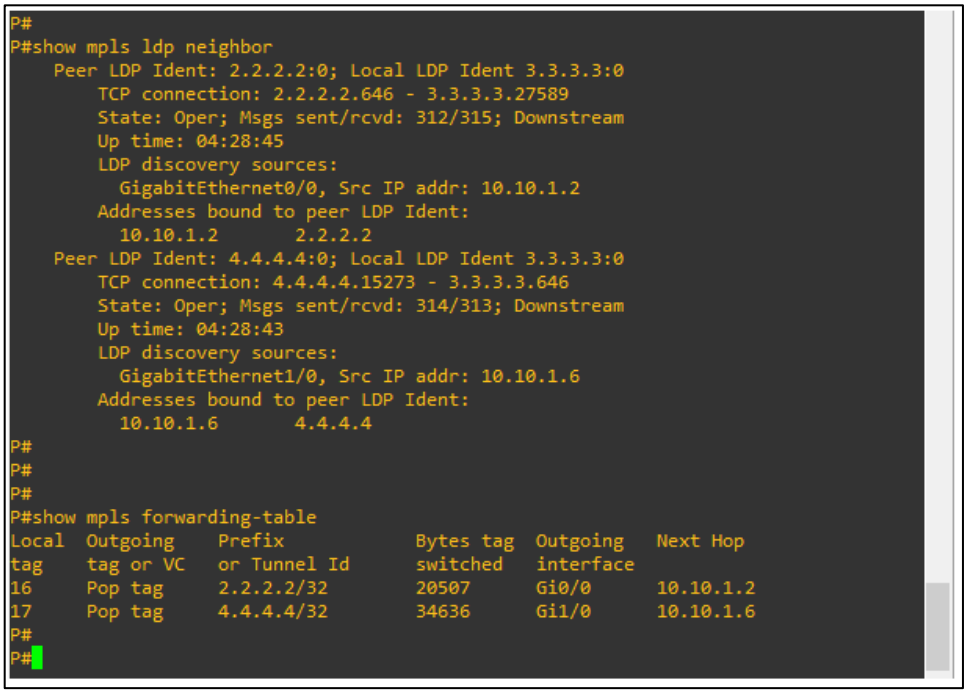


Figura N° 41: Etiquetas y Tablas MPLS – Router P
Fuente: Elaboración propia

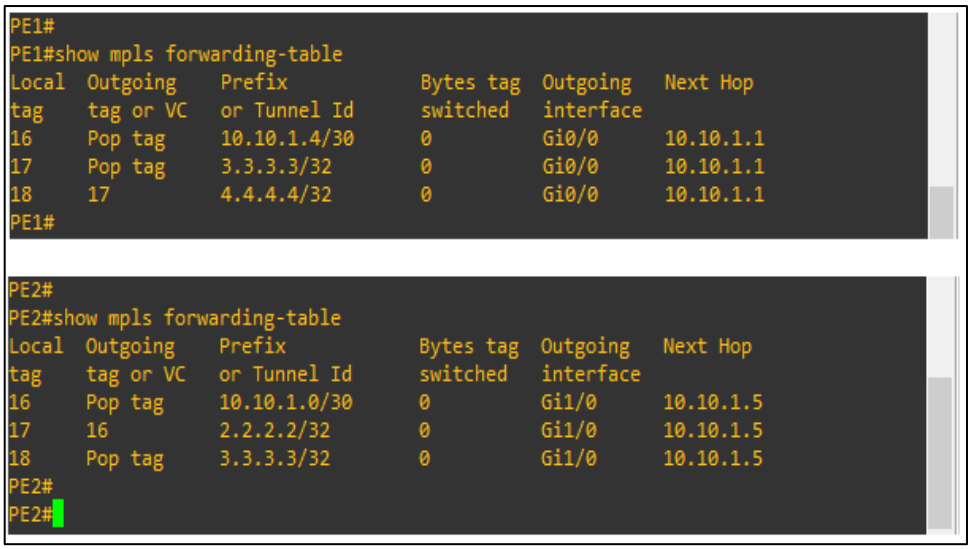


Figura N° 42: Etiquetas y Tablas MPLS – Routers PE1 y PE2
Fuente: Elaboración propia

Paso 3: VRF (*Virtual Routing and Forwarding*): Son las tablas de enrutamiento virtual y reenvió, estas tablas son independientes y el uso de estas sobre los routers PE asegura que el tráfico sobre una VPN no sea direccionado a otra.

En las siguientes Figuras N° 43 –44, se muestran las configuraciones respectivas.

Figura N° 43: Configuración VRF en el router PE1
Fuente: Elaboración propia

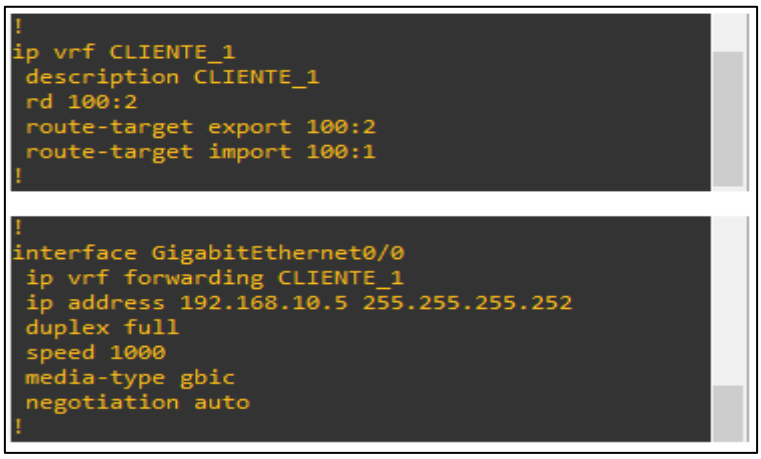


Figura N° 44: Configuración VRF en el router PE2
Fuente: Elaboración propia

En las siguientes Figuras N° 45 y 46, se presentan las tablas de ruteo VRF.

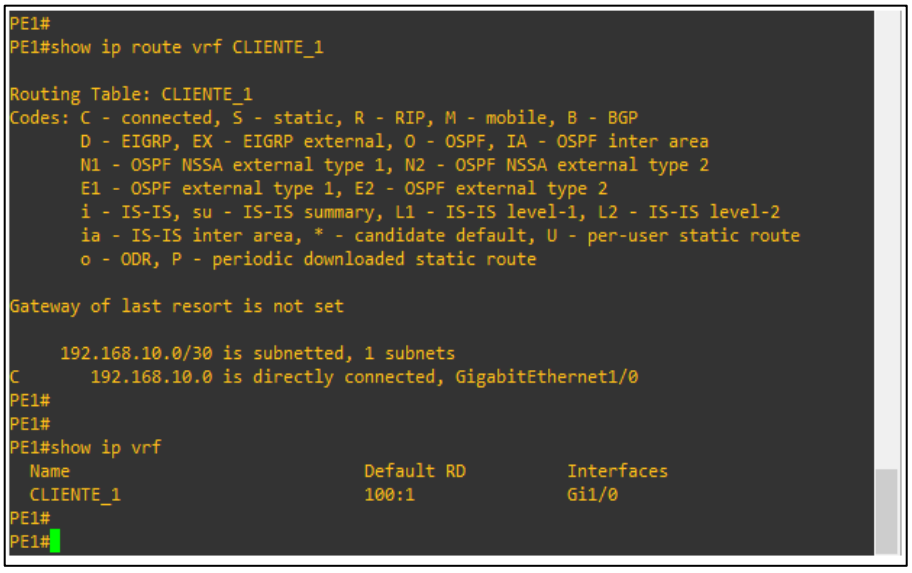


Figura N° 45: Tabla VRF en el router PE1
Fuente: Elaboración propia

```
PE2#
PE2#show ip route vrf CLIENTE_1

Routing Table: CLIENTE_1
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 1 subnets
C       192.168.10.4 is directly connected, GigabitEthernet0/0
PE2#
PE2#
PE2#show ip vrf
  Name                             Default RD          Interfaces
  CLIENTE_1                        100:2               Gi0/0
PE2#
PE2#
```

Figura N° 46: Tabla VRF en el router PE2
Fuente: Elaboración propia

Paso 4: MP – BGP (VPNV4): Las VPN (*Virtual Private Network*), se forman mediante la definición del cliente el cual se adiciona como miembro de una VRF, el router PE utiliza el BGP (Border Gateway Protocol) para propagar la información respecto a las rutas VPN´s así como las etiquetas en la red MPLS.

En las siguientes Figuras N° 47 y 48, se aprecian, las configuraciones en los routers PE como en los routers del cliente CE.

```
!
router bgp 10
 no synchronization
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 10
 neighbor 4.4.4.4 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 4.4.4.4 activate
 neighbor 4.4.4.4 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf CLIENTE_1
 neighbor 192.168.10.2 remote-as 100
 neighbor 192.168.10.2 activate
 no synchronization
 exit-address-family
!
```

Figura N° 47: Configuración del BGP y VPNV4 en el router PE1
Fuente: Elaboración propia

```
!
router bgp 10
 no synchronization
 bgp log-neighbor-changes
 neighbor 2.2.2.2 remote-as 10
 neighbor 2.2.2.2 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 2.2.2.2 activate
 neighbor 2.2.2.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf CLIENTE_1
 neighbor 192.168.10.6 remote-as 100
 neighbor 192.168.10.6 activate
 no synchronization
 exit-address-family
!
```

Figura N° 48: Configuración del BGP y VPNV4 en el router PE2
Fuente: Elaboración propia

En el router CE1 en la configuración del BGP, se declaran también los segmentos de la red LAN (véase Figura N° 49 y 50).

```
!
interface FastEthernet0/0
 ip address 192.168.10.2 255.255.255.252
 speed 100
 full-duplex
!
```

```
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 network 172.16.1.0 mask 255.255.255.0
 network 172.16.10.0 mask 255.255.255.0
 neighbor 192.168.10.1 remote-as 10
 neighbor 192.168.10.1 allowas-in
 no auto-summary
!
```

Figura N° 49: Configuración del BGP y VPNV4 en el router CE1
Fuente: Elaboración propia

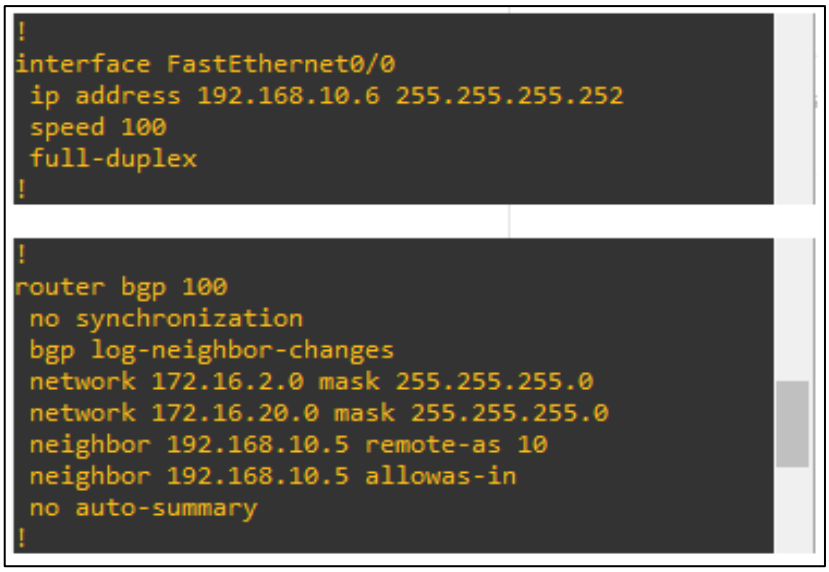


Figura N° 50: Configuración del BGP y VPNV4 en el router CE2
Fuente: Elaboración propia

En las siguientes Figuras 51 y 52, se aprecian las tablas de ruteo BGP y las VPN asociadas.

```
PE1#
PE1#show bgp vpnv4 unicast all summary
BGP router identifier 2.2.2.2, local AS number 10
BGP table version is 12, main routing table version 12
6 network entries using 894 bytes of memory
6 path entries using 408 bytes of memory
4/2 BGP path/bestpath attribute entries using 496 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1870 total bytes of memory
BGP activity 7/1 prefixes, 7/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
4.4.4.4         4    10     473     474       12    0    0 07:49:41        2
192.168.10.2    4   100      49      48       12    0    0 00:43:07        2
PE1#
PE1#
PE1#show ip bgp vpnv4 vrf CLIENTE_1
BGP table version is 12, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf CLIENTE_1)
*> 172.16.1.0/24    192.168.10.2             0             0 100 i
*>i172.16.2.0/24    4.4.4.4                  0    100      0 100 i
*> 172.16.10.0/24   192.168.10.2             0             0 100 i
*>i172.16.20.0/24   4.4.4.4                  0    100      0 100 i
PE1#
```

Figura N° 51: Tablas de BGP y VPNV4 en el router PE1
Fuente: Elaboración propia

```
PE2#
PE2#show bgp vpnv4 unicast all summary
BGP router identifier 4.4.4.4, local AS number 10
BGP table version is 13, main routing table version 13
6 network entries using 894 bytes of memory
6 path entries using 408 bytes of memory
4/2 BGP path/bestpath attribute entries using 496 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1870 total bytes of memory
BGP activity 8/2 prefixes, 8/2 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
2.2.2.2         4    10     475     474       13    0    0 07:50:33        2
192.168.10.6    4   100      48      49       13    0    0 00:43:37        2
PE2#
PE2#show ip bgp vpnv4 vrf CLIENTE_1
BGP table version is 13, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:2 (default for vrf CLIENTE_1)
*>i172.16.1.0/24    2.2.2.2                  0    100      0 100 i
*> 172.16.2.0/24    192.168.10.6             0             0 100 i
*>i172.16.10.0/24   2.2.2.2                  0    100      0 100 i
*> 172.16.20.0/24   192.168.10.6             0             0 100 i
PE2#
```

Figura N° 52: Tablas de BGP y VPNV4 en el router PE2
Fuente: Elaboración propia

b) Configuración de la LAN

En esta parte de la emulación se configuraron la LAN y su salida a internet, las oficinas creadas fueron la oficina principal y una sucursal cada una con su salida a internet independiente. En la oficina principal se trabajó con un segmento 172.16.1.0/24 para el enlace entre el Core1 y el router CE1 (véase Figura N° 53).

CE1

```
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
```

Core1

```
!
interface FastEthernet0/0
 description *** Unused for Layer2 EtherSwitch ***
 ip address 172.16.1.2 255.255.255.0
 duplex auto
 speed auto
!
```

Figura N° 53: Enlace entre el CE1 y el Core1
Fuente: Elaboración propia

En la sucursal se trabajó con un segmento 172.16.2.0/24 para el enlace entre el Core2 y el router CE2 (véase Figura N° 54).

CE2

```
!
interface FastEthernet0/1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
```

Core2

```
!
interface FastEthernet0/0
 description *** Unused for Layer2 EtherSwitch ***
 ip address 172.16.2.2 255.255.255.0
 duplex auto
 speed auto
!
```

Figura N° 54: Enlace entre el CE1 y el Core1
Fuente: Elaboración propia

Se configuro una VLAN 10 con el segmento 172.16.10.0/24 para la conexión de las máquinas virtuales en la oficina principal (véase Figura N° 55).

```
!
interface FastEthernet1/10
 switchport access vlan 10
 duplex full
 speed 100
!
interface FastEthernet1/11
 switchport access vlan 10
 duplex full
 speed 100
!
interface FastEthernet1/12
 switchport access vlan 10
 duplex full
 speed 100
!
```

```
!
interface Vlan10
 ip address 172.16.10.1 255.255.255.0
!
```

Figura N° 55: Interfaz VLAN 10 - Core1
Fuente: Elaboración propia

En la sucursal se configuro la VLAN 20 con el segmento 172.16.20.0/24 asignado para la conexión de las máquinas virtuales (véase Figura N° 56).

```
!
interface FastEthernet1/10
 switchport access vlan 20
 duplex full
 speed 100
!
interface FastEthernet1/11
 switchport access vlan 20
 duplex full
 speed 100
!

!
interface Vlan20
 ip address 172.16.20.1 255.255.255.0
!
```

Figura N° 56: Interfaz VLAN 20 – Core2
Fuente: Elaboración propia

Para el acceso a internet se trabajó con el protocolo de enrutamiento RIP versión 2, esto con la finalidad de emular el acceso a internet el cual es fundamental para el análisis del ancho de banda a través del protocolo NETFLOW.

Se configuro las interfaces de los routers CE y el ISP en ambas oficinas utilizando el segmento 20.20.1.0/30 para la oficina principal y el segmento 20.20.1.4/30 para la sucursal (véase Figura N° 57 y 58).

CE1

```
!
interface FastEthernet1/0
 description Internet
 ip address 20.20.1.2 255.255.255.252
 duplex auto
 speed auto
!
```

ISP1

```
!
interface FastEthernet0/0
 description ISP1
 ip address 20.20.1.1 255.255.255.252
 duplex auto
 speed auto
!
```

Figura N° 57: Enlace ISP1 – Oficina Principal
Fuente: Elaboración propia

CE2

```
!
interface FastEthernet1/0
 description Internet
 ip address 20.20.1.6 255.255.255.252
 duplex auto
 speed auto
!
```

ISP2

```
!
interface FastEthernet0/0
 description ISP2
 ip address 20.20.1.5 255.255.255.252
 duplex auto
 speed auto
!
```

Figura N° 58: Enlace ISP2 – Sucursal
Fuente: Elaboración propia

El acceso a Internet para ambas oficinas como se mencionó anteriormente se trabajó con el protocolo RIP versión 2, en los Core´s, routers CE e ISP para que se puedan conocer las redes. También se adiciono una ruta estática con la finalidad de encaminar el acceso al servicio de Internet desde las máquinas virtuales.

Estas configuraciones se pueden apreciar en las siguientes imágenes: (véase Figura N° 59 y 60).

CE1

```
!
router rip
 version 2
 network 20.0.0.0
 network 172.16.0.0
 no auto-summary
!
```

```
!
ip route 0.0.0.0 0.0.0.0 20.20.1.1
!
```

Core1

```
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
```

Figura N° 59: RIP – Oficina Principal
Fuente: Elaboración propia

CE2

```
!
router rip
 version 2
 network 20.0.0.0
 network 172.16.0.0
 no auto-summary
!
```

```
!
ip route 0.0.0.0 0.0.0.0 20.20.1.5
!
```

Core2

```
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.2.1
!
```

Figura N° 60: RIP – Sucursal
Fuente: Elaboración propia

En los routers ISP, se realizó la configuración del protocolo RIP versión 2 tal y como se configuro en los routers CE. Para obtener un servicio de internet, se emulo a través del puerto de red de la PC en el cual se está emulando la red, para tal caso se configuro el NAT y se asignó en las interfaces del router ISP, esta programación lo podemos apreciar en las siguientes Figuras N° 61 y 62.

```
!
interface FastEthernet0/0
 description ISP1
 ip address 20.20.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
router rip
 version 2
 network 20.0.0.0
 network 192.168.106.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list 100 interface FastEthernet0/1 overload
!
access-list 10 permit any
access-list 100 permit ip any any
```

Figura N° 61: Acceso a Internet - ISP1
Fuente: Elaboración propia

```
!
interface FastEthernet0/0
 description ISP2
 ip address 20.20.1.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
router rip
 version 2
 network 20.0.0.0
 network 192.168.106.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip nat inside source list 100 interface FastEthernet0/1 overload
!
access-list 100 permit ip any any
no cdp log mismatch duplex
!
```

Figura N° 62: Acceso a Internet – ISP2
Fuente: Elaboración propia

Con la red MPLS, la red LAN y el acceso al servicio de Internet, configurados en la oficina principal y en la sucursal, se procedió al despliegue de las máquinas virtuales de acuerdo con las direcciones IP asignadas.

c) Despliegue de máquinas virtuales

Las máquinas virtuales que ofrece el aplicativo del GNS3 y las máquinas virtuales desplegadas a través del aplicativo del Virtual Box nos permitieron emular el entorno de trabajo tanto en la oficina principal como en la sucursal, donde dichas máquinas de usuario tienen acceso a Internet, acceden a archivos de servidores y tienen conectividad entre ambas oficinas a través de las VLAN´s configuradas.

Para la oficina principal se desplegaron 3 máquinas virtuales, del cual una fue del mismo aplicativo del GNS3 (véase Figura N° 63) asignando su respectiva dirección IP estática (véase Figura N° 64).

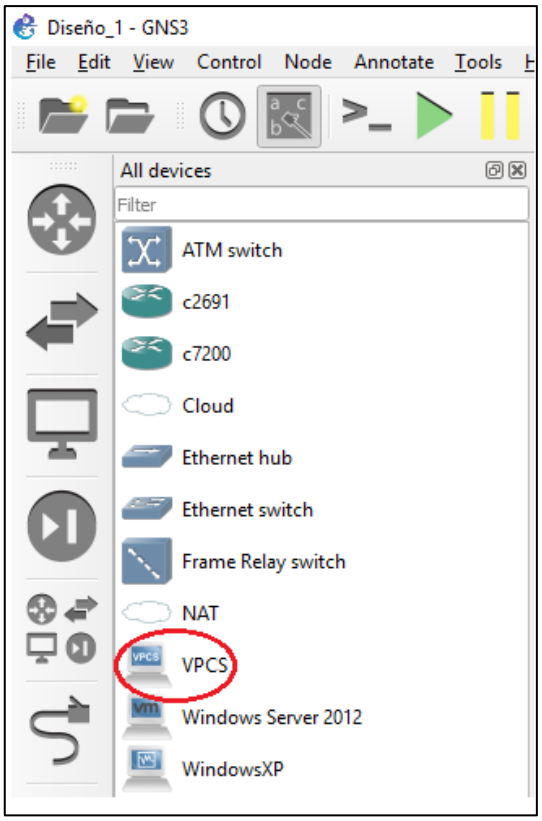


Figura N° 63: VPCS – PC del GNS3
Fuente: Elaboración propia

```
PC1>
PC1> show

NAME   IP/MASK              GATEWAY           MAC                LPORT  RHOST:PORT
PC1    172.16.10.10/24      172.16.10.1       00:50:79:66:68:00  10078  127.0.0.1:10079
       fe80::250:79ff:fe66:6800/64

PC1>
PC1>
```

Figura N° 64: Asignación de IP - PC1
Fuente: Elaboración propia

En el virtual box, se instalaron los sistemas operativos del Windows XP y del servidor Windows 2012 R2, elementos que se asignaron en la topología de la empresa DETCOM. Para el caso del Windows XP se replegaron dos instancias las cuales fueron asignadas una a cada oficina, de esta manera se podría emular el tráfico de salida hacia Internet y también el tráfico interno de acceso al servidor de aplicaciones.

En las siguientes imágenes se pueden visualizar las máquinas virtuales instaladas. (véase Figura N° 65 y 66).

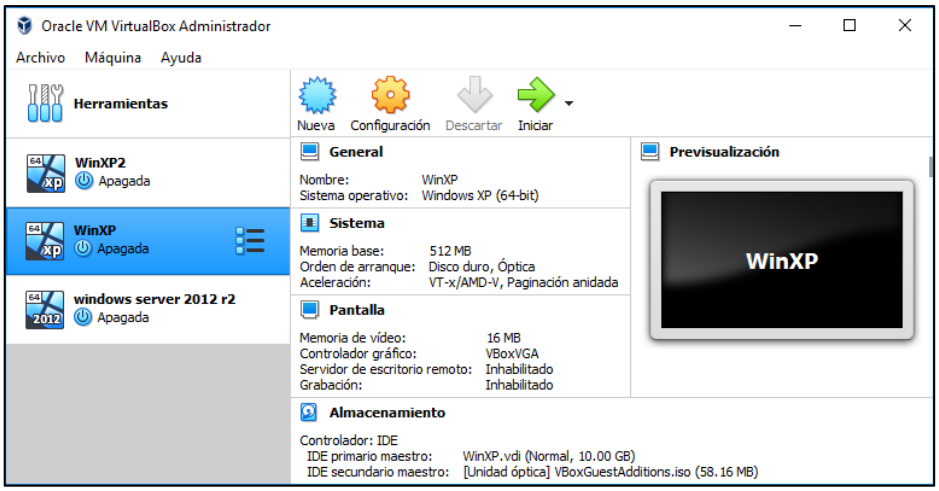


Figura N° 65: Máquinas Virtuales – Virtual Box
Fuente: Elaboración propia

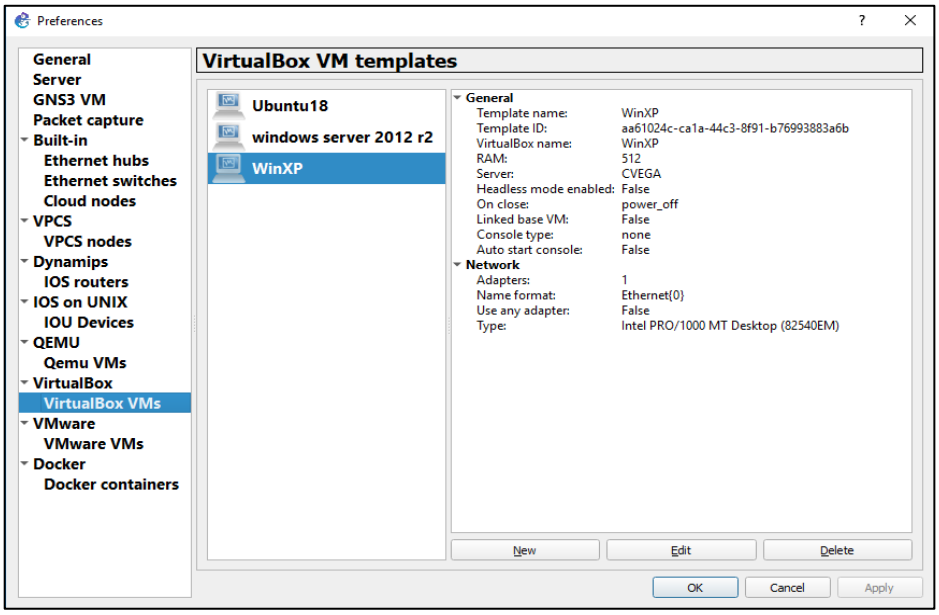


Figura N° 66: Asignación de VM – GNS3
Fuente: Elaboración propia

En la sucursal se desplego la PC2 asignando su dirección IP estática correspondiente (véase Figura N° 67).

Figura N° 67: Asignación de IP – PC2
Fuente: Elaboración propia

Con las máquinas virtuales instaladas y conectadas a los respectivos puertos del switch, se realizaron las pruebas de conectividad entre las oficinas y se validó el acceso hacia internet.

d) Pruebas de conectividad

Para las pruebas de conectividad en la topología configurada, se tomó en cuenta la comunicación entre dispositivos de la misma oficina y su acceso hacia internet, con el cual se validó los servicios ofrecidos, también se validó el acceso al servidor de aplicaciones.

En la siguiente imagen de la Figura N° 68, se muestra la respuesta de ping entre las maquinas PC1 y el Windows XP instaladas en la oficina principal.

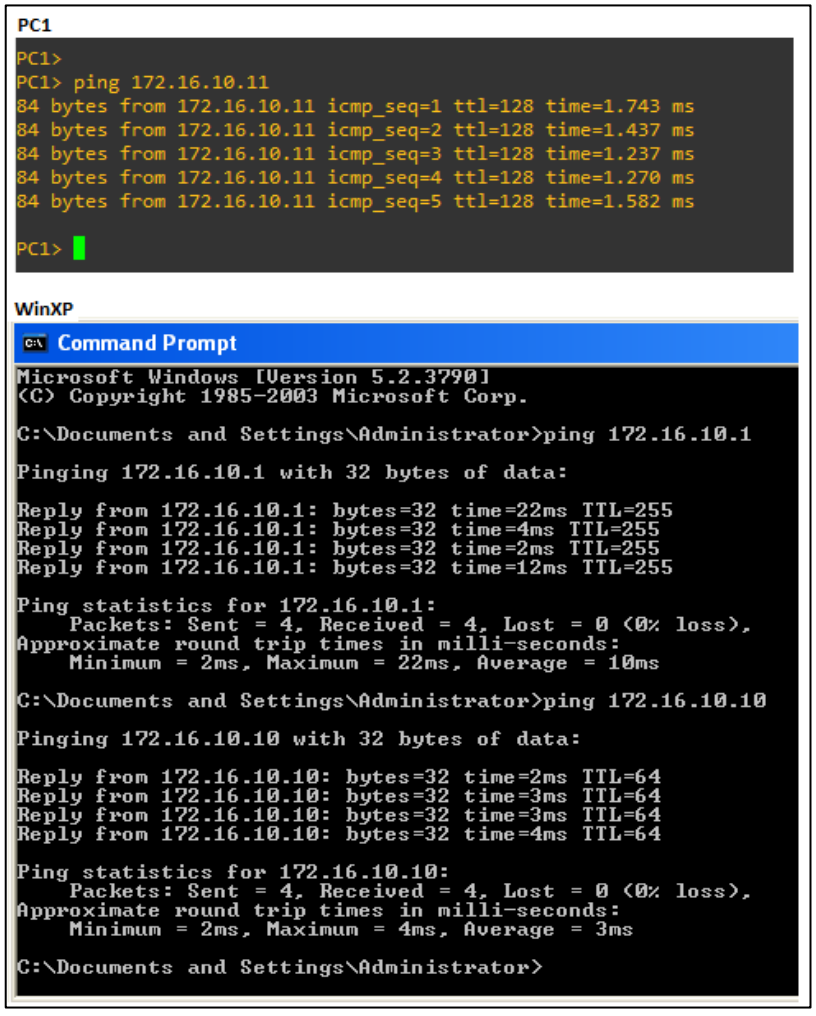


Figura N° 68: Ping entre PC1 - WinXP
Fuente: Elaboración propia

Al tener respuesta entre ambos equipos, se comprueba que la VLAN asignado a dicho segmento este operativo, en la siguiente Figura N° 69, se muestra la respuesta de ping hacia el servidor de aplicaciones.

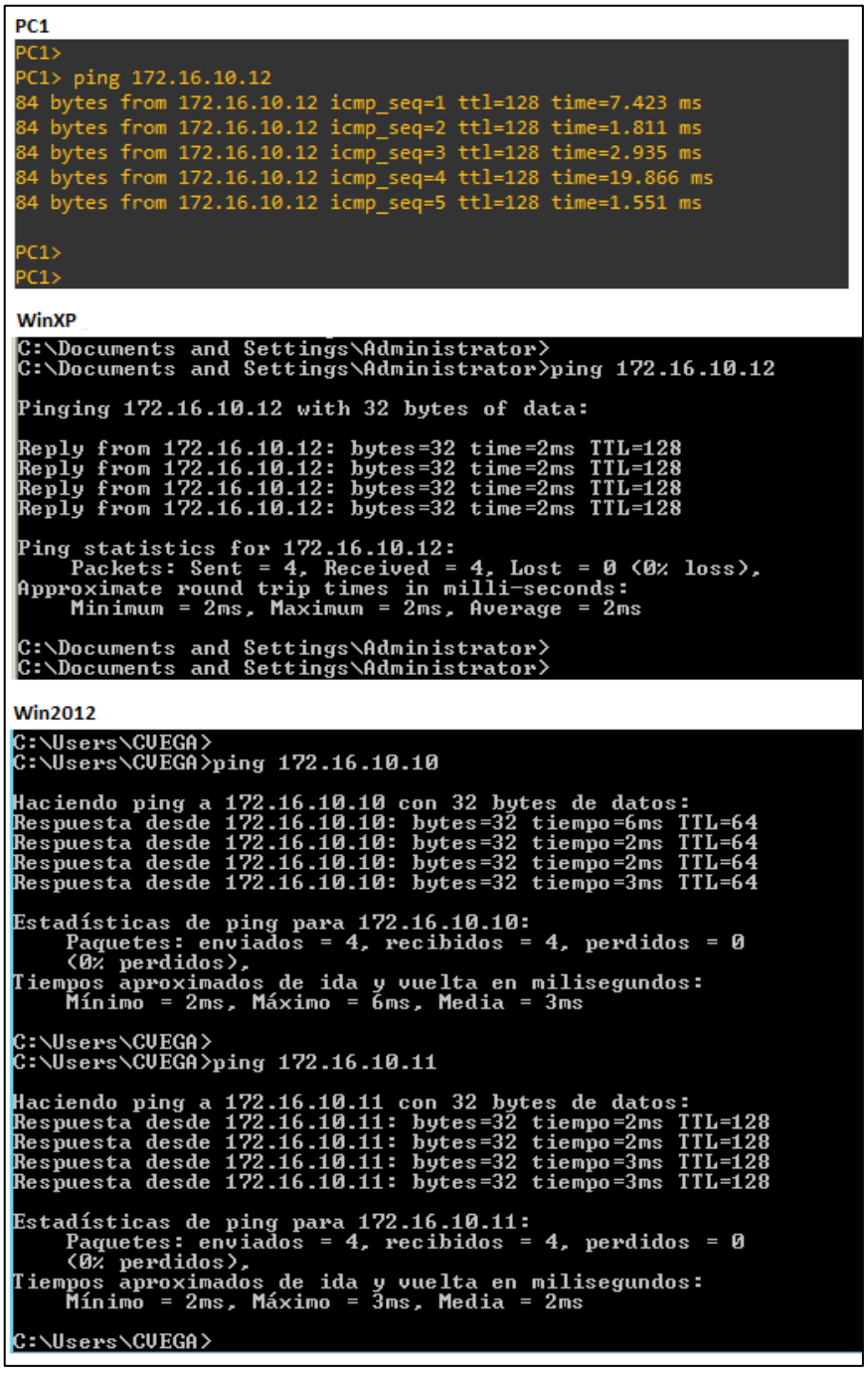


Figura N° 69: Ping entre PC1 – WinXP – Win2012
Fuente: Elaboración propia

Las pruebas de conectividad hacia el acceso a Internet desde las máquinas virtuales de la oficina principal se pueden observar en la Figura N° 70-72.

```
PC1>
PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=125 time=163.029 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=125 time=136.415 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=125 time=134.948 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=125 time=125.303 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=125 time=137.992 ms

PC1> trace 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   172.16.10.1   5.182 ms  9.893 ms  9.095 ms
 2   172.16.1.1   20.760 ms  20.727 ms  20.646 ms
 3   20.20.1.1   43.148 ms  30.393 ms  42.254 ms
 4   192.168.126.2   42.020 ms  43.176 ms  42.159 ms
 5     *  *  *
 6     *  *  *
 7     *  *  *
 8     *  *  *

PC1> ping www.google.com
www.google.com resolved to 142.250.64.164
84 bytes from 142.250.64.164 icmp_seq=1 ttl=125 time=135.125 ms
84 bytes from 142.250.64.164 icmp_seq=2 ttl=125 time=116.790 ms
84 bytes from 142.250.64.164 icmp_seq=3 ttl=125 time=114.066 ms
84 bytes from 142.250.64.164 icmp_seq=4 ttl=125 time=116.907 ms
84 bytes from 142.250.64.164 icmp_seq=5 ttl=125 time=116.425 ms

PC1>
PC1>
```

Figura N° 70: Ping hacia Internet – PC1
Fuente: Elaboración propia

```
C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=141ms TTL=125
Reply from 8.8.8.8: bytes=32 time=140ms TTL=125
Reply from 8.8.8.8: bytes=32 time=134ms TTL=125
Reply from 8.8.8.8: bytes=32 time=132ms TTL=125

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 132ms, Maximum = 141ms, Average = 136ms

C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     8 ms    10 ms    10 ms  172.16.10.1
  2    11 ms    21 ms    21 ms  172.16.1.1
  3    26 ms    33 ms    32 ms  20.20.1.1
  4    33 ms    42 ms    44 ms  192.168.126.2
  5    34 ms    42 ms    44 ms  192.168.0.1
  6    54 ms    53 ms    53 ms  10.141.64.1
  7    53 ms    53 ms    53 ms  10.150.144.153
  8    45 ms    53 ms    53 ms  10.95.156.46
  9   124 ms   130 ms   129 ms  72.14.202.206
 10   146 ms   153 ms   140 ms  108.170.253.1
 11   134 ms   127 ms   129 ms  216.239.51.215
 12   131 ms   139 ms   139 ms  dns.google [8.8.8.8]

Trace complete.

C:\Documents and Settings\Administrator>
C:\Documents and Settings\Administrator>ping www.youtube.com

Pinging youtube-ui.l.google.com [172.217.8.78] with 32 bytes of data:

Reply from 172.217.8.78: bytes=32 time=126ms TTL=125
Reply from 172.217.8.78: bytes=32 time=126ms TTL=125
Reply from 172.217.8.78: bytes=32 time=144ms TTL=125
Reply from 172.217.8.78: bytes=32 time=121ms TTL=125

Ping statistics for 172.217.8.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 121ms, Maximum = 144ms, Average = 129ms

C:\Documents and Settings\Administrator>_
```

Figura N° 71: Ping hacia Internet – WinXP
Fuente: Elaboración propia

Figura N° 72: Ping hacia Internet – Win2012
Fuente: Elaboración propia

De esta forma se comprueba la conectividad interna entre dispositivos y el servicio de internet, funcionalidad principal para la gestión de la red a través del OpManager. En la sucursal, las pruebas de conectividad se basaron en el acceso a Internet a través de su propio circuito, también se validó el servicio de la red MPLS el cual llega hacia la oficina principal y en especial al servidor de aplicaciones, dicho tráfico al pasar por la red MPLS va etiquetada comprobando la operatividad de las mismas.

En la siguiente Figura N° 73, se pueden observar el ping de respuesta entre la PC1 y la PC2.

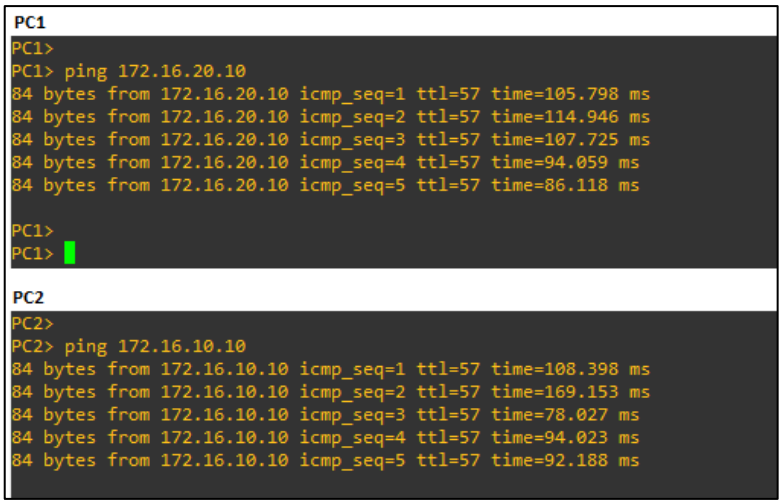


Figura N° 73: Ping entre PC1 y PC2
Fuente: Elaboración propia

En la Figura N° 74, se puede apreciar el ping de respuesta entre la PC2 y el servidor Windows Server 2012.

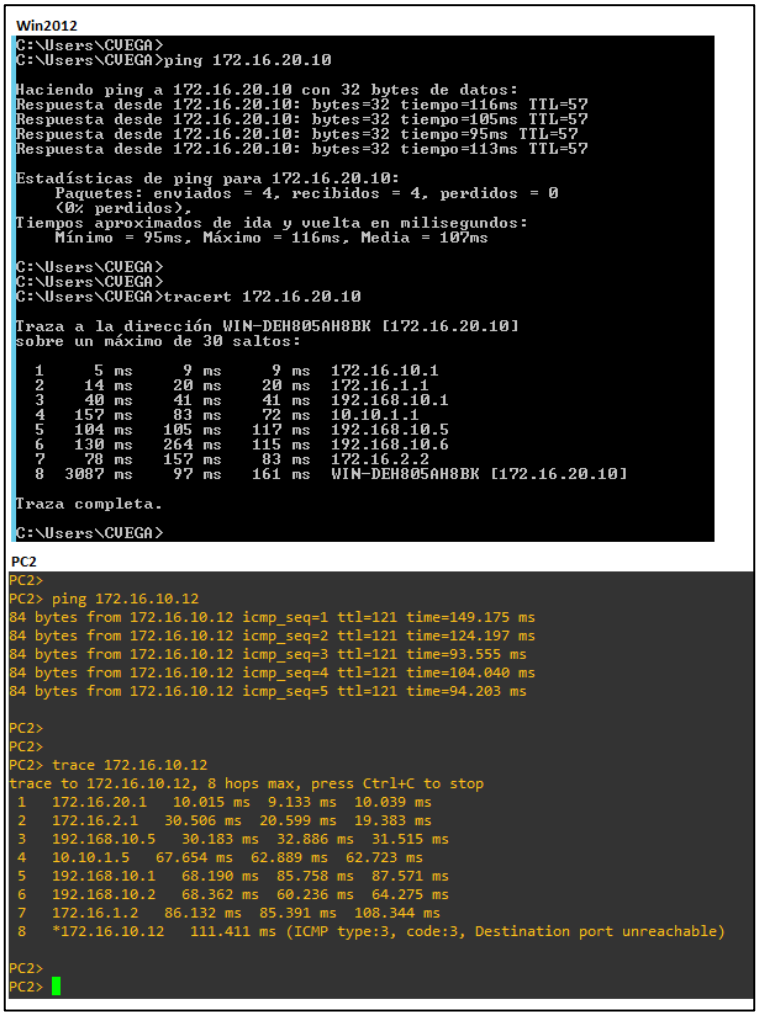


Figura N° 74: Ping entre PC2 y el servidor Win2012
Fuente: Elaboración propia

La operatividad de la red MPLS se puede apreciar en la Figura N° 75, realizado entre el Core 1 y el Core 2.

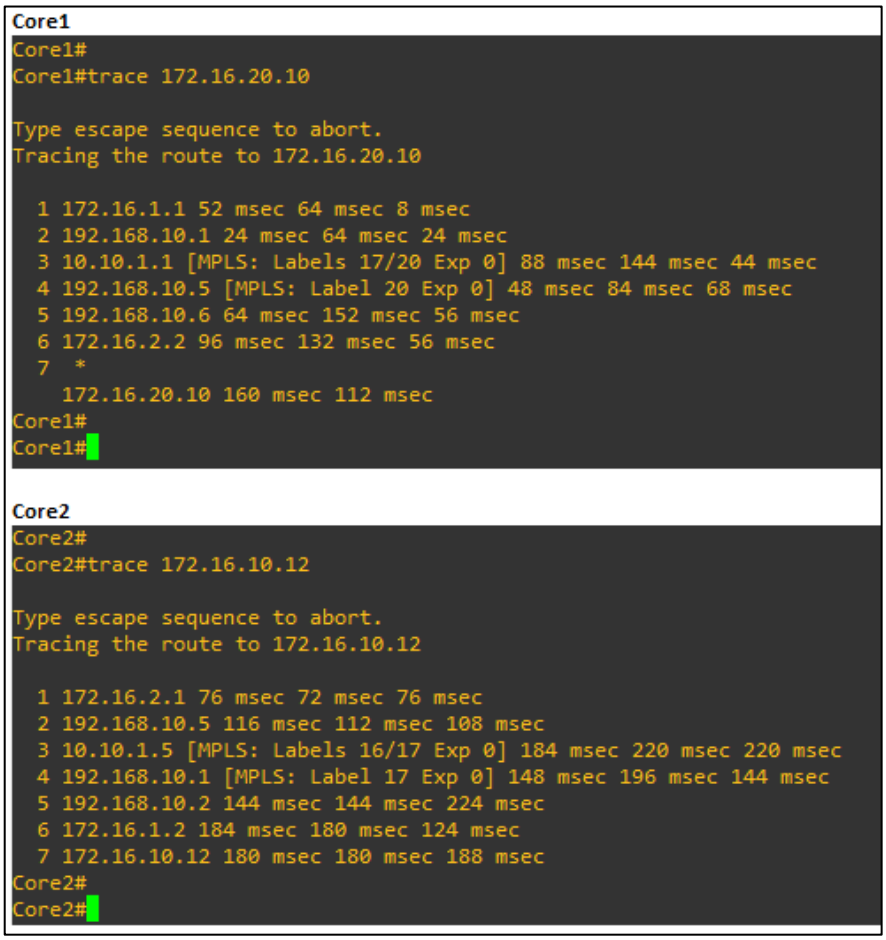


Figura N° 75: Trace entre el Core1 y el Core2
Fuente: Elaboración propia

Y para complementar en lo que respecta a la red MPLS, se muestra la tabla que se obtiene en el IP CEF (*Cisco Express Forwarding*), donde se pueden ver las entradas los cuales permiten mejorar el rendimiento de conmutación de la red (véase en la Figura N° 76).

CE1

```
CE1#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           20.20.1.1           FastEthernet1/0
0.0.0.0/32          receive
20.20.1.0/30        attached            FastEthernet1/0
20.20.1.0/32        receive
20.20.1.1/32        20.20.1.1           FastEthernet1/0
20.20.1.2/32        receive
20.20.1.3/32        receive
172.16.1.0/24       attached            FastEthernet0/1
172.16.1.0/32       receive
172.16.1.1/32       receive
172.16.1.2/32       172.16.1.2          FastEthernet0/1
172.16.1.255/32     receive
172.16.2.0/24       192.168.10.1        FastEthernet0/0
172.16.10.0/24      172.16.1.2          FastEthernet0/1
172.16.20.0/24      192.168.10.1        FastEthernet0/0
192.168.10.0/30     attached            FastEthernet0/0
192.168.10.0/32     receive
192.168.10.1/32     192.168.10.1        FastEthernet0/0
192.168.10.2/32     receive
192.168.10.3/32     receive
192.168.126.0/24    20.20.1.1           FastEthernet1/0
224.0.0.0/4         drop
Prefix              Next Hop            Interface
224.0.0.0/24        receive
255.255.255.255/32  receive
CE1#
```

CE2

```
CE2#
CE2#show ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           20.20.1.5           FastEthernet1/0
0.0.0.0/32          receive
20.20.1.4/30        attached            FastEthernet1/0
20.20.1.4/32        receive
20.20.1.5/32        20.20.1.5           FastEthernet1/0
20.20.1.6/32        receive
20.20.1.7/32        receive
172.16.1.0/24       192.168.10.5        FastEthernet0/0
172.16.2.0/24       attached            FastEthernet0/1
172.16.2.0/32       receive
172.16.2.1/32       receive
172.16.2.2/32       172.16.2.2          FastEthernet0/1
172.16.2.255/32     receive
172.16.10.0/24      192.168.10.5        FastEthernet0/0
172.16.20.0/24      172.16.2.2          FastEthernet0/1
192.168.10.4/30     attached            FastEthernet0/0
192.168.10.4/32     receive
192.168.10.5/32     192.168.10.5        FastEthernet0/0
192.168.10.6/32     receive
192.168.10.7/32     receive
224.0.0.0/4         drop
224.0.0.0/24        receive
Prefix              Next Hop            Interface
255.255.255.255/32  receive
CE2#
```

Figura N° 76: Tabla del IP CEF de los routers Ce1 y CE2
Fuente: Elaboración propia

En la Figura N° 77 siguiente se aprecia la funcionalidad del acceso hacia internet de la PC2.

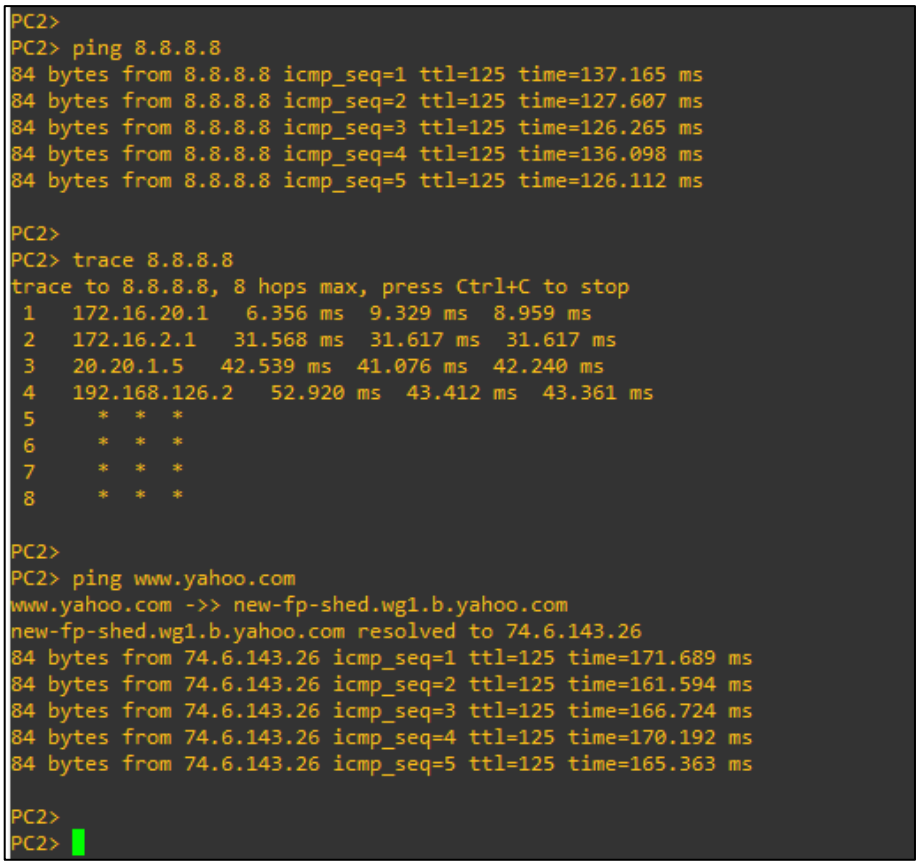


Figura N° 77: Ping hacia Internet – PC2
Fuente: Elaboración propia

Con estas validaciones de conectividad bidireccional entre ambas oficinas y el acceso hacia el servidor de aplicaciones, se procedió al desarrollo de la configuración de protocolo SNMP y NETFLOW en los dispositivos a gestionar y monitorear mediante el software OpManager.

4.2.4 Desarrollo de emulación del SNMP

a) Instalación de la plataforma de gestión centralizada - Opmanager

Esta plataforma de gestión centralizada se basó en el software Opmanager, del fabricante ManageEngine. Este software se descarga desde la página del fabricante y después se instala el ejecutable del software OpManager, este enlace nos brindó la opción de descarga para los sistemas operativos de Windows y Linux, en nuestro caso de investigación se eligió la versión para el sistema operativo Windows de 64 bits (véase en la Figura N°78), servidor que cuenta el cliente en la actualidad.

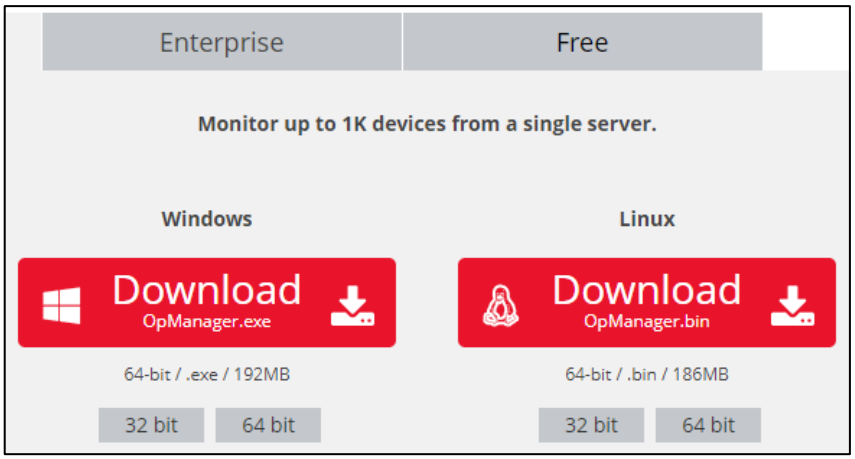


Figura N° 78: Ping hacia Internet – PC2
Fuente: https://www.manageengine.com/network-monitoring/download.html

Con el ejecutable descargado, se ejecutó la instalación en el servidor Windows 2012 R2, tal como se aprecian en las siguientes imágenes (véase Figura N° 79 y 80).

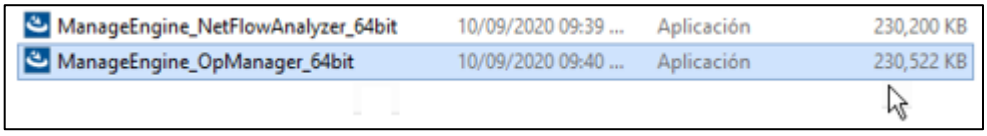


Figura N° 79: Archivo ejecutable del OpManager.
Fuente: Elaboración propia

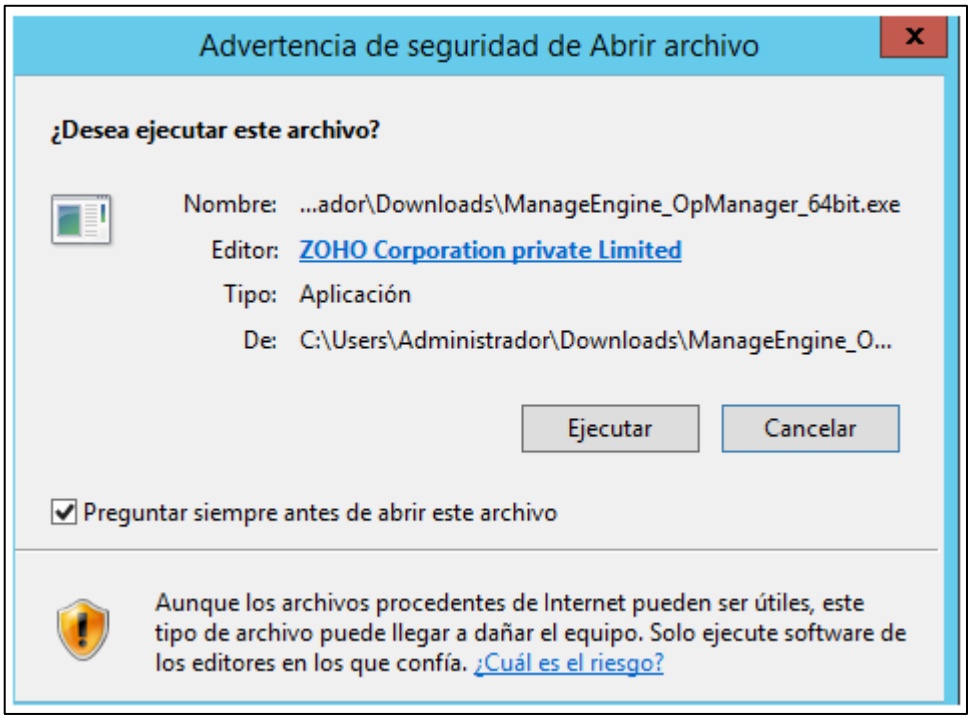


Figura N° 80: Instalación del OpManager.
Fuente: Elaboración propia

Entre los pasos más importantes dentro de la instalación del OpManager mencionaremos la validación del espacio de almacenamiento recomendado por el

fabricante, la designación del puerto para el Web Server, el puerto UDP para el módulo del Flowanalysis así como también la elección de la base de datos como se describió anteriormente en las funcionalidades del OpManager viene con la base de datos embebida del modelo PostgreSQL (véase Figura N° 81-84).

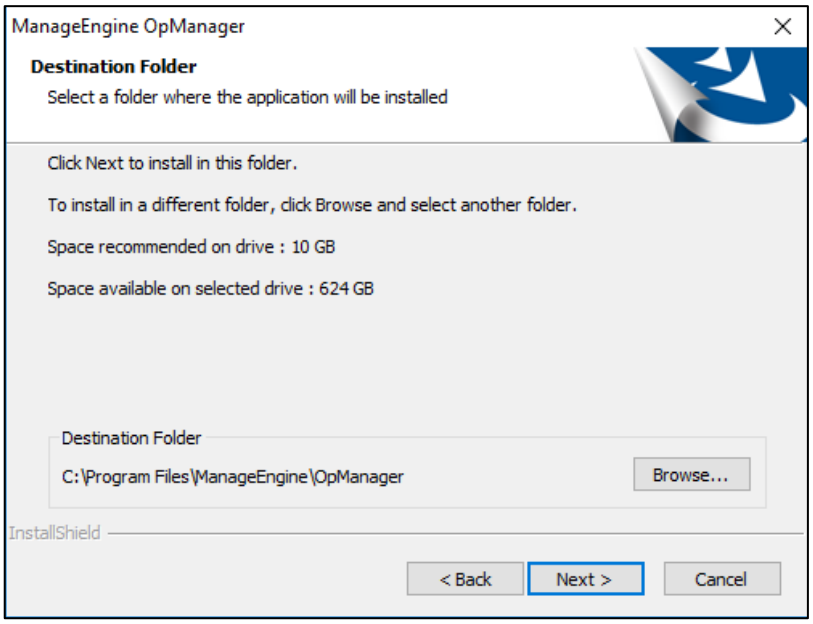


Figura N° 81: Validación del espacio de almacenamiento.
Fuente: Elaboración propia

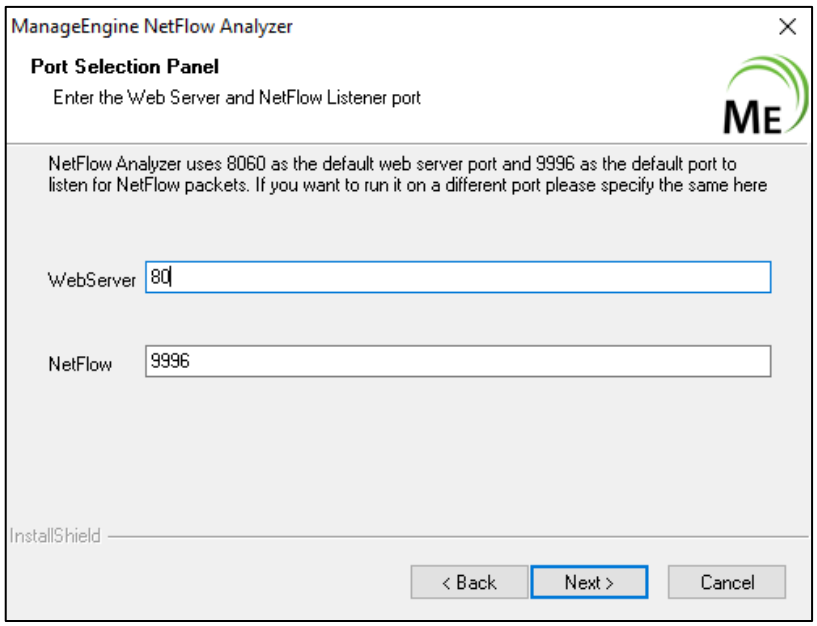


Figura N° 82: Designación de puertos.
Fuente: Elaboración propia

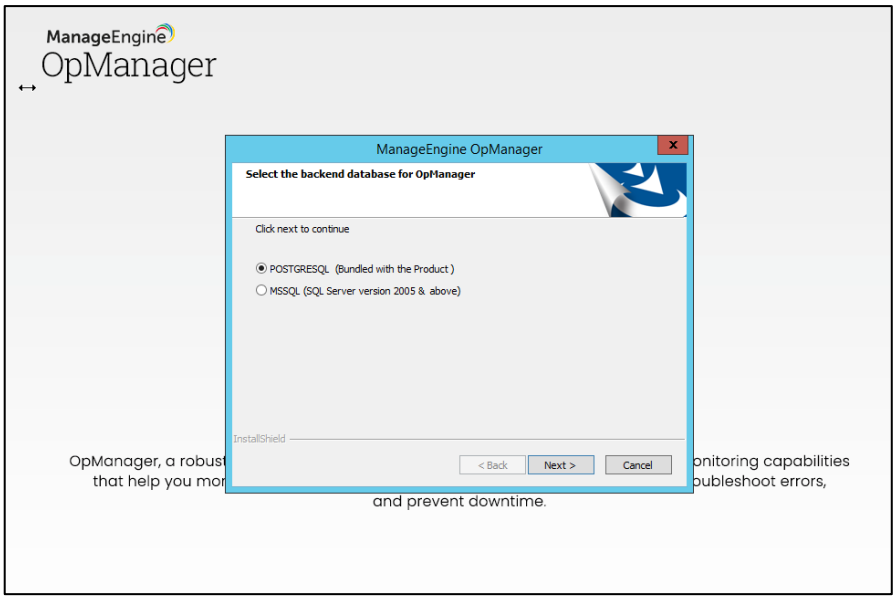


Figura N° 83: Designación de la base de datos.
Fuente: Elaboración propia

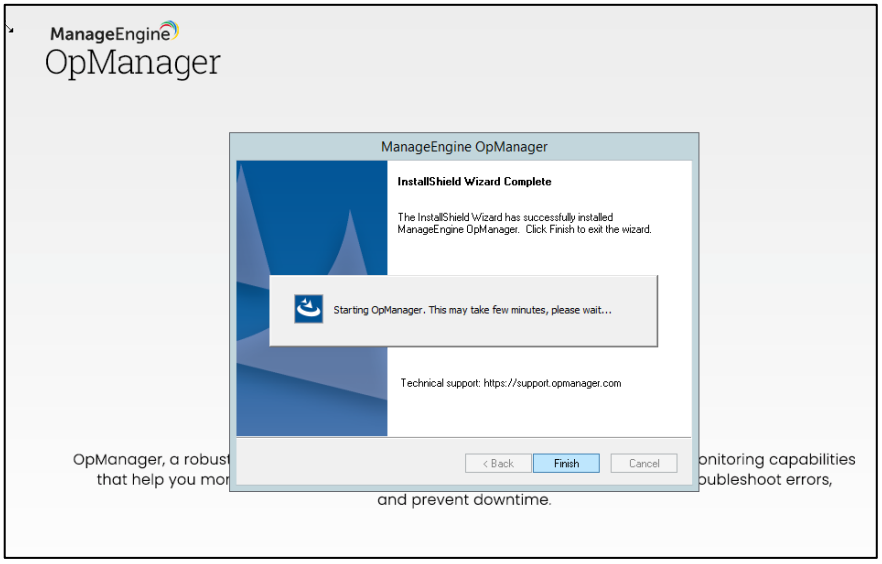


Figura N° 84: Inicialización del software.
Fuente: Elaboración propia

Finalizado el wizard de instalación, ya se tiene acceso al OpManager con los accesos por default los cuales pueden ser cambiados posteriormente. Los servicios relacionados al OpManager se ejecutaron automáticamente y una vez inicializado se muestra el browser de administración tal como se observó en la siguiente imagen (véase Figura N° 85).

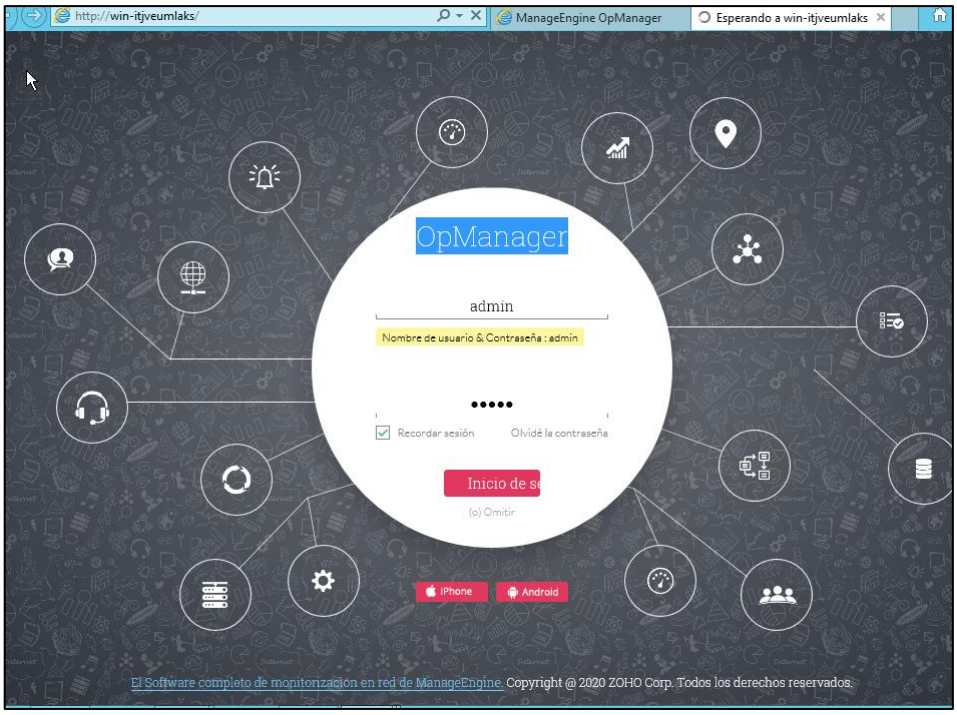


Figura N° 85: Browser del OpManager.
Fuente: Elaboración propia

En la primera vez de acceso al OpManager se visualizó que el software muestra solo al dispositivo del servidor con la dirección IP 172.16.10.12 (véase Figura N° 86). Esto puede cambiar de acuerdo a como el software vaya descubriendo a los demás dispositivos.

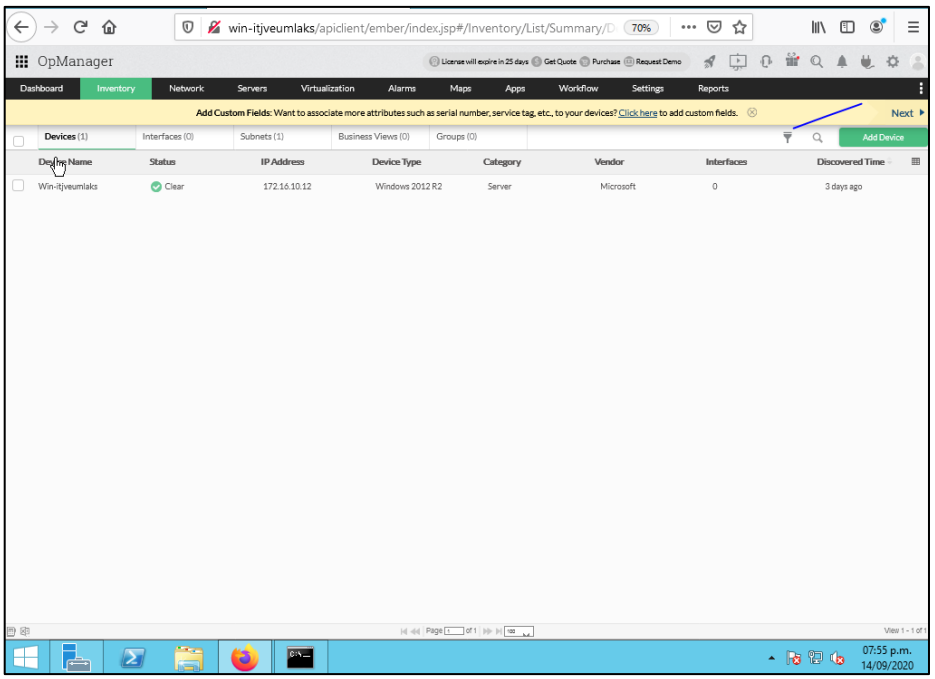


Figura N° 86: Ingreso al OpManager.
Fuente: Elaboración propia

b) Configuración del SNMP en los equipos de red

La configuración del protocolo SNMP se realizó en 2 equipos tanto de la oficina principal como de la sucursal, estos equipos envían la data al servidor de aplicaciones que en este caso es el Windows 2012 con la IP asignada 172.16.10.12.

La versión del SNMP es la versión 2, la comunidad de nombre "public" con los permisos de lectura y escritura, con este protocolo se obtuvo la funcionalidad de consultar y monitorear el hardware de dichos equipos, así como también del software. Con los comandos que se muestran en la Figura N° 87, consultados en la página del fabricante (Cisco SNMP) nos permitió obtener información referida al ancho de banda, el estado del disco, memoria y CPU, y una de las causas principales de las que no se tiene información actualmente es lo referido al fallo de equipos que se dan.

CE1

```
!
snmp-server community public RW
snmp-server ifindex persist
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server host 172.16.10.12 mri  ipsla
snmp-server host 172.16.10.12 public  envmon
no cdp log mismatch duplex
!
```

Core1

```
!
snmp-server community public RW
snmp-server ifindex persist
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server host 172.16.10.12 mri  ipsla
snmp-server host 172.16.10.12 public  envmon
no cdp log mismatch duplex
!
```

Figura N° 87: Configuración SNMP – CE1 y Core1
Fuente: Elaboración propia

En la sucursal los equipos asignados fueron el router CE2 y el switch Core2, los parámetros de comunidad, permisos y versión fueron los mismos configurados en los equipos CE1 y Core1. En la siguiente Figura N° 88, se puede apreciar las configuraciones realizadas.

CE2

```
!
snmp-server community public RW
snmp-server ifindex persist
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server host 172.16.10.12 mri  ipsla
snmp-server host 172.16.10.12 public  envmon
no cdp log mismatch duplex
!
```

Core2

```
!
snmp-server community public RW
snmp-server ifindex persist
snmp-server enable traps tty
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server host 172.16.10.12 mri  ipsla
snmp-server host 172.16.10.12 public  envmon
no cdp log mismatch duplex
!
```

Figura N° 88: Configuración SNMP – CE2 y Core2
Fuente: Elaboración propia

En la Tabla N°12, se detallan los comandos utilizados:

(ManageEngin-Netflow)

Tabla 12: Comandos SNMP

Comando	Descripción
snmp-server community public rw	Comando que hace referencia a la comunidad necesaria para la autenticación del MIB y los permisos a los objetos de lectura y escritura.
snmp-server enable traps tty	Permite la habilitación de notificaciones traps del tipo tcp.
snmp-server enable traps config	Permite la habilitación de notificaciones traps del tipo config.
snmp-server enable traps entity	Permite la habilitación de notificaciones traps del tipo entity.
snmp-server enable traps cpu threshold	Permite la habilitación de notificaciones traps relacionado al cpu.
snmp-server host (IP Server) version 2c public	Este comando hace referencia a la IP del host que recepcionara la información que se defina, la versión del SNMP a utilizar y el nombre de la comunidad.

snmp-server host (IP Server) traps public	Este comando hace referencia que los mensajes TRAPS serán enviados a la IP del host y a la comunidad respectiva.
snmp-server ifindex persist	La función proporciona un valor de índice de interfaz. El valor de ifIndex es un número de identificación único asociado con una interfaz física o lógica.
snmp-server host (IP Server) public envmon	La función de este comando hace referencia al monitoreo del medio de los mensajes traps.

Fuente: Elaboración propia

Con el comando “show snmp”, se pudo visualizar la información del SNMP, el contador de estado y la cadena de identificación del chasis. (véase Figura N° 89)

```
Core1#
Core1#show snmp
Chassis: FTX0945W0MY
170 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    439 Number of requested variables
    0 Number of altered variables
    8 Get-request PDUs
    162 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
170 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    170 Response PDUs
    0 Trap PDUs
SNMP Trap Queue: 0 dropped due to resource failure.

SNMP logging: enabled
    Logging to 172.16.10.12.162, 0/10, 0 sent, 0 dropped.
Core1#
```

Figura N° 89: Muestra del estado del SNMP
Fuente: Elaboración propia

SNMP es un protocolo importante en cualquier entorno de red, que fue útil para monitorizar los equipos ubicados en las diferentes oficinas de la empresa por el cual sus funciones son notificar alertas que ocurran en el dispositivo para que el administrador de TI pudiera dar una solución a la mayor brevedad posible.

c) Configuración del OpManager

-MENU INVENTORY: Descubrimiento de dispositivos:

Una vez instalado el software de monitoreo y gestión ManageEngine – Opmanager, los dispositivos (router – switch) que apuntan al servidor se descubrirán automáticamente (véase Figura 90), dado que la configuración de protocolo SNMP ya se realizó en los dispositivos.

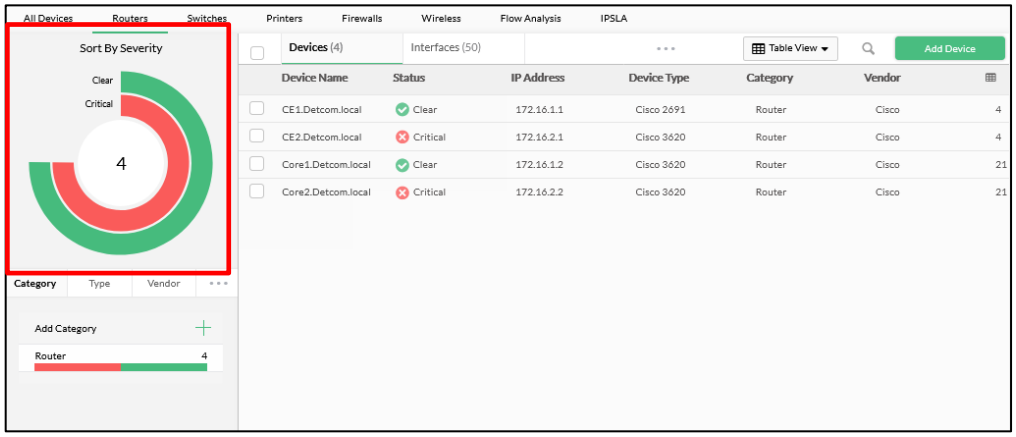


Figura N° 90: Inventory – Devices – Agregación automática de equipos.
Fuente: Elaboración propia

Sin embargo, hubo dispositivos que no aparecieron en la lista cuando se inicializó el Opmanager. En este caso tuvimos que agregar de forma manual como se muestra en el siguiente detalle de la Figura 91.

Paso 1: Se realizó click en "Add devices" para agregar el dispositivo a monitorear.

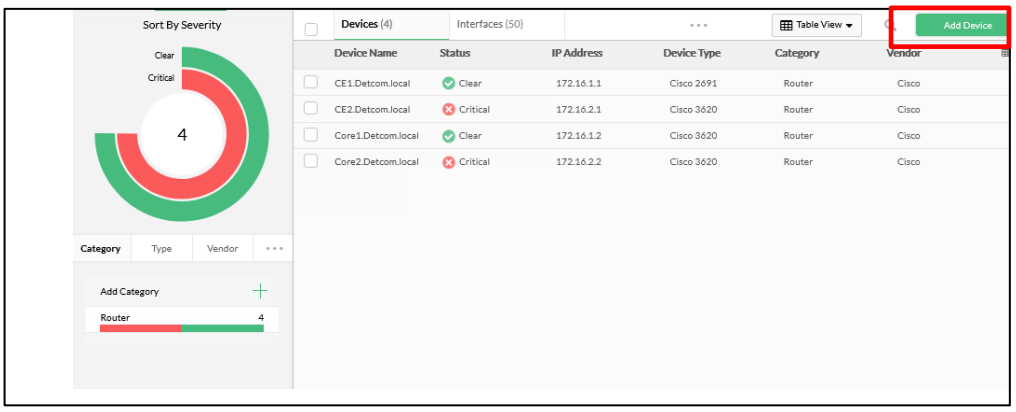


Figura N° 91: Inventory – Devices – Agregación manual de equipos.
Fuente: Elaboración propia

Paso 2: Se agregó la IP del dispositivo a monitorear y las credenciales del SNMP como se muestra en la Figura N° 92:

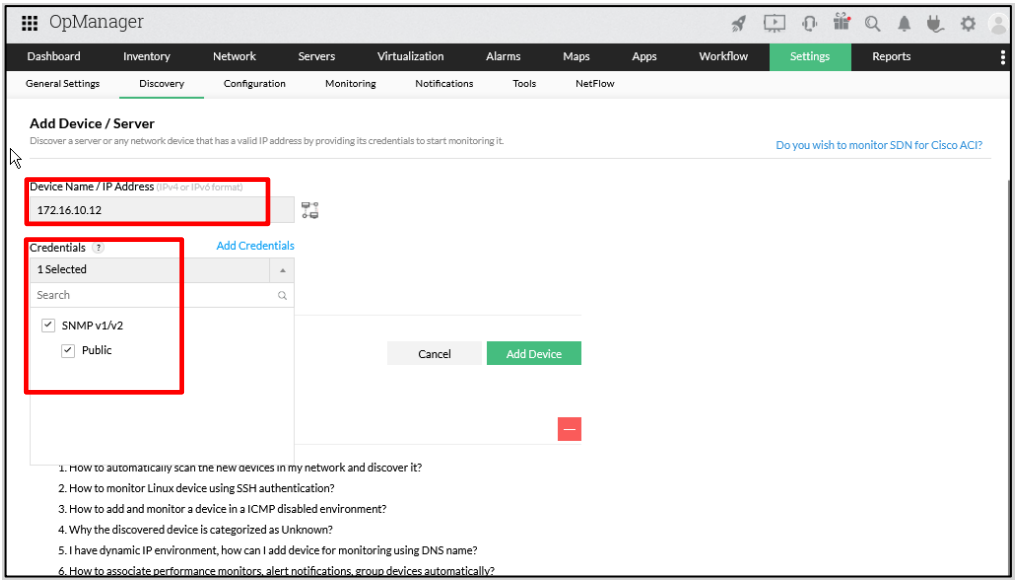


Figura N° 92: Inventory – Devices – Agregación manual de equipos.
Fuente: Elaboración propia

Paso 3: Una vez ingresado la IP y credenciales, se volvió a dar click en "add device" y se esperó mientras el dispositivo se descubre en el sistema (véase Figura N° 93 - 94).

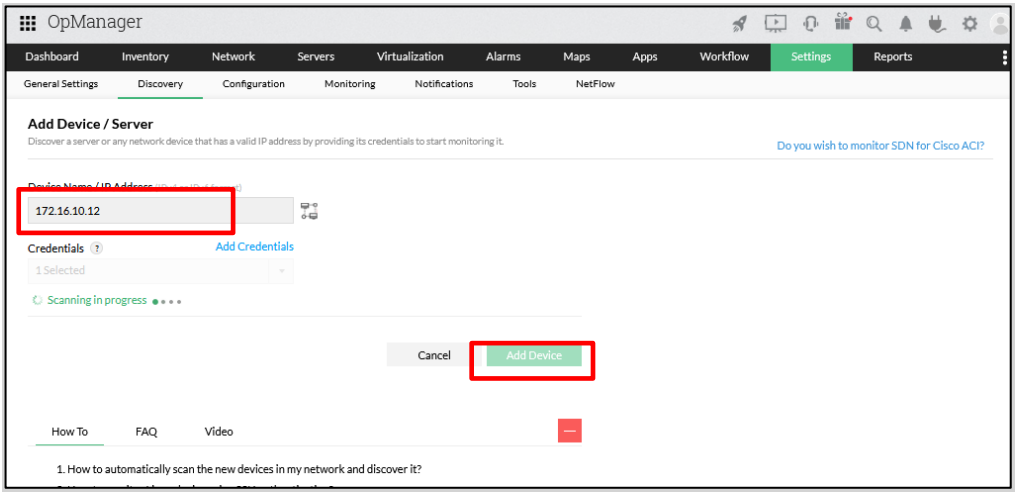


Figura N° 93: Inventory – Devices – Agregación manual de equipos.
Fuente: Elaboración propia

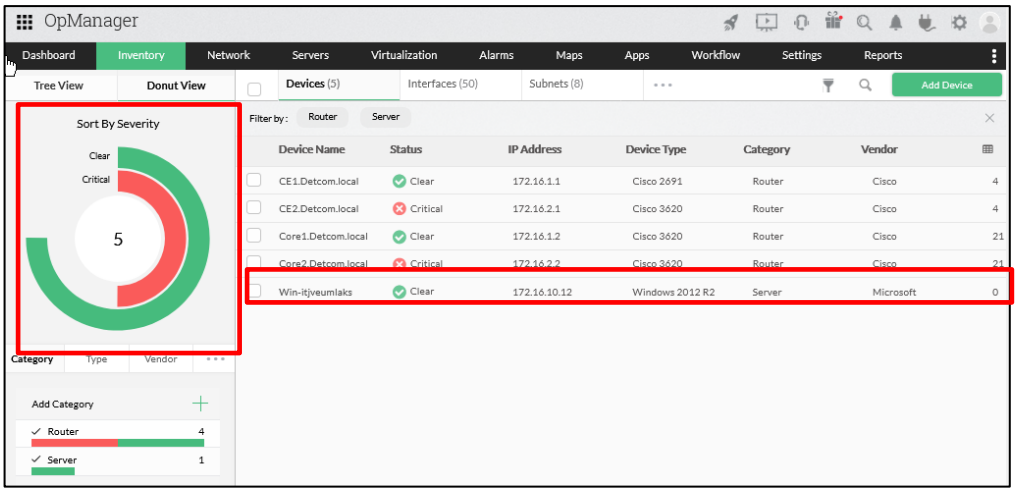


Figura N° 94: Inventory – Devices – Agregación manual de equipos.
Fuente: Elaboración propia

Paso 4: Cuando el dispositivo se descubrió, se mostró la información en device summary. Este nos brindó la información a detalle de este como: IPAdress, DNS name, manufacturer, serial number, type, vendor, system description (véase Figura N° 95).

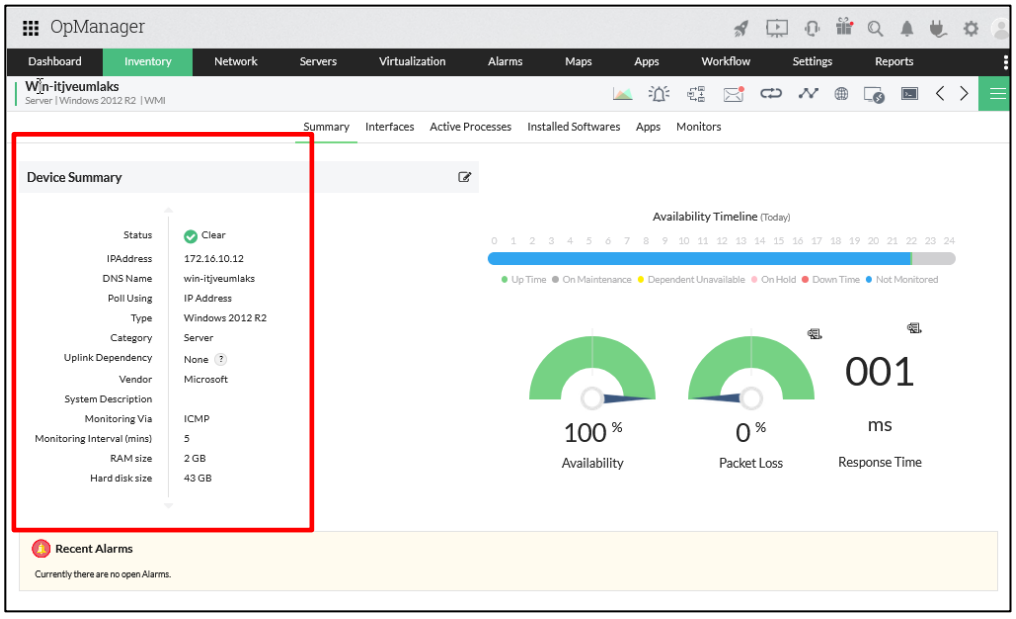


Figura N° 95:Inventory – Devices – Agregación manual de equipos.
Fuente: Elaboración propia

Paso 5: Adicionalmente, se observó que aparecieron monitores en custom dials, los cuales nos brindaron detalles como la salud del equipo (CPU, DISK y memoria) como se muestra en las Figura N° 96.

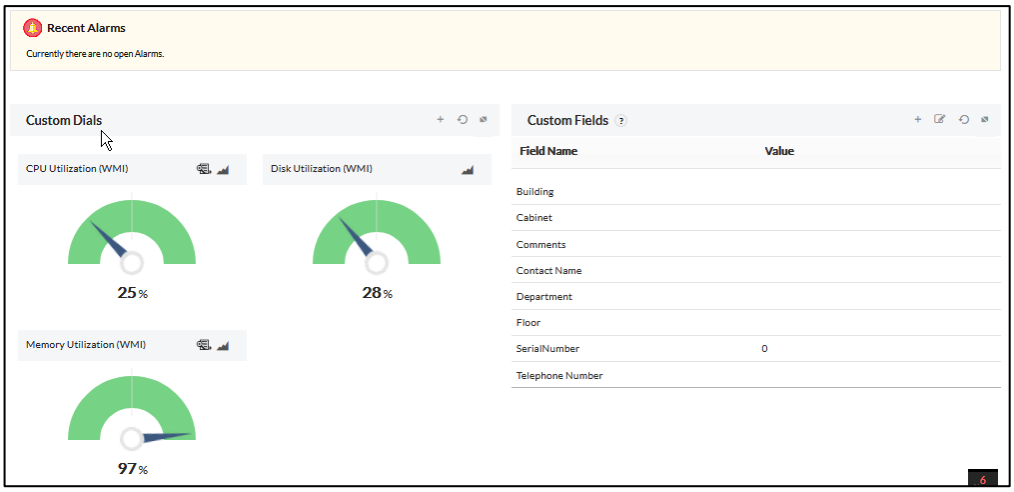


Figura N° 96: Agregación manual de equipos.
Fuente: Elaboración propia

d) Funcionalidades del Opmanager

-FILTRO POR ALERTA

Una vez registrados los equipos en el Opmanager se observó las funciones que están activas como el "Sort by severity", Figura N° 97, el cual nos mostró diferentes tipos de alertas las cuales están activas en la red.

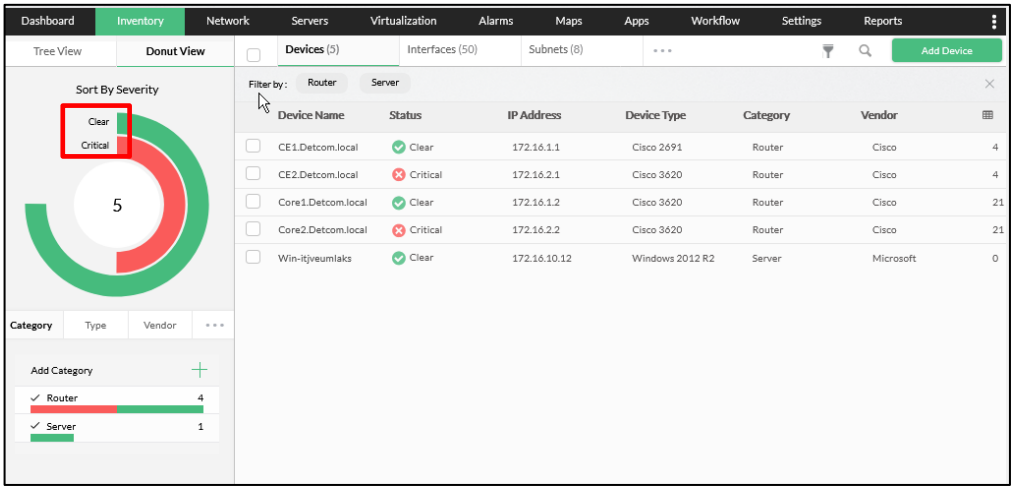


Figura N° 97: Filtro por alerta – Sort by severity – Alertas activas
Fuente: Elaboración propia

Desde esta opción, pudimos filtrarlo por el tipo de alerta como se pudo observar en la Figura N° 98. donde filtramos alarmas de tipo critical activas en la red

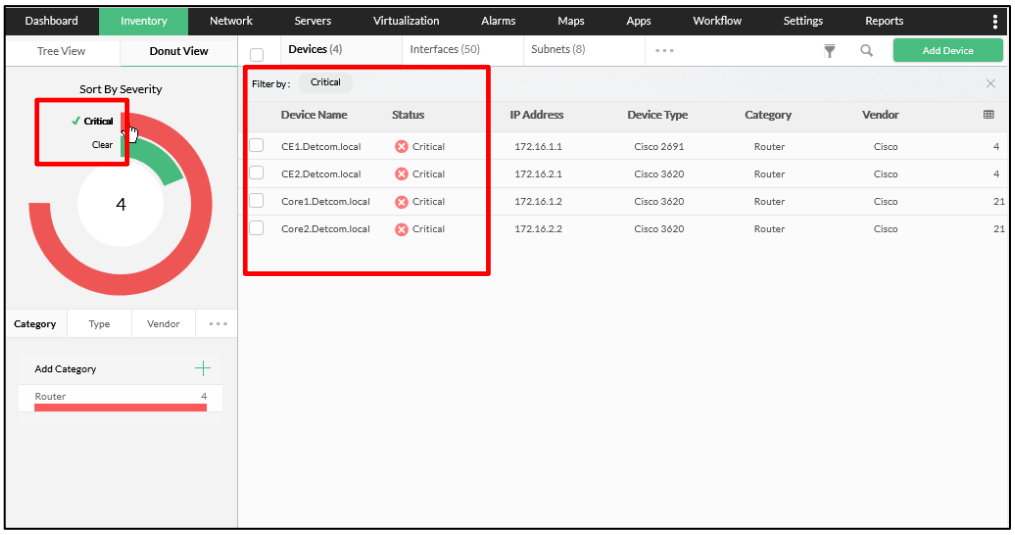


Figura N° 98: Filtro por alerta – Sort by severity – alarmas critical activas de la red
Fuente: Elaboración propia

-FILTRO POR TIPO

Para este filtro se observó que se puede elegir la lista por devices, interfaces, subnets, business views y groups como se muestra en la Figura N° 99.

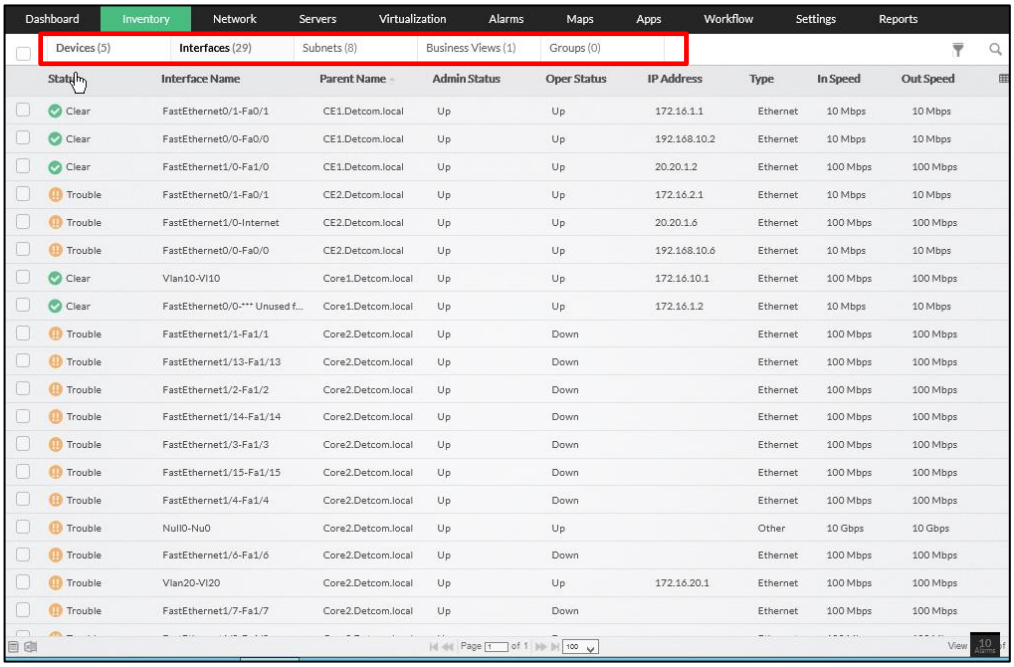


Figura N° 99: Filtro por tipo – Interfaces
Fuente: Elaboración propia

-MENU DASHBOARD:

Configuración de vistas y monitoreo, en esta opción dashboard Figura N° 100 se pudo configurar distintas vistas de manera personalizada, la cual nos permitió observar información puntual de los dispositivos de la red LAN.

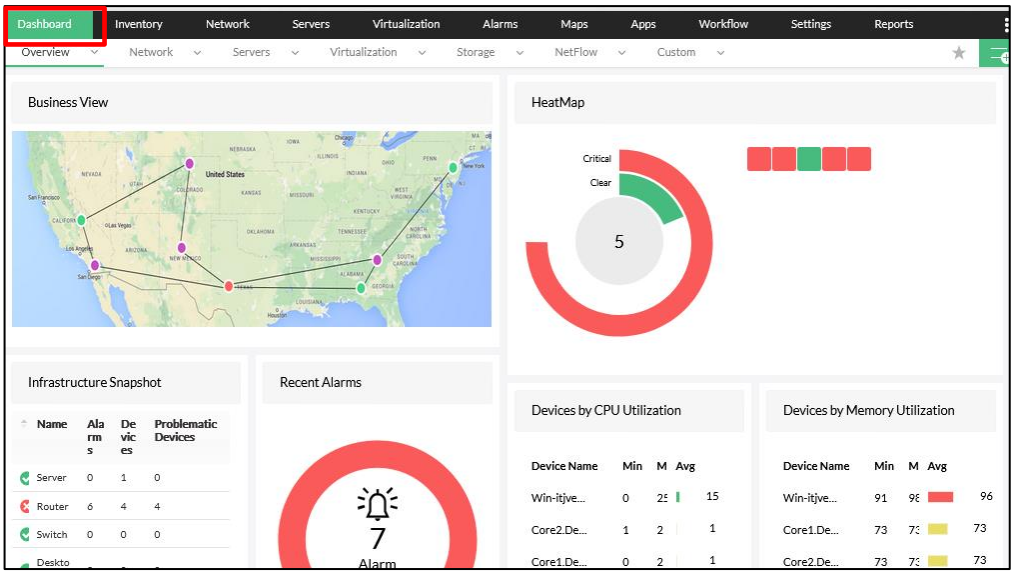


Figura N° 100: Menu dashboard - configuración
Fuente: Elaboración propia

-MAPA Y BUSINES VIEW

En esta opción de Maps pudimos ubicar geográficamente las sedes como se observa en la Figura N°101

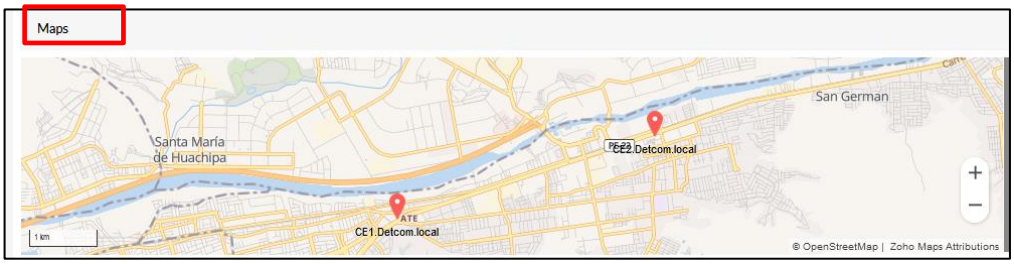


Figura N° 101- Menu dashboard - Mapa
Fuente: Elaboración propia

También, pudimos agregar las vistas business view personalizadas (véase la Figura N° 102) como la topología lógica de la red.

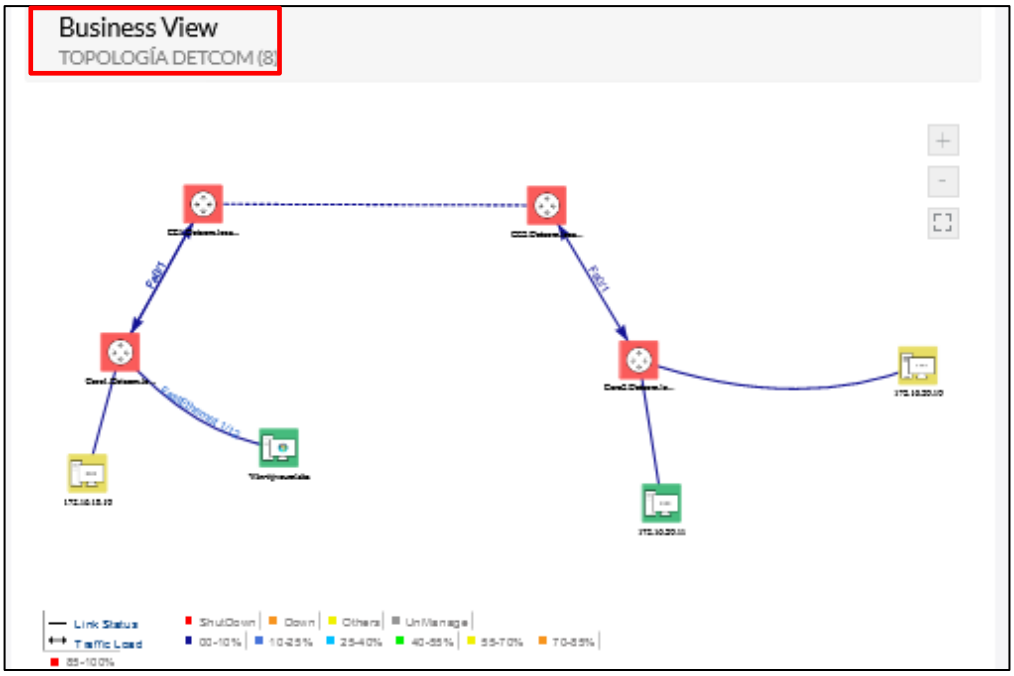


Figura N° 102: Menu dashboard – Business view
Fuente: Elaboración propia

-HEATMAP

En esta función se visualizó todos los dispositivos y si alguno de ellos se encontraba alarmado como se puede apreciar en la Figura N° 103.

Estado de alarmas:

Verde: Libre de Alarmas.

Amarillo: Alarma de atención o primera alerta, no son críticas.

Naranja: Alarma de Trouble o segunda alerta, indica que es necesario revisar debido a que puede generarse una alerta critica.

Rojo: Alarma Critica, representa el envío de alarmas que afectan gravemente la salud del equipo.

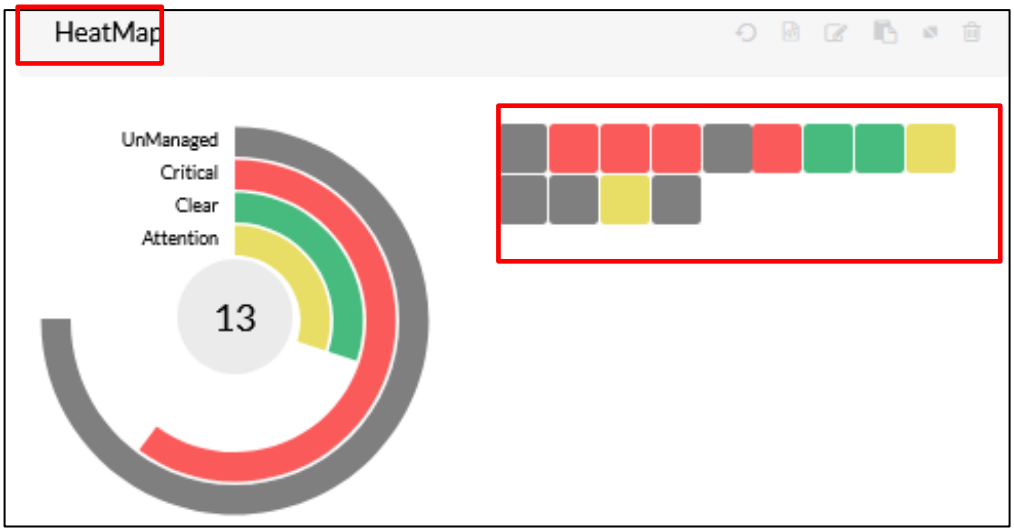


Figura N° 103: Menu dashboard – HeatMap
Fuente: Elaboración propia

-MONITORES – DEVICES BY CPU UTILIZATION

En esta función se agregó este monitor Figura N°104 el cual nos permitió ver el top de dispositivos monitoreados con mayor consumo de CPU.

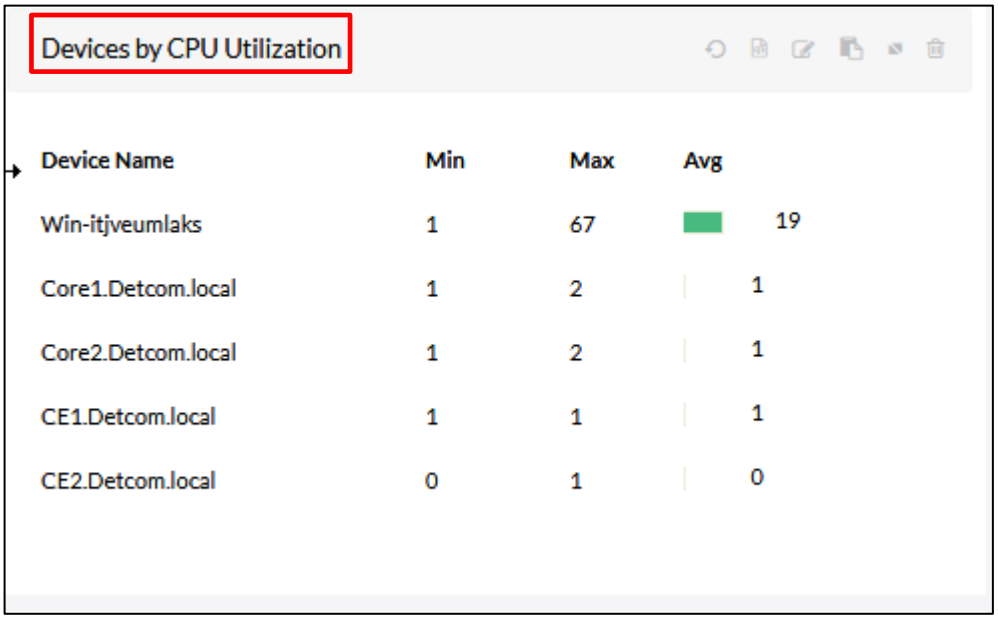


Figura N° 104:Menu dashboard – Monitores – Devices by CPU utilization
Fuente: Elaboración propia

-MONITORES – DEVICES BY MEMORY UTILIZATION

Mediante este monitor Figura N° 105 podemos ver el top de dispositivos monitoreados con mayor consumo de Memoria.

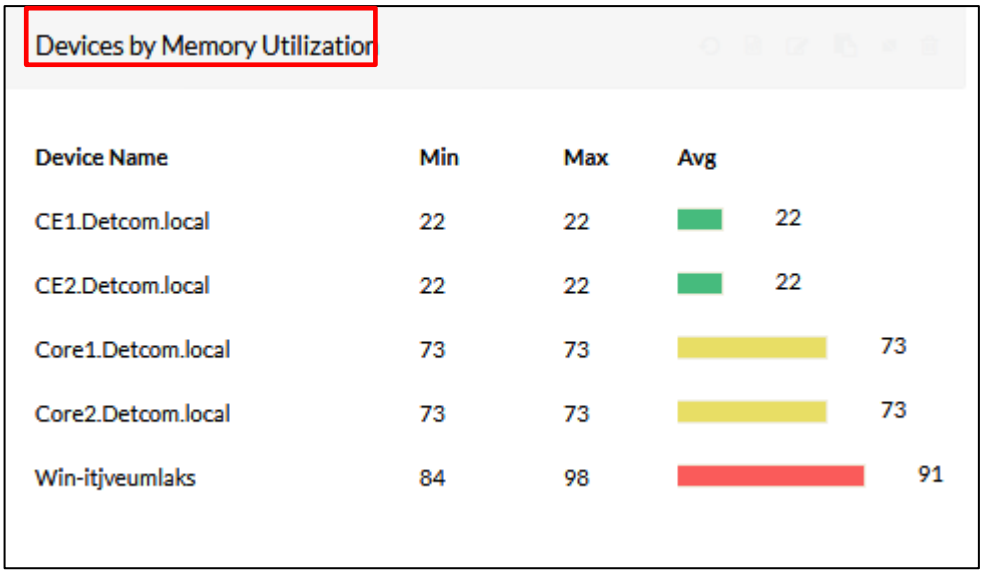


Figura N° 105: Menu dashboard – Monitores – Devices by Memory Utilization
Fuente: Elaboración propia

-MONITORES – DEVICES DOWN

Acá se observó los dispositivos caídos dentro de la red, al no tener conectividad con el servidor de monitoreo se activa la alarma de device down (véase Figura N° 106).

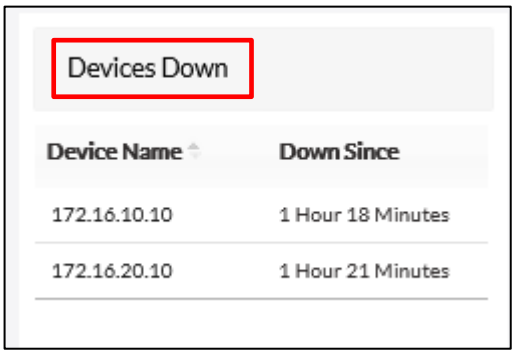
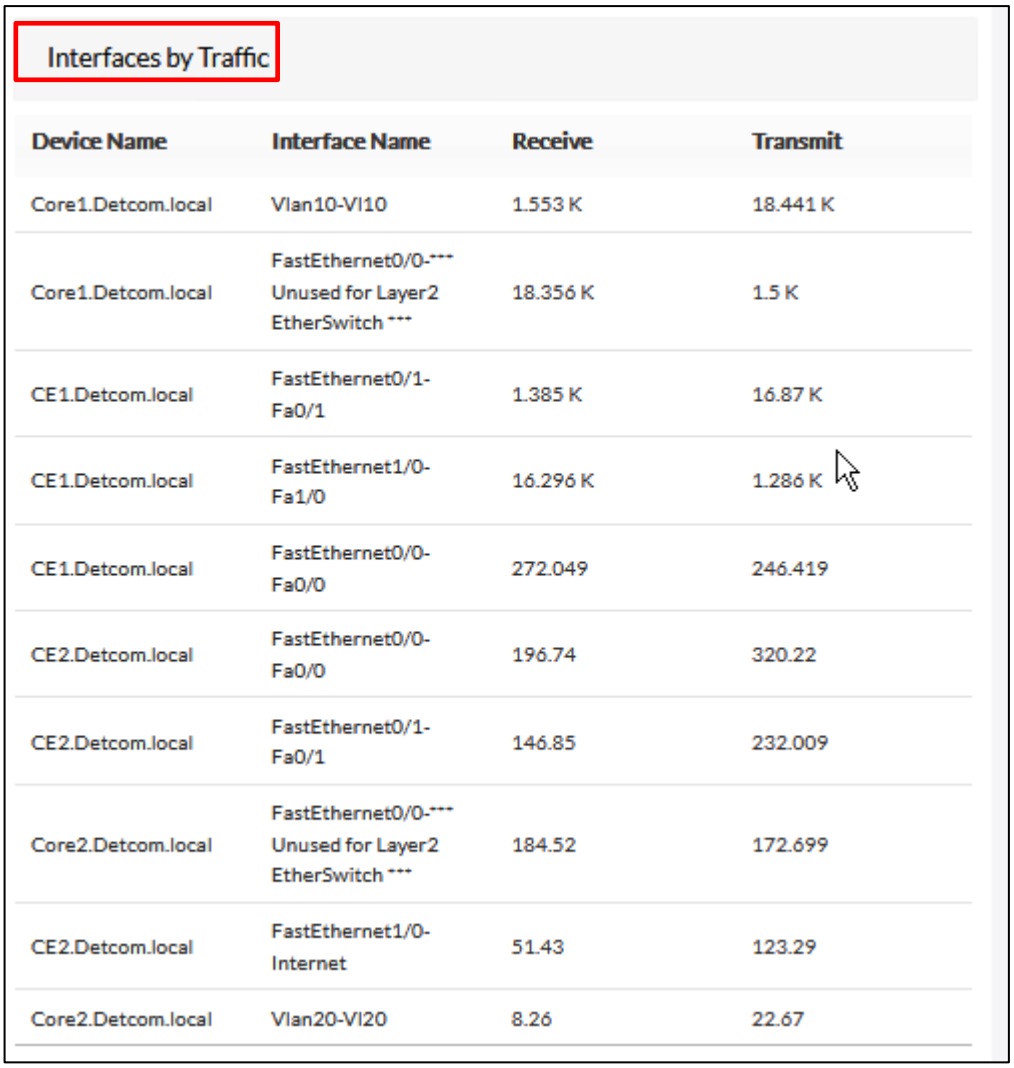


Figura N° 106: Menu dashboard – Monitores – Devices Down
Fuente: Elaboración propia

-MONITORES – INTERFACES BY TRAFFIC

Se observó la Figura N° 107 una lista del consumo de ancho de banda de las interfaces de los dispositivos monitoreados.



Interfaces by Traffic

Device Name	Interface Name	Receive	Transmit
Core1.Detcom.local	Vlan10-Vl10	1.553 K	18.441 K
Core1.Detcom.local	FastEthernet0/0-*** Unused for Layer2 EtherSwitch ***	18.356 K	1.5 K
CE1.Detcom.local	FastEthernet0/1-Fa0/1	1.385 K	16.87 K
CE1.Detcom.local	FastEthernet1/0-Fa1/0	16.296 K	1.286 K
CE1.Detcom.local	FastEthernet0/0-Fa0/0	272.049	246.419
CE2.Detcom.local	FastEthernet0/0-Fa0/0	196.74	320.22
CE2.Detcom.local	FastEthernet0/1-Fa0/1	146.85	232.009
Core2.Detcom.local	FastEthernet0/0-*** Unused for Layer2 EtherSwitch ***	184.52	172.699
CE2.Detcom.local	FastEthernet1/0-Internet	51.43	123.29
Core2.Detcom.local	Vlan20-Vl20	8.26	22.67

Figura N° 107: Menu dashboard – Monitores – Interfaces by traffic
Fuente: Elaboración propia

4.2.5 Desarrollo de emulación del NETFLOW

a) Configuración del NETFLOW en los routers

La configuración para habilitar el protocolo NETFLOW en la topología de la empresa DETCOM se realizó en los routers CE1 y CE2 ubicados en la oficina principal y en la sucursal, en los cuales se determinó realizar el monitoreo en las interfaces que van hacia la MPLS y las interfaces que dan el acceso a internet.

Para cada interfaz se configuro un flujo de exportación independiente, los exportadores se asignaron a los monitores de flujo para exportar los datos de la caché del monitor de flujo hacia el colector NetFlow que en este caso es el OpManager. Cada exportador se personalizo para cumplir con los requisitos del monitor a los que se exportan los datos.

En las siguientes imágenes (véase Figura N° 108 y 109) se presentan las configuraciones del flujo de grabación y del flujo de exportación y como se relaciona con el flujo de monitoreo. Estos comandos fueron consultados de la página del fabricante (ManageEngin-Netflow). También se configuro el muestreo aleatorio para el monitoreo de las interfaces.

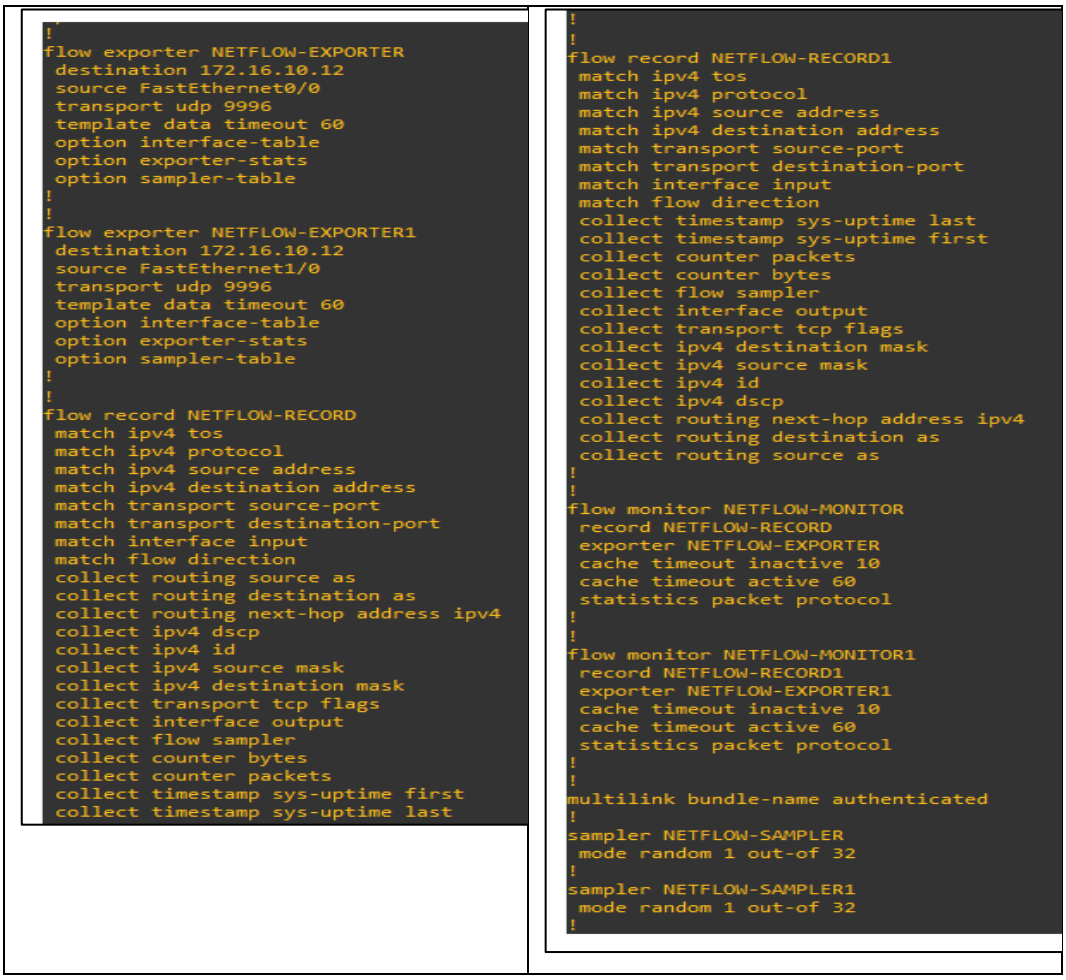


Figura N° 108: Configuración Netflow – CE1
Fuente: Elaboración propia

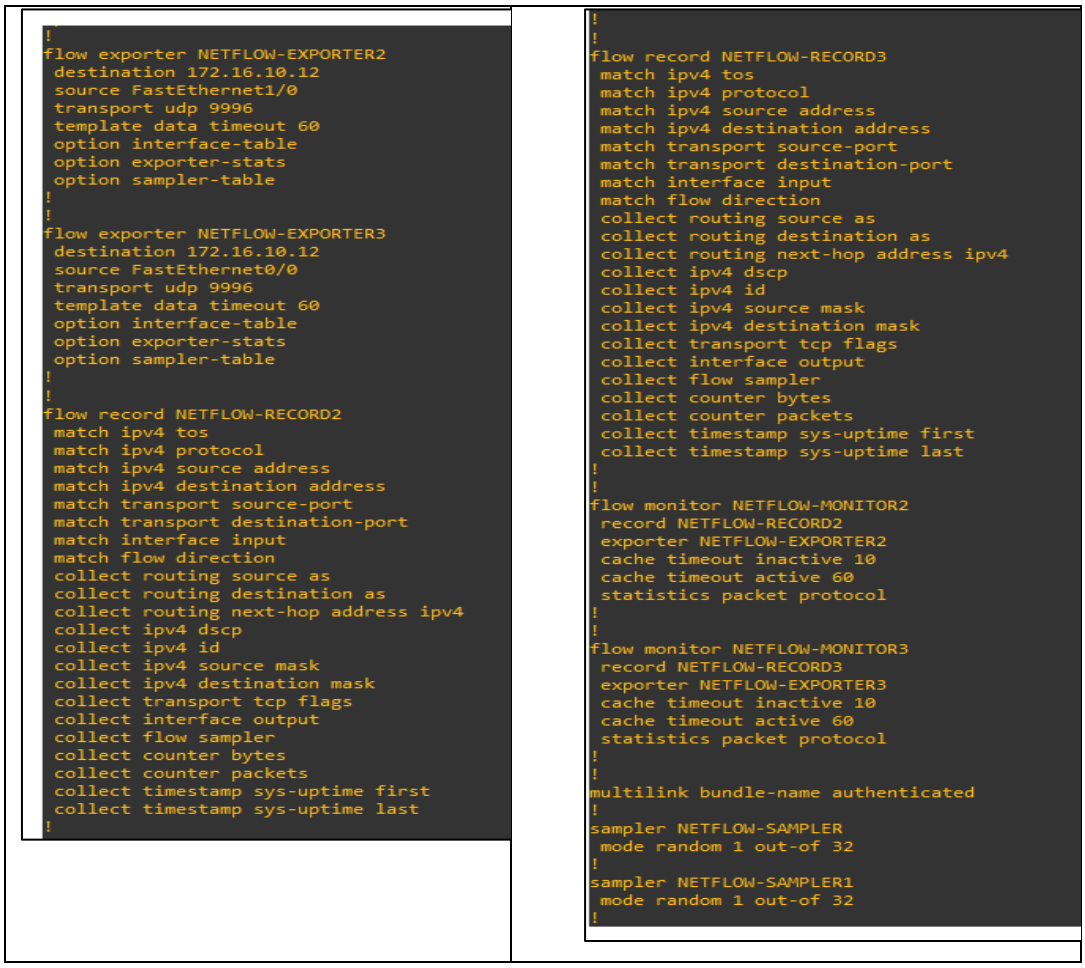


Figura N° 109: Configuración Netflow – CE2
Fuente: Elaboración propia

Con las funcionalidades de monitoreo configuradas para el protocolo NETFLOW, se procedió a la asignación en las interfaces, como se mencionó anteriormente, las interfaces a monitorear abarcan al enlace hacia la MPLS y hacia el acceso a Internet. En las siguientes imágenes se muestra la configuración realizada (véase Figura N° 110 y 111).

```
!
interface FastEthernet0/0
 ip address 192.168.10.2 255.255.255.252
 ip flow monitor NETFLOW-MONITOR sampler NETFLOW-SAMPLER input
 ip flow monitor NETFLOW-MONITOR sampler NETFLOW-SAMPLER1 output
 ip flow ingress
 ip flow egress
 speed 100
 full-duplex
!
!
interface FastEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 duplex auto
 speed auto
!
!
interface FastEthernet1/0
 description Internet
 ip address 20.20.1.2 255.255.255.252
 ip flow monitor NETFLOW-MONITOR1 sampler NETFLOW-SAMPLER input
 ip flow monitor NETFLOW-MONITOR1 sampler NETFLOW-SAMPLER1 output
 ip flow ingress
 ip flow egress
 duplex auto
 speed auto
!
```

Figura N° 110: Configuración Interfaces a monitorear – CE1
Fuente: Elaboración propia

```
!
interface FastEthernet0/0
 ip address 192.168.10.6 255.255.255.252
 ip flow monitor NETFLOW-MONITOR3 sampler NETFLOW-SAMPLER input
 ip flow monitor NETFLOW-MONITOR3 sampler NETFLOW-SAMPLER1 output
 ip flow ingress
 ip flow egress
 speed 100
 full-duplex
!
!
interface FastEthernet0/1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
!
interface FastEthernet1/0
 description Internet
 ip address 20.20.1.6 255.255.255.252
 ip flow monitor NETFLOW-MONITOR2 sampler NETFLOW-SAMPLER input
 ip flow monitor NETFLOW-MONITOR2 sampler NETFLOW-SAMPLER1 output
 ip flow ingress
 ip flow egress
 duplex auto
 speed auto
!
```

Figura N° 111: Configuración Interfaces a monitorear – CE2
Fuente: Elaboración propia

Por último, se configuro la versión del protocolo usado para el NETFLOW el cual consistió en la versión 9, la captura de longitud de paquetes, así como el destino del collector quien sería el OpManager y el puerto ya declarado en la instalación del mismo UDP 9996, tener en cuenta que estos dos últimos parámetros también se declararon en la configuración del flow exporter. (véase Figura N° 112 y 113).

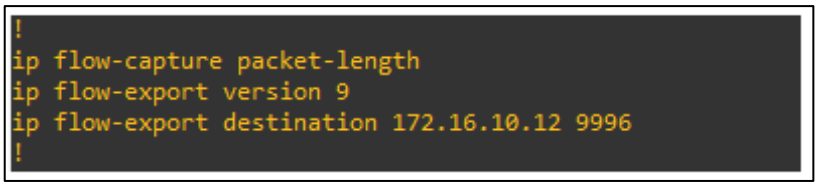


Figura N° 112: Configuración versión del NETFLOW – CE1
Fuente: Elaboración propia

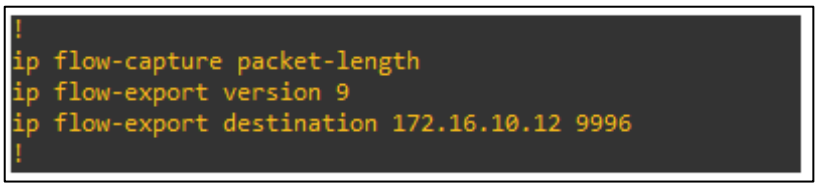


Figura N° 113: Configuración versión del NETFLOW – CE2
Fuente: Elaboración propia

Con el siguiente comando se pudo mostrar la configuración del flow exporter (véase Figura N° 114).

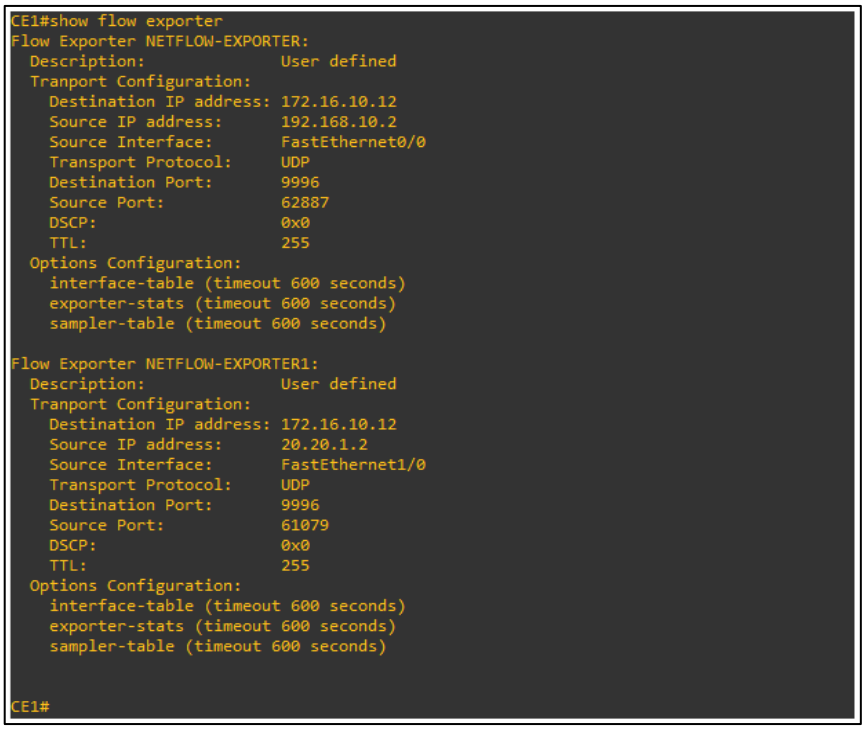


Figura N° 114: Show flow exporter – CE1
Fuente: Elaboración propia

Con el comando del *show flow monitor*, se pudo ver las instancias relacionadas al *flow record* y *flow exporter* (véase Figura N° 115).

```
CE1#show flow monitor NETFLOW-MONITOR
Flow Monitor NETFLOW-MONITOR:
  Description:       User defined
  Flow Record:       NETFLOW-RECORD
  Flow Exporter:     NETFLOW-EXPORTER
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 327700 bytes
    Inactive Timeout:  10 secs
    Active Timeout:    60 secs
    Update Timeout:    1800 secs
  Stats:
    protocol distribution

CE1#
```

Figura N° 115: Show flow monitor – CE1
Fuente: Elaboración propia

Con el siguiente comando "show ip cache verbose flow" se pudo ver el flujo estadístico detalladas en la cache: (véase Figura N° 116).

```
CE1#show ip cache verbose flow
IP packet size distribution (3916 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .421 .044 .101 .018 .008 .012 .014 .011 .007 .000 .008 .007 .001 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .000 .001 .013 .325 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 747 added
  12599 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  2 active, 1022 inactive, 1494 added, 747 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-WWW             18      0.0         2   137      0.0       1.0       9.2
TCP-BGP              1      0.0         1    44      0.0       0.0      15.1
TCP-other           60      0.0        47   706      0.2       4.9       8.4
UDP-DNS             21      0.0         1    66      0.0       0.0      15.5
UDP-other          544      0.0         1   166      0.0       1.2      15.4
ICMP               102      0.0         1    71      0.0       1.7      15.6
Total:             746      0.0         5   552      0.3       1.5      14.7

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop             B/Pk  Active
Fa1/0          20.20.1.1       Null           224.0.0.9       11 C0  10       1
0208 /30 0                     0208 /24 0     0.0.0.0                112     0.0
Min plen:      112                            Max plen:       112

CE1#
```

Figura N° 116: Show ip cache verbose Flow – CE1
Fuente: Elaboración propia

Los comandos utilizados en la configuración del protocolo NETFLOW son listadas en la siguiente Tabla N°13:

Tabla 13: Comandos NETFLOW

Comando	Descripción
flow exporter (exporter name)	Comando que hace referencia a la creación del exportador de flujo.
destination (IP del host)	Especifica la dirección IP del servidor destino del exportador.
source (Interface del router)	Especifica la interfaz local desde la cual el exportador utilizará la dirección IP como dirección IP de origen para los datagramas exportados.
transport (udp) (Puerto udp)	Especifica el puerto UDP en el que el sistema de destino está escuchando datagramas exportados.
template data timeout 60	Configura el reenvío de plantillas en función de un tiempo de espera.
option interface-table	Configura la opción de la tabla de interfaz para exportadores de flujo.
option exporter-stats	Configura la opción de estadísticas de exportador para exportadores de flujo.
option sampler-table	Configura la opción de exportación de información del muestreador para exportadores de flujo.
flow record (record name)	Permite configurar un registro de flujo para un monitor de flujo.
match ipv4 tos	Configura IPv4 ToS como campo clave.
match ipv4 protocol	Configura el protocolo IPv4 como campo clave.
match ipv4 source address	Configura la dirección de origen IPv4 como campo clave.
match ipv4 destination address	Configura la dirección de destino IPv4 como campo clave.
match transport source-port	Configura el puerto de origen de transporte como un campo clave.
match transport destination-port	Configura el puerto de destino del transporte como campo clave.

match interface input	Configura la interfaz de entrada como un campo clave.
match flow direction	Configura la dirección en la que se supervisó el flujo como campo clave.
collect routing source as	Configura uno o más de los campos de atributos de enrutamiento de origen como un campo sin clave y permite recopilar los valores de los flujos. Configura el campo del sistema autónomo como un campo no clave y permite recopilar el valor en el campo del sistema autónomo de los flujos.
collect routing destination as	Configura uno o más de los campos de atributos de enrutamiento de destino como un campo sin clave y permite recopilar los valores de los flujos. Configura el campo del sistema autónomo como un campo no clave y permite recopilar el valor en el campo del sistema autónomo de los flujos.
collect routing next-hop address ipv4	Configura el valor de la dirección del siguiente salto como un campo sin clave y permite recopilar información sobre el próximo salto de los flujos. El tipo de dirección (IPv4 o IPv6) está determinado por la siguiente palabra clave ingresada en este caso es: ipv4
collect ipv4 dscp	Configura el campo de punto de código de servicios diferenciados (DSCP) como un campo sin clave y permite recopilar el valor en los campos de tipo de servicio (ToS) IPv4 DSCP de los flujos.
collect ipv4 id	Configure el indicador IPv4 IS como un campo sin clave y habilite la recopilación del valor en el campo ID de IPv4 de los flujos.
collect ipv4 source mask	Configura la máscara de dirección de origen IPv4 como un campo sin clave y permite

	recopilar el valor de la máscara de dirección de origen IPv4 de los flujos.
collect ipv4 destination mask	Configura la máscara de dirección de destino IPv4 como un campo sin clave y permite recopilar el valor de la máscara de dirección de destino IPv4 de los flujos.
collect transport tcp flags	Configura uno o más de los indicadores de TCP como un campo sin clave y permite recopilar los valores del flujo.
collect interface output	Configura la interfaz de salida como un campo sin clave y permite recopilar la interfaz de salida de los flujos.
collect flow sampler	Configura el ID del muestreador de flujo como un campo sin clave y habilita la recopilación del ID del muestreador que está asignado al monitor de flujo.
collect counter bytes	Configura el número de bytes que se ven en un flujo como un campo sin clave y permite recopilar el número total de bytes del flujo.
collect counter packets	Configura la cantidad de paquetes que se ven en un flujo como un campo sin clave y permite recopilar la cantidad total de paquetes del flujo.
collect timestamp sys-uptime first	Configura el tiempo de actividad del sistema para el momento en que se vió el primer paquete de los flujos como un campo no clave y permite recopilar marcas de tiempo según el tiempo de actividad del sistema para el momento en que se vió el primer paquete de los flujos.
collect timestamp sys-uptime last	Configura el tiempo de actividad del sistema para el momento en que se vió el último paquete de los flujos como un campo no clave y permite recopilar marcas de tiempo según el tiempo de actividad del sistema

	para el momento en que se vió el paquete más reciente de los flujos.
flow monitor (Nombre del flujo de monitor)	Comando que hace referencia a la creación del monitor de flujo.
record (Flow record creado)	Flow record asignado al monitor
exporter (Flow exporter creado)	Flow exporter asignado al monitor
cache timeout inactive 10	Especifica el tiempo de espera del flujo inactivo. La cantidad de segundos que un flujo inactivo permanece en la caché antes de que se borre. El rango es de 10 a 600.
cache timeout active 60	Tiempo de espera del flujo activo. La cantidad de minutos que un flujo activo permanece en la caché antes de que se borre. El rango es de 1 a 60.
statistics packet protocol	Permite la recopilación de estadísticas de distribución de protocolos para monitores NetFlow flexibles.
sampler (Nombre de la muestra)	Permite configurar un muestreador de flujo.
mode random 1 out of 32	Configura un intervalo de paquetes para un muestreador de flujo. El rango de la tasa de muestreo es de 1 a 32,768 paquetes.
interface (FastEthernet0/0)	Especifica la interfaz del router donde se configurará el monitoreo.
ip flow monitor (Flow monitor creado) sampler (sampler creado) input	Nombre de un monitor de flujo que se configuró previamente. Habilita un muestreador de flujo para este monitor de flujo usando el nombre de un muestreador que se configuró previamente. Supervisa el tráfico que recibe el router en la interfaz.
ip flow monitor (Flow monitor creado) sampler (sampler creado) output	Nombre de un monitor de flujo que se configuró previamente. Habilita un muestreador de flujo para este monitor de flujo usando el nombre de un muestreador

	que se configuró previamente. Supervisa el tráfico que transmite el router en la interfaz.
ip flow ingress	Habilita la contabilidad de NetFlow (ingreso) para el tráfico que llega a una interfaz.
ip flow egress	Habilita la contabilidad de salida de NetFlow para el tráfico que reenvía el router.
ip flow-capture packet-length	Permite habilitar la captura de valores de la Capa 2 o campos adicionales de la Capa 3 en el tráfico de NetFlow. El packet-length captura el valor del campo de longitud del paquete de los datagramas IP en un flujo.
ip flow-export versión 9	Especifica que el datagrama del flujo exporter utiliza el formato de la Versión 9.
ip flow-export destination (IP del host) puerto (UDP)	Dirección IP o nombre de host del servidor a la que desea enviar la información de NetFlow y el número del puerto UDP en el que el servidor está escuchando esta entrada.

Fuente: Elaboración propia

Con el protocolo NETFLOW, el administrador de la red podrá monitorear de manera eficiente el uso del ancho de banda para la planificación de la capacidad y la asignación de recursos y poder prever que mejoras realizar para tener un sistema en buenas condiciones.

b) Configuración del FlowAnalysis

-NETWORK- Netflow: Agregación de interfaces

Esta opción nos permitió ver el tráfico de consumo por interfaces, sin embargo, antes tuvimos que habilitar la interfaz por equipo de la siguiente manera:

Paso 1: Se realizó click en "License managment" para agregar la interfaz a monitorear (véase Figura N° 117).

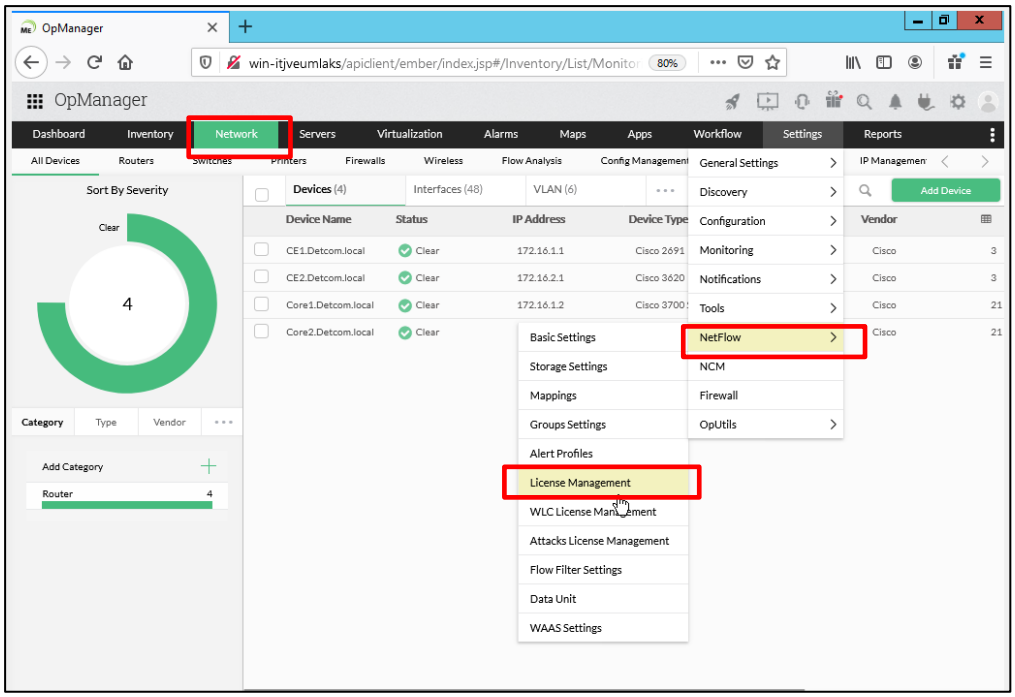


Figura N° 117: NETWORK – NETFLOW
Fuente: Elaboración propia

Paso 2: Se declaró las interfaces que se iban a monitorear por equipo como se muestra en la Figura N° 118.

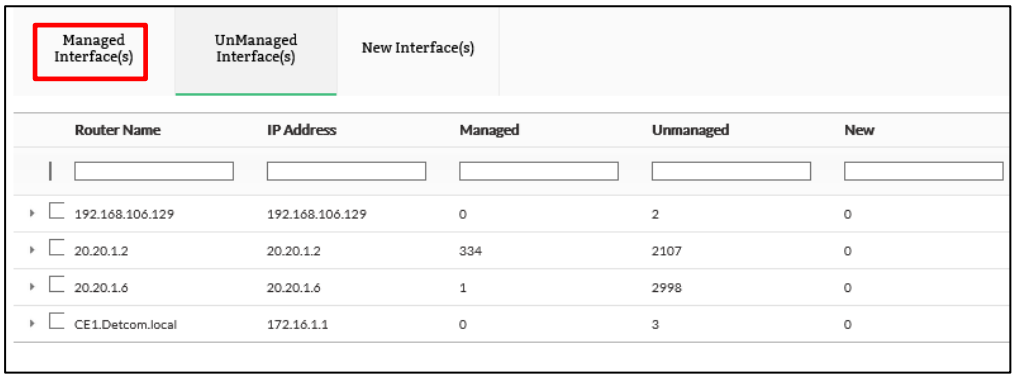


Figura N° 118: NETWORK-NETFLOW
Fuente: Elaboración propia

Paso 3: Una vez habilitada las interfaces de monitoreo por equipo, apareció en la opción de FLOW ANALYSIS, siguiendo la siguiente ruta: NETWORK-> Flow Analysis Figura N° 119.

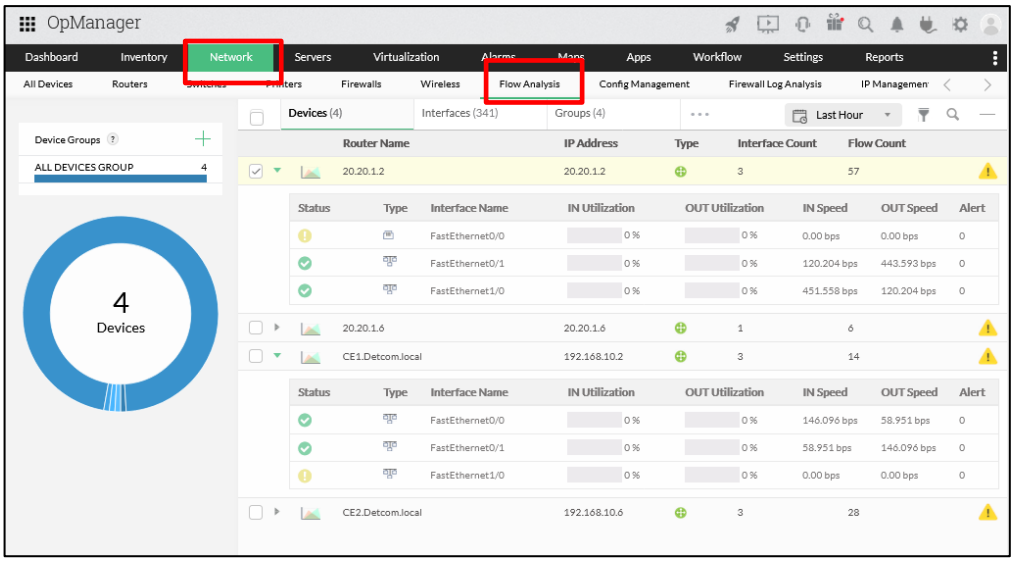


Figura N° 119: NETWORK – NETFLOW
Fuente: Elaboración propia

Paso 4: Aquí nos permitió elegir la interfaz a la cual podremos monitorear y consultar el detalle de tráfico en la Figura N° 120.

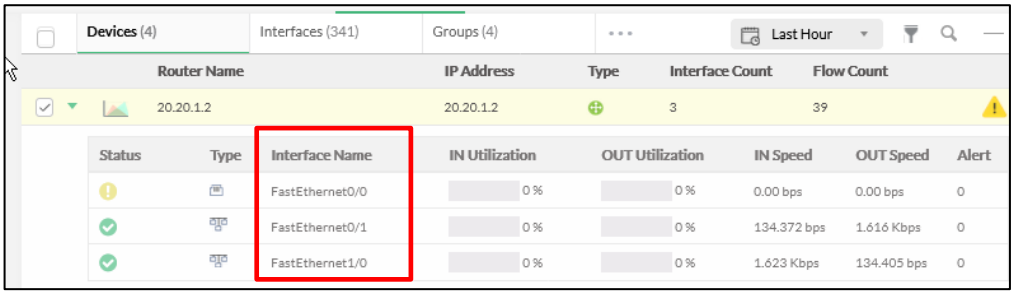


Figura N° 120: NETWORK – NETFLOW
Fuente: Elaboración propia

Paso 5: Se configuro el ancho de banda de cada enlace, como se muestra en la Figura N° 121 para tener el correcto detalle de emulación:

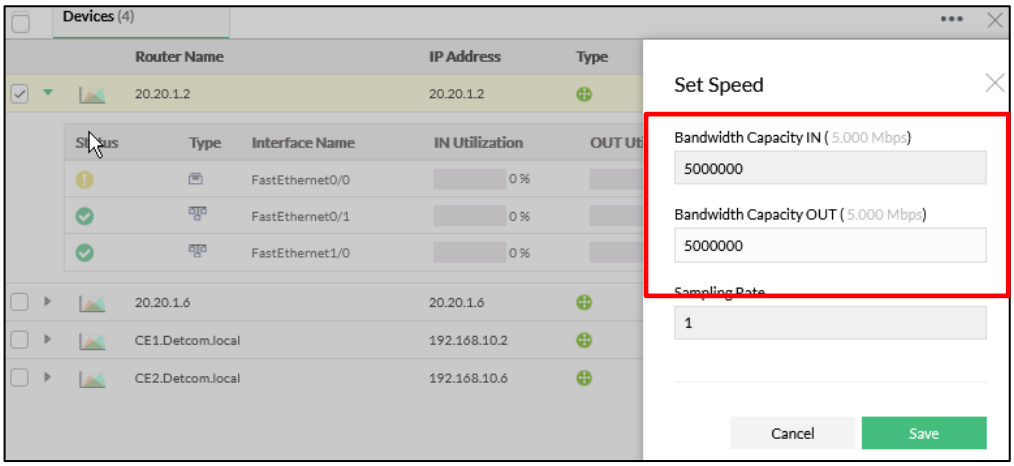


Figura N° 121:NETWORK – NETFLOW
Fuente: Elaboración propia

c) Funcionalidades del FlowAnalysis

-Flow Analysis – Tráfico de consumo

Una vez ingresado a la interface que seleccionamos, tuvimos la opción de “traffic” el cual mostro el tráfico por interface con un periodo de fecha configurable, de esta manera tenemos un mayor detalle de información de tráfico de consumo (véase Figura N° 122).

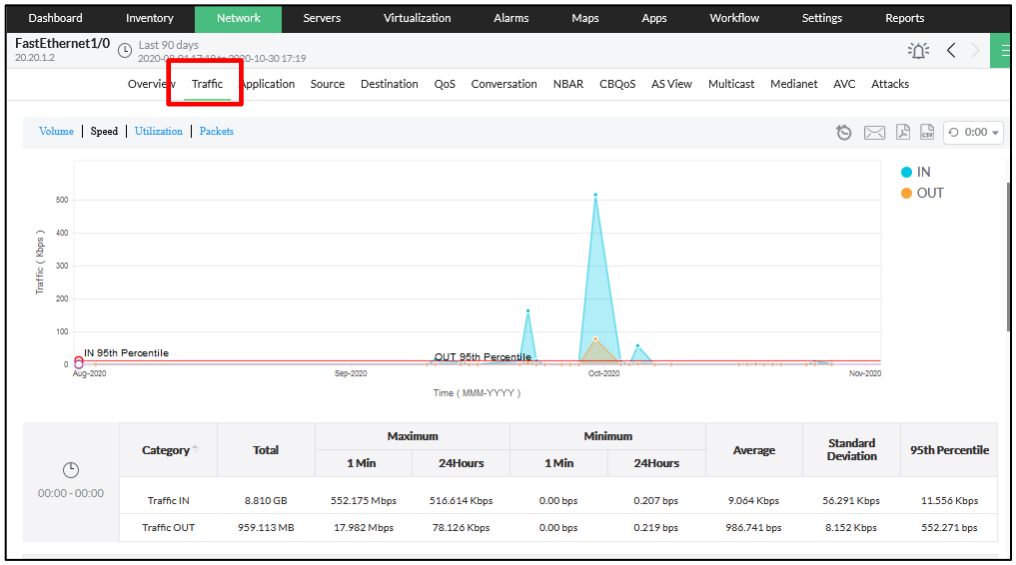


Figura N° 122: NETWORK –Flow analysis – Device traffic
Fuente: Elaboración propia

Se conto con la opción de Application, por la cual pudimos ver el consumo de aplicativos más usados por los usuarios con un periodo de fecha configurable Figura N° 123.

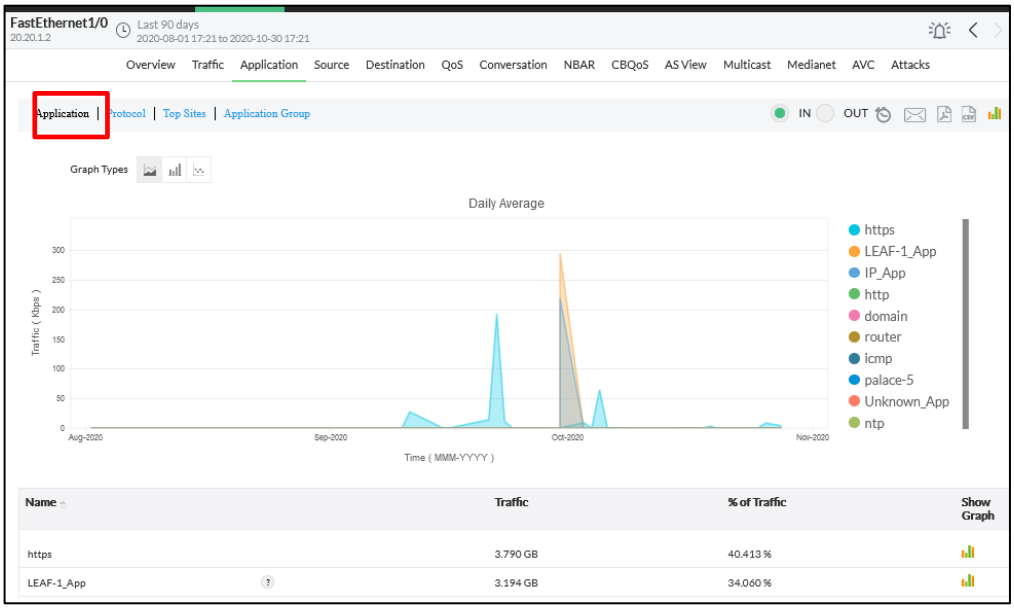


Figura N° 123: NETWORK –Flow analysis – Application
Fuente: Elaboración propia

Se conto con la opción de Protocol, por la cual pudimos ver el historial de protocolos más usados por los usuarios con un periodo de fecha configurable Figura N° 124.

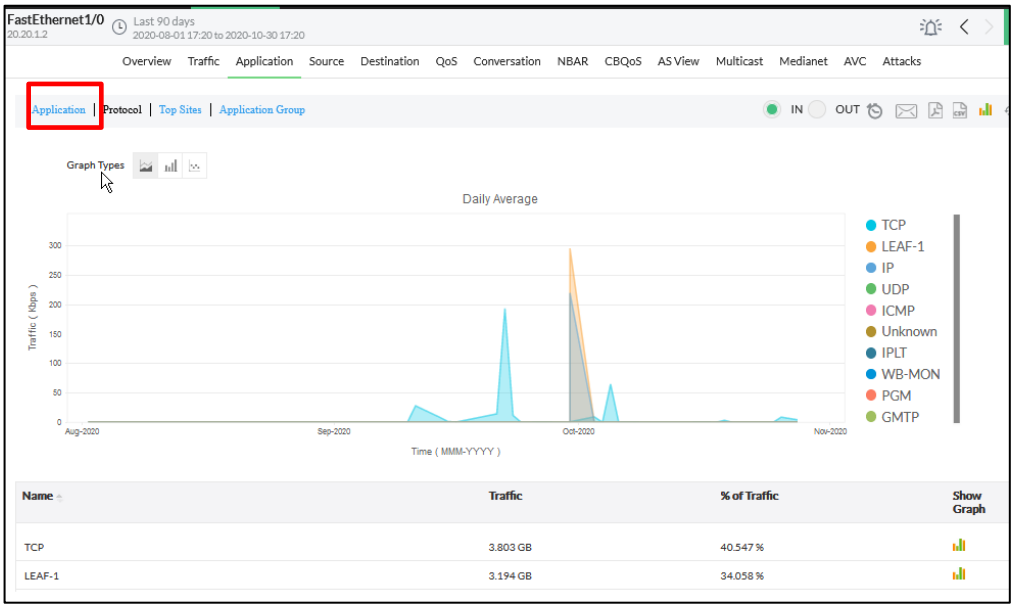


Figura N° 124: NETWORK –Flow analysis – Protocol
Fuente: Elaboración propia

Tuvimos las opciones de poder ver la IP de origen, para este caso 172.16.10.12 quien es la que está consumiendo mayor tráfico como se muestra en la Figura N° 125.

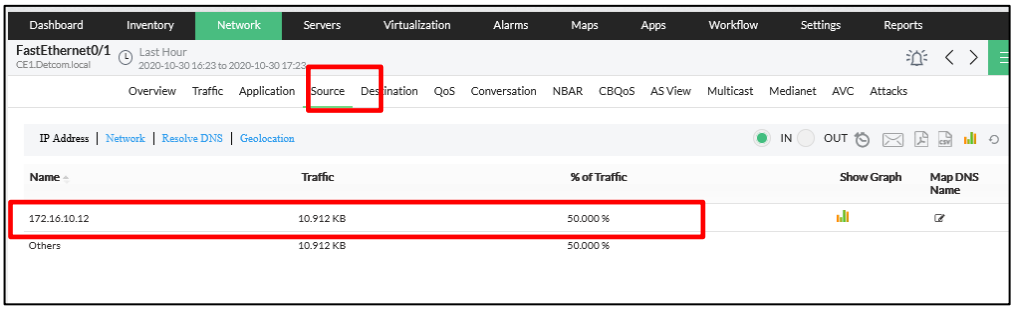


Figura N° 125: NETWORK –Flow analysis – Source
Fuente: Elaboración propia

Asimismo, pudimos ver la IP de destino, para este caso 172.16.2.2 quien la IP a donde se hace las consultas, como se muestra en la Figura N° 126.

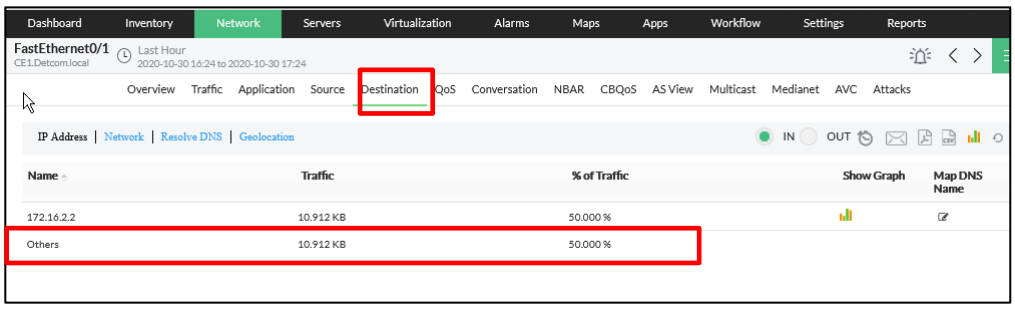


Figura N° 126: NETWORK - Flow analysis - Destination
Fuente: Elaboración propia

Entonces, se pudo ver la conversación entre estas IP's lo cual nos mostros un escenario más detallado del consumo que se da desde el origen- destino ya que observamos tanto la IP Origen, IP Destino, aplicación y la cantidad de tráfico de consumo Figura N° 127.

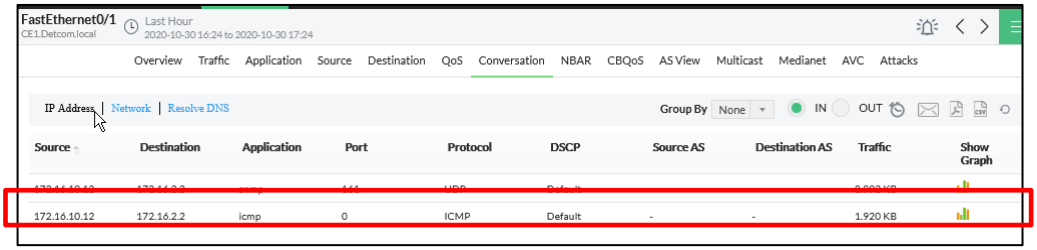


Figura N° 127: NETWORK –Flow analysis – Conversation
Fuente: Elaboración propia

4.3 Escenario de pruebas y análisis de resultados

El escenario de trabajo para poder generar tráfico e incidencias, basándonos en el cuadro de soporte proporcionado por la empresa DETCOM y con nuestros objetivos establecidos se desarrollaron los siguientes escenarios que se muestra en la siguiente Tabla N°14:

Tabla 14: Cuadro de Incidencias emuladas

OBJETIVOS	TIPO	PRUEBA	RESULTADO
Visibilidad y análisis del ancho de banda en la LAN.	Escenario 1	Generación de tráfico a internet desde las máquinas virtuales	-Visibilidad del ancho de banda: Monitoreo en tiempo real del uso hacia internet. -Análisis del ancho de banda: Reportes de utilización (%) del ancho de banda en tiempo real e histórico, teniendo información granulada de IP Origen, IP Destino y aplicativos de uso.
	Escenario 2	Generación de tráfico de la LAN (utilización del Filezilla) – Serv App	-Visibilidad del ancho de banda: Monitoreo en tiempo real a nivel LAN.

			-Análisis del ancho de banda: Reportes de utilización (%) del ancho de banda en tiempo real e histórico de uso, teniendo información granulada de IP Origen, IP destino y protocolo de uso.
Análisis de rendimiento de la LAN.	Escenario 3	Generación y visualización de rendimiento de la salud de dispositivos.	Análisis a nivel de hardware mediante los reportes de utilización de la salud de dispositivos a nivel de LAN en tiempo real e histórico de uso.
	Escenario 4	Envió de protocolo ICMP para la visualización de latencia y perdida de paquetes.	Análisis de rendimiento de la LAN en tiempo en real e histórico de reportes de latencia y perdida de paquetes.
Administración de incidencias en la LAN	Escenario 5	Apagado y desconexión de equipos router y switch en la red.	Monitoreo y gestión de incidencias a nivel de alarmas presentadas.
	Escenario 6	Caída de la red MPLS	Monitoreo y gestión de incidencias a nivel de disponibilidad del enlace entre oficinas.
	Escenario 7	Apagado y desconexión de puertos a nivel de usuario.	Monitoreo y gestión de incidencias a nivel de interfaz de usuario.

Fuente: Elaboración propia

Con las estaciones de trabajo desplegadas en cada oficina se realizó los falsos positivos generando los siguientes escenarios:

Escenario 1: Generación de tráfico a internet desde las máquinas virtuales

CE2: Monitoreo y visibilidad del tráfico hacia internet, por un periodo de una semana Figura N° 128.

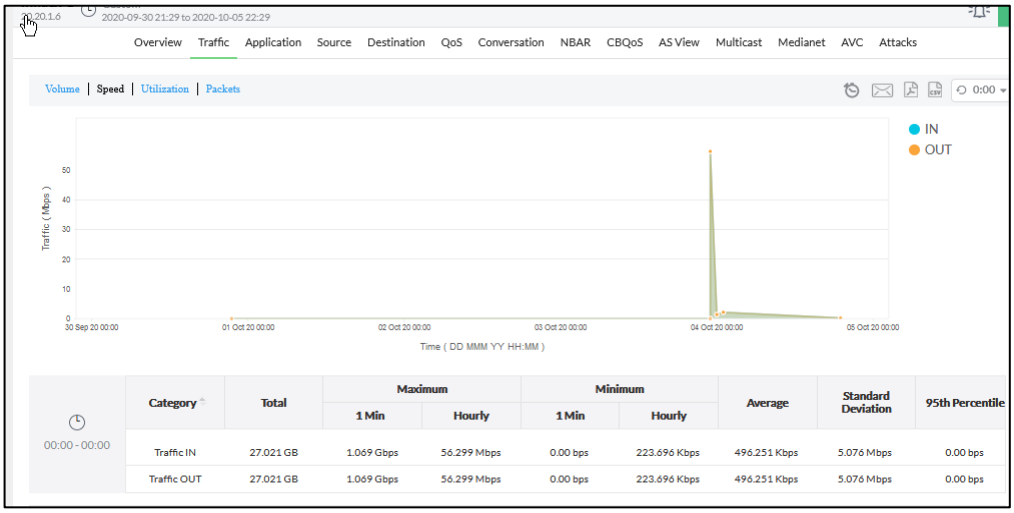


Figura N° 128: Escenario 1 – Tráfico hacia internet CE2
Fuente: Elaboración propia

CE2: Se monitoreo y visualizo la utilización del ancho de banda de la interfaz FastEthernet 1/0 hacia internet, por un periodo de una semana Figura N°. 129.

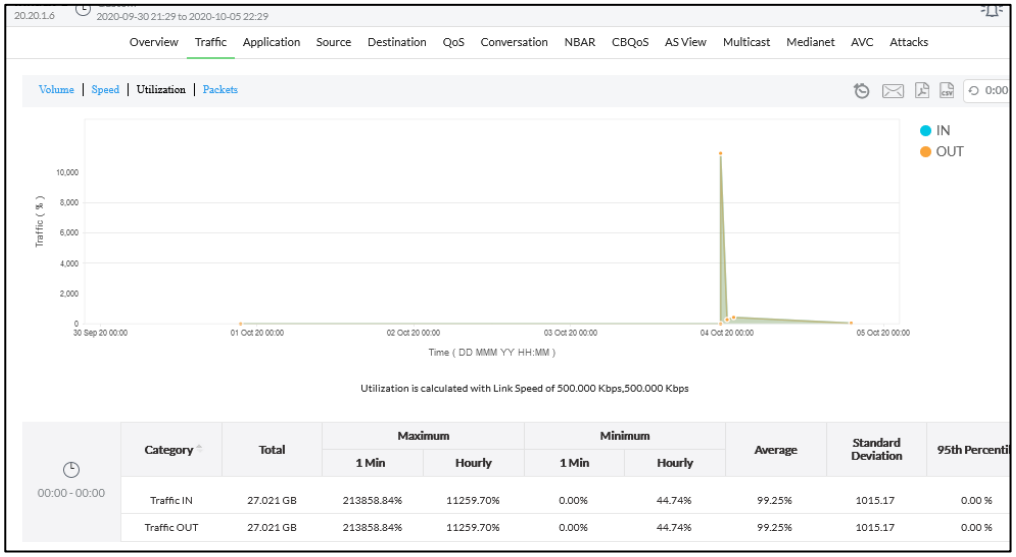


Figura N° 129: Escenario 1 – Tráfico hacia internet CE2
Fuente: Elaboración propia

CE1: Se monitoreo y visualizo el tráfico hacia internet, por un periodo de una semana Figura N° 130.

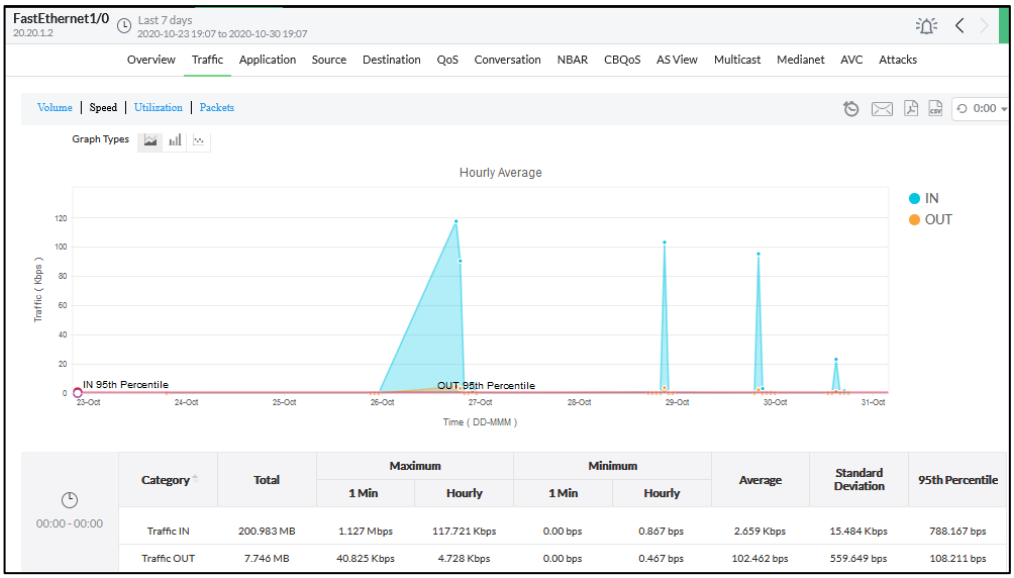


Figura N° 130: Escenario 1 – Tráfico hacia internet CE1
Fuente: Elaboración propia

CE1: Se monitoreo y visualizo la utilización del ancho de banda de la interfaz FastEthernet 1/0 hacia internet, por un periodo de una semana Figura N° 131.

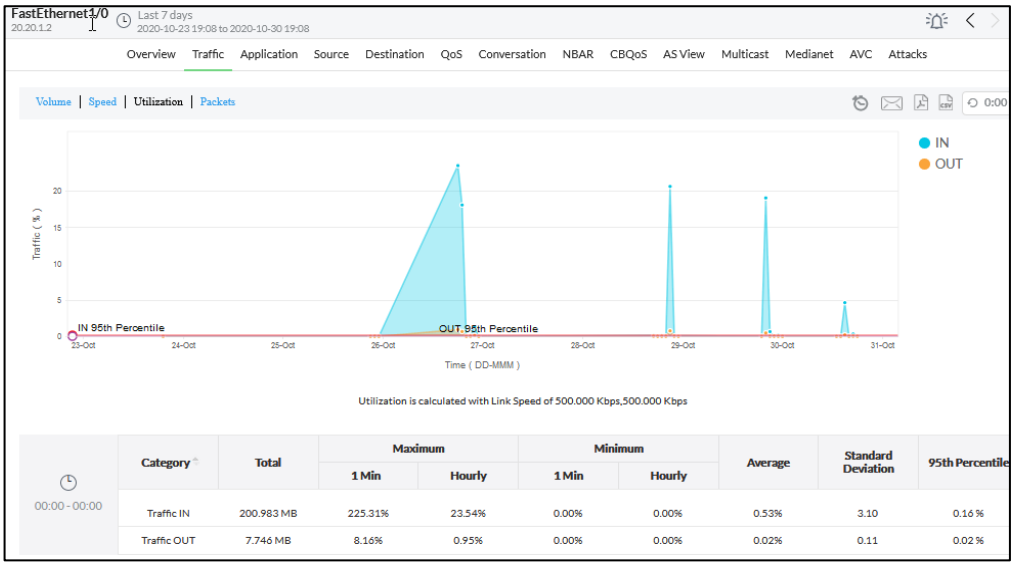


Figura N° 131: Escenario 1 – Utilización del ancho de banda de internet CE1
Fuente: Elaboración propia

Se monitoreo y visualizo los aplicativos de consumo por la interfaz FastEthernet 1/0 Figura N° 132.

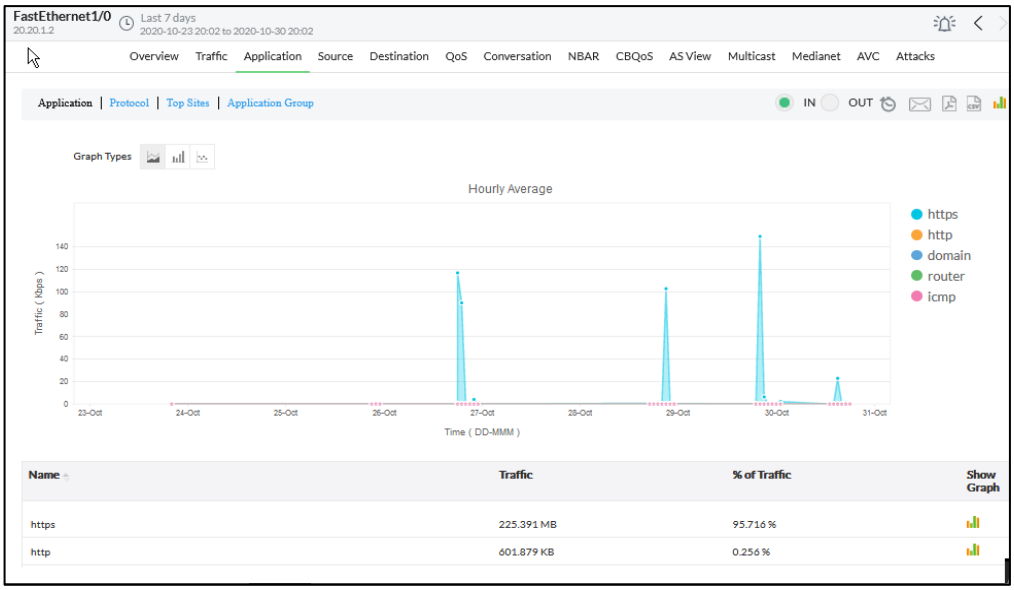


Figura N° 132: Escenario 1 – Utilización de aplicativos CE1
Fuente: Elaboración propia

Se monitoreo y visualizo las conversaciones en la interfaz FastEthernet 1/0 para ver la IP de origen con mayor consumo (véase la Figura N° 133).

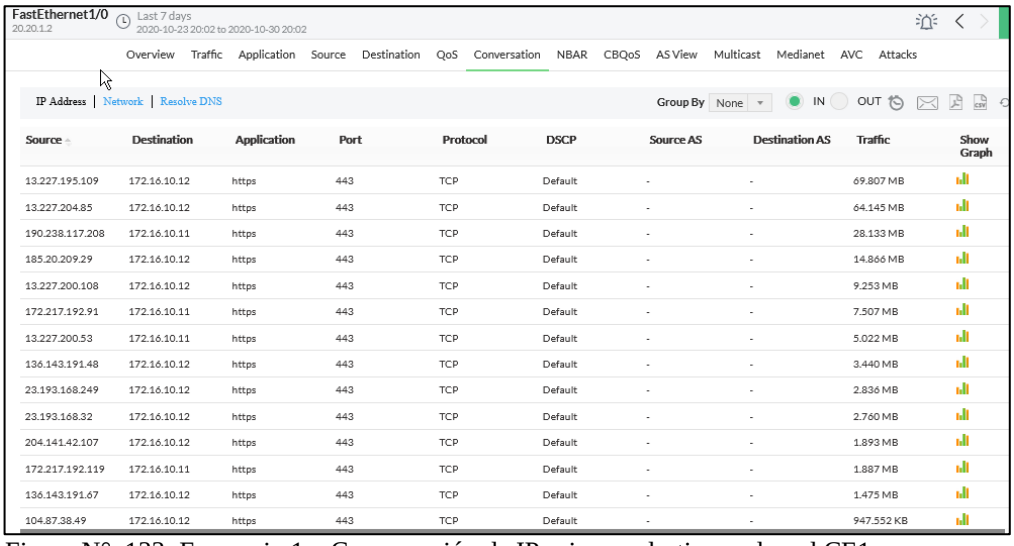


Figura N° 133: Escenario 1 – Conversación de IP origen – destino en la red CE1
Fuente: Elaboración propia

Con esta información pudimos realizar la consulta en internet de la IP de destino, para saber el aplicativo de uso (véase la Figura N° 134).

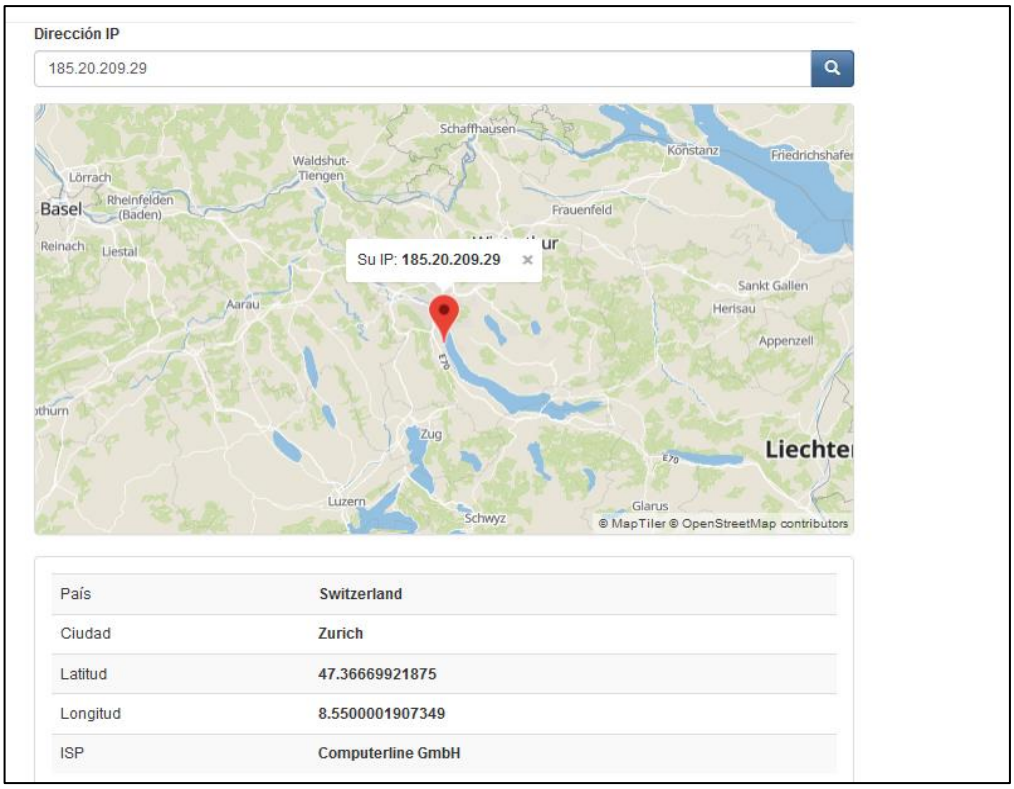


Figura N° 134: Escenario 1 – Utilización del ancho de banda de internet
Fuente: Elaboración propia

Escenario 2: Generación de tráfico de la LAN (utilización del Filezilla) – Serv App CE2 - SERVIDOR: Se visualizó el ancho de banda con el cual se pudo monitorear en tiempo real a nivel LAN como se muestra en la Figura N° 135.

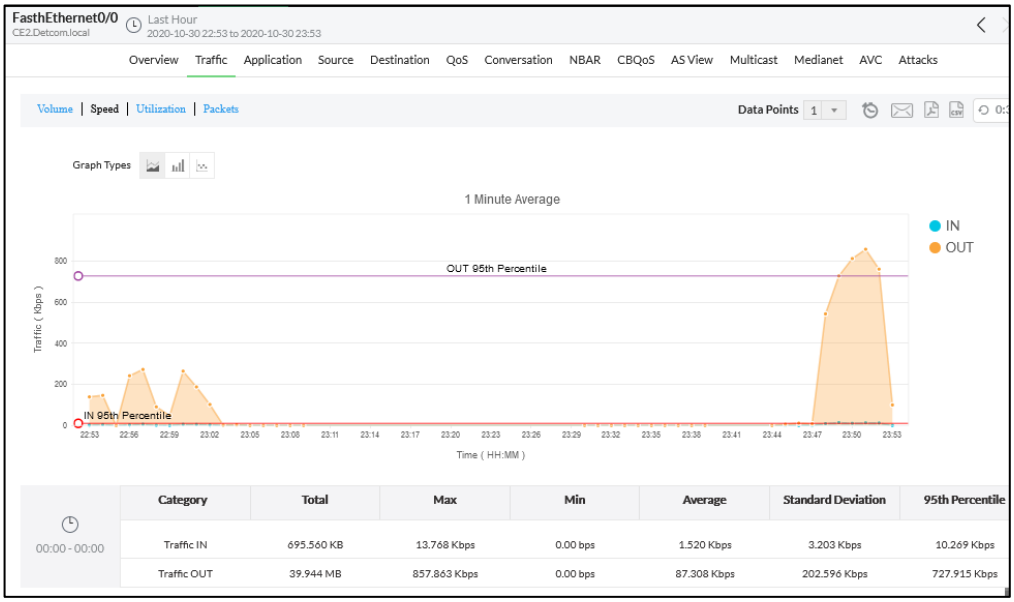


Figura N° 135: Escenario 2 – Tráfico LAN CE2 - SERVIDOR
Fuente: Elaboración propia

CE2 - SERVIDOR: Se generó tráfico desde el servidor FTP hasta los equipos LAN hasta el CE2 (véase la Figura N° 136).

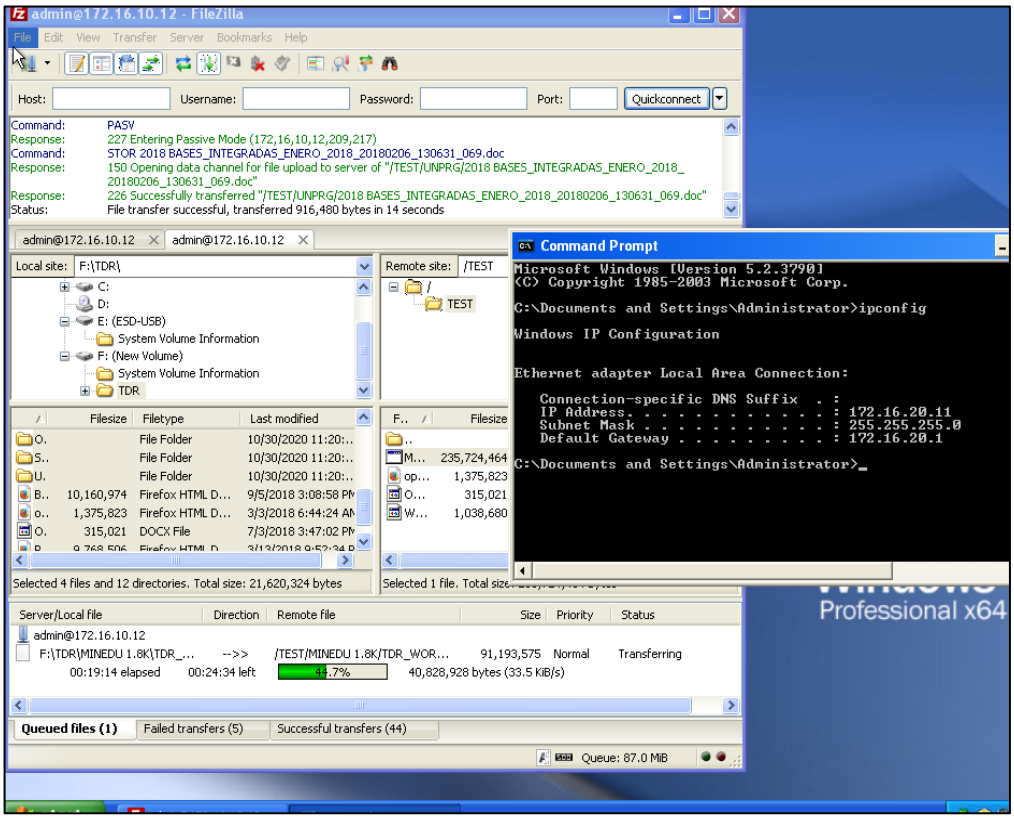


Figura N° 136: Escenario 2 – Tráfico LAN CE2 - SERVIDOR
Fuente: Elaboración propia

CE2 - SERVIDOR: Se capturó el tráfico desde el servidor FTP – hasta el CE2 (véase la Figura N° 137).

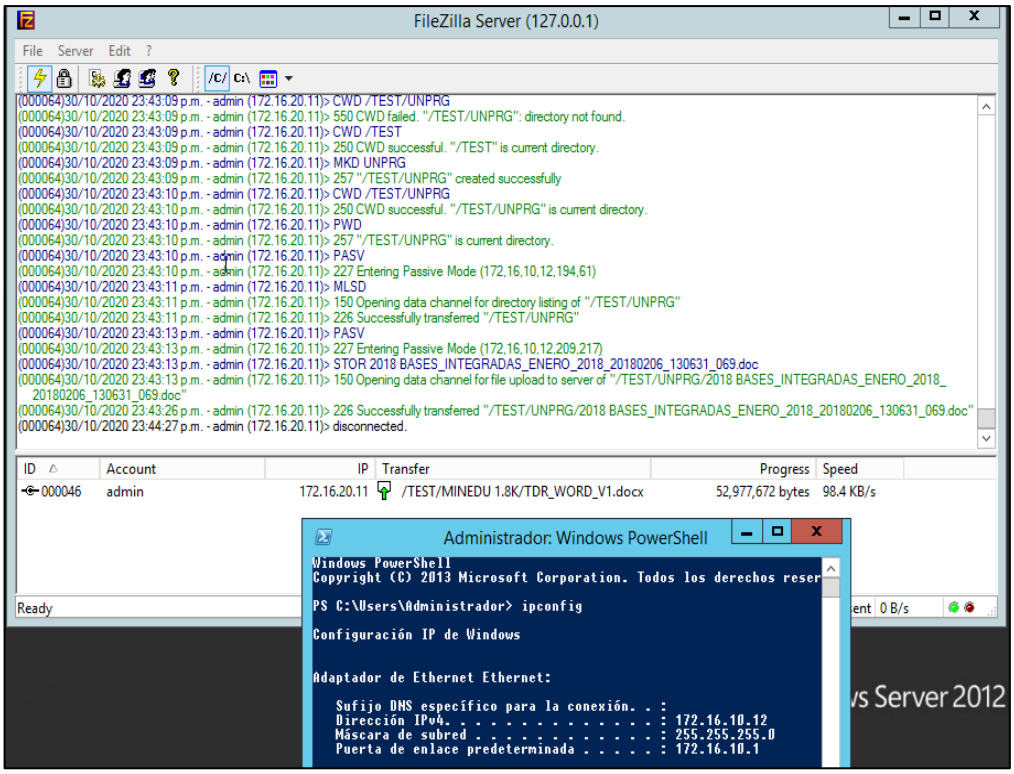


Figura N° 137: Escenario 2 – Tráfico LAN CE2 - SERVIDOR
Fuente: Elaboración propia

CE2 - SERVIDOR: También, se capturó el tráfico desde el servidor FTP – hasta el CE2 observando la descarga y utilización del ancho de banda como se muestra en la Figura N° 138.

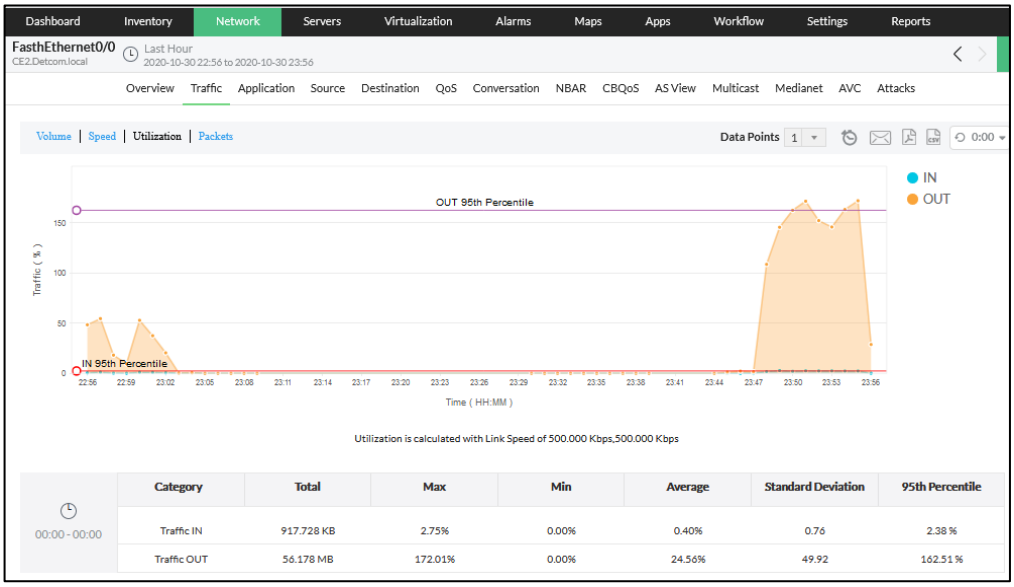


Figura N° 138: Escenario 2 – Tráfico LAN CE2 - SERVIDOR
Fuente: Elaboración propia

CE2 - SERVIDOR: Se obtuvo la conversación desde el servidor FTP – hasta el CE2 observando las aplicaciones, puertos y protocolos que se utilizan todo desde la herramienta de monitoreo y gestión (véase la Figura N° 139).

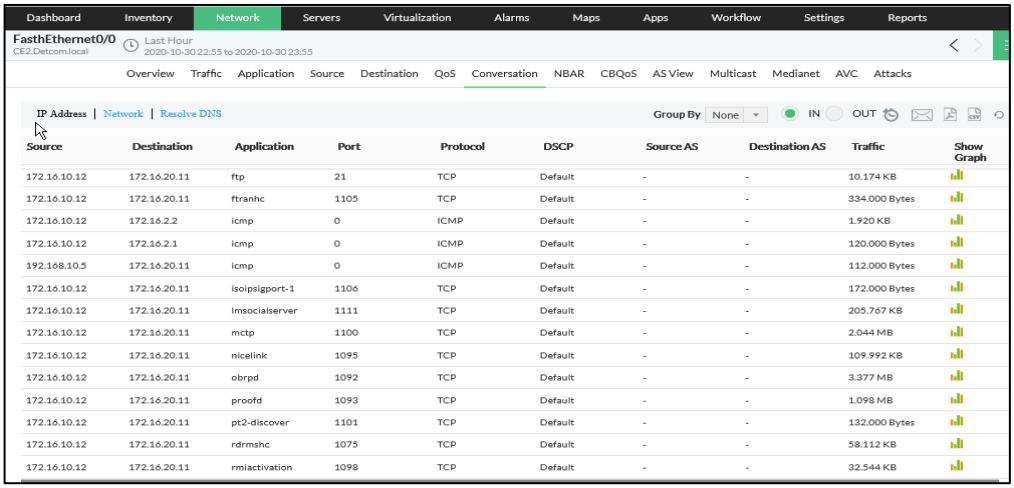


Figura N° 139: Escenario 2 – Tráfico LAN CE2 - SERVIDOR
Fuente: Elaboración propia

CE1 - SERVIDOR: Se capturó el tráfico desde el servidor FTP – hasta el CE1 observando la carga y el tráfico del ancho de banda como se muestra en la Figura N° 140 desde el puerto FastEthernet 0/0.

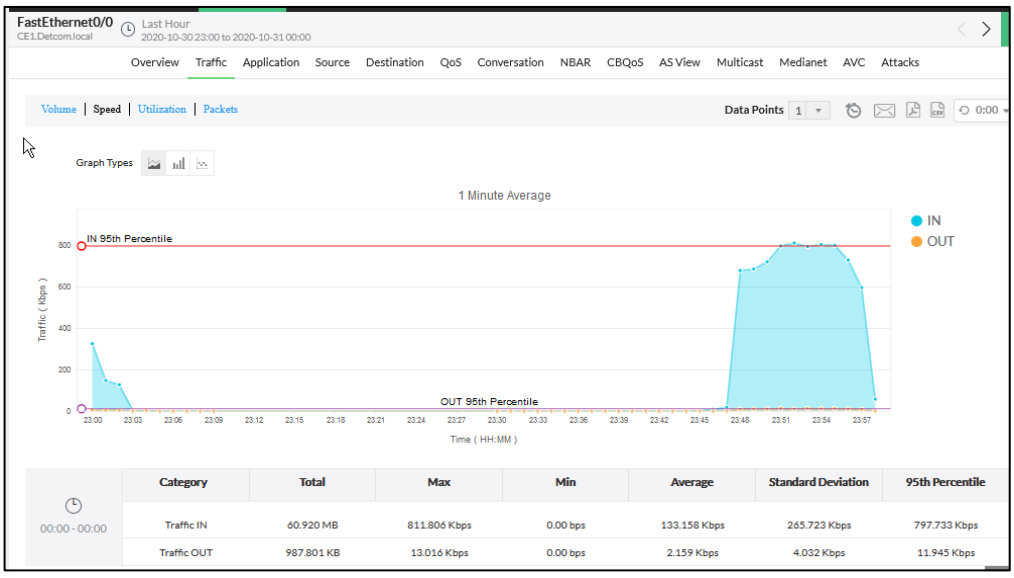


Figura N° 140: Escenario 2 – Tráfico LAN CE1 - SERVIDOR
Fuente: Elaboración propia

CE1 - SERVIDOR: Se capturo el tráfico desde el servidor FTP – hasta el CE1 observando la descarga y utilización del ancho de banda de la herramienta de monitoreo y gestión como se muestra en la Figura N° 141.

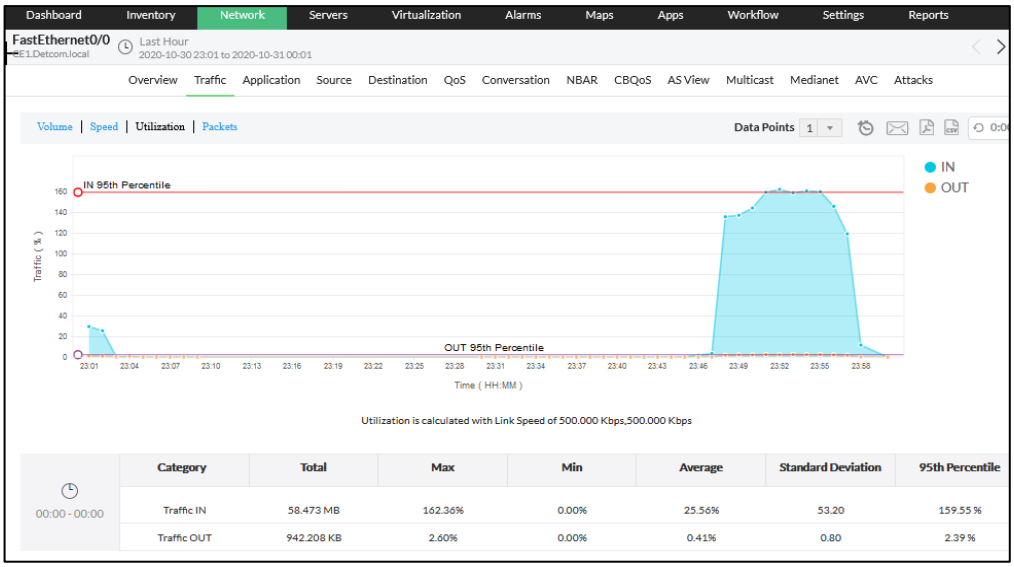


Figura N° 141: Escenario 2 – Tráfico LAN CE1 - SERVIDOR
Fuente: Elaboración propia

CE1 - SERVIDOR: Se capturo la conversación desde el servidor FTP – hasta el CE1 observando las aplicaciones, puertos y protocolos que se utilizan (véase la Figura N° 142).

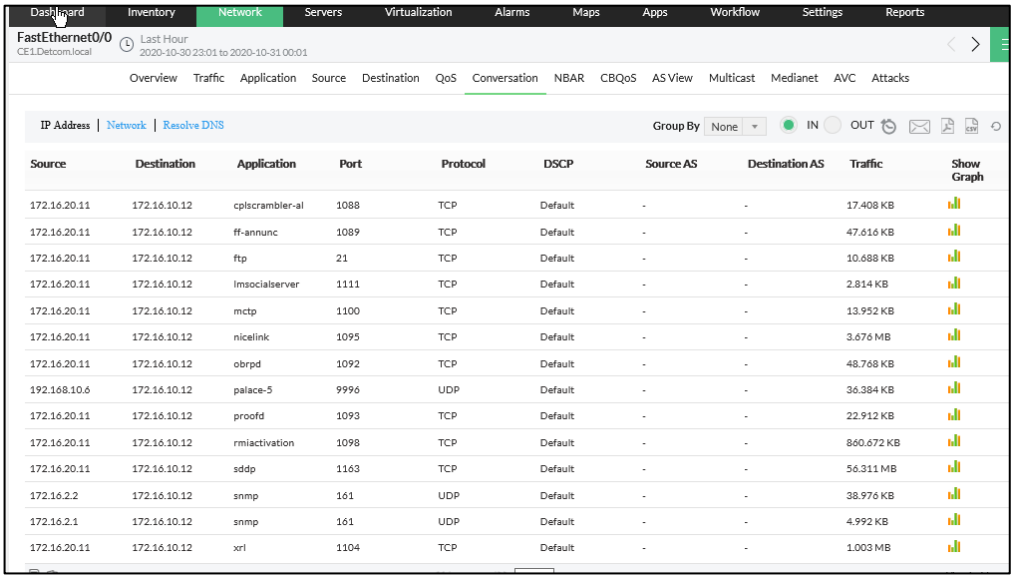


Figura N° 142: Escenario 2 – Tráfico LAN CE1 - SERVIDOR
Fuente: Elaboración propia

Escenario 3: Se género y visualizo el rendimiento de la salud de dispositivos.

Core1- Dispositivo: Ejecutando un comando para visualizar el rendimiento del CPU en tiempo real desde el mismo equipo como se muestra en la Figura N° 143.

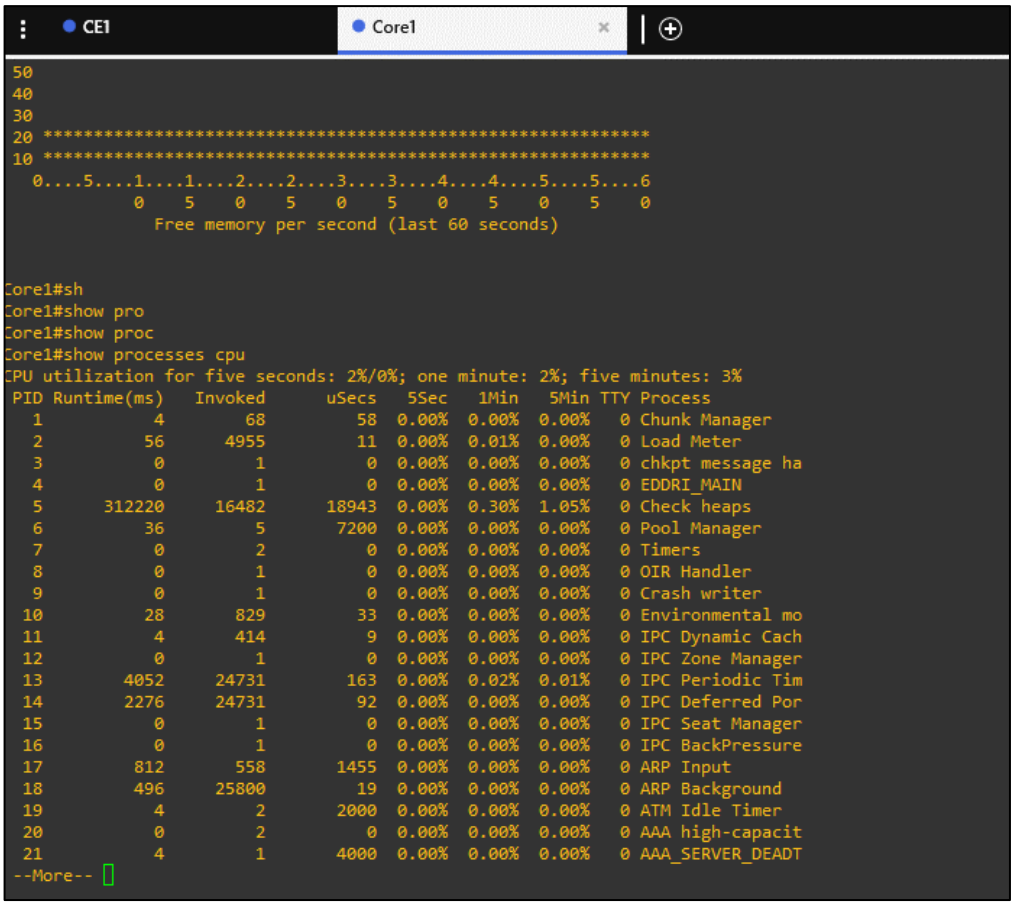


Figura N° 143: Escenario 3 – Core1 Visualización de salud de equipos – CPU Dispositivo
Fuente: Elaboración propia

Core1- Opmanager: Esto pudimos validarlo desde la herramienta de monitoreo y gestión que los valores fueron los mismos y que se está visualizando el correcto rendimiento del CPU en tiempo real como se muestra en la Figura N° 144.

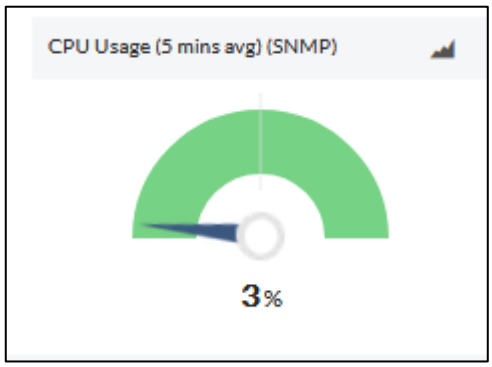


Figura N° 144: Escenario 3 – Core1 Visualización de salud de equipos - CPU Opmanager
Fuente: Elaboración propia

Core1 – Opmanager: Adicionalmente, pudimos verlo de forma gráfica e histórica en la herramienta como se muestra en la Figura N° 145.

Figura N° 145Escenario 3 – Core1 Visualización de salud de equipos – CPU Opmanager
Fuente: Elaboración propia

Core1- Dispositivo: Se ejecuto un comando para visualizar el rendimiento de la memoria en tiempo real desde el mismo equipo como se muestra en la Figura N° 146.

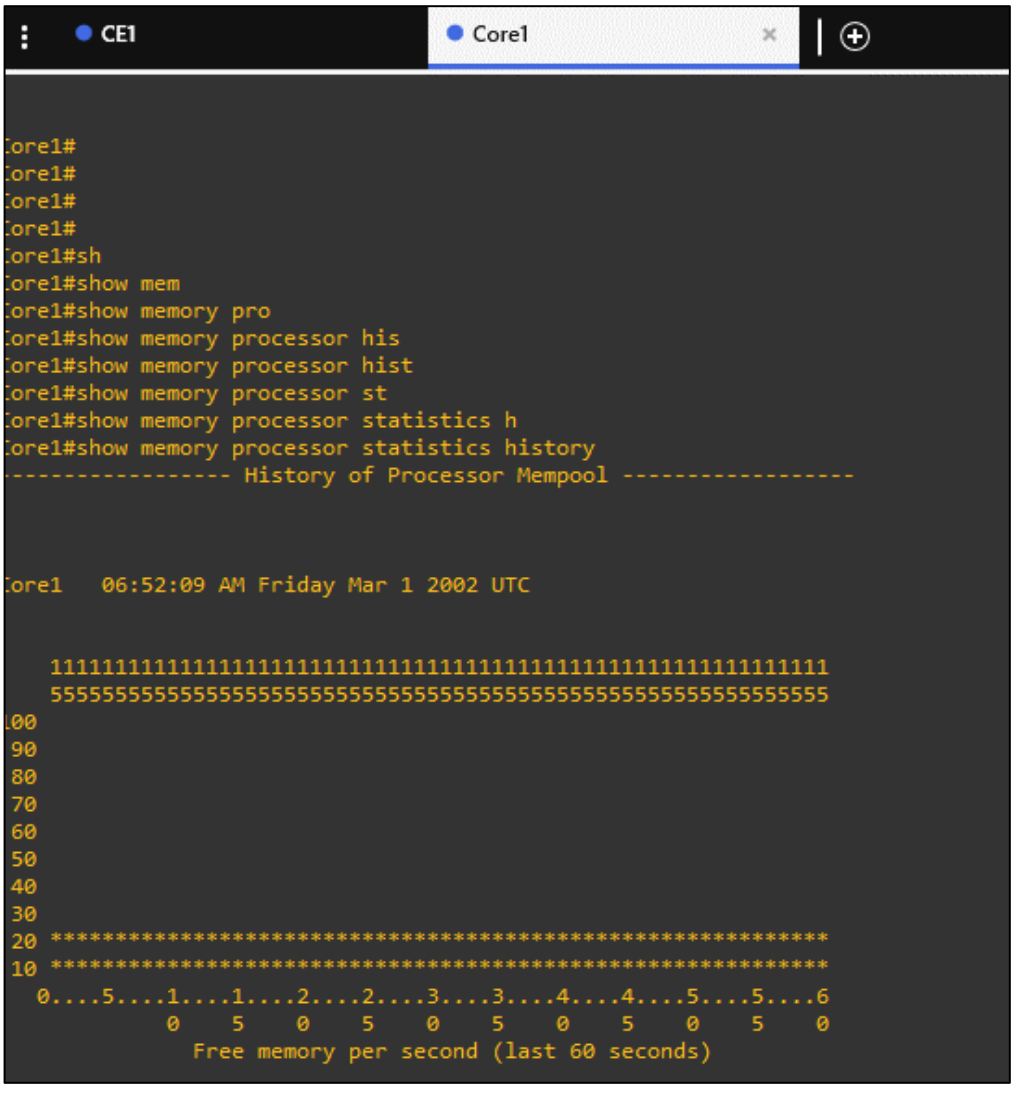


Figura N° 146: Escenario 3 – Core1 Visualización de salud de equipos – Memoria Dispositivo
Fuente: Elaboración propia

Core1- Opmanager: Esto podemos validarlo desde la herramienta de monitoreo y gestión que los valores son los mismos y que se está visualizando el correcto rendimiento de la memoria en tiempo real como se muestra en la Figura N° 147.

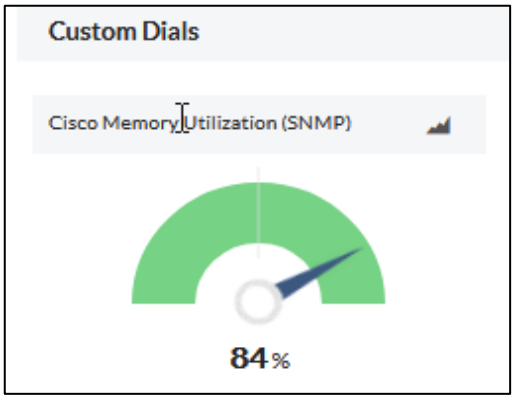


Figura N° 147: Escenario 3 – Core1 Visualización de salud de equipos - Memoria Opmanager
Fuente: Elaboración propia

Core1 – Opmanager: Adicionalmente esto se pudo ver de forma gráfica e histórica en la herramienta como se muestra en la Figura N° 148.

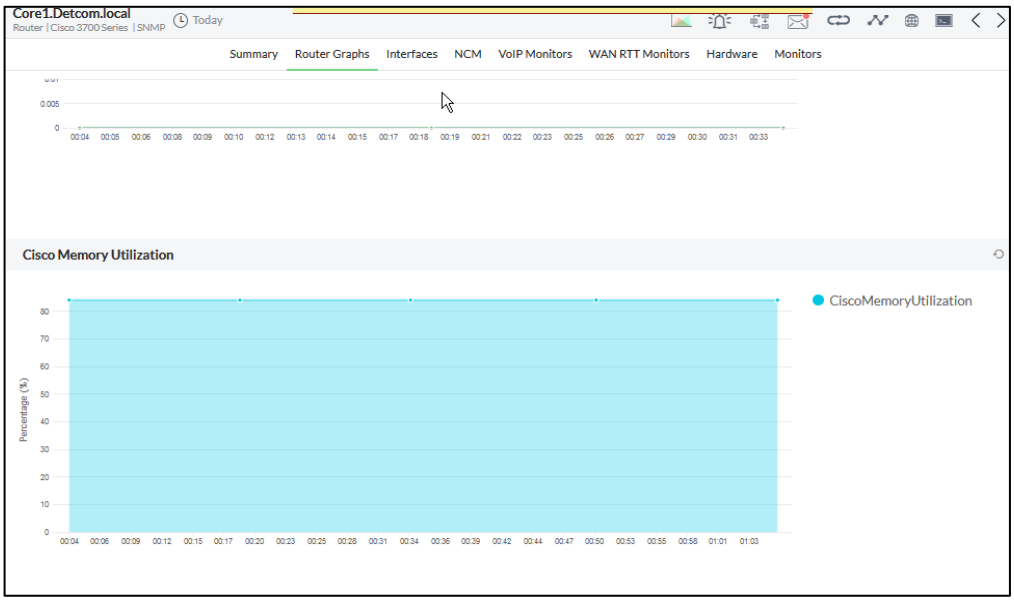


Figura N° 148: Escenario 3 – Core1 Visualización de salud de equipos – Memoria Opmanager
Fuente: Elaboración propia

Las mismas pruebas del escenario 3 se replicaron en el equipo CE1:

CE1- Dispositivo: Se ejecuto un comando para visualizar el rendimiento del CPU en tiempo real desde el mismo equipo como se muestra en la Figura N° 149.

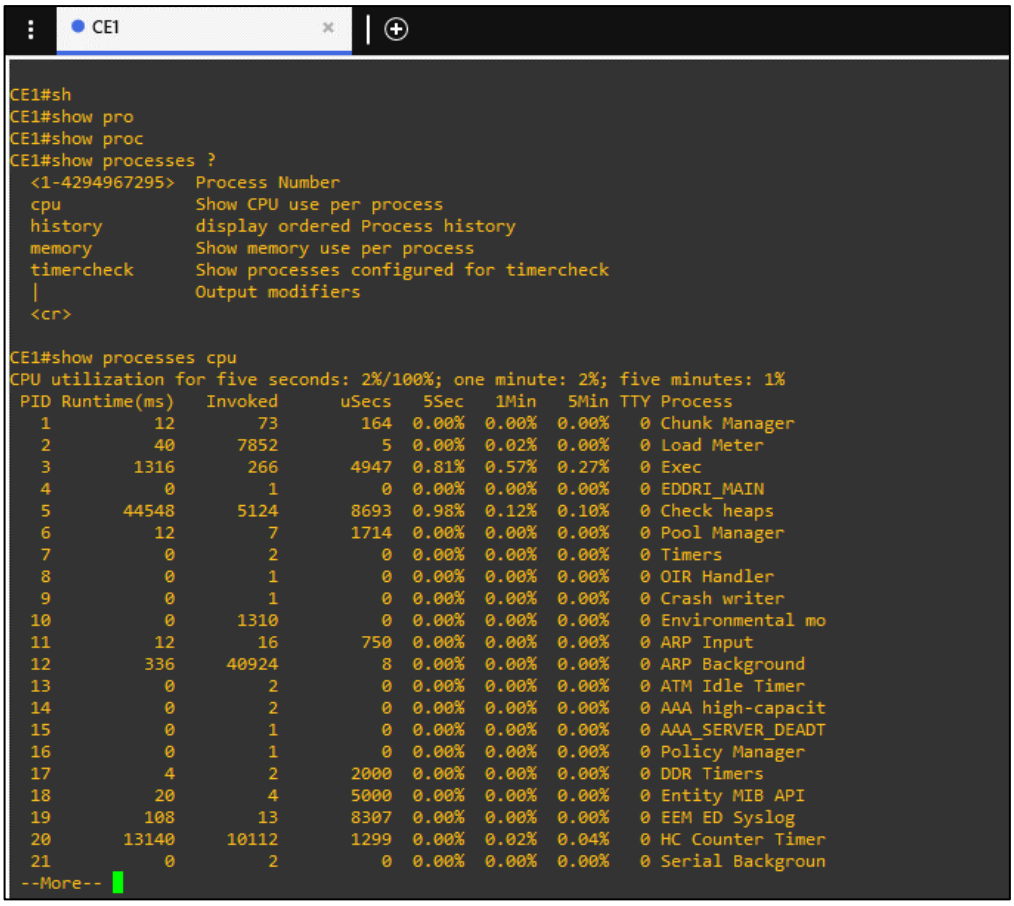


Figura N° 149: Escenario 3 – CE1 Visualización de salud de equipos – CPU Dispositivo
Fuente: Elaboración propia

CE1 – Opmanager: Adicionalmente esto se pudo ver de forma gráfica e histórica en la herramienta como se muestra en la Figura N° 150.

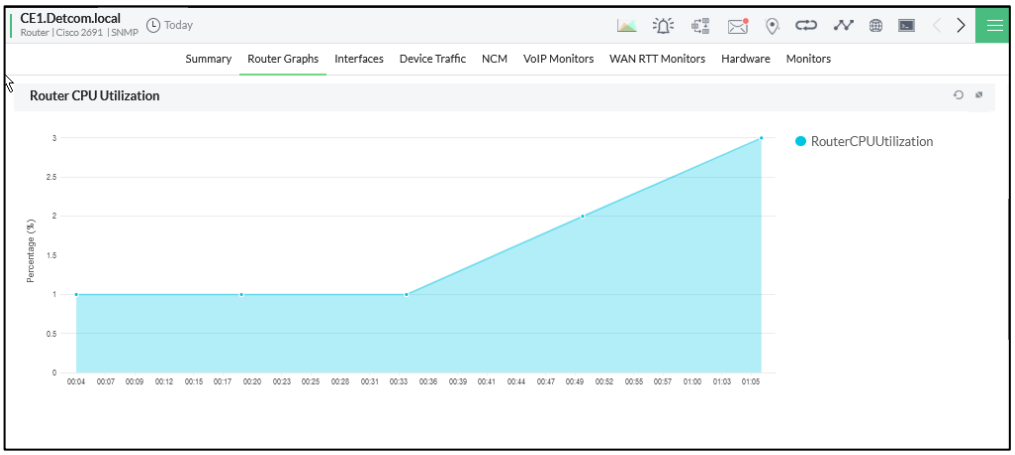


Figura N° 150: Escenario 3 – CE1 Visualización de salud de equipos – CPU Opmanager
Fuente: Elaboración propia

CE1- Dispositivo: se ejecutó un comando para visualizar el rendimiento de la memoria en tiempo real desde el mismo equipo como se muestra en la Figura N° 155.

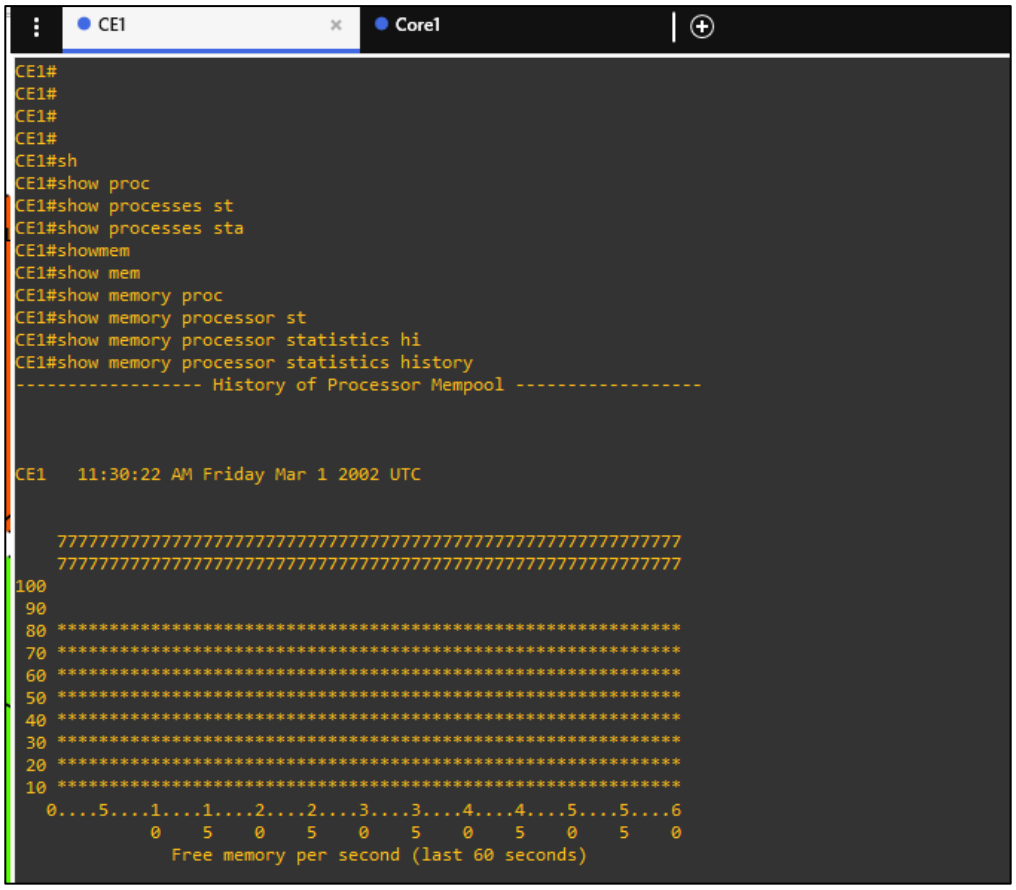


Figura N° 151 : Escenario 3 – CE1 Visualización de salud de equipos – Memoria Dispositivo
Fuente: Elaboración propia

CE1 – Opmanager: Adicionalmente esto se pudo ver de forma gráfica e histórica en la herramienta como se muestra en la Figura N° 152.

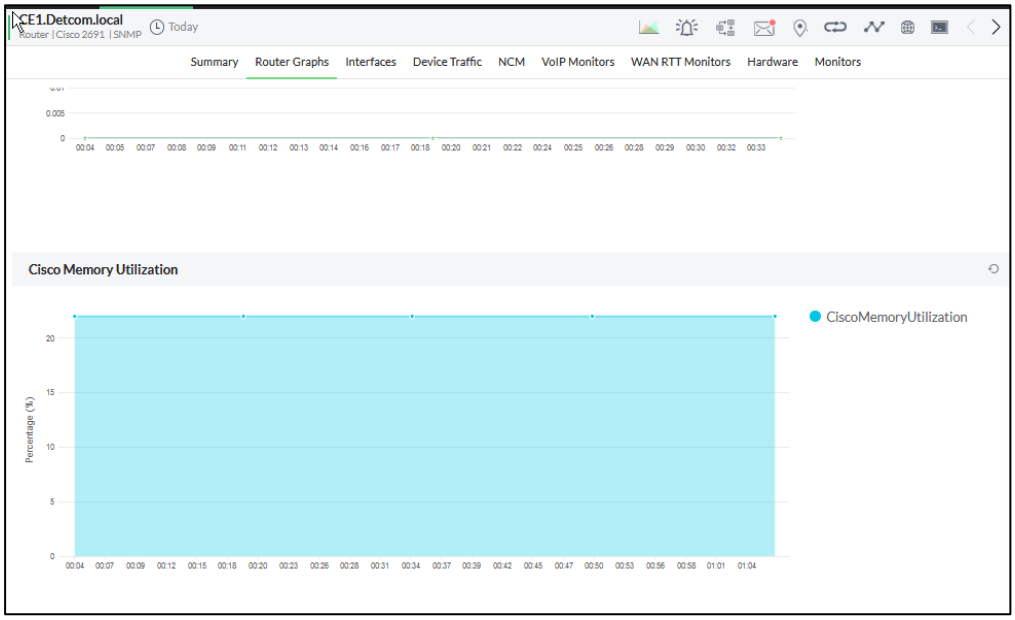


Figura N° 152: Escenario 3 – CE1 Visualización de salud de equipos – Memoria Opmanager
Fuente: Elaboración propia

Escenario 4: Se envió protocolo ICMP para la visualización de latencia y perdida de paquetes.

CE1 - Dispositivo: Se generó un envió de paquete ICMP para capturar en tiempo real la latencia y perdida de paquetes desde el dispositivo como se muestra en la Figura N° 153.

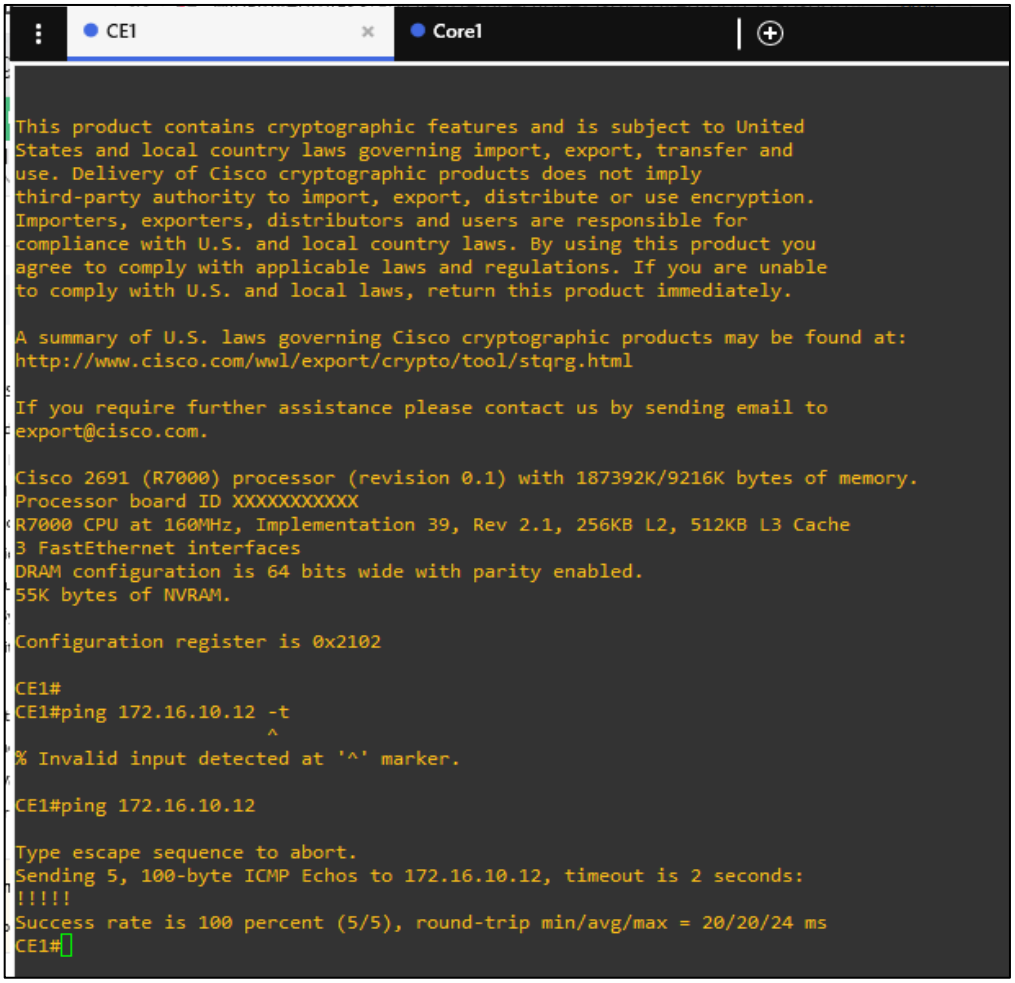


Figura N° 153: Escenario 4 – CE1 Envió de protocolo ICMP para la visualización de latencia y perdida de paquetes - Dispositivo
Fuente: Elaboración propia

CE1 - Opmanager: La información que obtuvimos del dispositivo será la misma que está recopilando, esta se vió en la herramienta de gestión y monitoreo como se muestra en la Figura N° 154.

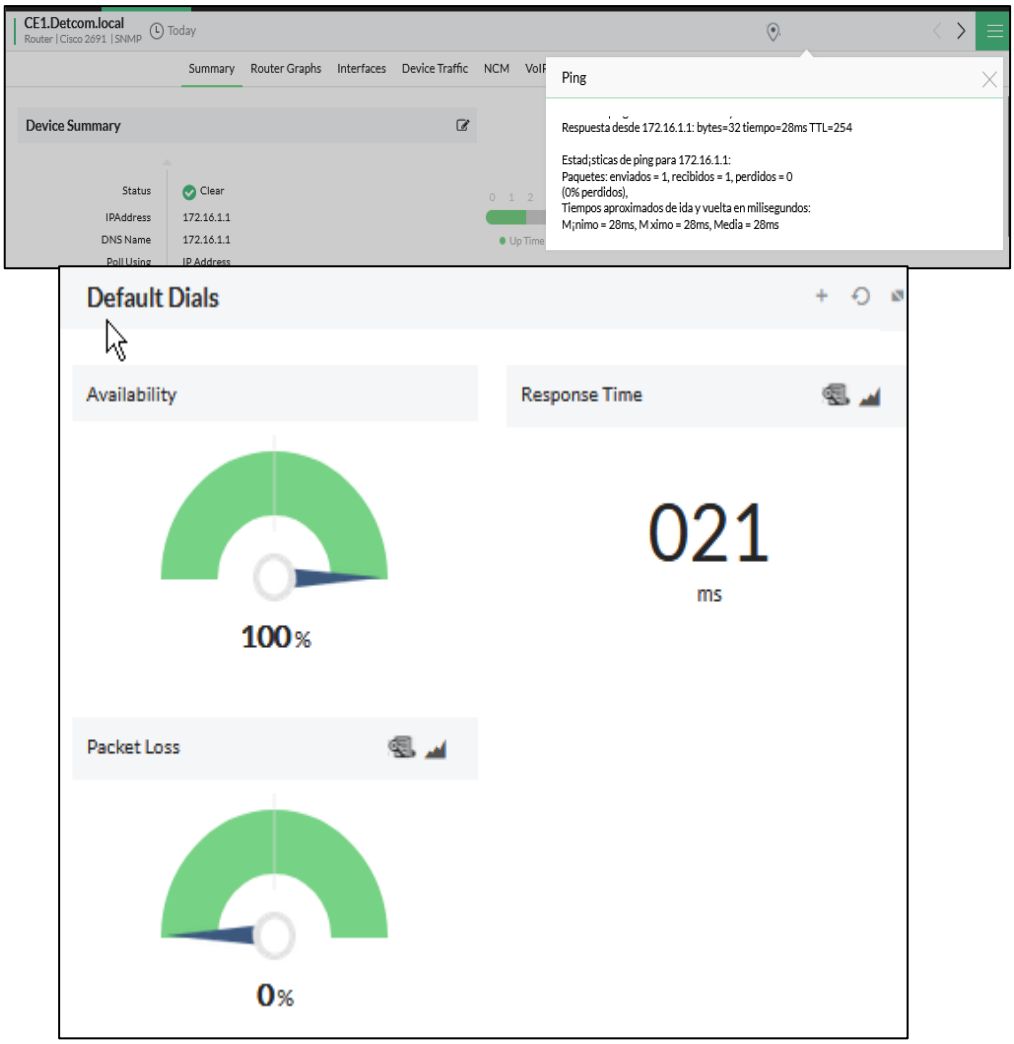


Figura N° 154: Escenario 4 – CE1 Envió de protocolo ICMP para la visualización de latencia y perdida de paquetes - Opmanager
Fuente: Elaboración propia

Core2 - Dispositivo: Se generó un envió de paquete ICMP para capturar en tiempo real la latencia y perdida de paquetes desde el dispositivo como se muestra en la Figura N° 155.

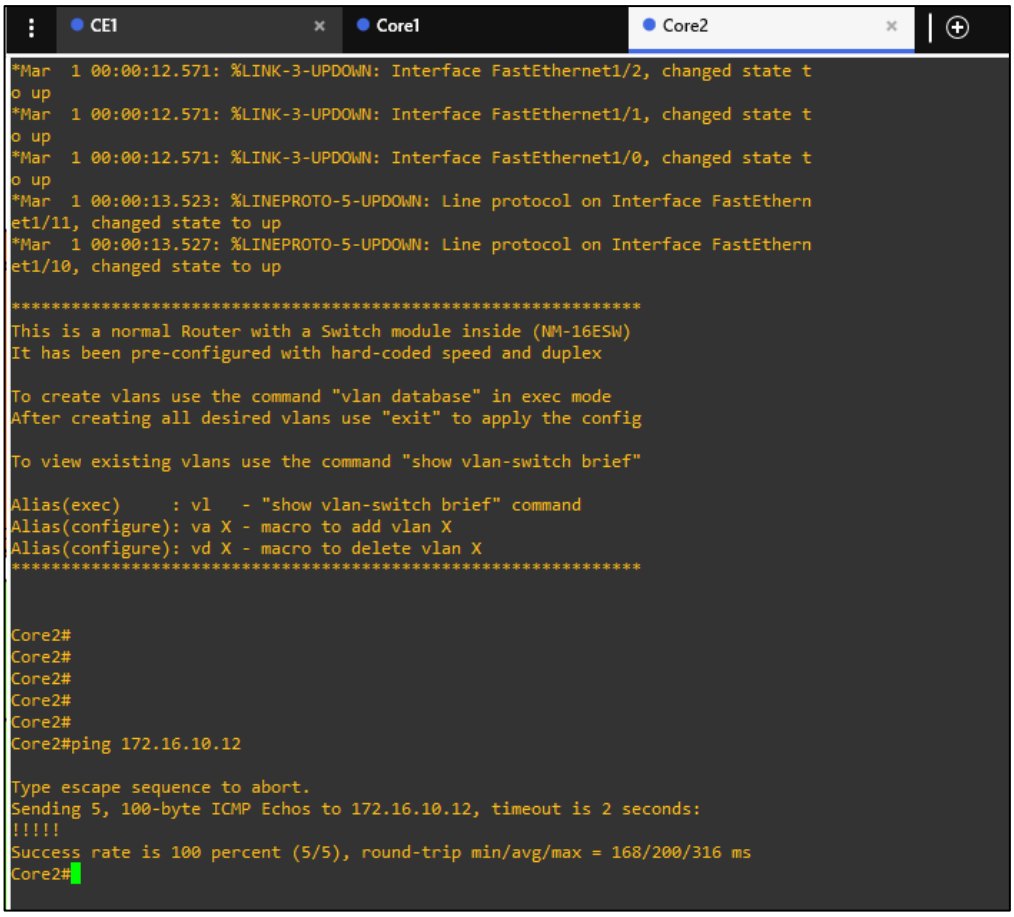


Figura N° 155: Escenario 4 – Core2 Envió de protocolo ICMP para la visualización de latencia y perdida de paquetes - Dispositivo
Fuente: Elaboración propia

Core2 - Opmanager: La información que observamos en el dispositivo será la misma que está recopilando y se visualizó en la herramienta de gestión y monitoreo como se muestra en la Figura N° 156.

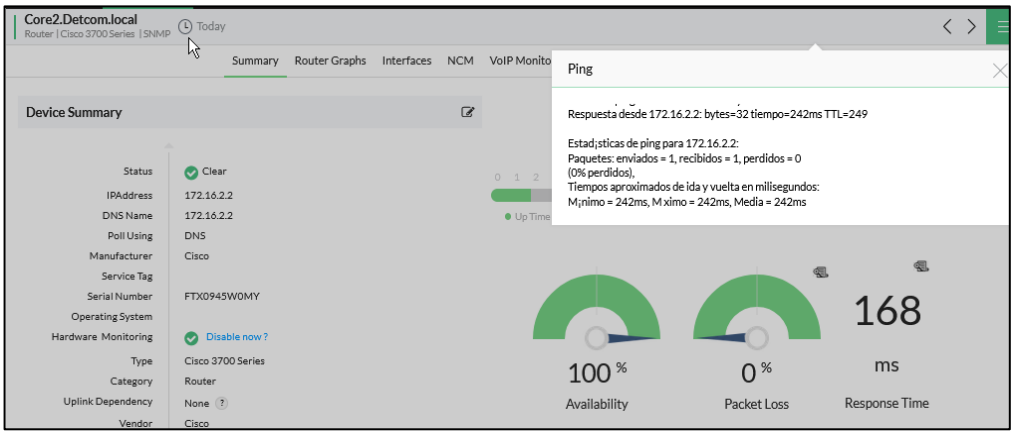


Figura N° 156: Escenario 4 – Core2 Envió de protocolo ICMP para la visualización de latencia y perdida de paquetes - Opmanager
Fuente: Elaboración propia

Escenario 5: Apagado y desconexión de equipos router y switch en la red.

Core 2 - Dispositivo: Se generó el apagado del dispositivo como se muestra en la Figura N° 157 para generar una alarma en la herramienta de monitoreo y gestión.

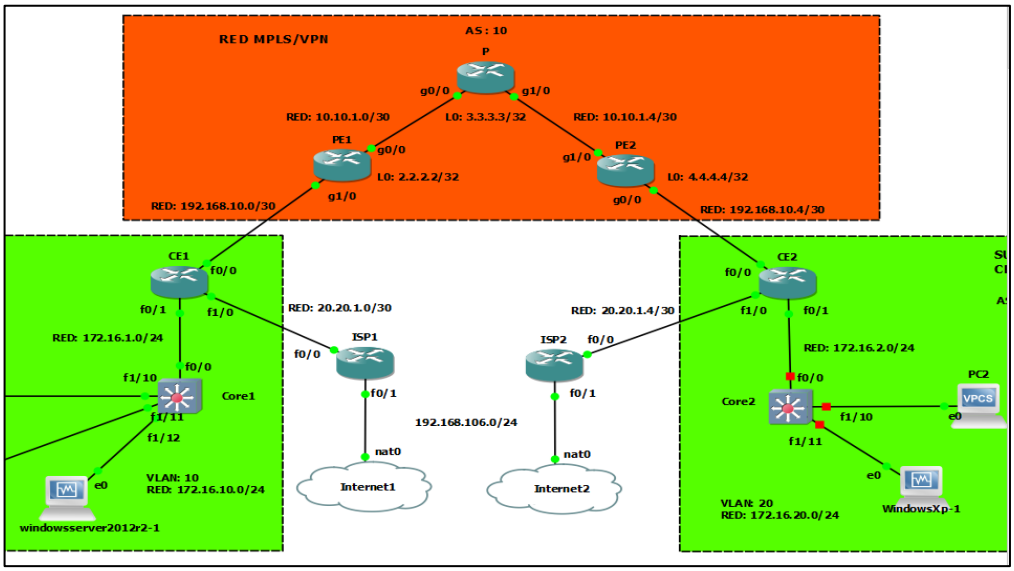


Figura N° 157: Escenario 5 – Core2 Apagado y desconexión de equipos router y switch en la red - Dispositivo
Fuente: Elaboración propia

Core 2 - Opmanager: Se visualizó el apagado del dispositivo en el Opmanager como se muestra en la Figura N° 158. la alarma de sondeo se activó.

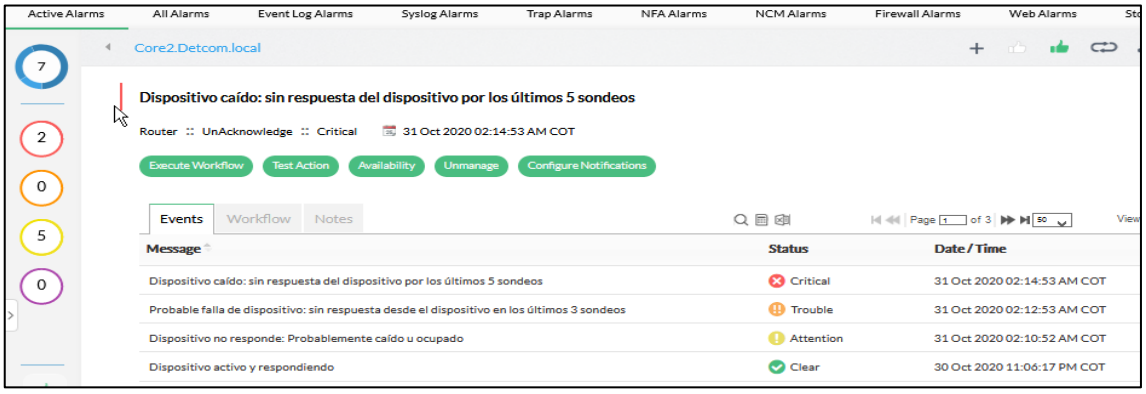


Figura N° 158: Escenario 5 – Core2 Apagado y desconexión de equipos router y switch en la red - Opmanager
Fuente: Elaboración propia

Core 2 - Opmanager: El servidor por defecto tiene la regla configurada para enviar cinco sondeos los cuales al no recibir respuesta se activó una alarma para informar de una anomalía en la red como se mostró en la Figura N° 159.

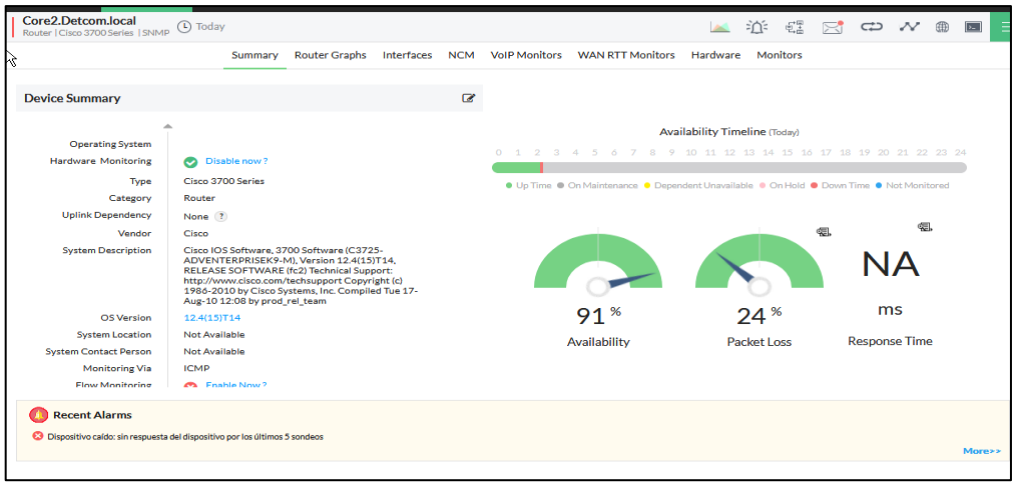


Figura N° 159: Escenario 5 – Core2 Apagado y desconexión de equipos router y switch en la red - Opmanager
Fuente: Elaboración propia

Core 2 - Opmanager: Estas alarmas aparecieron de forma automática en un pop-up como se muestra en la Figura N° 160.

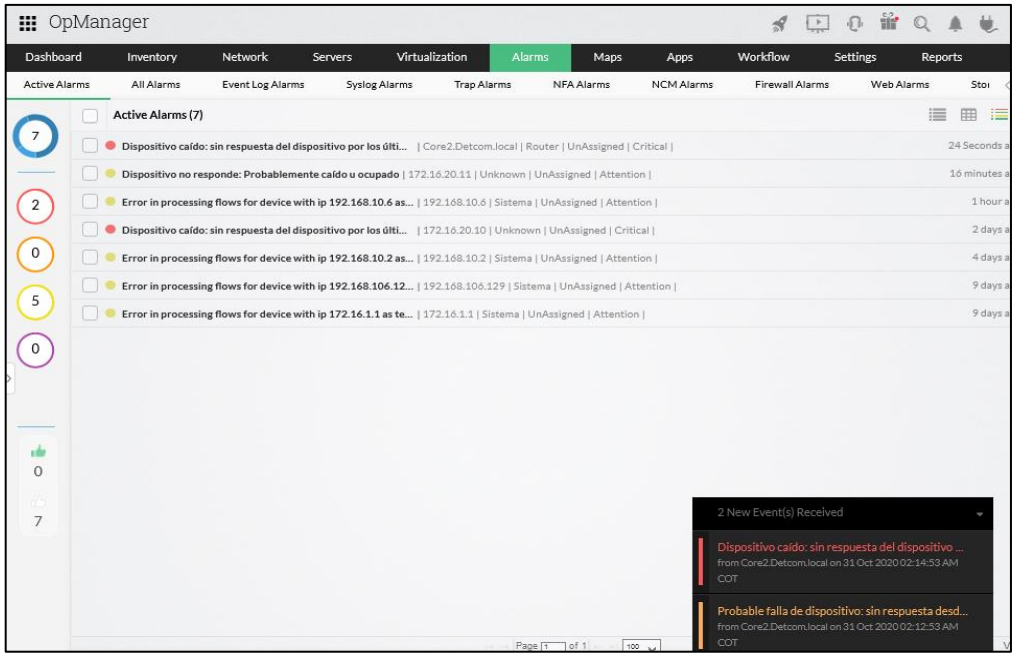


Figura N° 160: Escenario 5 – Core2 Apagado y desconexión de equipos router y switch en la red - Opmanager
Fuente: Elaboración propia

Core 2 – CE 2- Dispositivo: Para este punto se sumó la caída del dispositivo CE2, generando una caída total del servicio en la sede. (véase la Figura N° 161).

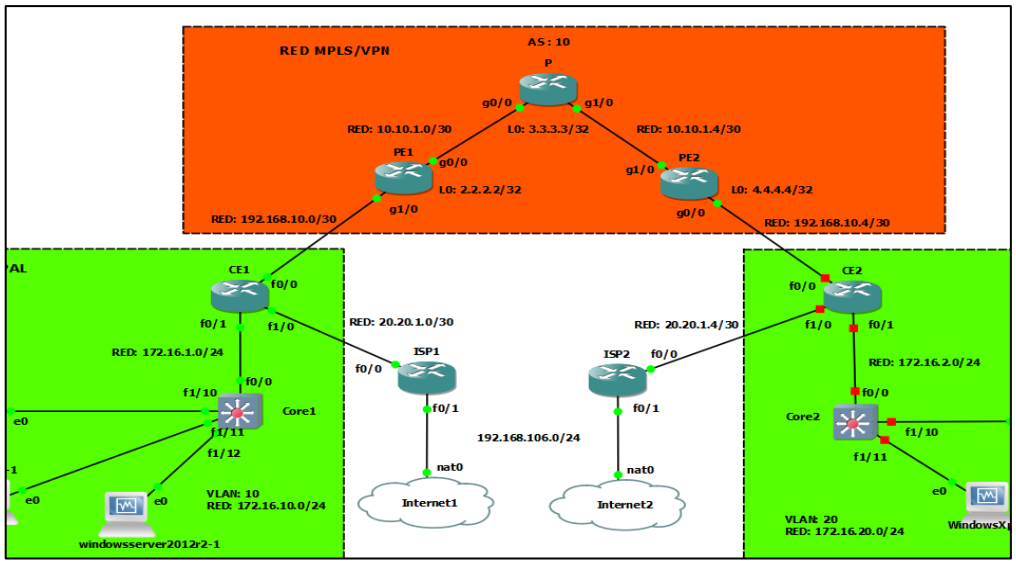


Figura N° 161: Escenario 5 – Core2-CE2 Apagado y desconexión de equipos router y switch en la red - Dispositivo
Fuente: Elaboración propia

Core 2 – CE 2- Opmanager: Se visualizó el apagado de los dos dispositivos en el Opmanager, como se muestra en la Figura N° 162 se activó un pop-up indicando que se tienen dos dispositivos alarmados.

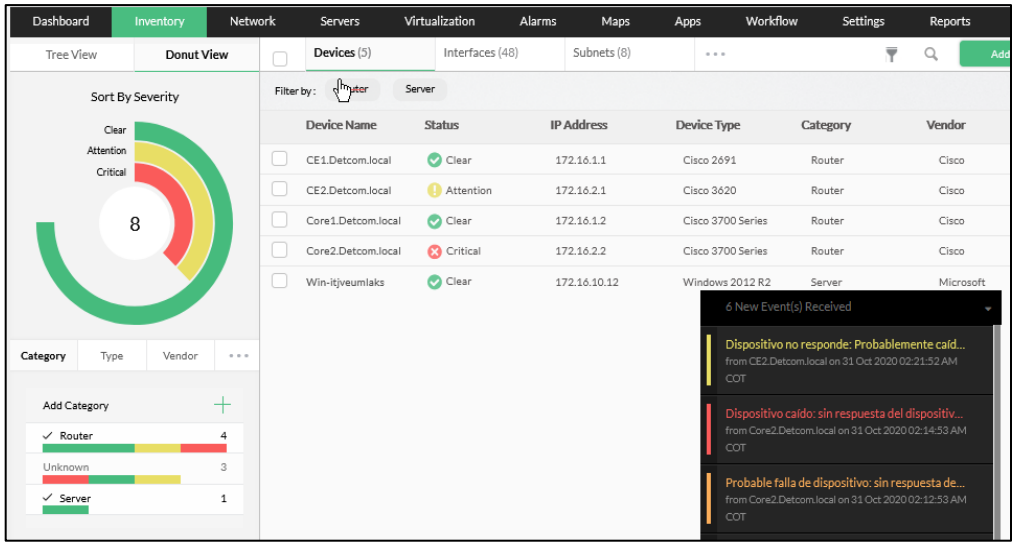


Figura N° 162: Escenario 5 – Core2-CE2 Apagado y desconexión de equipos router y switch en la red - Dispositivo
Fuente: Elaboración propia

Core 2 – CE 2- Dispositivo: Asimismo, se realizó el encendido de los dispositivos para recuperar el servicio en la sede y esto se visualizó en la herramienta de monitoreo y gestión (véase Figura N° 163).

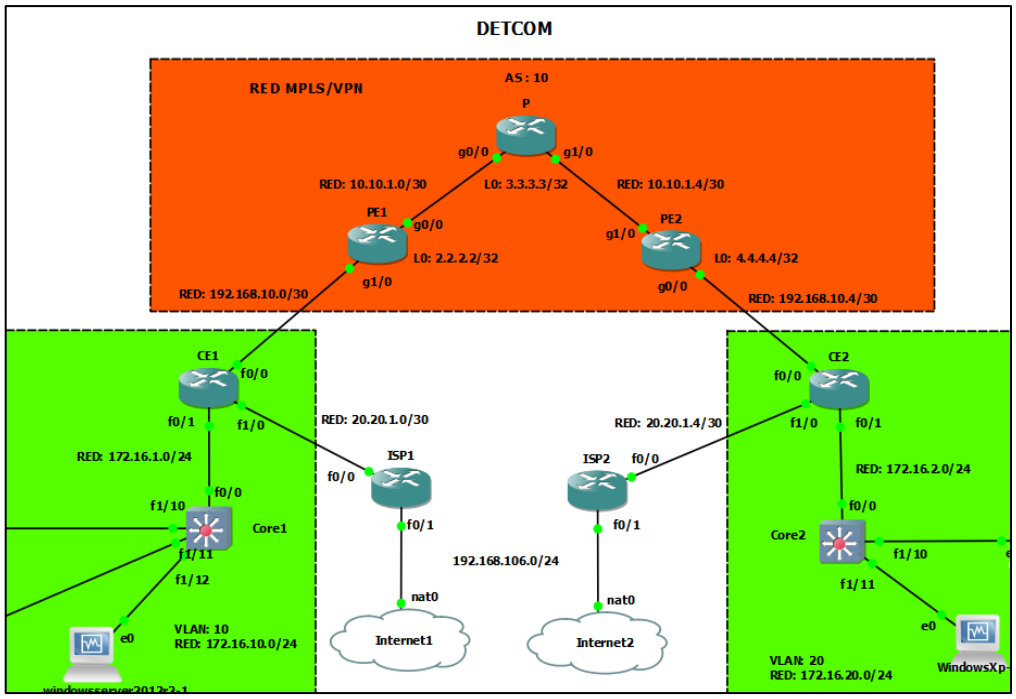


Figura N° 163: Escenario 5 – Core2-CE2 Apagado y desconexión de equipos router y switch en la red - Dispositivo
Fuente: Elaboración propia

Core 2 – CE 2- Opmanager: La herramienta detectó de manera automática la recepción del sondeo y se activó la alarma de “dispositivo activo y respondiendo” como se muestra en la Figura N° 164.

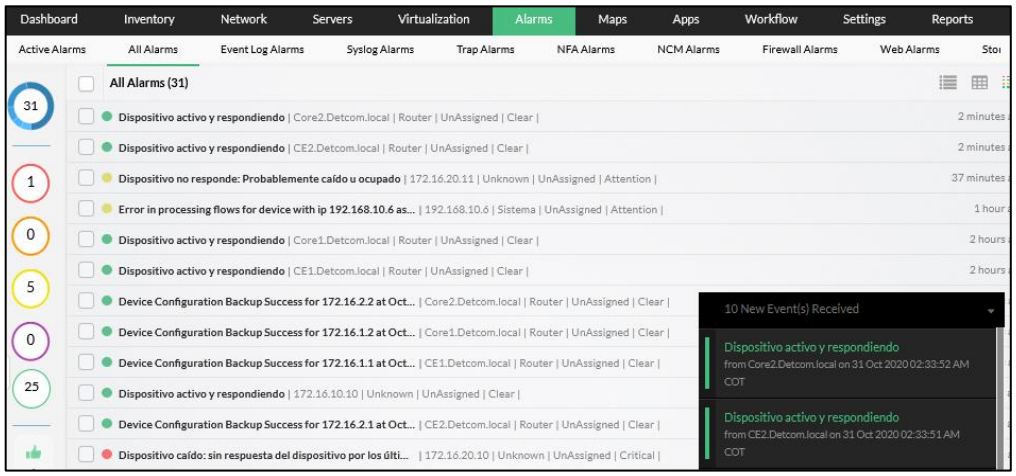


Figura N° 164: Escenario 5 – Core2-CE2 Apagado y desconexión de equipos router y switch en la red - Opmanager
Fuente: Elaboración propia

Escenario 6: Caída de la red MPLS.

MPLS- RED: Se generó una caída en la red MPLS para ver cómo reaccionaba la herramienta frente a este evento. (véase la Figura N° 165).

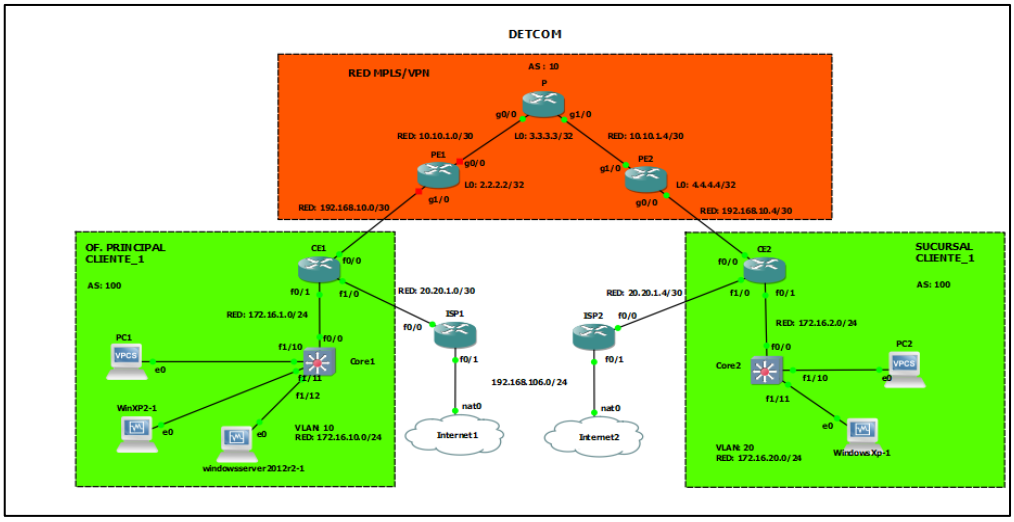


Figura N° 165: Escenario 6 – MPLS- Caída de la red MPLS - Red
Fuente: Elaboración propia

MPLS- Opmanager: Se visualizó la activación de alarmas de caída total de una sede, esto se debió a la falta conectividad entre los dispositivos. En la siguiente imagen se muestra las alarmas véase Figura N° 166.

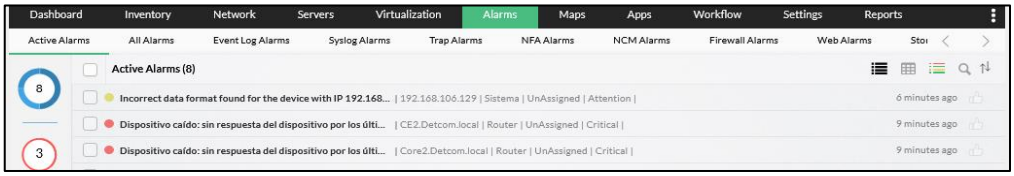


Figura N° 166: Escenario 6 – MPLS- Caída de la red MPLS - Opmanager
Fuente: Elaboración propia

Escenario 7: Apagado y desconexión de puertos a nivel de usuario.

Core1 – Dispositivo: Se apagó el puerto fastethernet1/10 para simular la caída o desconexión a nivel de usuario como se muestra en la Figura N° 167.

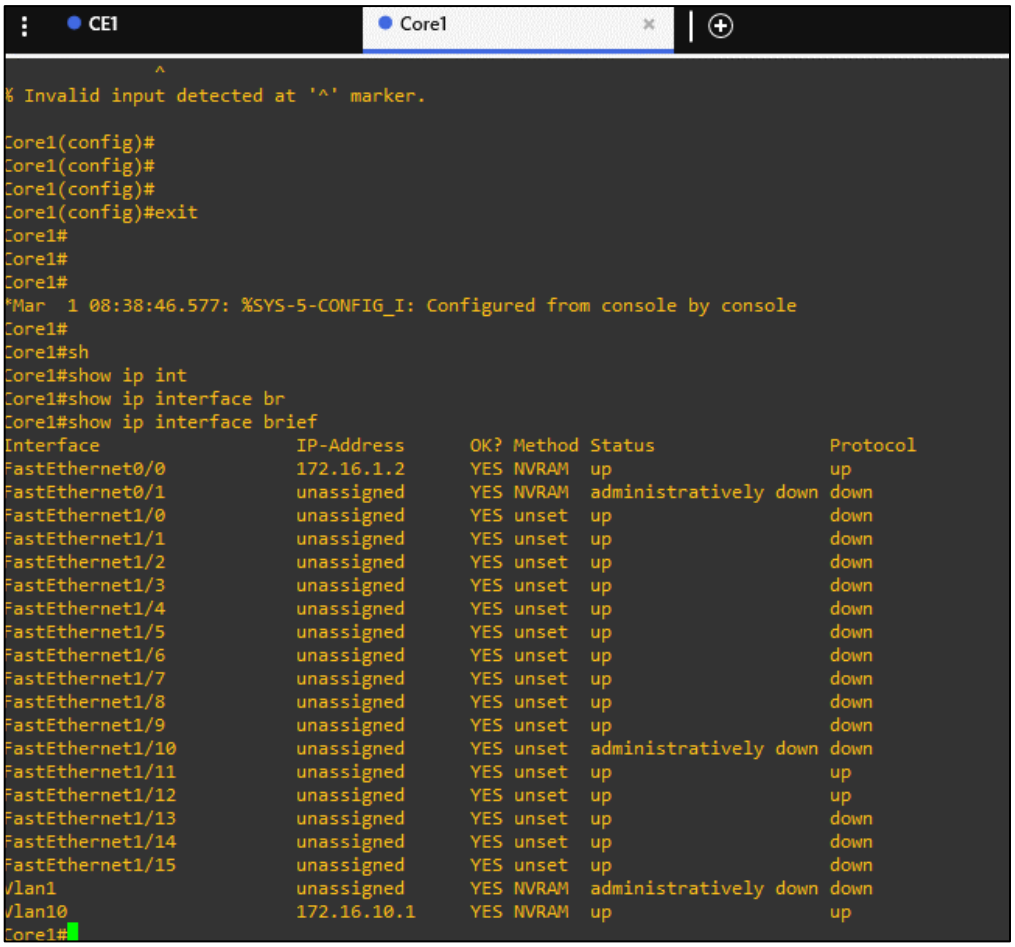


Figura N° 167: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Dispositivo
Fuente: Elaboración propia

Core1 – Dispositivo: Se apagó el puerto fastethernet1/10 para simular la caída o desconexión a nivel de usuario como se muestra en la Figura N° 168.

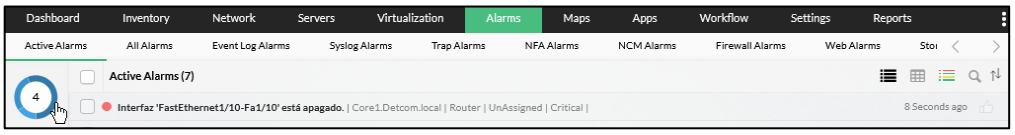


Figura N° 168: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager
Fuente: Elaboración propia

Core1 – Opmanager: Esta caída del puerto fastethernet1/10 se reflejó en la herramienta de monitoreo y gestión, activándose un pop up que nos informó del suceso de un evento como se muestra en la Figura N° 169.

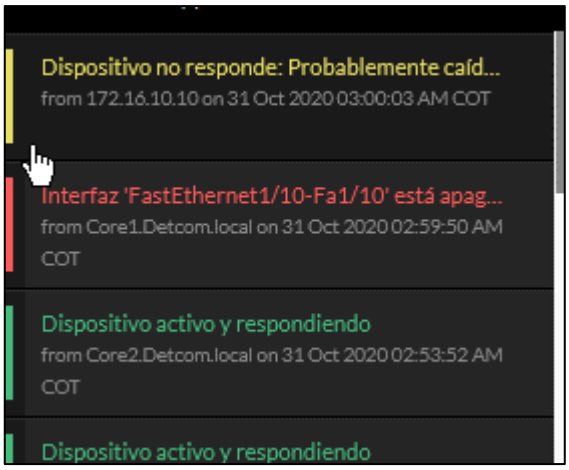


Figura N° 169: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager
Fuente: Elaboración propia

Core1 – Opmanager: Cuando se ingresó a la alarma, se obtuvo un mayor detalle e información como el nombre del puerto, hora y fecha del evento como se muestra en la Figura N° 170.

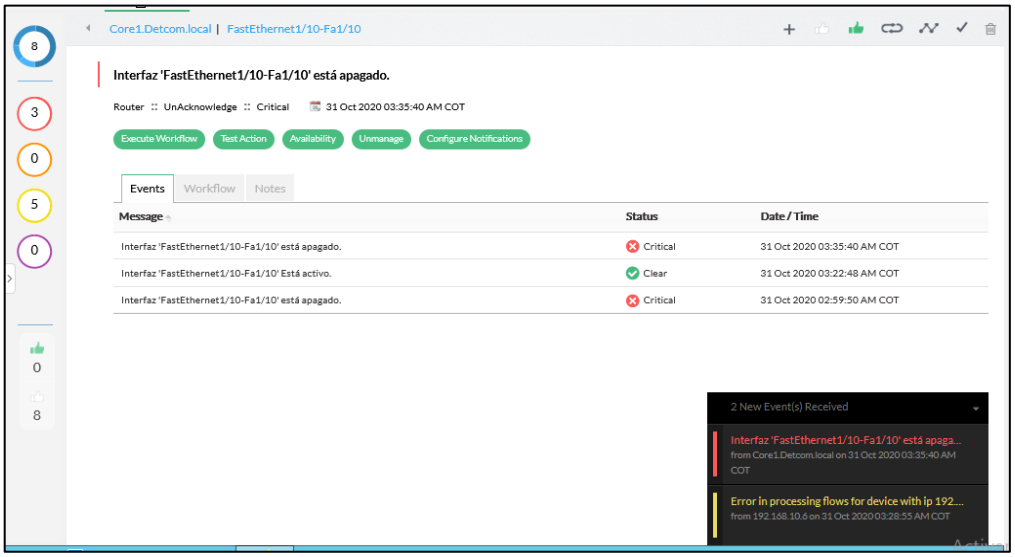


Figura N° 170: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager
Fuente: Elaboración propia

Core1 – Opmanager: Asimismo, se ingresó al equipo alarmado en cual se vió la alarma que se encontraba activa, para mayor detalle ver la Figura N° 171.

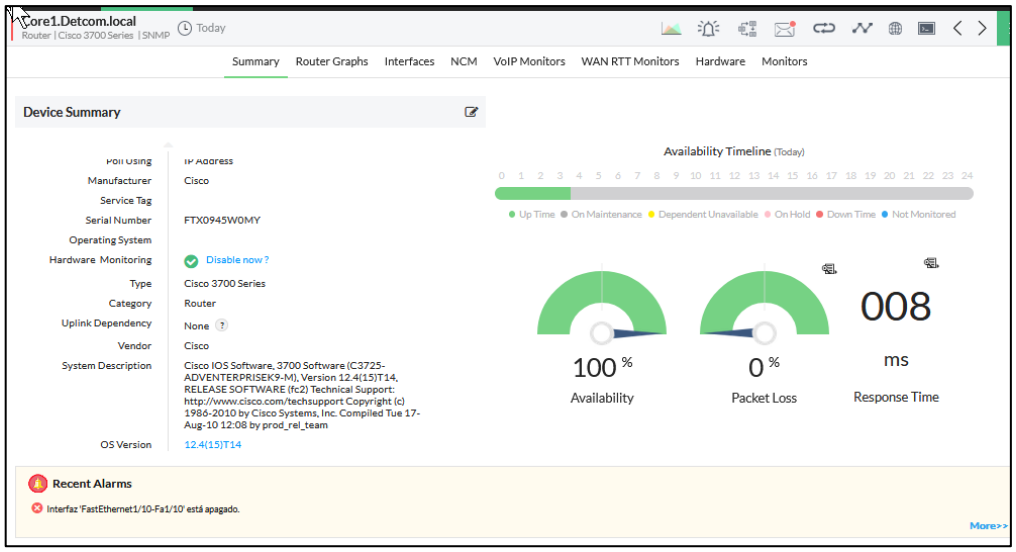


Figura N° 171: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager
Fuente: Elaboración propia

Core1 – Opmanager: Después volvimos a encender el puerto y se vió que automáticamente se refleja el cambio de estado del puerto en la herramienta como se muestra en la Figura N° 172. pasando el estado del puerto a activo.

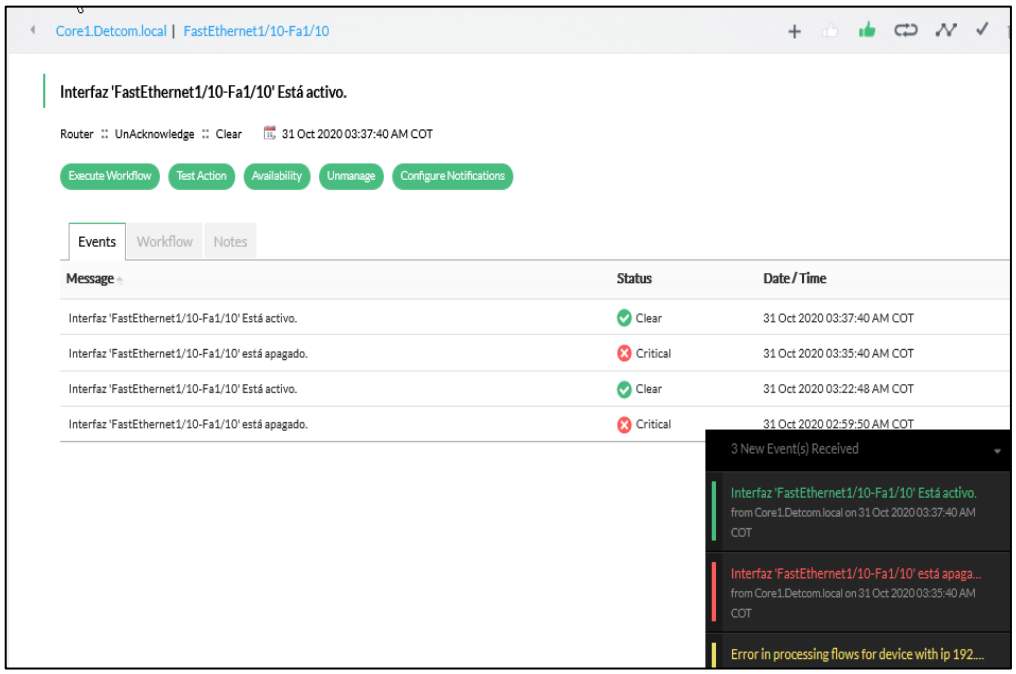


Figura N° 172: Escenario 7– Apagado y desconexión de puertos a nivel de usuario - Opmanager
Fuente: Elaboración propia

CAPITULO V: ASPECTOS ADMINISTRATIVOS

5.1 Recursos humanos

La elaboración del presente proyecto se desarrolló en dos fases, esto debido a la pandemia del Covid-19, que restringió el acceso a las instalaciones del cliente, motivo por el cual la primera fase se basa al tiempo invertido en la emulación de replicar parte de la topología actual del cliente. En la Tabla 15 observamos las horas hombre que se invirtió en el desarrollo de la emulación indicada.

Tabla 15: Horas hombre por mes para la emulación

N°	TAREAS	FRECUENCIA	CANTIDAD (PROMEDIO)	TIEMPO POR TAREA (PROMEDIO EN HRS)	TIEMPO TOTAL (HRS)	TIEMPO TOTAL HORAS POR MES
1	Reuniones con el cliente	Semanal	2	0.5	1	4
2	Visita técnica	Mensual	5	1.5hrs	7.5	7.5
3	Configuración y emulación de la topología	Semanal	2	3.5	7	28
4	Pruebas de incidencias	Mensual	2	1	2	2
5	Ejecución de reportes	Mensual	1	1	1	1
TOTAL DE HORAS EN EL MES						**42.5**

Fuente: Elaboración propia

En la segunda fase hacemos referencia al tiempo de ejecución que tomó la implementación y configuración tanto del software OpManager así como la configuración de los protocolos SNMP y NETFLOW en los equipos de la LAN (router y switching) y la capacitación brindada tanto en modo usuario como a nivel administrador. En la siguiente Tabla 16 se muestran los tiempos en el despliegue de la solución brindada.

Tabla 16: Implementación de la solución por días

N°	TAREAS	EQUIPOS	PERSONAL	TIEMPO	TIEMPO TOTAL (HRS)	TIEMPO TOTAL HORAS POR MES
1	Configuración de los protocolos SNMP y NETFLOW	Router y Switching	1	2 días	4	8
2	Implementación del OpManager	Servidor de Aplicaciones	1	1 día	4	4
3	Marcha blanca	Dispositivos LAN	1	5 días	1.5	7.5
4	Capacitación a Nivel de usuario	Personal de soporte TI	1	1 día	2	2
5	Capacitación a Nivel de administrador	Personal de soporte TI y Jefe de TI	1	2 días	4	8
TOTAL DE HORAS EN EL MES						**29.5**

Fuente: Elaboración propia

5.2 Materiales

En el presente proyecto, los materiales involucrados que se necesitarán para la implementación del software de gestión y monitoreo involucran lo siguiente (véase Tabla 17):

Tabla 17: Equipos utilizados

Equipo/Software	Descripción	Estado
Servidor	PowerEdge R630 - Dell	Proporcionado por la empresa
Sistema Operativo	Windows 2012 R2	Proporcionado por la empresa
Software	OpManager	Adquisición

Fuente: Elaboración propia

Para la emulación de la topología presentada se utilizó las siguientes aplicaciones (véase Tabla 18):

Tabla 18: Aplicaciones utilizadas

Equipo/Software	Descripción	Estado
GNS3	Software de emulación de redes LAN, WAN y MPLS	Obtención de forma gratuita
IOS Router 7200	Software del router de enlace MPLS	Obtención del fabricante Cisco
IOS Router 2691	Software del router enlace MPLS	Obtención del fabricante Cisco
ISO Switch 3725	Software del switch Core de la LAN	Obtención del fabricante Cisco
Virtual Box	Software de emulación de máquinas virtuales	Obtención de forma gratuita
FileZilla FTP	Software de emulación del servicio FTP	Obtención de forma gratuita
Sistema Operativo	Windows XP	Obtención de forma gratuita
Sistema Operativo	Windows 2012 R2	Obtención de forma gratuita
Software de Gestión y Monitoreo	OpManager	Obtención del fabricante ManageEngine.
Computadora	Sistema donde se instalaron las aplicaciones descritas	Equipo al cual se adiciono memoria RAM.

Fuente: Elaboración propia

5.3 Presupuesto

En esta parte presentamos los costos asociados al proyecto, los cuales los podemos definir de la siguiente manera.

INVERSIÓN CAPEX:

A continuación, se presenta la Tabla 19 de costos de inversión el cual incluye únicamente el costo por licenciamiento dado que el software de monitoreo y gestión se obtuvo de forma gratuita desde la página del fabricante ManageEngine.

Tabla 19: Costo CAPEX del proyecto

CAPEX						
		ESTIMACIÓN		NEGOCIACIÓN		
ITEM	PROVEEDOR	P. UNIT.	P. TOTAL(E)	P. UNIT.	P. TOTAL(N)	DIFERENCIA(E-N)
Sistema de monitoreo Opmanager Profesional Perpetual y configuración (10 Dispositivos)	ManageEngine	$ 620.00	$ 620.00	$558.00	$ 558.00	$ 62.00
Capacitación de Opmanager para 3 Personas	Partner de ManageEngine	$ 320.00	$ 320.00	$ 280.00	$ 280.00	$ 40.00

Fuente: Elaboración propia

INVERSIÓN OPEX:

En la Tabla 20, se presentan los costos de operación del proyecto, los cuales involucran la implementación, configuración, capacitación y soporte tanto del OpManager como de los dispositivos de la red LAN (routers y switching).

Tabla 20: Costo OPEX del proyecto

OPEX (1 AÑO)					
ITEM	PROVEEDOR	UNIT	CANT.	P. UNIT. X Mes	P. TOTAL
Soporte 5*8	Partner de ManageEngine	1	12	$ 120.00	$ 1,440.00

Fuente: Elaboración propia

Adicionalmente presentamos el detalle del SLA (Service Level Agreement) del soporte propuesto en el OPEX:

-El cliente debe garantizar acceso remoto hacia el servidor.

-Tiempo de respuesta: 1 Hora.

-Tiempo de solución de incidentes críticas: 4 Horas

-Tiempo de solución de incidentes media: 16 Horas

-Tiempo de solución de incidentes baja: 24 Horas

ANALISIS VAN(Valor actual neto) Y TIR(Tasa interna de retorno) - RENTABLIDAD

En esta investigación se asignó una inversión de $2,380.00 ~ S/ 8,544.20, por la sensibilidad de la información no se puede compartir el flujo de caja real del área de TI, por este motivo y experiencias propias se asume un flujo de caja basados en una estimación por un periodo de 5 años. En la Tabla 21 se presenta el costo de inversión.

Tabla 21: Costo de inversión

COSTO DE INVERSIÓN	
ITEM	**PRECIO**
COSTO CAPEX	$ 940.00
COSTO OPEX	$ 1,440.00
TOTAL	**$ 2,380.00**

Fuente: Elaboración propia

En la presenta Tabla 22 se muestra el flujo de caja asumido para el área TI para un periodo de 5 años.

Tabla 22: Flujo de caja de TI

	FLUJO DE CAJA DE TI				
ITEMS / AÑOS	**2020(S/)**	**2021(S/)**	**2022(S/)**	**2023(S/)**	**2024(S/)**
INGRESOS ANUALES					
Caja chica	9,840.45	12,385.75	11,739.26	13,220.63	14,170.04
TOTAL DE INGRESO ANUAL	9,840.45	12,385.75	11,739.26	13,220.63	14,170.04
EGRESOS ANUALES					
Horas extras	8,536.36	8,536.36	8,536.36	8,536.36	8,536.36
Movilidades	1,235.25	1,235.25	1,235.25	1,235.25	1,235.25
Otros	516.89	475.93	218.37	383.29	345.33
TOTAL DE EGRESO ANUAL	10,288.50	10,247.54	9,989.98	10,154.90	10,116.94
UTILIDAD	- 448.05	2,138.21	1,749.28	3,065.73	4,053.09
Saldo inicial	250.00	- 198.05	1,940.15	3,689.43	6,755.16
FLUJO DE CAJA	**- 198.05**	**1,940.15**	**3,689.43**	**6,755.16**	**10,808.25**

Fuente: Elaboración propia

En la siguiente Tabla 23, se observa que el proyecto es rentable (VAN > 0 y TIR> 0) por este motivo se justifica su implementación.

Tabla 23: Tabla de rentabilidad

RENTABILIDAD	
INTERES	0.1
VAN	S/ 6,976.04
TASA INTERNA DE RETORNO (TIR)	27.64%

Fuente: Elaboración propia

5.4 Cronograma de actividades

En la presente Figura N° 173-175, se muestra el cronograma de actividades referidas a la presente investigación de tesis.

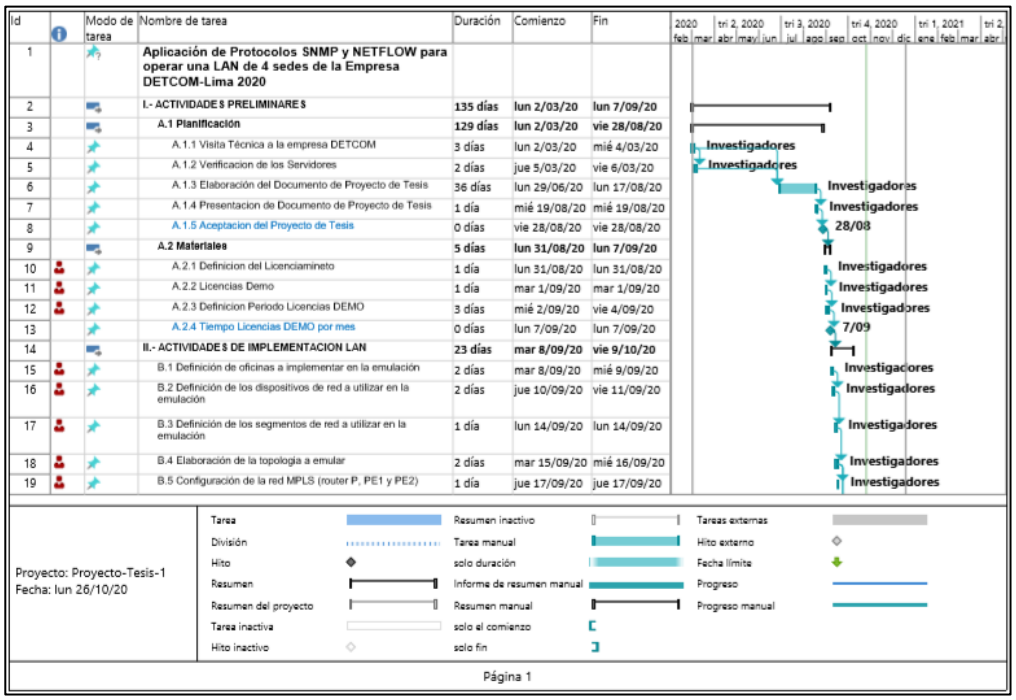


Figura N° 173: Cronograma de actividades
Fuente: Elaboración propia

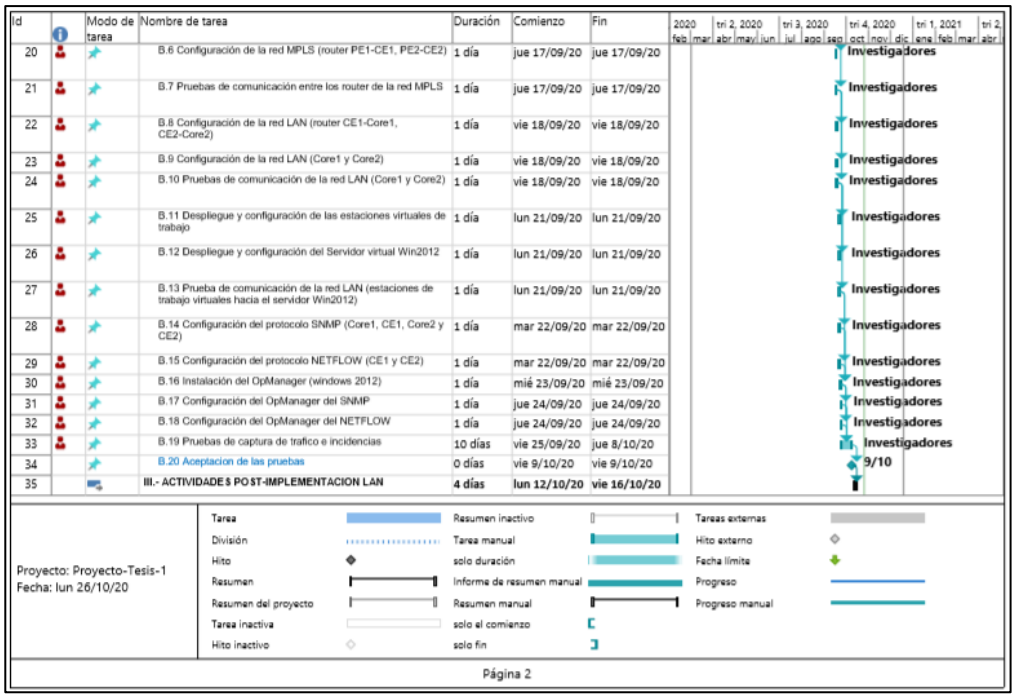


Figura N° 174: Cronograma de actividades
Fuente: Elaboración propia

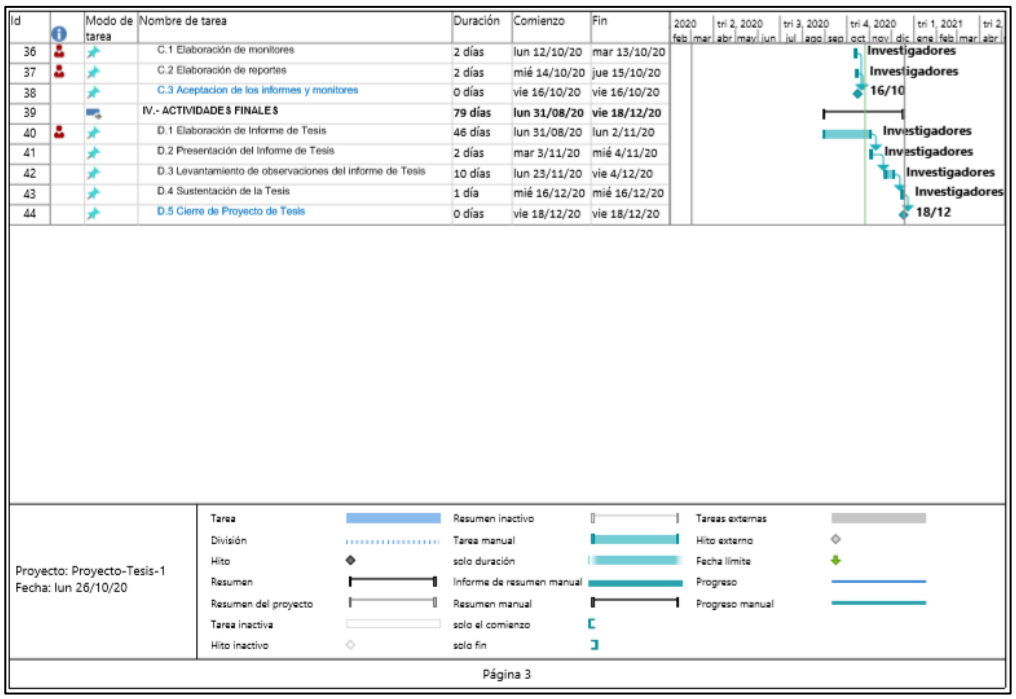


Figura N° 175: Cronograma de actividades
Fuente: Elaboración propia

CONCLUSIONES

1. El aplicar los protocolos SNMP y NETFLOW favoreció en la visibilidad y análisis del ancho de banda en la LAN porque el administrador de red ahora puede monitorear en tiempo real el uso del ancho de banda de salida hacia internet y entre oficinas. Con la herramienta de monitoreo y gestión se puede parametrizar su ancho de banda de salida a internet para prevenir la saturación de este y con los reportes obtenidos analizar de forma granulada el uso del servicio por parte de los usuarios y tomar decisiones que favorezcan a mejorar el acceso y disponibilidad.

2. Emplear los protocolos SNMP y NETFLOW incidió en el análisis de rendimiento de la LAN porque ahora el administrador de red puede monitorear la salud de los dispositivos de la red, determinar la latencia y perdidas de paquetes a través de la herramienta de monitoreo y gestión, así poder determinar en qué momento o porque se presentan retardos en la LAN. Los reportes presentan datos específicos que ayudan en el análisis para el mejoramiento continuo de la LAN.

3. Al aplicar los protocolos SNMP y NETFLOW ayudó en gran medida la administración de incidencias en la LAN porque el administrador de red visualiza alarmas que reportan una desconexión o evento en un dispositivo de una oficina, disponibilidad del enlace entre oficinas e incidencias a nivel de interfaz de usuario. De esta manera poder actuar de forma proactiva y eficiente en la resolución del problema, Los reportes benefician en la toma rápida de decisiones para solucionar incidencias o en su defecto si se detectan muchas incidencias poder determinar el origen del problema.

La aplicación de los protocolos SNMP y NETFLOW en los dispositivos de la red ayudó en gran medida a tener una mejor gestión y monitoreo de la LAN tanto en la oficina principal como en las sucursales, esto se pudo comprobar en los resultados obtenidos de las pruebas de emulación realizadas cumpliendo así con los objetivos planteados en la presente investigación. Con la herramienta de monitoreo y gestión implementado se puede visualizar la información enviada desde los dispositivos de la red respecto a los

protocolos SNMP y NETFLOW, con estos datos recopilados se pueden tomar decisiones de mejora en la LAN que ayudará a futuro en nuevas implementaciones necesarias para la empresa.

RECOMENDACIONES

1. La empresa DETCOM cuenta con salidas al servicio a internet independiente en cada oficina, al tener una red gestionada y obtener reportes o informes personalizados de acuerdo con el uso de los servicios de Internet, se puede sustentar en un futuro contar con un solo circuito de Internet, y con un ancho de banda acorde al uso de los usuarios y específicamente al buen uso del servicio. Esto traerá un ahorro de costos de servicios a la empresa y un acceso a Internet gestionado y controlado.

2. En base a los reportes de rendimiento de hardware que se obtienen de la herramienta de monitoreo y gestión, se podrá elaborar un plan de actualizaciones de IOS para los router y switching que se tienen en gestión, cambios en el hardware, elaborar un plan de mantenimiento y mejorar el rendimiento de operación de los dispositivos de la LAN.

3. Configuración de las alarmas vía correo, móvil y/o SMS. De esta manera poder actuar de una manera más rápida y eficiente frente a una incidencia que pueda afectar la operación de la LAN.

4. Al tener informes referidos al enlace de internet, y tener una visualización del tráfico que se cursa de entrada y salida, se puede optar como mejoras en la parte de seguridad y acceso en poder adquirir un equipo firewall, con el cual podrá aplicar políticas de acceso a internet, controlar el ingreso hacia la LAN mediante accesos VPN y actuar de forma rápida y efectiva ante cualquier amenaza de ataque que se podrían presentar.

5. En caso el cliente quiera instalar una sede a nivel nacional se recomienda tener en cuenta la factibilidad con el operador para la MPLS, y para el caso del software de monitoreo y gestión ya que es una solución escalable se tiene que dimensionar nuevas licencias y soporte para los nuevos dispositivos.

REFERENCIAS BIBLIOGRÁFICAS

Alcócer, C. (2000). *Redes de Computadoras (2da Ed.).* Lima - Perú: Infolink E.I.R.L.

Ariganello, E. (2016). *Redes Cisco-Guia de estudio para la certificaciòn CCNA Routing y Switching.* Bogota: Ra-Ma.

Ariganello, E., & Barrientos, S. E. (2016). *Redes Cisco - Guía de estudio para la certificación CCNP Routing y Switching.* Bogota: Ra-Ma.

Auvik.com. (2019). *The evoluiton of NETFLOW*. Obtenido de https://www.auvik.com/franklyit/blog/netflow-basics/. Recuperado:06 de junio del 2020.

Becerra, O. E. (2016). *IMPLEMENTACIÓN DE MONITOREO DE RED UTILIZANDO LOS PROTOCOLOS ICMP Y SNMP. (Tesis de Pregrado).* UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA, La Libertad, Ecuador. Obtenido de https://repositorio.upse.edu.ec/xmlui/handle/46000/2583. Recuperado:11 de julio del 2020.

Behar, D. (2008). *Metodología de la Investigación.* Bogota: Shalom.

Bhardwaj, R. (2019). *SNMP vs Netflow.* Obtenido de https://ipwithease.com/snmp-vs-netflow/ Recuperado:21 de noviembre del 2020.

Calvo, G. A. (2016). *Gestión de redes telemáticas.* Malaga, España: IC Editorial.

Case, J., McCloghrie, Rose, M., & Waldbusser, S. (1996). *RFC 1901 Introduction to Community-basedSNMPv2.* Obtenido de https://www.ietf.org/rfc/rfc1901.txt. Recuperado:22 de junio del 2020.

Case, J., Mundy, R., Partain, D., & Stewart, B. (2002). *RFC 3410 Introduction and Applicability Statements for Internet Standard Management Framework.* Obtenido de https://tools.ietf.org/html/rfc3410. Recuperado:16 de mayo del 2020.

Cisco. (2018). *Sistema de administración de red: Informe oficial de Mejores Prácticas.* Obtenido de https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/15114-NMS-bestpractice.html. Recuperado:02 de mayo del 2020.

Cisco SNMP. (2008). *Trampas de SNMP (Protocolo simple de gestión de redes) compatibles con IOS de Cisco y cómo configurarlas.* Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/simple-network-management-protocol-snmp/13506-snmp-traps.html. Recuperado:07 de julio del 2020.

Claise, E. (2004). *RFC3954. Cisco Systems NetFlow Services Export Version 9.* Obtenido de https://www.ietf.org/rfc/rfc3954.txt. Recuperado:17 de mayo del 2020.

Davin, J., Case, J., Fedor, M., & Schoffstall, M. (1987). *RFC 1028 A Simple Gateway Monitoring Protoco.* Obtenido de https://tools.ietf.org/html/rfc1028. Recuperado:19 de junio del 2020.

Davin, J., J., C., M., F., & M., S. (1988). *RFC 1067 A Simple Network Management Protocol.* Obtenido de https://tools.ietf.org/html/rfc1067. Recuperado:13 de mayo del 2020.

Fernández, H. O. (2019). *Implementación de un servidor como gestión y monitoreo de servicios para la red de datos en la Ugel HUAMANGA, 2018. (Tesis de Pregrado).* Universidad Nacional de San Cristóbal de Huamanga , Ayacucho - Perú. Obtenido de http://repositorio.unsch.edu.pe/handle/UNSCH/3612. Recuperado:07 de agosto del 2020.

Fernandez, J. M. (2016). *Tarlogic Cybersecurity Experts*. Obtenido de https://www.tarlogic.com/blog/los-watering-hole-attacks/.Recuperado: 22 de agosto del 2020.

Ford, M., & Lew, K. (1998). *Tecnologías de Interconectividad de Redes.* España: Paperback.

Garcia Calvache, R. (2020). *¿QUÉ ES UN ISP?* Obtenido de https://desafiohosting.com/que-es-un-isp/. Recuperado: 22 de agosto del 2020.

Gómez Beas, D. (2016). *Resolución de incidencias en redes telemáticas (UF1881).* Malaga, España: IC Editorial. Recuperado el 19 de Setiembre de 2020, de https://elibro.net/es/lc/bibliourp/titulos/44149. Recuperado: 17 de julio del 2020.

Grupo de desarrollo global de PostgreSQL. (2020). *¿Qué es PostgreSQL?* Obtenido de https://www.postgresql.org/about/. Recuperado: 22 de agosto del 2020.

IONOS. (2020). *HTTPS: qué significa y por qué es importante.* Obtenido de https://www.ionos.es/digitalguide/hosting/cuestiones-tecnicas/que-es-https/. Recuperado: 09 de agosto del 2020.

J., C., M., F., M., S., & J., D. (1988). *RFC 1067 A Simple Network Management Protocol.* Obtenido de https://tools.ietf.org/html/rfc1067. Recuperado: 09 de agosto del 2020.

James, K., & Keith, R. (2017). *Network Routing: Algorithms, Protocols, and Arquitecture.* EEUU: Morgan Kaufmann.

Juane, P. E. (2015). *Analysis of possibilities to use information from NetFlow protocol for improvement of performance of Wide Area Network. (Tesis de Pregrado).* Universidad Autonima de Madrid , Madrid - España. Obtenido de https://repositorio.uam.es/handle/10486/668156. Recuperado: 07 de julio del 2020.

Lewis, W. (2009). *LAN inalambrica y conmutada, guia de estudio de CCNA Exploration.* Madrid, España: Pearson Educación.

ManageEngine. (2020). *Conceptos básicos del protocolo SNMP*. Obtenido de https://www.manageengine.com/es/network-monitoring/what-is-snmp.html. Recuperado: 09 de agosto del 2020.

ManageEngineBlog. (2019). *¿Qué es NetFlow?* Obtenido de https://manageengine.com.mx/blog_v2_post/que-es-netflow. Recuperado: 09 de agosto del 2020.

ManageEngineNetFlowAnalyzer. (2020). *Análisis de tráfico de red con NetFlow Analyzer*. Obtenido de https://manageengine.com.mx/netflow-analyzer/caracteristicas/analisis-de-trafico-de-red-con-netflow-analyzer. Recuperado: 09 de agosto del 2020.

ManageEngineOpManager. (2020). *Análisis del tráfico de red*. Obtenido de https://www.manageengine.com/latam/network-monitoring/software-monitoreo-de-ancho-de-banda.html. Recuperado: 09 de agosto del 2020.

ManageEngin-Netflow. (s.f.). *Configuring new Cisco 2900 and 4900 Series Switches with NetFlow Analyzer.* Obtenido de https://www.manageengine.com/products/netflow/help/configuring-cisco-2900-and-4900-series.html. Recuperado: 09 de agosto del 2020.

Medhi, D., & Ramasamy, K. (2017). *Network Routing: Algorithms, Protocols, and Architectures.* EEUU: Morgan Kaufmann.

Nica, L. (2020). *¿Qué es el ciberdelito y cómo puede prevenirlo?* Obtenido de https://www.avast.com/es-es/c-cybercrime. Recuperado: 09 de agosto del 2020.

Noction.com. (2019). *Blog/snmp-and-NETFLOW*. Obtenido de https://www.noction.com/blog/snmp-and-NETFLOW. Recuperado: 09 de agosto del 2020.

Ocampo Zuñiga, A. (2015). *Emuladores de red.* Obtenido de https://aocampoz.wordpress.com/2015/05/02/emuladores-de-red/.Recuperado: 09 de agosto del 2020.

Odom, W. (2017). *Cisco CCNA Routing and Switching ICND2 200-101 Official Cert Guide.* EEUU: Indianapolis.

PaesslerAg. (2020). *IT Explained: NetFlow*. Obtenido de https://www.paessler.com/it-explained/netflow#section2. Recuperado: 13 de junio del 2020.

Perez, D. (2018). *Redes Cisco - Curso práctico de formación para la certificación CCNA.* Bogota: Alfa y Omega.

Porto, J., & Gardey, A. (2013). *Definicion.de*. Obtenido de https://definicion.de/monitoreo/. Recuperado: 11 de julio del 2020.

Porto, J., & Gardey, A. (2016). *Definicion.de*. Obtenido de https://definicion.de/averia/. Recuperado: 13 de agosto del 2020.

Porto, J., & Merino, M. (2017). *Definicion.de*. Obtenido de https://definicion.de/ancho-de-banda/.Recuperado: 13 de agosto del 2020.

Quispe, C. J. (2019). *Implementación de un prototipo de monitoreo de dispositivos de comunicación y usuarios finales utilizando el protocolo SNMP basada en software libre para una empresa e-Commerce. (Tesis de Pregrado).* Universidad Nacional Mayor de San Marcos , Lima - Perú. Obtenido de http://cybertesis.unmsm.edu.pe/handle/20.500.12672/11017. Recuperado: 09 de julio del 2020.

Ramirez, D. E. (2019). *Alternativas de configuración con el uso de los protocolos SYSLOG y SNMP para la gestión de red de redes avanzadas.* Universidad Nacional Agraria de la Selva , Tingo Maria - Perú. Obtenido de http://repositorio.unas.edu.pe/handle/UNAS/1645. Recuperado: 09 de julio del 2020.

Ramirez, I. (2020). *Máquinas virtuales: qué son, cómo funcionan y cómo utilizarlas.* Obtenido de https://www.xataka.com/especiales/maquinas-virtuales-que-son-como-funcionan-y-como-utilizarlas

Romero, D. (2013). *Metodología de redes(FCAPS).* Obtenido de http://www.davidromerotrejo.com/2013/04/metodologia-de-redes-fcaps.html. Recuperado: 11 de julio del 2020.

Sampieri, R. (2014). *Metodología de la Investigación.* Mexico: McGRAW-HILL.

Significados.com. (2015). *Telemetría*. Obtenido de https://www.significados.com/telemetria/. Recuperado: 26 de julio del 2020.

Significados.com. (2017). *Software libre*. Obtenido de https://www.significados.com/software-libre/. Recuperado: 26 de julio del 2020.

Stallings, W. (2004). *Comunicaciones y rede de computadores (7a. ed.)*. Mexico: Pearson Educación.

Ucha, F. (2010). *Definición ABC*. Obtenido de https://www.definicionabc.com/general/optimo.php. Recuperado: 28 de julio del 2020.

Vachon, B. y. (2009). *Acceso a la WAN - Guia de estudio de CCNA Exploration.* Madrid: Pearson Educacion S.A.

Varela, H. A. (2010). *Blog de Redes*. Obtenido de Evolución de las Redes: https://pondalpar113.wordpress.com/evolucion-de-las-redes/. Recuperado: 11 de julio del 2020.

VMware. (2020). *Análisis de Red*. Obtenido de https://www.vmware.com/co/topics/glossary/content/network-analytics.html.Recuperado: 28 de julio del 2020.

Wendell, O. (2017). *Cisco CCNA- Routing and Switching ICND2 200-105.* Indaniapolos - USA: Cisco press.

Zambrano, M. D. (2015). *Propuesta de utilización de herramientas de telemetría, para identificar técnicas de ciberdelitos como watering hole, en redes de infraestructura (caso de estudio netflow de cisco). (Tesis de Maestria).* Pontificia Universidad Católica del Ecuador, Quito - Ecuador. Obtenido de http://repositorio.puce.edu.ec/handle/22000/8437. Recuperado: 29 de julio del 2020.

Zhu, A. (2018). *SFlow vs NetFlow vs SNMP: What Are the Differences?* Obtenido de http://www.cables-solutions.com/sflow-vs-netflow-vs-snmp-differences.html. Recuperado: 21 de noviembre del 2020.

ANEXOS

Anexo N°1: Matriz de consistencia interna

<table>
<tr><td colspan="3">APLICACIÓN DE PROTOCOLOS SNMP Y NETFLOW PARA OPERAR UNA LAN DE 4 SEDES DE LA EMPRESA DETCOM - LIMA 2020</td></tr>
<tr><td>PROBLEMA GENERAL</td><td>OBJETIVO GENERAL</td><td>VARIABLES</td></tr>
<tr><td rowspan="4">¿Cómo aplicar los protocolos SNMP y NETFLOW para operar una LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima- 2020?</td><td rowspan="4">Aplicar protocolos SNMP y NETFLOW para operar una LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima - 2020.</td><td>VARIABLE INDEPENDIENTE:</td></tr>
<tr><td>SNMP</td></tr>
<tr><td>NETFLOW</td></tr>
<tr><td>VARIABLE DEPENDIENTE:</td></tr>
<tr><td colspan="2">PROBLEMAS ESPECÍFICOS</td><td>OBJETIVOS ESPECÍFICOS</td></tr>
<tr><td>¿Cómo aplicar los protocolos SNMP y NETFLOW para la visibilidad y análisis del ancho de banda en la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima?</td><td colspan="2">Aplicar los protocolos SNMP y NETFLOW para la visibilidad y análisis del ancho de banda en la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima.</td></tr>
<tr><td>¿Cómo aplicar los protocolos SNMP y NETFLOW para el análisis de rendimiento de la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima?</td><td colspan="2">Emplear los protocolos SNMP y NETFLOW para el análisis de rendimiento de la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima.</td></tr>
<tr><td>¿Cómo aplicar los protocolos SNMP y NETFLOW para la administración de incidencias en la LAN de 4 sedes</td><td colspan="2">Aplicar los protocolos SNMP y NETFLOW para la administración de incidencias en la LAN de 4 sedes de la empresa DETCOM en la ciudad de Lima.</td></tr>
</table>

de la empresa DETCOM en la ciudad de Lima?	

Anexo N°2: Matriz de operacionalización de variables

APLICACIÓN DE PROTOCOLOS SNMP Y NETFLOW PARA OPERAR UNA LAN DE 4 SEDES DE LA EMPRESA DETCOM - LIMA 2020			
VARIABLES INDEPENDIENTES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES
SNMP	(ManageEngine, 2020) define el SNMP como uno de los protocolos ampliamente aceptados para administrar y monitorizar elementos de red. La mayoría de los elementos de red de nivel profesional vienen con un agente SNMP incluido. Estos agentes deben estar habilitados y configurados para comunicarse con el sistema de administración de red (NMS) (párr. 2).	El protocolo SNMP nos permitirá monitorear la salud de equipos, el cual se aplicará en la administración de incidencias de la LAN.	Monitoreo de salud de equipos
		El protocolo SNMP permitirá gestionar la red para lo cual se aplicará en el análisis de rendimiento.	Gestión de red
NETFLOW	Según (Claise, 2004) lo define como un protocolo que sirve para recopilar información sobre el tráfico de la red, este flujo se define como una secuencia unidireccional	El protocolo NETFLOW nos permitirá monitorear el flujo de red, el cual se empleará para la visibilidad y análisis de ancho de banda.	Monitoreo del flujo de red

	de paquetes con algunas propiedades comunes que pasan a través de un dispositivo de red. Estos flujos recopilados se exportan a un dispositivo externo, el recopilador NETFLOW (párr. 2).	El protocolo NETFLOW nos permitirá analizar el flujo de red y por lo tanto poder aplicarlo en el análisis de rendimiento.	Análisis de flujo de red
VARIABLE DEPENDIENTE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES
LAN	La LAN con el concepto de (Stallings, 2004) quien manifiesta lo siguiente; "Al igual que las redes WAN, una LAN es una red de comunicaciones que interconecta varios dispositivos y proporciona un medio para el intercambio de información entre ellos" (p. 17)	Con el protocolo SNMP podremos monitorear constantemente la red y detectar eventos que pondrían afectar la disponibilidad del equipo.	Administración de incidencias
		Con el protocolo NETFLOW se obtendrá el monitoreo de flujo de red que atañe el ancho de banda.	Visibilidad y análisis del ancho de banda
		Con los protocolos SNMP y NETFLOW se obtendrá un análisis de rendimiento de la LAN.	Análisis del rendimiento.

Anexo N°3: Cuadro de Incidencias – Empresa DETCOM

Tabla 24: Cuadro saturación de ancho de banda Enero – Marzo

ANCHO DE BANDA SATURADO POR EL USUARIO						
OFICINAS	**TOTAL INCIDENTES**	**Total Incidentes SATURADOS POR ANCHO DE BANDA**	**%**	**Tiempo promedio de solución(horas)**	**No alcanzo KPI 4.5 Hrs.**	**Alcanzo KPI 4.5 Hrs.**
SEDE PRINCIPAL	27	6	22.22%	7.23	3	3
SEDE A	53	7	13.21%	14.56	5	2
SEDE B	55	3	5.45%	4.18	2	1
SEDE C	85	8	9.41%	8.70	6	2
TOTAL	**220**	**24**	**10.91%**	**-**	**16**	**8**

Fuente: Empresa DETCOM – Departamento TI

Tabla 25: Cuadro incidencias de saturación de CPU Enero – Marzo

SATURACIÓN DE CPU						
OFICINAS	**TOTAL INCIDENTES**	**Total Incidentes SATURADOS POR CPU**	**%**	**Tiempo promedio de solución**	**No alcanzo KPI 4.5h**	**Alcanzo KPI 4.5h**
SEDE PRINCIPAL	27	4	14.81%	13.97	2	2
SEDE A	53	5	9.43%	4.97	3	2
SEDE B	55	7	12.73%	4.06	4	3
SEDE C	85	6	7.06%	27.41	4	2
TOTAL	**220**	**22**	**10.00 %**	**-**	**13**	**9**

Fuente: Empresa DETCOM – Departamento TI

Tabla 26: Cuadro incidencias de saturación de memoria Enero – Marzo

SATURACIÓN DE MEMORIA						
OFICINAS	**TOTAL INCIDENTES**	**Total Incidentes SATURADOS POR MEMORIA**	**%**	**Tiempo promedio de solución**	**No alcanzo KPI 4.5h**	**Alcanzo KPI 4.5h**
SEDE PRINCIPAL	27	3	11.11%	5.85	1	2
SEDE A	53	2	3.77%	24.44	2	0
SEDE B	55	5	9.09%	6.65	2	3
SEDE C	85	5	5.88%	13.72	4	1
TOTAL	**220**	**15**	**6.82%**	**-**	**9**	**6**

Fuente: Empresa DETCOM – Departamento TI

Tabla 27: Cuadro incidencias de intermitencias en el servicio Enero - Marzo

INTERMITENCIA EN SU SERVICIO						
OFICINAS	**TOTAL INCIDENTES**	**Total Incidentes SATURADOS POR INTERMITENCIA**	**%**	**Tiempo promedio de solución**	**No alcanzo KPI 4.5h**	**Alcanzo KPI 4.5h**
SEDE PRINCIPAL	27	0	0.00%	-	0	0
SEDE A	53	21	39.62%	4.42	7	14
SEDE B	55	12	21.82%	7.78	5	7
SEDE C	85	34	40.00%	9.17	13	21
TOTAL	**220**	**67**	**30.45%**	**-**	**25**	**42**

Fuente: Empresa DETCOM – Departamento TI

Tabla 28: Cuadro total de incidencias Enero – Marzo

PROGRESO DE TICKET ACUMULADOS 2020 -DETCOM						
OFICINAS	**VPN INCIDENTES**	**Total de Incidentes**	**Resueltos**	**Tiempo promedio de solución**	**No alcanzo KPI 4.5h**	**Alcanzo KPI 4.5h**
SEDE PRINCIPAL	27	27	27	8.60	12	15
SEDE A	61	61	61	7.05	25	36
SEDE B	42	42	42	23.19	22	20
SEDE C	79	79	79	12.92	42	37
TOTAL			**209**	**-**	**101**	**108**
%			**100%**	**-**	**48%**	**52%**

Fuente: Empresa DETCOM – Departamento TI

Anexo N°4: Hoja de datos del software OpManager

Anexo N°4: Hoja de Datos OpManager (Continua)

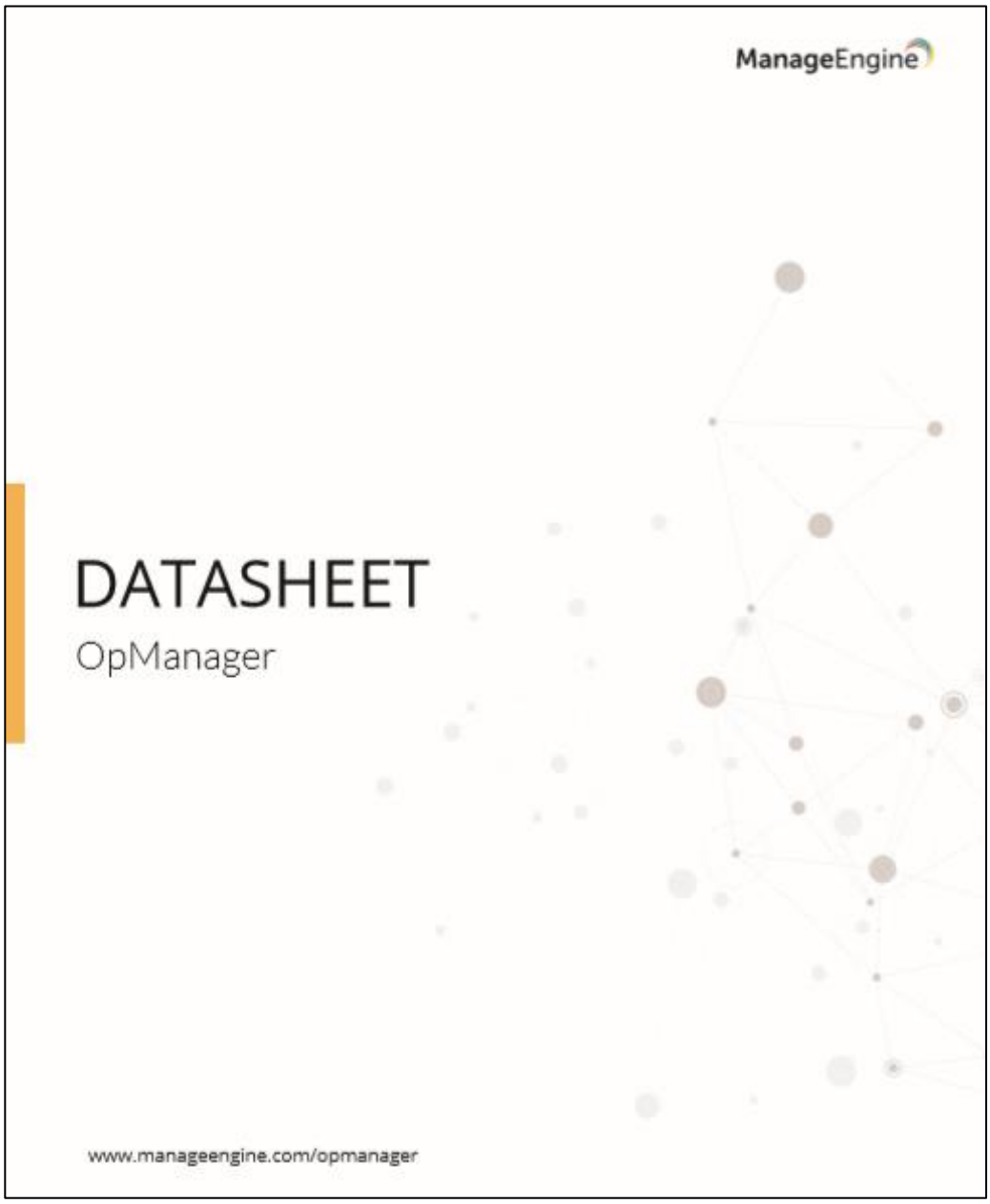


Figura N° 176: Datasheet - Opmanager
Fuente: https://download.manageengine.com/network-monitoring/opmanager_datasheet.pdf

Anexo N°4: Hoja de Datos OpManager (Continua)

ManageEngine OpManager is an enterprise-ready, affordable network monitoring solution that identifies network faults in real time. It helps you quickly troubleshoot network faults and maintain server uptime 24/7. It is 100 percent web based and can be set up in hours.

Features

Comprehensive monitoring

Monitor availability, health, and performance of your network devices such as switches, routers, servers, interfaces, firewalls, and other networking hardware for more than 2,000 metrics - all within OpManager.

Support for Hybrid Networks

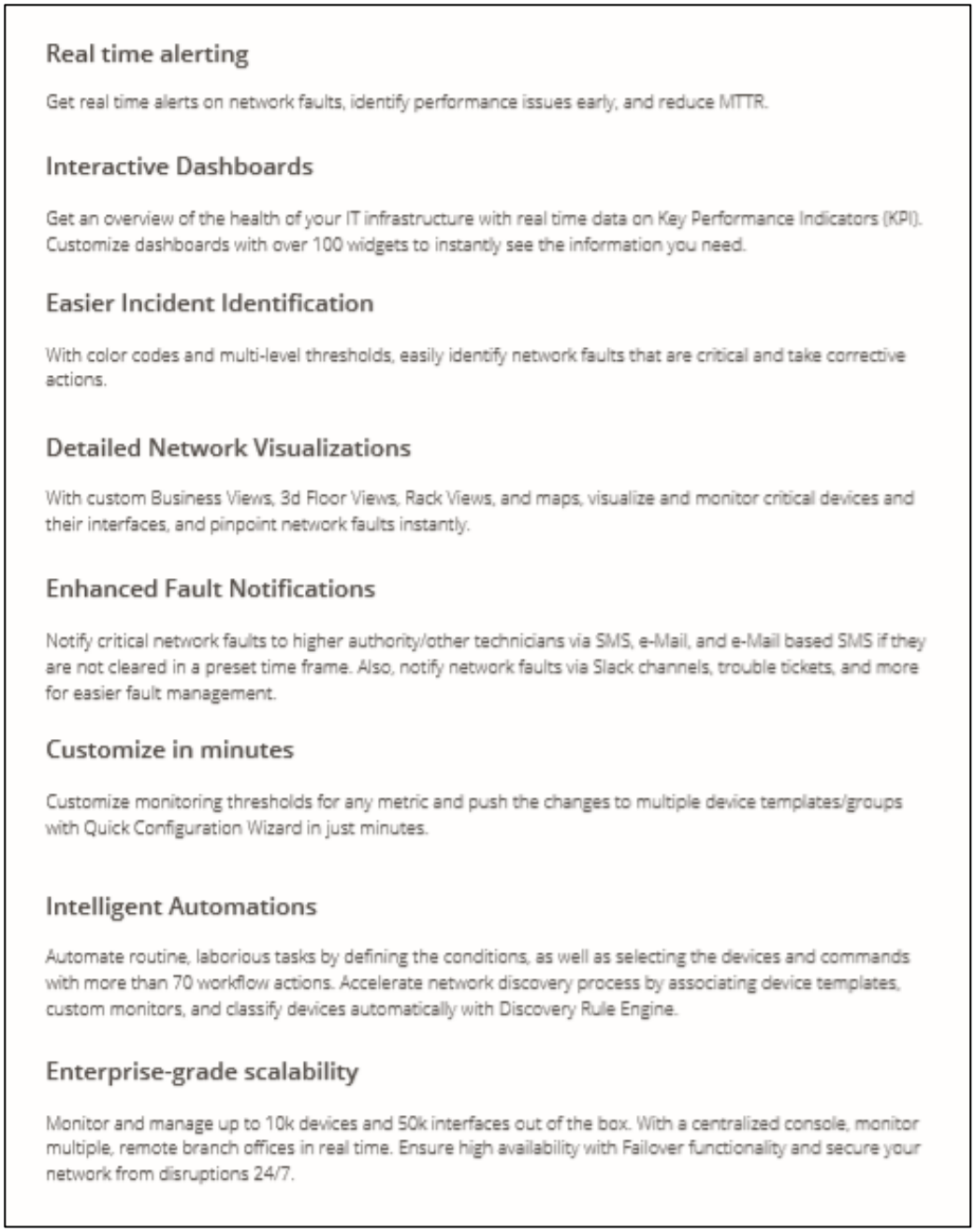
Monitor Microsoft Hyper-V, VMware, Citrix XenServer, Nutanix Infrastructure, Cisco UCS, and other essential applications such as Exchange, Active Directory, services, and processes for faults and performance.

Manage multi-vendor hardware

With more than 53,000 vendor templates, monitor and manage hardware from vendors including the likes of Cisco, Juniper, Fortigate, Aruba, and many more. Customize templates to address your organization's unique needs.

Figura N° 177- Datasheet Opmanager
Fuente: https://download.manageengine.com/network-monitoring/opmanager_datasheet.pdf

Anexo N°4: Hoja de Datos OpManager (Continua)



Real time alerting

Get real time alerts on network faults, identify performance issues early, and reduce MTTR.

Interactive Dashboards

Get an overview of the health of your IT infrastructure with real time data on Key Performance Indicators (KPI). Customize dashboards with over 100 widgets to instantly see the information you need.

Easier Incident Identification

With color codes and multi-level thresholds, easily identify network faults that are critical and take corrective actions.

Detailed Network Visualizations

With custom Business Views, 3d Floor Views, Rack Views, and maps, visualize and monitor critical devices and their interfaces, and pinpoint network faults instantly.

Enhanced Fault Notifications

Notify critical network faults to higher authority/other technicians via SMS, e-Mail, and e-Mail based SMS if they are not cleared in a preset time frame. Also, notify network faults via Slack channels, trouble tickets, and more for easier fault management.

Customize in minutes

Customize monitoring thresholds for any metric and push the changes to multiple device templates/groups with Quick Configuration Wizard in just minutes.

Intelligent Automations

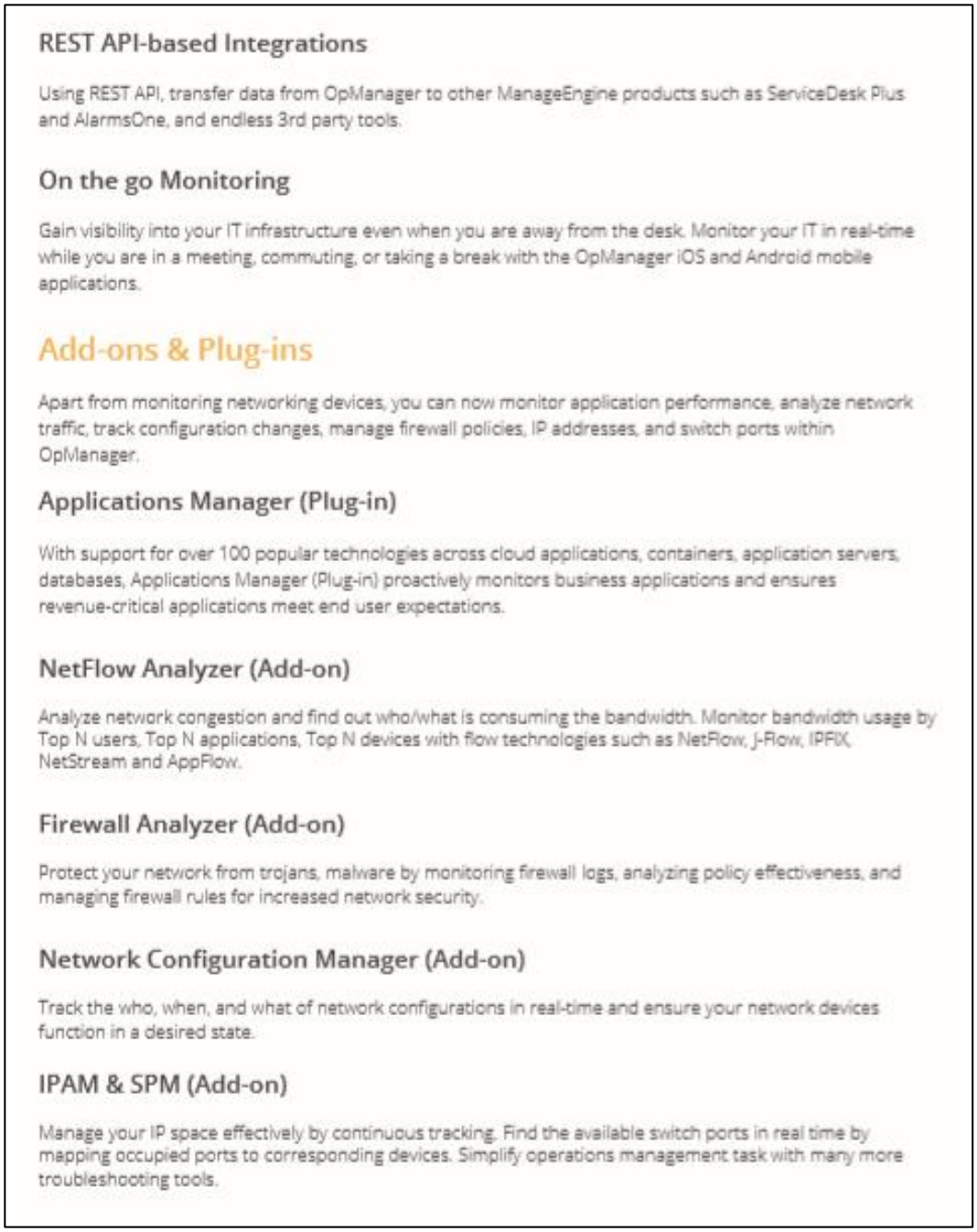
Automate routine, laborious tasks by defining the conditions, as well as selecting the devices and commands with more than 70 workflow actions. Accelerate network discovery process by associating device templates, custom monitors, and classify devices automatically with Discovery Rule Engine.

Enterprise-grade scalability

Monitor and manage up to 10k devices and 50k interfaces out of the box. With a centralized console, monitor multiple, remote branch offices in real time. Ensure high availability with Failover functionality and secure your network from disruptions 24/7.

Figura N° 178- Datasheet Opmanager
Fuente: https://download.manageengine.com/network-monitoring/opmanager_datasheet.pdf

Anexo N°4: Hoja de Datos OpManager (Continua)



REST API-based Integrations

Using REST API, transfer data from OpManager to other ManageEngine products such as ServiceDesk Plus and AlarmsOne, and endless 3rd party tools.

On the go Monitoring

Gain visibility into your IT infrastructure even when you are away from the desk. Monitor your IT in real-time while you are in a meeting, commuting, or taking a break with the OpManager iOS and Android mobile applications.

Add-ons & Plug-ins

Apart from monitoring networking devices, you can now monitor application performance, analyze network traffic, track configuration changes, manage firewall policies, IP addresses, and switch ports within OpManager.

Applications Manager (Plug-in)

With support for over 100 popular technologies across cloud applications, containers, application servers, databases, Applications Manager (Plug-in) proactively monitors business applications and ensures revenue-critical applications meet end user expectations.

NetFlow Analyzer (Add-on)

Analyze network congestion and find out who/what is consuming the bandwidth. Monitor bandwidth usage by Top N users, Top N applications, Top N devices with flow technologies such as NetFlow, J-Flow, IPFIX, NetStream and AppFlow.

Firewall Analyzer (Add-on)

Protect your network from trojans, malware by monitoring firewall logs, analyzing policy effectiveness, and managing firewall rules for increased network security.

Network Configuration Manager (Add-on)

Track the who, when, and what of network configurations in real-time and ensure your network devices function in a desired state.

IPAM & SPM (Add-on)

Manage your IP space effectively by continuous tracking. Find the available switch ports in real time by mapping occupied ports to corresponding devices. Simplify operations management task with many more troubleshooting tools.

Figura N° 179- Datasheet Opmanager
Fuente: https://download.manageengine.com/network-monitoring/opmanager_datasheet.pdf

Anexo N°4: Hoja de Datos OpManager

Editions

To better suit your monitoring needs, OpManager is now available in 3 editions.

Standard

- Network Discovery
- Server, switch, and interface Monitoring
- Syslog and Eventlog Monitoring
- File/Folder Monitoring
- Customizable Dashboard
- Business Views
- Alarm Escalation
- IOS & Android mobile applications
- 3rd Party Integrations
- Scales up to 1,000 devices
- Starts @ 245 USD for 10 devices

Professional

- Everything in Standard Edition and
- Layer2 Discovery
- Discovery Rule Engine
- Virtual Environment monitoring
- URL, AD, Exchange Server, MS SQL
- Monitoring
- REST API Access
- NOC View Widgets
- IT Workflows
- Forecast Reports
- Multi-Language Support
- Scales up to 1,000 devices
- Starts @ 345 USD for 10 devices

Enterprise

- Everything in Professional Edition and
- Multi-site Monitoring
- Up to 180 days data maintenance
- Failover Support
- Scales up to 10,000 devices out of the box
- Starts @ 11,545 USD for 250 devices

Minimum System Requirements

To manage up to 1k devices.

CPU : Intel Xeon Quad Core, 2.5 Ghz
Ram Size : 16 GB
Hard Disk : 40 GB

OS Windows : Windows 10/8/7, Windows Server 2012 R2/ 2012/2008 R2/2008.
OS Linux : Ubuntu, Red Hat, Suse, Fedora and Mandriva (Mandrake Linux)
Database : MSSQL 2008, 2012, 2014 and 2016 | OpManager bundled PostgreSQL

Minimum System Requirements

To manage up to 10k interfaces or 10k devices.

CPU : Intel Xeon Quad Core, 2.5GHz
Ram Size : 32 GB
Hard Disk : 100 GB

OS Windows : Windows 10/8/7, Windows Server 2012 R2/ 2012/2008 R2/2008.
OS Linux : Ubuntu, Red Hat, Suse, Fedora and Mandriva (Mandrake Linux)
Database : MSSQL 2008, 2012, 2014 and 2016 | OpManager bundled PostgreSQL

For detailed system requirements, click here.

NASA Kingston SIEMENS MARVEL

Telephone Number	Alternate number	Mail
Call Toll free : +1 888 720 9500	US:+1 888 791 1189 | Intl:+1 925 924 9500 | Aus: 1800 631 268 UK: 0800 028 6590 | CN:+86 400 660 8680	opmanager-support@manageengine.com

Figura N° 180: Datasheet Opmanager
Fuente: https://download.manageengine.com/network-monitoring/opmanager_datasheet.pdf

Anexo N°5: Formato de autorización

Universidad Ricardo Palma

Escuela de Posgrado

AUTORIZACIÓN PARA REALIZAR LA INVESTIGACIÓN

DECLARACIÓN DEL RESPONSABLE DEL AREA O DEPENDENCIA DONDE SE REALIZARÁ LA INVESTIGACIÓN

Dejo constancia que el área o dependencia que dirijo, ha tomado conocimiento del proyecto de tesis titulado:

APLICACIÓN DE PROTOCOLOS SNMP Y NETFLOW PARA OPERAR UNA LAN DE 4 SEDES DE LA EMPRESA DETCOM LIMA 2020

el mismo que es realizado por el Sr./Srta. Estudiante (Apellidos y nombres):

-Dett Sotelo, Bryan Alexis
-Vega Santiago, Edwin Cesar

, en condición de estudiante - investigador del Programa de:

Programa de titulación por tesis 2020

Así mismo señalamos, que según nuestra normativa interna procederemos con el apoyo al desarrollo del proyecto de investigación, dando las facilidades del caso para aplicación de los instrumentos de recolección de datos.
En razón de lo expresado doy mi consentimiento para el uso de la información y/o la aplicación de los instrumentos de recolección de datos:

Nombre de la empresa:	Autorización para el uso del nombre de la Empresa en el Informe Final	
Detcom S.A.C.		SI X
		NO

Apellidos y Nombres del Jefe/Responsable del área	Cargo del Jefe/Responsable del área:
Valle Dett, Hugo	Gerente General

Teléfono fijo (incluyendo anexo) y/o celular:	Correo electrónico de la empresa:
351 - 7904	havs @ dettcompany.com

DETCOM S.A.C.
HUGO VALLE DETT
Gerente

Firma

7/11/2020

Fecha