



# **UNIVERSIDAD TÉCNICA DEL NORTE**

**FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS**

**CARRERA DE INGENIERÍA ELECTRÓNICA Y REDES DE  
COMUNICACIÓN**

**TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL  
TÍTULO DE INGENIERÍA EN ELECTRÓNICA Y REDES DE  
COMUNICACIÓN**

**TEMA**

**OPTIMIZACIÓN DE LA ADMINISTRACIÓN EN LA RED DE  
DATOS DE LA UNIVERSIDAD TÉCNICA DEL NORTE  
IMPLEMENTANDO UN SISTEMA DE MONITOREO DE EQUIPOS Y  
SERVICIOS UTILIZANDO SOFTWARE LIBRE**

**AUTOR: JEANPIERRE WENCESLAO CASTRO FLORES**

**DIRECTOR: ING. EDGAR MAYA**

**IBARRA-ECUADOR**

**2015**



## UNIVERSIDAD TÉCNICA DEL NORTE

### BIBLIOTECA UNIVERSITARIA

## AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

### 1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la universidad. Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de Identidad	1722548656
Apellidos y Nombres	Jeanpierre Wenceslao Castro Flores
Dirección	Urb. Mastodonde calle 2c, Carcelén. Quito.
Email	jeamstein@hotmail.com
Teléfono Fijo	023813538
Teléfono Móvil	0992434492/0996385463

DATOS DE LA OBRA	
Título	OPTIMIZACIÓN DE LA ADMINISTRACIÓN EN LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DEL NORTE IMPLEMENTANDO UN SISTEMA DE MONITOREO DE EQUIPOS Y SERVICIOS UTILIZANDO SOFTWARE LIBRE
Autor	Castro Flores Jeanpierre Wenceslao
Fecha	01/06/2015
Programa	Pregrado
Título por el que se aspira	Ingeniería en Electrónica y Redes de Comunicación
Director	Ing. Edgar Maya

## 2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Jeanpierre Wenceslao Castro Flores, con cédula de identidad Nro. 1722548656, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.



---

Firma

Nombre: Jeanpierre Wenceslao Castro Flores

Cédula: 1722548656



## UNIVERSIDAD TÉCNICA DEL NORTE

### FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

#### CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asumen (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros

Ibarra, 01 de Junio del 2015

EL AUTOR:

A handwritten signature in blue ink, appearing to read "Jeanpierre", is written above a horizontal line.

Firma

Nombre: Jeanpierre Wenceslao Castro Flores

Cédula: 1722548656



## UNIVERSIDAD TÉCNICA DEL NORTE

### FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

#### CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, **Jeanpierre Wenceslao Castro Flores**, con cédula de identidad Nro. 1722548656, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor de la obra o trabajo de grado denominado: **“OPTIMIZACIÓN DE LA ADMINISTRACIÓN EN LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DEL NORTE IMPLEMENTANDO UN SISTEMA DE MONITOREO DE EQUIPOS Y SERVICIOS UTILIZANDO SOFTWARE LIBRE”**, que ha sido desarrollado para optar por el título de: **Ingeniería en Electrónica y Redes de Comunicación** en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

A handwritten signature in blue ink, appearing to read "Jeanpierre", is written above a horizontal line.

Firma

Nombre: Jeanpierre Wenceslao Castro Flores

Cédula: 1722548656



## UNIVERSIDAD TÉCNICA DEL NORTE

### FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

#### DECLARACIÓN

Yo, Jeanpierre Wenceslao Castro Flores, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que este no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte.

A handwritten signature in blue ink, appearing to read 'Jeanpierre', is written above a horizontal line.

Firma

Nombre: Jeanpierre Wenceslao Castro Flores

Cédula: 1722548656



## UNIVERSIDAD TÉCNICA DEL NORTE

### FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

#### CERTIFICACIÓN

Certifico, que el presente trabajo de titulación “**OPTIMIZACIÓN DE LA ADMINISTRACIÓN EN LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DEL NORTE IMPLEMENTANDO UN SISTEMA DE MONITOREO DE EQUIPOS Y SERVICIOS UTILIZANDO SOFTWARE LIBRE**” fue desarrollado en su totalidad por el Sr. Jeanpierre Wenceslao Castro Flores, bajo mi supervisión.

A handwritten signature in blue ink, consisting of several loops and strokes, positioned above a horizontal line.

Ing. Edgar Maya

DIRECTOR DE PROYECTO

## AGRADECIMIENTOS

*Ante todo a Dios por brindarme la oportunidad de la vida.*

*A mis padres y hermanas por su apoyo incondicional*

*Al Ing. Edgar Maya, director de tesis e Ing. Carlos Vasquez docente de la carrera, por su ayuda y asesoría en el desarrollo de este proyecto de titulación.*

*A los docentes de la Carrera de Ingeniería Electrónica y Redes de Comunicación por su guía en mi formación académica.*

*Al Departamento de Informática de la Universidad Técnica del Norte, por darme la confianza y oportunidad de desarrollar este trabajo, en especial al Ing. Msc. Fernando Garrido, ex director del mismo e Ing. Cosme Ortega, por su ayuda y recomendaciones en el avance del tema.*

*Jeanpierre W. Castro*



## DEDICATORIA

*Este proyecto de titulación lo dedico a mis padres Wenceslao Castro y Maribel Flores por ser mi ejemplo de superación y constancia, que por medio de su apoyo, motivación y cariño me permitieron culminar este trabajo y superar las barreras que se fueron presentando en mi camino.*

*Jeanpierre W. Castro*

## CONTENIDO

CAPITULO I.....	1
FUNDAMENTOS SOBRE ADMINISTRACIÓN DE RED .....	1
1.1    INTRODUCCIÓN .....	1
1.2    GESTIÓN DE RED.....	1
1.2.1    DEFINICIÓN.....	1
1.3    ARQUITECTURAS DE GESTIÓN DE RED .....	2
1.3.1    MODELO TMN.....	2
1.3.2    MODELO OSI .....	8
1.3.3    MODELO DE INTERNET .....	15
1.4    SISTEMA DE MONITOREO DE RED .....	30
1.4.1    INTRODUCCIÓN .....	30
1.4.2    COMPARATIVA DE SOFTWARE DE MONITOREO.....	30
1.4.3    NAGIOS CORE.....	33
1.4.4    LICENCIAS.....	34
1.4.5    OBJETIVOS Y NECESIDADES.....	34
1.4.6    DEPENDENCIAS .....	35
1.4.7    ESTRUCTURA DE ARCHIVOS .....	36
1.4.8    ARCHIVOS DE CONFIGURACIÓN.....	37
CAPITULO II.....	40
PLANEACIÓN EN LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DEL NORTE “SITUACIÓN ACTUAL” .....	40
2.1    INTRODUCCIÓN .....	40
2.2    FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS .....	42
2.2.1    INTRODUCCIÓN .....	42
2.2.2    LABORATORIO DE COMPUTACIÓN I .....	42
2.2.3    LABORATORIO DE COMPUTACIÓN II.....	45
2.2.4    LABORATORIO DE COMPUTACIÓN III Y LABORATORIO DE COMPUTACIÓN V .....	48
2.2.5    LABORATORIO DE COMPUTACIÓN IV .....	52
2.2.6    LABORATORIO DE COMPUTACIÓN VI Y LABORATORIO DE COMPUTACIÓN VII.....	56
2.2.7    CUBÍCULOS PROFESORES.....	61
2.2.8    SALA DE PROFESORES .....	64
2.2.9    CUARTO DE EQUIPOS FICA .....	65
2.3    FACULTAD DE INGENIERÍA EN CIENCIAS AGROPECUARIAS Y AMBIENTALES .....	71
2.4    FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS .....	71
2.5    FACULTAD DE EDUCACIÓN CIENCIA Y TECNOLOGÍA.....	72
2.6    FACULTAD DE CIENCIAS DE LA SALUD .....	73
2.7    AUDITORIO AGUSTÍN CUEVA .....	74
2.8    EDIFICIO DE POSTGRADO .....	74
2.9    EDUCACIÓN FÍSICA .....	75
2.10    BIBLIOTECA.....	76
2.11    GARITA .....	77
2.12    DEFINICIÓN DE EQUIPOS MONITOREADOS .....	77
CAPITULO III .....	82
ADMINISTRACIÓN DE SOFTWARE.....	82
3.1    POLÍTICAS PARA MONITOREAR EQUIPOS LINUX.....	82
3.1.1    CONFIGURACIÓN DEL AGENTE DE MONITOREO .....	83
3.1.2    PLUGIN.....	85

3.1.3	CONFIGURACIÓN DE COMANDOS .....	85
3.1.4	CONFIGURACIÓN DE PLANTILLAS PARA EQUIPOS .....	87
3.1.5	CONFIGURACIÓN DE PLANTILLAS PARA SERVICIOS.....	88
3.1.6	DEFINICIÓN DE EQUIPOS .....	90
3.1.7	DEFINICIÓN DE SERVICIOS .....	90
3.2	POLÍTICAS PARA MONITOREAR SWITCHES.....	92
3.2.1	CONFIGURACIÓN DE AGENTES DE MONITOREO .....	92
3.2.2	PLUGIN.....	94
3.2.3	CONFIGURACIÓN DE COMANDOS .....	94
3.2.4	CONFIGURACIÓN DE PLANTILLAS PARA EQUIPOS .....	96
3.2.5	CONFIGURACIÓN DE PLANTILLAS PARA SERVICIOS.....	97
3.2.6	DEFINICIÓN DE EQUIPOS .....	98
3.2.7	DEFINICIÓN DE SERVICIOS .....	99
3.2.8	WIRELESS CONTROLLER Y PUNTOS DE ACCESO INALAMBRICO .....	100
3.2.9	CONFIGURACIÓN DE AGENTES DE MONITOREO .....	100
3.2.10	PLUGIN.....	101
3.2.11	CONFIGURACIÓN DE COMANDOS .....	101
3.2.12	CONFIGURACIÓN DE PLANTILLAS PARA EQUIPOS .....	102
3.2.13	CONFIGURACIÓN DE PLANTILLAS PARA SERVICIOS.....	104
3.2.14	DEFINICIÓN DE EQUIPOS .....	105
3.2.15	DEFINICIÓN DE SERVICIOS .....	105
3.3	CONFIGURAR UN NUEVO GRUPO DE QUIPOS .....	107
3.4	CONFIGURAR UN NUEVO PERIODO DE TIEMPO DE MONITOREO.....	107
3.5	ENVÍO DE NOTIFICACIONES.....	108
3.5.1	CONFIGURACIÓN DE PLANTILLA PARA CONTACTOS .....	108
3.5.2	DEFINICIÓN DEL GRUPO DE CONTACTOS .....	109
3.5.3	DEFINICIÓN DE CONTACTO .....	110
3.6	MÓDULO DE GRÁFICAS PNP4NAGIOS .....	110
3.6.1	CONFIGURACIÓN DEL COMANDO DE EJECUCIÓN .....	110
3.6.2	CONFIGURACIÓN DE PLANTILLA PARA SERVICIOS .....	111
3.6.3	DEFINICIÓN DE GRÁFICAS PARA SERVICIOS.....	112
CAPITULO IV .....		113
RENDIMIENTO DE LA RED DE DATOS DE LA UTN .....		113
4.1	INTRODUCCIÓN .....	113
4.2	MEDICIÓN DEL TRÁFICO DE LA RED .....	113
4.2.1	ANÁLISIS GENERAL DE TRÁFICO .....	114
4.3	POLÍTICAS PARA CONOCER EL RENDIMIENTO DE LA RED DESDE NAGIOS .....	117
4.3.1	CAPA DE DISTRIBUCIÓN DE LA UTN.....	118
CAPÍTULO V.....		124
CONTROL DE FALLAS .....		124
5.1	INTRODUCCIÓN .....	124
5.2	POLÍTICAS PARA EL CONTROL DE FALLAS .....	124
5.2.1	ESTADO DE HOST .....	125
5.2.2	ESTADO DE SERVICIOS .....	125
5.2.3	UN ALTO NÚMERO DE INSTANCIAS DE PUERTOS STP.....	127
5.2.4	BUCLES DE REENVÍO DE CAPA 2 .....	133
5.2.5	RECONOCIMIENTO DEL HOST .....	134
5.2.6	RECURSOS DE HARDWARE (TCAM) NO DISPONIBLES PARA LAS ACL DE SEGURIDAD .....	136
5.2.7	PROTOCOLO HSRP Y PORTCHANNEL.....	139

CAPITULO VI .....	141
ANÁLISIS COSTO BENEFICIO .....	141
6.1    INTRODUCCIÓN .....	141
5.2    PRESUPUESTO DE INVERSIÓN .....	141
5.2.1    PRESUPUESTO DE HARDWARE .....	141
5.2.2    PRESUPUESTO DE SOFTWARE .....	142
5.2.3    ANÁLISIS DE GASTOS EN SOFTWARE PROPIETARIO.....	142
5.2.4    PRESUPUESTO TOTAL .....	143
5.2.5    ANÁLISIS COSTO BENEFICIO .....	143
CAPITULO VII .....	145
CONCLUSIONES Y RECOMENDACIONES.....	145
7.1    CONCLUSIONES .....	145
7.2    RECOMENDACIONES .....	147
ANEXO A .....	149
MANUAL DE ADMINISTRADOR.....	149
ANEXO B .....	167
GUÍA DE INSTALACIÓN.....	167
NAGIOS CORE .....	167
NAGIOSQL.....	171
PNP4NAGIOS.....	181
ANEXO C .....	195
SPANNING TREE PORTFAST BPDU GUARD ENHANCEMENT .....	195
ANEXO D .....	200
SPANNING-TREE PROTOCOL ENHANCEMENTS USING LOOP GUARD AND BPDU SKEW DETECTION FEATURES.....	200
ANEXO E.....	212
SPANNING TREE PROTOCOL ROOT GUARD ENHANCEMENT.....	212
ANEXO F.....	219
UNDERSTANDING AND CONFIGURING THE UNIDIRECTIONAL LINK DETECTION PROTOCOL FEATURE.....	219
REFERENCIAS BIBLIOGRÁFICAS .....	226

# ÍNDICE DE FIGURAS

## CAPÍTULO I

Figura 1. Relación general entre una TMN y una red de telecomunicaciones.....	4
Figura 2. Bloques de función de la TMN .....	6
Figura 3. Ejemplo de arquitectura física simplificada para una TMN .....	8
Figura 4. Visión de gestión compartida del modelo OSI .....	9
Figura 5. Interacción de gestión de sistemas CMIP/CMIS .....	14
Figura 6. El rol de SNMP.....	16
Figura 7. Ejemplo de gestión de red distribuida .....	18
Figura 8. PDU SNMP .....	19
Figura 9. Relación entre el Gestor y el Agente .....	20
Figura 10. Modelo de comunicación TCP/IP y SNMP .....	22
Figura 11. Árbol de Objetos SMI.....	25
Figura 12. Árbol MIB II.....	27

## CAPÍTULO II

Figura 13. Topología Lógica UTN.....	41
Figura 14. Mapeo de red - Laboratorio I – FICA.....	45
Figura 15. Mapeo de red - Laboratorio II – FICA .....	48
Figura 16. Mapeo de red - Laboratorio V – FICA .....	51
Figura 17. Mapeo de red - Laboratorio III – FICA.....	52
Figura 18. Mapeo de red - Lab IV – FICA .....	55
Figura 19. Mapeo de red - Laboratorio IV.....	56
Figura 20. Mapeo de red - Laboratorio VII – FICA .....	60
Figura 21. Mapeo de red - Laboratorio VI – FICA.....	61
Figura 22. Mapeo de red - Cubículos Profesores – FICA .....	63
Figura 23. Mapeo de red - Sala de Profesores – FICA .....	65
Figura 24. Mapeo de red - Cuarto de Equipos FICA – Switch 4.....	68
Figura 25. Mapeo de red - Cuarto de Equipos FICA – Switch 5.....	69
Figura 26. Mapeo de red - Cuarto de Equipos FICA – Switch 6.....	70

## CAPÍTULO III

Figura 27. Funcionamiento del agente NRPE.....	83
Figura 28. Archivo de configuración del agente NRPE.....	84
Figura 29. Archivo de configuración nrpe.cfg.....	84
Figura 30. Monitoreo de routers y switches utilizando SNMP .....	93
Figura 31. Habilitando SNMP en switch 3com, paso 1 .....	93
Figura 32. Habilitando SNMP en switch 3COM, paso 2 .....	94

## CAPÍTULO IV

Figura 33. Distribución global de datos de acuerdo al tipo de protocolo utilizando NTOP.....	114
Figura 34. Vista histórica del protocolo HTTP en la red .....	115
Figura 35. Vista histórica de la aplicación Windows Live Messenger en la red .....	115
Figura 36. Vista histórica del protocolo NetBios-IP la red .....	116
Figura 37. Vista histórica del protocolo DNS en la red .....	116
Figura 38. Vista histórica del protocolo FTP en la red .....	116
Figura 39. Mapa de red – Sistema de monitoreo NAGIOS.....	117
Figura 40. Despliegue de servicios.....	117
Figura 41. Servicios ejecutados en el SW-Zeus.....	118
Figura 42. Servicios ejecutados en el SW-Zeus.....	119
Figura 43. Tráfico de red en el SW-Zeus .....	120
Figura 44. Servicios ejecutados en el SW-Zeus.....	120
Figura 45. Servicios ejecutados en el SW-Aristóteles .....	121
Figura 46. Servicios ejecutados en el SW-Aristóteles .....	122
Figura 47. Tráfico de red en el SW-Aristóteles .....	122
Figura 48. Servicios en el SW-Aristóteles.....	123
Figura 49. Servicios en el SW-Aristóteles.....	123
Figura 50. Servicios en el SW-Aristóteles.....	123
Figura 51. Servicios en el SW-Aristóteles.....	123

## CAPÍTULO V

Figura 52. Estado de servicios y equipos en el sistema NAGIOS.....	125
Figura 53. Estado de host.....	125
Figura 54. Estado de servicio .....	126
Figura 55. Servicios monitoreados en los switches de distribución de la UTN .....	127
Figura 56. Comando show processes cpu.....	129
Figura 57. Comando show platform health .....	129
Figura 58. Comando show platform cpu packet statistics.....	131
Figura 60. Comando show spanning-tree summary.....	132

Figura 60. Comando show processes cpu.....	134
Figura 61. Comando show platform health .....	135
Figura 62. Comando show platform cpu packet statistics.....	135
Figura 63. Comando show logging .....	137
Figura 64. Comando show processes cpu.....	137
Figura 65. Comando show platform health .....	138
Figura 66. Comando show platform cpu packet statistics.....	138

## ÍNDICE DE TABLAS

### CAPÍTULO I

Tabla 1. Interfaces Normalizadas .....	8
Tabla 2. Comparativa de las versiones de SNMP .....	17
Tabla 3. Tipos de datos SMIV1 .....	26
Tabla 4. Descripción de los grupos de la Mib-II.....	27
Tabla 5. Comparativa de Sistemas de Monitoreo .....	32
Tabla 6. Dependencias de software utilizadas por NAGIOS .....	35
Tabla 7. Contenido del archivo cgi.cfg - NAGIOS CORE .....	37
Tabla 8. Contenido del archivo nagios.cfg - NAGIOS CORE.....	38
Tabla 9. Contenido del directorio objects - NAGIOS CORE.....	38

### CAPÍTULO II

Tabla 10. Equipos de cómputo - Laboratorio I - FICA .....	43
Tabla 11. Equipos de telecomunicaciones - Laboratorio I - FICA.....	43
Tabla 12. Utilización y software instalado - Laboratorio I – FICA.....	43
Tabla 13. Equipos de cómputo - Laboratorio II - FICA.....	46
Tabla 14. Equipos de telecomunicaciones - Laboratorio II - FICA.....	46
Tabla 15. Utilización y software instalado - Laboratorio II – FICA .....	46
Tabla 16. Equipos de cómputo - Laboratorio III – FICA.....	49
Tabla 17. Equipos de cómputo - Laboratorio V – FICA.....	49
Tabla 18. Equipos de telecomunicaciones - Laboratorio III - FICA .....	49
Tabla 19. Utilización y software instalado - Laboratorio III - FICA.....	50
Tabla 20. Utilización y software instalado - Laboratorio V – FICA .....	50
Tabla 21. Equipos de cómputo - Laboratorio IV – FICA .....	53
Tabla 22. Equipos de telecomunicaciones - Laboratorio IV – FICA .....	53
Tabla 23. Utilización y software instalado - Laboratorio IV – FICA .....	53
Tabla 24. Equipos de cómputo - Laboratorio VII – FICA .....	57
Tabla 25. Equipos de cómputo - Laboratorio VI – FICA .....	57
Tabla 26. Equipos de telecomunicaciones - Laboratorio VII – FICA .....	58
Tabla 27. Utilización y software instalado - Laboratorio VII – FICA.....	59
Tabla 28. Utilización y software instalado - Laboratorio VI – FICA.....	59
Tabla 29. Equipos de telecomunicaciones - Cubículos Profesores – FICA.....	62
Tabla 30. Equipos de telecomunicaciones - Sala de Profesores – FICA .....	64
Tabla 31. Servidores – FICA .....	65
Tabla 32. Equipos de telecomunicaciones – Cuarto de Equipos FICA .....	66
Tabla 33. Equipos de telecomunicaciones - FICAYA .....	71
Tabla 34. Ubicación de puntos de red – FICAYA .....	71
Tabla 35. Equipos de telecomunicaciones – FACAE .....	72
Tabla 36. Ubicación de puntos de red – FACAE.....	72
Tabla 37. Equipos de telecomunicaciones - FECYT .....	72
Tabla 38. Ubicación de puntos de red – FECYT.....	73
Tabla 39. Equipos de telecomunicaciones - SALUD.....	73
Tabla 40. Ubicación de puntos de red – SALUD .....	73
Tabla 41. Equipos de telecomunicaciones - AUDITORIO.....	74
Tabla 42. Ubicación de puntos de red - AGUSTÍN CUEVA.....	74
Tabla 43. Equipos de telecomunicaciones – POSGRADO .....	75
Tabla 44. Ubicación de puntos de red - POSGRADO .....	75
Tabla 45. Equipos de telecomunicaciones - EDUCACIÓN FÍSICA .....	75
Tabla 46. Ubicación de puntos de red - EDUCACIÓN FÍSICA.....	76
Tabla 47. Equipos de telecomunicaciones -BIBLIOTECA .....	76
Tabla 48. Ubicación de puntos de red – BIBLIOTECA .....	76
Tabla 49. Equipos de telecomunicaciones - GARITA .....	77
Tabla 50. Ubicación de puntos de red – GARITA.....	77
Tabla 51. Equipos de conmutación alojados en el Edificio Central .....	78
Tabla 52. Equipos de conmutación alojados en la FICA .....	79
Tabla 53. Equipos de conmutación alojados en la FICAYA.....	79
Tabla 54. Equipos de conmutación alojados en la FECYT.....	79
Tabla 55. Equipos de conmutación alojados en la FACAE .....	79
Tabla 56. Equipos de conmutación alojados en la FCCSS .....	79
Tabla 57. Equipos de conmutación alojados en el CAI .....	79
Tabla 58. Equipos de conmutación alojados en POSTGRADO.....	80
Tabla 59. Equipos de conmutación alojados en la BIBLIOTECA .....	80

Tabla 60. Puntos de acceso inalámbrico alojados en el Edificio Central.....	80
Tabla 61. Puntos de acceso inalámbrico alojados en la FICA.....	80
Tabla 62. Puntos de acceso inalámbrico alojados en la FACAE.....	80
Tabla 63. Puntos de acceso inalámbrico alojados en la FECYT .....	80
Tabla 64. Puntos de acceso inalámbrico alojados en Bienestar Universitario .....	80
Tabla 65. Puntos de acceso inalámbrico alojados en exteriores .....	81
Tabla 66. Puntos de acceso inalámbrico alojados en la FICAYA .....	81
Tabla 67. Puntos de acceso inalámbrico alojados en la FCCSS.....	81
Tabla 68. Puntos de acceso inalámbrico alojados en el CAI.....	81
Tabla 69. Puntos de acceso inalámbrico alojados en Postgrado.....	81
Tabla 70. Puntos de acceso inalámbrico Autónomos.....	81
Tabla 71. Puntos de acceso inalámbrico alojados en áreas públicas .....	81

### CAPÍTULO III

Tabla 72. Descripción de la ejecución de plugin en el agente NRPE.....	84
Tabla 73. Plugin utilizados en equipos LINUX .....	85
Tabla 74. Ejemplo de configuración de comando en servicios LINUX .....	86
Tabla 75. Ejecución de comandos para equipos LINUX .....	86
Tabla 76. Plantilla base para la configuración de equipos LINUX (generic-host-server).....	87
Tabla 77. Plantilla de configuración de equipos LINUX (linux-server).....	88
Tabla 78. Plantilla base para la configuración de servicios LINUX (generic-service) .....	89
Tabla 79. Plantilla de configuración de servicios (local-service).....	90
Tabla 80. Ejemplo de definición de equipo (servidor-moodle).....	90
Tabla 81. Ejemplo de definición de servicio (servidor-Moodle).....	91
Tabla 82. Definición del parámetro check_command para servicios LINUX .....	91
Tabla 83. Plugin utilizados en switches.....	94
Tabla 84. Ejemplo de configuración de comandos para switches .....	95
Tabla 85. Ejecución de comandos para switches.....	95
Tabla 86. Plantilla base para la configuración de switches (generic-host-switch).....	96
Tabla 87. Plantilla de configuración de switches.....	97
Tabla 88. Plantilla de configuración de servicios en switches (generic-service).....	98
Tabla 89. Ejemplo de definición de equipo (sw-Fica) .....	98
Tabla 90. Ejemplo de definición de servicio (sw-Fica).....	99
Tabla 91. Definición del parámetro check_command para servicios en un switch .....	100
Tabla 92. Descripción de la ejecución de plugin para el chequeo de switches .....	100
Tabla 93. Plugin utilizados en puntos de acceso y en el Wireless Controller .....	101
Tabla 94. Ejemplo de configuración de comandos para el Wireless Controller y puntos de acceso.....	102
Tabla 95. Ejecución de comandos para el Wireless Controller y puntos de acceso.....	102
Tabla 96. Plantilla base para la configuración del Wireless Controller y puntos de acceso (generic-host-wireless).....	103
Tabla 97. Plantilla de configuración del Wireless Controller y puntos de acceso (Wireless) .....	103
Tabla 98. Plantilla de configuración de servicios para el Wireless Controller y puntos de acceso (Wireless-Service).....	104
Tabla 99. Ejemplo de definición de equipo (ap-fica-pa2d).....	105
Tabla 100. Ejemplo de definición de servicios (ap-fica-pa2d).....	106
Tabla 101. Definición del parámetro check_command para servicios en el.....	106
Tabla 102. Descripción de la ejecución de plugin para el chequeo del Wireless Controller y puntos de acceso .....	106
Tabla 103. Grupos de equipos creados en el .....	107
Tabla 104. Ejemplo de configuración de grupo de equipos .....	107
Tabla 105. Ejemplo de configuración de grupo de equipos .....	108
Tabla 106. Plantilla de configuración de contactos (generic-contact).....	109
Tabla 107. Ejemplo de definición del grupo de contactos .....	110
Tabla 108. Ejemplo de definición de contacto.....	110
Tabla 109. Comando para procesar los datos de rendimiento .....	111
Tabla 110. Plantilla para generar graficas de rendimiento de servicios.....	112
Tabla 111. Ejemplo de definición de servicio y uso de la plantilla de gráficas, para los datos de rendimiento .....	112

### CAPÍTULO V

Tabla 112. Módulos de supervisión en los switch de distribución de la UTN.....	127
Tabla 113. Fórmula para calcular el número de instancias STP.....	128
Tabla 114. Instancias STP en el SW-Zeus.....	128
Tabla 115. Procesos de alta y baja prioridad .....	129
Tabla 116. Procesos de plataforma.....	130
Tabla 117. Colas de la CPU .....	131
Tabla 118. Disponibilidad de la TCAM en los switches de core UTN .....	136
Tabla 119. Motores de supervisión compatibles con los switches de core UTN .....	139
Tabla 120. Presupuesto de inversión para el servidor de monitoreo .....	141
Tabla 121. Presupuestos de inversión para el software implementado en el sistema de monitoreo .....	142
Tabla 122. Presupuestos de inversión para el software propietario whatsupgold .....	142

## RESUMEN

El presente proyecto consiste en la implementación de un sistema de monitoreo para la red de datos de la UTN utilizando software libre mediante herramientas OpenSource y freeware, por lo que no se requiere la compra de ninguna licencia para el funcionamiento del sistema con el objetivo de conocer el estado, rendimiento y disponibilidad en la red.

El primer capítulo expone el fundamento teórico necesario para el desarrollo del proyecto. Se describen brevemente los fundamentos sobre administración de red, arquitecturas de gestión de red tales como el modelo TMN, OSI e INTERNET y el análisis para la elección del sistema de monitoreo a implementar.

El segundo capítulo inicia con el análisis de la situación actual en la red de datos de la UTN que incluye el mapeo de la red e identificación de equipos de comunicaciones que serán integrados en el sistema de monitoreo.

El tercer capítulo detalla el proceso de administración del software, políticas de administración del sistema de monitoreo, manejo de archivos, definición de plantillas, definición de equipos, servicios y configuración del sistema.

En el cuarto capítulo se analizó el rendimiento de la red de datos de la UTN, monitoreando directamente la capa de distribución la cual soporta las configuraciones de red y todo el tráfico que cursa por la misma.

El quinto capítulo describe los procedimientos a realizar para el control de fallas en la red, se analizó la configuración de la capa de distribución para identificar posibles vulnerabilidades que podrían originar problemas en el rendimiento de la red de datos de la UTN.



El sexto capítulo detalla el análisis Beneficio/Costo realizado para medir el nivel de aceptación del proyecto, considerando que no se tendrá ningún beneficio económico por el mismo, más que el beneficio de complementar la administración en la red, permitiendo tener una idea más clara del estado, funcionamiento y operatividad en la misma.

Finalmente el séptimo capítulo expone las conclusiones y recomendaciones obtenidas durante la elaboración de este proyecto de titulación.

## ABSTRACT

This project involves the implementation of a monitoring system for data network UTN using free software by OpenSource and freeware tools, so that the purchase of any license isn't required to operate the system with the aim of meeting status, performance and availability on the network.

The first chapter exposes the theoretical foundation necessary for development of the project. The basics of network management, network management architectures such as TMN model, OSI and INTERNET and analysis for the selection of the monitoring system to be implemented are briefly described.

The second chapter begins with an analysis of the current situation in the data network UTN including network mapping and identification of communications equipment that will be integrated into the monitoring system.

The third chapter details process management software, management policies monitoring system, file management, template definition, definition of equipment, services and system configuration.

In the fourth chapter the network performance data was analyzed UTN directly monitor the distribution layer which supports network configurations and all traffic coursing through it.

The fifth chapter describes the procedures to be performed to control network failures, the configuration of the distribution layer was analyzed to identify potential vulnerabilities that could cause problems in the network performance data of the UTN.

The sixth chapter details the benefit / cost analysis to measure the level of acceptance of the project, whereas any economic benefit There shall be no for the same, but the benefit of complementing the administration in the network, allowing to have a clearer idea of the state, functioning and operating in the same.

Finally the seventh chapter presents the conclusions and recommendations obtained during the development of this project qualification.

## PRESENTACIÓN

El crecimiento de internet y de las redes empresariales crea la necesidad de la gestión en su correcto funcionamiento y la planificación estratégica de su crecimiento con la finalidad de controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable, en consecuencia los fabricantes de dispositivos de red como routers switches o servidores han ido incorporando a sus equipos el software que les permite ser administrados y monitoreados como es SNMP que es un protocolo que permite la gestión de redes desde cualquier plataforma.

Los modelos de gestión de red permiten la configuración, control y resolución de problemas de los componentes de una red y cumplir con los requerimientos definidos en la organización.

La herramienta seleccionada para la implementación del sistema de monitoreo fue NAGIOS por cumplir con los requerimientos propuestos como permitir el manejo de reportes, generación de gráficas y envío de notificaciones, hace uso del protocolo SNMP para obtener información de los equipos en la red, también utiliza agentes externos para monitorear equipos WINDOWS o LINUX.

La red de datos de la UTN<sup>1</sup> dispone de dos switches CATALYST 4506-E como equipos de distribución, el rendimiento en la red de datos de la UTN se monitoreó directamente desde estos switches por el sistema NAGIOS, ya que estos equipos soportan todo el tráfico y mantienen la configuración lógica de la red.

---

<sup>1</sup> UTN: Universidad Técnica del Norte.

## **CAPITULO I**

### **FUNDAMENTOS SOBRE ADMINISTRACIÓN DE RED**

#### **1.1 INTRODUCCIÓN**

La complejidad creciente en las redes de comunicaciones tiende a aplicar técnicas y herramientas que permitan una correcta administración de los recursos dentro de la red, manteniéndola operativa a niveles aceptables de funcionamiento y monitoreada la mayor parte del tiempo, con la finalidad de conocer el rendimiento de la red, la topología e interconexión de equipos y el tráfico de información que soporta diariamente. Todos estos requerimientos han favorecido la evolución de la gestión de red para llevar a cabo de manera controlada y automatizada los procesos orientados a la solución de problemas.

#### **1.2 GESTIÓN DE RED**

##### **1.2.1 DEFINICIÓN**

“Un sistema de comunicación se define como una arquitectura de red que se encuentra interconectada mediante medios de transmisión y protocolos que permiten la utilización de recursos informáticos dentro de la red” (Huidobro, Blanco, & Jordán, 2008, pág. 202), la finalidad de la gestión de red es mantener los distintos sistemas de comunicación en óptimo funcionamiento el mayor tiempo posible.

La gestión de red es un conjunto de herramientas para monitorizar y controlar la red de forma integral, consiste en la utilización de hardware y software implementado entre componentes de red existentes para conseguir los requerimientos de tiempo real, desempeño operacional y calidad de servicio a un precio razonable. (Huidobro, Blanco, & Jordán, 2008, págs. 202-205)

El software de gestión de sistemas proporciona una administración centralizada de los equipos de la red. Este servicio incluye:

- Colección de información del inventario de hardware y software.
- Distribución e instalación del software.
- Compartición de aplicaciones de red.
- Resolución de problemas de hardware y software (Frisch, 2002).

## **1.3 ARQUITECTURAS DE GESTIÓN DE RED**

### **1.3.1 MODELO TMN<sup>2</sup>**

#### **1.3.1.1 Definición**

El modelo TMN se basa en proporcionar una arquitectura organizada para la interconexión de diversos tipos de sistemas de operaciones y equipos de telecomunicaciones para el intercambio de información de gestión utilizando una arquitectura estándar con interfaces normalizadas, incluidos protocolos y mensajes. Proporciona funciones de gestión y comunicaciones para la operación, administración y mantenimiento de una red de telecomunicaciones y aprovisionamiento de sus servicios en un entorno de múltiples fabricantes (Martí, 2009).

El modelo TMN está basado en el modelo OSI<sup>3</sup> para la interconexión de sistemas abiertos, que adopta el modelo gestor-agente para las relaciones entre sistemas o entre sistemas y equipos, sin embargo son dos modelos de gestión muy distintos. TMN ha sido desarrollado para su proyección al futuro mientras que el modelo de gestión OSI como un sub-set de servicios TMN. (Martí, 2009, pág. 81)

---

<sup>2</sup> TMN: Telecommunications Management Network (Red de Gestión de las Telecomunicaciones )

<sup>3</sup> OSI: Open Systems Interconnection (Interconexión de Sistemas Abiertos)

Las instituciones más importantes, participantes en la estandarización de TMN son la UIT-T<sup>4</sup>, ETSI<sup>5</sup>, ISO<sup>6</sup>, ANSI<sup>7</sup>. TMN es capaz de gestionar:

- Redes Telefónicas, Redes LAN<sup>8</sup> y WAN<sup>9</sup>.
- ISDN<sup>10</sup>
- Redes de servicios móviles, servicio de red inteligente y de valor agregado.
- Redes digitales avanzadas de banda ancha como SONET/SDH<sup>11</sup>, ATM<sup>12</sup>, (B-ISDN<sup>13</sup>), etc.

### 1.3.1.2 Relación de una TMN con una red de telecomunicaciones

Una red de telecomunicaciones consta de diversos equipos analógicos, digitales, sistemas de transmisión, sistemas de conmutación, multiplexores, terminales de señalización, procesadores frontales, ordenadores principales, controladores de agrupaciones, servidores de ficheros, etc. Estos equipos reciben genéricamente el nombre de elementos de red. (UIT-T. Recomendación M.3010, 2000, pág. 7)

Desde el punto de vista conceptual, una TMN es una red separada que asegura la interfaz con una red de telecomunicaciones en diversos puntos para el envío y recepción de información hacia y desde la segunda red y para el control de sus operaciones, una TMN puede utilizar partes de la red de telecomunicaciones para proporcionar sus comunicaciones, como se muestra en la figura 1 (UIT-T. Recomendación M.3010, 2000).

---

<sup>4</sup> UIT-T: Telecommunication Standardization Sector (Sector de normalización de las telecomunicaciones)

<sup>5</sup> ETSI: European Telecommunications Standards Institute (Instituto de estandarización europeo de telecomunicaciones)

<sup>6</sup> ISO: International Organization for Standardization (Organización internacional de estandarización)

<sup>7</sup> ANSI: American National Standards Institute (Instituto nacional americano de estandarización)

<sup>8</sup> LAN: Local Area Network (Red de área local)

<sup>9</sup> WAN: Wide Area Network (Red de área extensa)

<sup>10</sup> ISDN: Integrated Services Digital Network (Red digital de servicios integrados)

<sup>11</sup> SONET/SDH : Synchronous Optical Network/Synchronous Digital Hierarchy (Red óptica síncrona / Jerarquía digital síncrona)

<sup>12</sup> ATM: Asynchronous Transfer Mode (Modo de Transferencia Asíncrona)

<sup>13</sup> B-ISDN: Broadband Integrated Services Digital Network (Red Digital de Servicios Integrados de Banda Ancha)

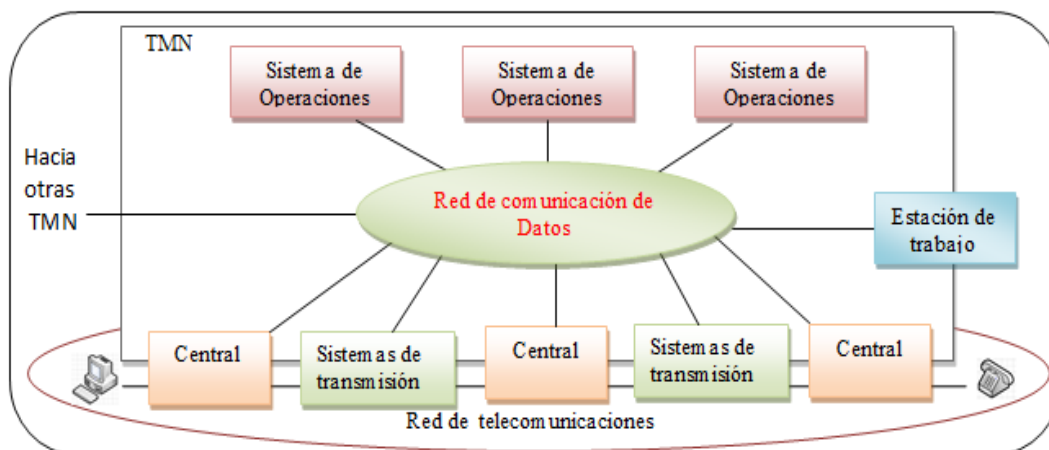


Figura 1. Relación general entre una TMN y una red de telecomunicaciones  
Fuente: Recomendación UIT-T M. 3010, 2000, p. 7

### 1.3.1.3 Arquitectura

Las recomendaciones que regulan la TMN son de la serie M.3xxx de la UIT-T y definen los siguientes modelos y arquitecturas.

#### 1.3.1.3.1 Arquitectura funcional de la TMN

Esta arquitectura es un marco de funcionalidad de gestión estructural y genérico sujeto a normalización. El modelo funcional utiliza las cinco áreas funcionales establecidas por OSI, estas son:

- Gestión de Fallos.
- Gestión de Contabilidad.
- Gestión de Configuración.
- Gestión de Rendimiento.
- Gestión de Seguridad (UIT-T. Recomendación M.3010, 2000).

Se divide en bloques para cumplir con la gestión de red como se indica en la figura 2, a continuación se describen cada bloque:



- OSF<sup>14</sup>: Procesan la información relativa a la gestión de red con el objeto de monitorizar y controlar las funciones de gestión.
- WSF<sup>15</sup>: Proporciona los mecanismos para que un usuario pueda interactuar con la información gestionada por la TMN.
- NEF<sup>16</sup>: Este bloque actúa como agente, susceptible de ser monitorizado y controlado. Estos bloques proporcionan las funciones de intercambio de datos entre los usuarios de la red de telecomunicaciones gestionada.
- QA<sup>17</sup>: Se utiliza para conectar a la TMN aquellas entidades que no soportan los puntos de referencia estandarizados por TMN.
- Función de Mediación: Se encarga de garantizar que la información intercambiada entre los bloques de tipo OSF o NEF cumplan con requisitos de gestión, puede realizar funciones de almacenamiento, adaptación, filtrado y condensación de la información.
- TF<sup>18</sup>: Proporciona funcionalidad para conectar dos entidades funcionales con mecanismos de comunicación incompatibles. Cuando la TF se utiliza dentro de una TMN, la función de transformación conecta dos bloques de función, cada uno de ellos soporta un mecanismo de comunicación normalizado, pero diferente. Cuando se utiliza en la frontera de una TMN, la función de transformación se puede emplear como comunicación entre dos TMN o bien entre una TMN y un entorno no TMN, cuando se utiliza en la frontera de dos TMN la TF conecta dos bloques de función, uno en cada TMN, cada uno de los cuales soporta un mecanismo de comunicación normalizado pero diferente. Cuando el bloque TF se utiliza entre una TMN y un entorno no TMN, el TF conecta un bloque de función con un mecanismo de comunicación normalizado en una TMN a una entidad funcional con un mecanismo

---

<sup>14</sup> OSF: Systems Operation function (Función de operación de sistemas)

<sup>15</sup> WSF: Function Workstation (Función de estación de trabajo)

<sup>16</sup> NEF: Network Element Function (Función de elemento de red)

<sup>17</sup> QA: Adapter Q (Adaptador Q)

<sup>18</sup> TF: Transformation Function (Función de transformación)

de comunicación no normalizado en el entorno no TMN. El bloque TF consolida y amplía la funcionalidad y alcance asociado con los bloques de función de mediación y de adaptador Q.

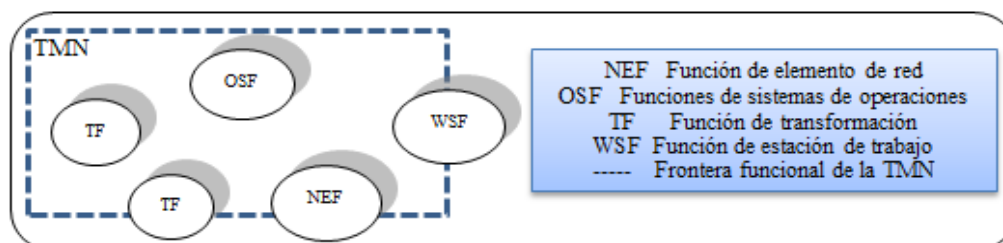


Figura 2. Bloques de función de la TMN  
Fuente: Recomendación UIT-T M.3010, 2000, p.10

### 1.3.1.3.2 Arquitectura de la información de la TMN

La comunicación entre el sistema de gestión y los recursos que se gestionan sigue el modelo gestor-agente de OSI, en este modelo, el sistema de gestión (gestor) no se comunica directamente con los recursos gestionados sino a través de otra aplicación (agente) que es la que tiene la responsabilidad directa sobre ellos. Desde el principio, el modelo TMN adoptó una tecnología orientada a objetos para definir y modelar la información de gestión. Los recursos se modelan como clases de objetos gestionados, que representan las características relevantes para el sistema de gestión, son por tanto, una visión parcial de los recursos de red. (UIT-T. Recomendación M.3010, 2000, pág. 20)

Los parámetros definidos de todas las clases de objetos se mantienen en la MIB<sup>19</sup>, que se organiza siguiendo el árbol de contención y de nombrado de las clases de objetos. La MIB forma la base común de conocimiento entre el sistema de gestión y los agentes de gestión. “El sistema de gestión realiza operaciones sobre los objetos gestionados, representados en la MIB, y el agente se encarga de traducir estas operaciones en acciones sobre los recursos físicos de la red” (UIT-T. Recomendación M.3010, 2000, págs. 21,22).

<sup>19</sup> MiB: Management Information Base (Base de Información Gestión)

De igual forma, cualquier información que se produce en los elementos de red es enviada al sistema de gestión como una notificación emitida por el objeto gestionado que representa el recurso. El modelo TMN utiliza el lenguaje GDMO<sup>20</sup> para la definición de las clases de objetos gestionados así como para sus relaciones mientras que para la definición de los tipos de datos utiliza ASN.1<sup>21</sup>. El modelo de comunicación define los protocolos que se utilizan entre el gestor y los agentes, para las siete capas del modelo OSI, siendo en la capa de aplicación donde se definen los protocolos específicos para la gestión de redes y servicios, en esta capa se incluye CMISE<sup>22</sup> que se compone de CMIS<sup>23</sup> el cual especifica los servicios y de CMIP<sup>24</sup> el protocolo de comunicaciones. Las aplicaciones intercambian información utilizando las primitivas CMIS, que permiten a un gestor conocer y modificar (si está autorizado) el valor de los atributos de un objeto gestionado y ejecutar sobre él las acciones que tenga definidas. De igual forma, los objetos gestionados pueden emitir notificaciones hacia el gestor cuando ocurra algún evento de importancia, pudiendo el gestor definir qué eventos le interesan (UIT-T. Recomendación M.3010, 2000).

### 1.3.1.3.3 Arquitectura física de la TMN

La arquitectura física se encarga de definir como se implementan los bloques funcionales mediante equipamiento físico y los puntos de referencia en interfaces, estructurada a partir de los siguientes elementos:

- Bloques Físicos
- Interfaces Físicas

---

<sup>20</sup> GDMO: Directris Managed Objects Definition (Directriz de Definición de Objetos Gestionados)

<sup>21</sup> ASN.1: Syntax Notation abstracta1 (Notación de sintaxis abstracta 1)

<sup>22</sup> CMISE: Element Common Management Information Services (Elemento Común de Servicios de Información de Gestión)

<sup>23</sup> CMIS: Common Service Management Information (Servicio común de Información de gestión)

<sup>24</sup> CMIP: Protocol Common Management Information (Protocolo de Información de Administración Común)

La figura 3 muestra un ejemplo de arquitectura física para una TMN y en la tabla 1 se muestra una breve descripción de cada interfaz física (UIT-T. Recomendación M.3010, 2000).

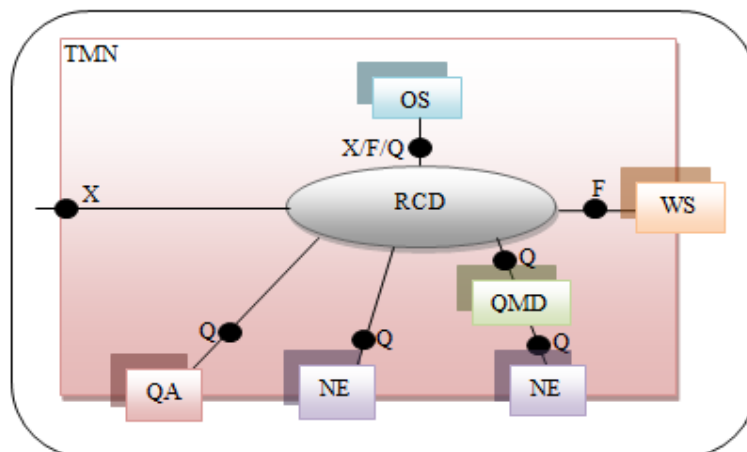


Figura 3. Ejemplo de arquitectura física simplificada para una TMN  
Fuente: Recomendación UIT-T M.3010, 2000, p.24

Tabla 1. Interfaces Normalizadas

Fuente: Recomendación UIT-T M.3010, 2000, p.27- 28

INTERFAZ Q	INTERFAZ F	INTERFAZ X
<ul style="list-style-type: none"> <li>• Se aplica en los puntos de referencia Q</li> <li>• Se encuentra caracterizada por información compartida entre el OS y los elementos de la TMN con los que asegura la interfaz directamente</li> </ul>	<ul style="list-style-type: none"> <li>• Es aplicada en los puntos de referencia f</li> <li>• Conectan estaciones de trabajo con los bloques físicos de la TMN mediante una RCD</li> </ul>	<ul style="list-style-type: none"> <li>• Es aplicada en el punto de referencia x</li> <li>• Interconecta dos TMN</li> <li>• Interconecta una TMN con otras redes o sistemas que utilicen una interfaz semejante a las de la TMN.</li> <li>• Requiere mayor seguridad que la interfaz q</li> <li>• Fija los límites de acceso disponible desde fuera de la TMN</li> </ul>

## 1.3.2 MODELO OSI

### 1.3.2.1 Definición

El modelo de gestión OSI desarrollada conjuntamente por ISO y CCITT<sup>25</sup>, tiene como función supervisar, controlar y mantener una red de datos, se basa en el uso de protocolos del nivel de aplicación para el intercambio de información de gestión según el paradigma Gestor-Agente (Martí, 2009).

<sup>25</sup> CCITT: Consultative Committee for International Telegraphy and Telephony (Comité consultivo internacional de telegrafía y telefonía)

A fin de realizar la gestión de sistemas, debe existir un conocimiento de gestión compartido entre el gestor y el agente. El conocimiento de gestión compartido se presenta en forma de aplicaciones de gestión distribuidas y por tanto las visiones respectivas de cada sistema final pueden ser diferentes si los objetos gestionados contenidos dentro de los sistemas abiertos asociados no son similares, véase la figura 4. (Martí, 2009, págs. 61,62)

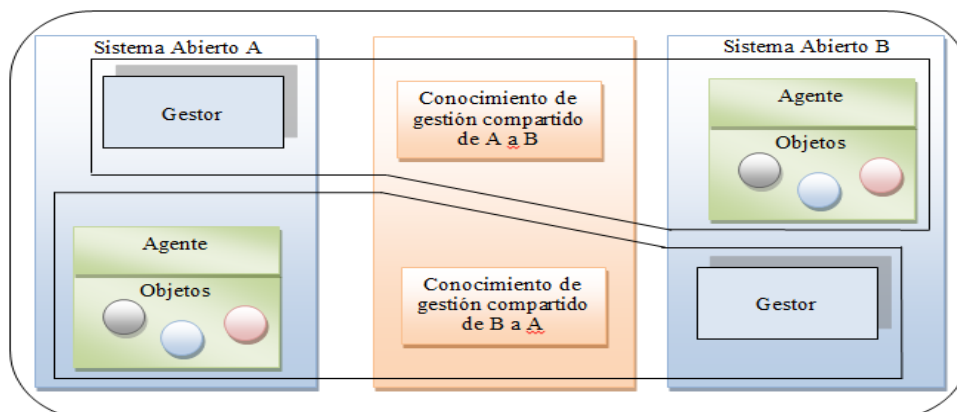


Figura 4. Visión de gestión compartida del modelo OSI  
Fuente: Recomendación UIT-T X.701, 1997, p.15

### 1.3.2.2 Áreas funcionales de la gestión OSI

La gestión OSI define cinco áreas funcionales:

- Gestión de fallos
- Gestión de contabilidad
- Gestión de configuración
- Gestión de funcionamiento
- Gestión de seguridad

#### 1.3.2.2.1 Gestión de fallos

Los fallos tienen como consecuencia:

- Hacer que los sistemas abiertos dejen de satisfacer sus objetivos operacionales.
- Pueden ser persistentes o transitorios.

- Los fallos se manifiestan como sucesos particulares (por ejemplo, errores) en la operación de un sistema abierto.

La detección de errores proporciona la capacidad para reconocer fallos, por ello esta gestión comprende:

- Detección.
- Aislamiento.
- Corrección de fallos.

Incluye funciones para:

- Mantener y examinar cuadernos de error (error logs).
- Aceptar notificaciones de detección de error y reaccionar a las mismas.
- Rastrear e identificar fallos.
- Efectuar secuencias de pruebas de diagnóstico.
- Eliminar fallos. (UIT-T. Recomendación X.700, 1992, pág. 4)

#### **1.3.2.2.2 Gestión de contabilidad**

La gestión de contabilidad permite establecer cargos (o tasas) por el uso de recursos e identificar costos correspondientes a la utilización de esos recursos. Incluye funciones como:

- Informar a los usuarios de costos ocasionados o recursos consumidos.
- Permitir el establecimiento de límites de contabilidad y asociar calendarios de tarifas a la utilización de recursos.

- Permitir la combinación de costos cuando se invoquen múltiples recursos para alcanzar un objetivo de comunicación dado. (UIT-T. Recomendación X.700, 1992, pág. 4)

#### **1.3.2.2.3 Gestión de configuración**

La gestión de configuración permite:

- Identificar, ejercer control, tomar datos y proporcionar datos para sistemas abiertos.
- Sus funciones son realizadas con el fin de preparar, inicializar, poner en marcha y tener en cuenta la operación continua y la terminación de servicios de interconexión.

Incluye funciones para:

- Establecer los parámetros que controlan la operación rutinaria del sistema abierto.
- Asociar nombres con objetos gestionados y conjuntos de objetos gestionados.
- Inicializar y cerrar objetos gestionados.
- Reunir, a petición, información sobre la condición actual del sistema abierto.
- Obtener anuncios de cambios significativos en la condición del sistema abierto.
- Cambiar la configuración del sistema abierto. (UIT-T. Recomendación X.700, 1992, pág. 4)

#### **1.3.2.2.4 Gestión de funcionamiento**

La gestión de funcionamiento permite evaluar el comportamiento de recursos y la efectividad de actividades de comunicación. Incluye funciones como:

- Reunir información estadística.
- Mantener y examinar cuadernos de historiales de estados de sistemas.
- Determinar el rendimiento del sistema en condiciones naturales y artificiales.

- Cambiar los modos de operación del sistema con el fin de efectuar actividades de gestión del funcionamiento. (UIT-T. Recomendación X.700, 1992, pág. 5)

#### **1.3.2.2.5 Gestión de seguridad**

La gestión de seguridad tiene como fin soportar la aplicación de políticas de seguridad por medio de funciones que incluyen:

- La creación, supresión y control de servicios y mecanismos de seguridad.
- La distribución de información relativa a la seguridad.
- Señalación de sucesos relacionados con la seguridad. (UIT-T. Recomendación X.700, 1992, pág. 5)

#### **1.3.2.3 Modelo para la gestión OSI**

##### **1.3.2.3.1 Base de información de gestión**

La MIB, se define como:

- Es un tipo de base de datos que contiene información jerárquica estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones, es la información dentro de un sistema abierto que puede ser transferida o afectada mediante la utilización de protocolos de gestión OSI.
- Está compuesta por una serie de objetos gestionados dentro de un sistema abierto, que representan los dispositivos como enrutadores y conmutadores en la red, no obstante solamente los objetos gestionados relacionados con el entorno OSI están sujetos a normalización. Cada objeto manejado en una MIB tiene un identificador de objeto único e incluye el tipo de objeto, el nivel de acceso (lectura o escritura), restricciones de tamaño y la información del rango del objeto.



- La estructura lógica de la información de gestión está normalizada. (Martí, 2009, pág. 76)

GDMO, proporciona un lenguaje para la definición de objetos gestionados dentro de los sistemas basados en el modelo TMN y OSI, define un conjunto de plantillas para especificar la información de gestión, es un lenguaje de descripción estructurada para especificar las clases, comportamientos y atributos de los objetos así como también clases que se pueden heredar, básicamente, GDMO especifica cómo un fabricante de productos de red debe describir el producto de manera formal para que otros puedan escribir programas compatibles con dicho producto. Las definiciones de los objetos creados con GDMO y las herramientas relacionadas forman la MIB, GDMO utiliza ASN.1, como las reglas de sintaxis en la codificación de atributos en la definición de los objetos es por ello que existe cierta analogía con la SMI<sup>26</sup> utilizada en el Modelo de Gestión de Internet (Martí, 2009).

#### **1.3.2.3.2 CMIP/CMIS**

El Protocolo Común de Información de Gestión CMIP, es el protocolo de gestión de red correspondiente al modelo ISO/OSI, provee mecanismos de intercambio de información, entre un administrador y elementos remotos de red utilizando CMIS que define un sistema de servicios de información de gestión mediante un conjunto de primitivas relacionadas con objetos de la MIB. Dada la poca implementación del modelo OSI, se ha intentado adaptar el protocolo CMIP para su uso en redes TCP/IP, en lo que se conoce como CMOT (CMIP sobre TCP/IP), CMIP se planteó como un competidor de SNMP<sup>27</sup>, y de hecho tiene muchas más funcionalidades. De todas formas, precisamente su complejidad y el consumo de recursos que conlleva es lo que han hecho que su uso se encuentre bastante limitado, mientras que SNMP se implementa de forma masiva (Martí, 2009).

---

<sup>26</sup> SMI: Structure of Management Information (Estructura de Información de Gestión)

<sup>27</sup> SNMP: Simple Network Management Protocol (Protocolo Simple de Gestión de Red)

Los elementos clave de este modelo de arquitectura son:

- El Proceso de Aplicación de gestión de sistemas (SMAP): Software local de un equipo (sistema) gestionado que implementa las funciones de gestión para ese sistema (host, router, etc.). Tiene acceso a los parámetros del sistema y puede, por tanto, gestionarlo, así como comunicarse con SMAP de otros sistemas.
- Entidad de aplicación de gestión de sistemas (SMAE): Entidad de nivel de aplicación responsable del intercambio de información de gestión con SMAE de otros nodos, especialmente con el sistema que hace las funciones de centro de control de red. Para esta función se utiliza un protocolo normalizado (CMIP).
- Entidad de gestión de nivel (LME): Proporciona funciones de gestión específicas de cada capa del modelo OSI.
- Base de información de gestión (MIB). (Martí, 2009, pág. 64)

SMAP puede tomar el papel de agente o de gestor. El papel de gestor corresponde al centro de control de red, y el de agente a los sistemas gestionados, un gestor solicita información o solicita la ejecución de comandos a los sistemas gestionados. El agente interactúa con el gestor y es responsable de administrar los objetos de su sistema como se muestra en la figura 5 (Martí, 2009).

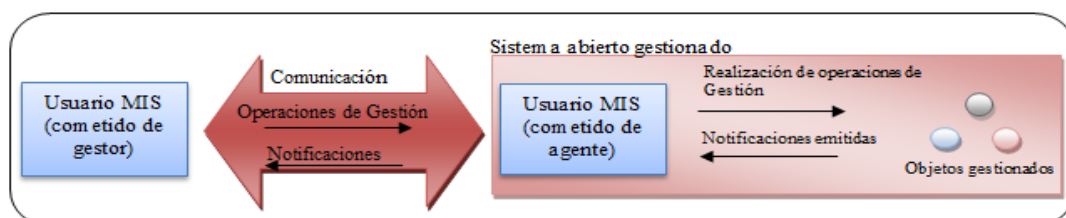


Figura 5. Interacción de gestión de sistemas CMIP/CMIS  
Fuente: Recomendación UIT-T X.701, 1997, p.10

Primitivas del servicio CMIS:

- M-EVENT-REPORT: Usado por un agente para notificar la ocurrencia de un evento a un gestor.

- M-GET: Usado por un gestor para obtener información de un agente.
- M-SET: Usado por un gestor para modificar información de un agente.
- M-ACTION: Usado por un gestor para invocar un procedimiento predefinido especificado como parte de un objeto de un agente. La petición indica el tipo de acción y los parámetros de entrada.
- M-CREATE: Usado para crear una nueva instancia de una clase de objetos.
- M-DELETE: Usado para eliminar uno o más objetos.
- M-CANCEL-GET: Usado para finalizar una operación GET larga. (Martí, 1999, págs. 65,66)

### 1.3.3 MODELO DE INTERNET

#### 1.3.3.1 Definición

SNMP nace de la pila de protocolos TCP/IP que es el protocolo estándar para la conexión en Internet, esta pila de protocolos fue desarrollada por el Departamento de Defensa de los Estados Unidos de Norteamérica y sus estándares o documentos RFC<sup>28</sup> son publicados por la IETF<sup>29</sup>, inicialmente el protocolo de gestión ampliamente utilizado era el ICMP (Protocolo de control mensajes de Internet), posteriormente al crecer la complejidad en las redes de datos debido al incremento de equipos y a los requerimientos en la disponibilidad y rendimiento en los mismos se hizo necesario el desarrollo de nuevos y mejores protocolos y es allí donde SNMP aparece.

SNMP se define como protocolo asimétrico de petición-respuesta basado en el modelo de interrupción-sondeo directo, esto significa que una entidad no necesita esperar una respuesta después de enviar un mensaje, por lo que puede enviar otros mensajes o realizar otras actividades (Douglas & Schmidt, 2005).

---

<sup>28</sup> RFC: Request for Comments (Solicitudes de Comentario)

<sup>29</sup> IETF : Task Force Internet Engineering (Fuerza de tareas de ingeniería de internet)

### 1.3.3.2 Gestión de red y vigilancia

“El núcleo de SNMP es un conjunto de operaciones (operaciones para reunir información) que proporciona a los administradores la capacidad de conocer el estado de algún dispositivo basado en SNMP” (Martí, 2009, pág. 155). Por ejemplo se puede utilizar para comprobar la velocidad de una interfaz Ethernet o conocer la temperatura interna de un conmutador y que se advierta cuando es demasiado alta. SNMP se suele asociar con la gestión de routers, pero es importante entender que se puede utilizar para administrar muchos tipos de dispositivos. Mientras que su predecesor SGMP<sup>30</sup>, fue desarrollado para administrar routers, SNMP se puede utilizar para administrar sistemas Unix, Windows impresoras, fuentes de alimentación y cualquier dispositivo que soporte el protocolo. Esto incluye no sólo dispositivos físicos, sino también software, tales como servidores web y bases de datos.

Otro aspecto de la gestión de la red es la monitorización de la red, es decir, el seguimiento de toda la red en lugar de hacerlo con solo un dispositivo. La figura 6 muestra un esquema de gestión de red descentralizado y distribuido entregado por SNMP (Martí, 2009).

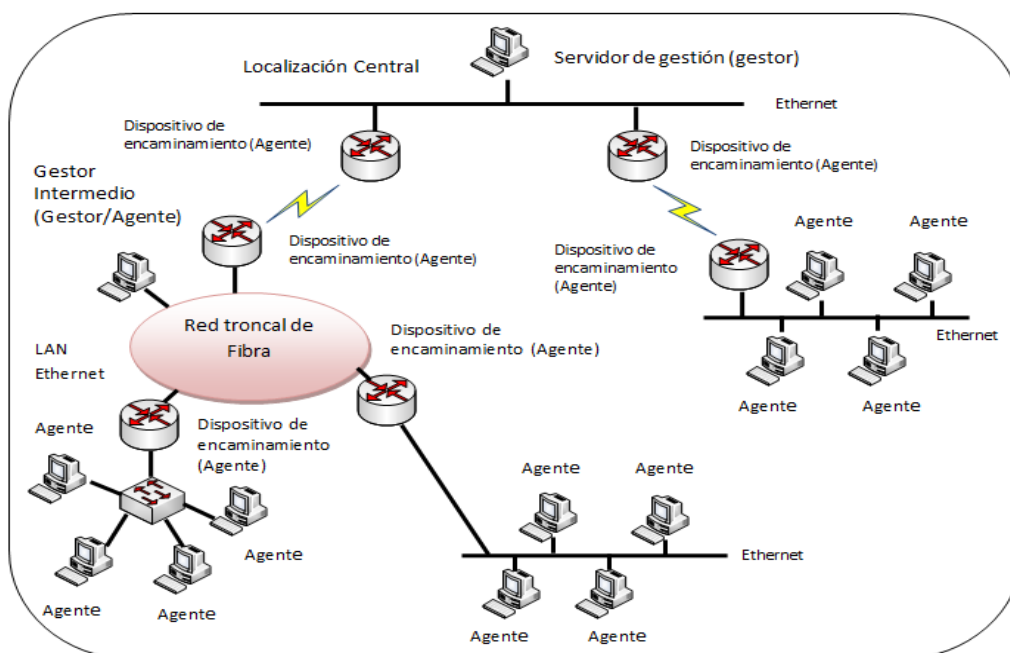


Figura 6. El rol de SNMP  
Fuente: (Stallings, 2004, pág. 797)

<sup>30</sup> SGMP: Monitoring Protocol Simple Gateway (Protocolo de Monitoreo de Puerta de Enlace Simple)

### 1.3.3.3 Versiones de SNMP

“La IETF es responsable de definir los protocolos estándar que rigen el tráfico de Internet, incluyendo SNMP. La tabla 2 muestra una comparativa entre las diferentes versiones de SNMP” (Douglas & Schmidt, 2005, pág. 9).

Tabla 2. Comparativa de las versiones de SNMP  
Fuente: (Douglas & Schmidt, 2005, págs. 9-10)

VERSIÓN	DESCRIPCIÓN	AUTENTICACIÓN	ENCRYPTADO	SEGURIDAD
SNMPV1	Usa el modelo basado en comunidades	Community string	No	No autenticación No Encriptado
SNMPV2 SNMPV2C	Usa el modelo basado en comunidades	Community string	No	No autenticación No Encriptado
SNMPV3	Utiliza nombres de usuarios para comprobar la autenticación	USM	No	No autenticación No Encriptado
SNMPV3	Variante de SNMPv3 que provee una autenticación basada en los algoritmos de HMAC-SHA o HMAC-MD5	USM + MD5 o SHA	No	Autenticación No Encriptado
SNMPV3	Configuración más segura de SNMPV3 que provee algoritmos de autenticación y encriptación DES de 56 bits	USM + MD5 o SHA	DES	Autenticación Encriptado

### 1.3.3.4 Gestores y Agentes

En el mundo de SNMP hay dos tipos de entidades, los gestores y agentes. El gestor es un servidor que ejecute algún tipo de sistema de software que puede manejar las tareas de administración de una red, a menudo referido como NMS<sup>31</sup>, el cual es responsable del sondeo y recepción de capturas de información de gestión de los agentes instalados en router, switches, servidores Unix o Windows. Esta información puede ser utilizada después para determinar si algún tipo de acontecimiento catastrófico ha ocurrido. Los trap son emitidos por el agente para decirle al NMS que algo ha sucedido, se envían de forma asincrónica y no en respuesta a consultas. El NMS es además responsable de la realización de acciones, basadas en la información que recibe del agente. La segunda entidad, el agente, es una pieza de software que se ejecuta en los dispositivos de red. Puede ser un

<sup>31</sup> NMS: Network Management Stations (Estaciones de administración de red)

programa separado (un demonio, en lenguaje Unix) o puede ser incorporado en el sistema operativo (por ejemplo, el IOS de Cisco). Hoy en día, la mayoría de dispositivos IP<sup>32</sup> vienen con algún tipo de agente SNMP construido, lo que vuelve más sencilla la gestión de red. (Douglas & Schmidt, 2005, pág. 10)

Desde una estación de gestión se emiten tres tipos de mensajes SNMP: GetRequest (solicitud-obtener), GetNextRequest (solicitud-obtener siguiente) y SetRequest (solicitud establecer). Los tres mensajes son confirmados por el agente mediante un mensaje GetResponse, el cual se pasa a la aplicación de gestión. Además, un agente puede emitir un mensaje de excepción o trap en respuesta a un evento que afecte a la MIB, las solicitudes de gestión se envían al puerto UDP<sup>33</sup> 161, mientras que el agente envía los traps al puerto UDP 162, como se muestra en la figura 7.

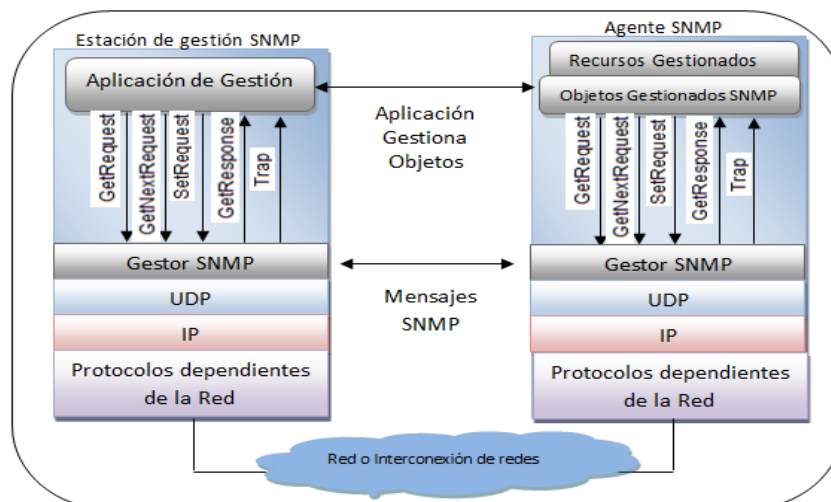


Figura 7. Ejemplo de gestión de red distribuida  
Fuente: (Stallings, 2004, pág. 799)

El agente proporciona información sobre la gestión de los dispositivos de red. Por ejemplo, el agente en un router es capaz de realizar seguimiento del estado de cada una de sus interfaces, el NMS consulta el estado de cada interfaz y se toman las medidas adecuadas impuestas por el administrador en cada caso. Cuando el agente percibe algún problema en el

<sup>32</sup> IP: Internet Protocol (Protocolo de internet)

<sup>33</sup> UDP: User Datagram Protocol (Protocolo de datos de usuario)

sistema monitoreado puede iniciar el envío de trap hacia el NMS sin esperar ninguna consulta del mismo, aunque esto presentaría un mayor consumo de recursos por parte del sistema monitoreado, el agente también podría enviar el correspondiente "todo está bien - trap" cuando haya una transición de un estado incorrecto a uno correcto de funcionamiento, como se muestra en la figura 9. Es importante tener en cuenta que las encuestas y los trap pueden ocurrir al mismo tiempo, no hay restricciones sobre cuándo puede el NMS consultar al agente o cuando el agente puede enviar traps. La figura 8 muestra el formato de la PDU utilizada por SNMP en sus versiones 1 y 2, SNMPv2 maneja el mismo formato para las PDU GETRequest, GetNexRequest, SetRequest, GetResponys y cumplen con la misma función que en SNMPv1, la diferencia radica en que SetRequest es la única que mantiene su modo de operación completo (todo o nada), las tres PDU restantes no funcionan de esta manera, es decir si la operación con uno de los objetos falla, la operación con el resto de objetos solicitados si se ejecuta (Douglas & Schmidt, 2005).

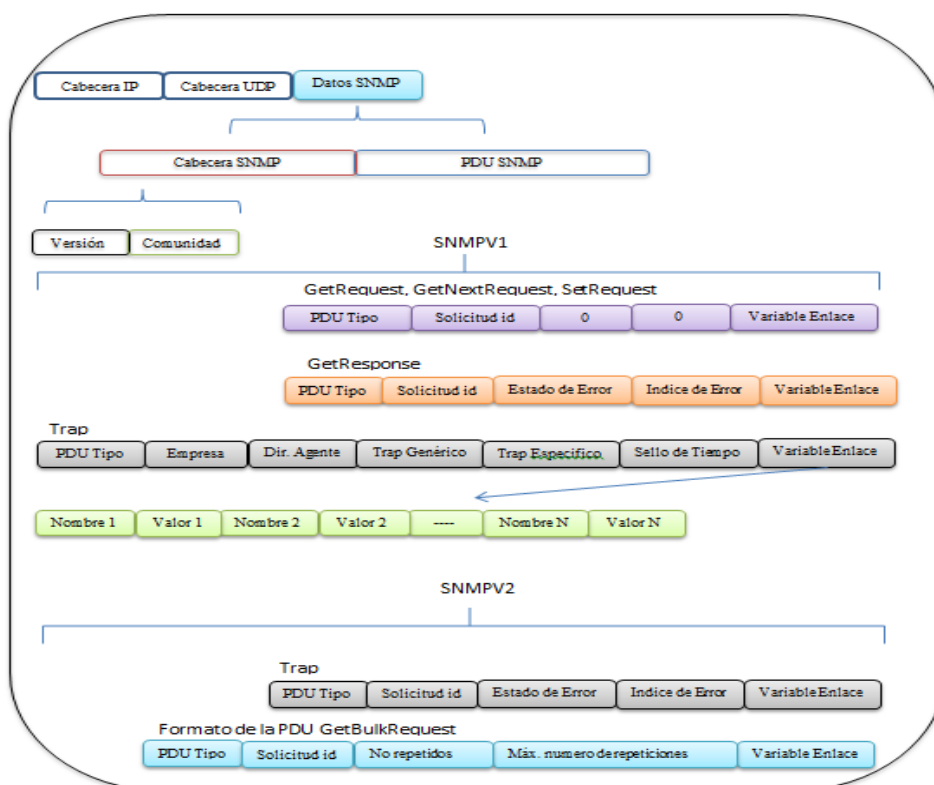


Figura 8. PDU SNMP

Fuente: Vertical Horizons - SNMP Message Format, (2010), recuperado de: <http://verticalhorizons.in/snmp-message-format-snmp-pdu-format/>

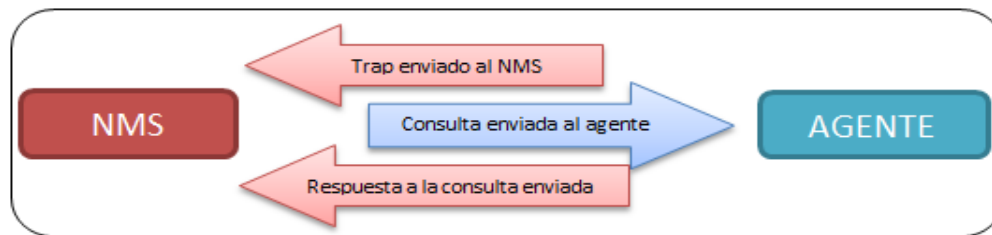


Figura 9. Relación entre el Gestor y el Agente  
Fuente: (Douglas & Schmidt, 2005, pág. 4)

### 1.3.3.5 SMI y MIB

La Estructura de Gestión de Información (SMI), proporciona una forma de definir objetos administrados y su comportamiento. Un agente tiene en su poder una lista de objetos a los que hace un seguimiento, uno de tales objetos puede ser por ejemplo el estado de funcionamiento de una interfaz física en un router. La Base de información de gestión (MIB) se puede considerar como una base de datos de objetos gestionados al que el agente hace un seguimiento. Cualquier tipo de estado o información estadística al que se puede acceder por el NMS se define en una MIB (Martí, 2009).

La SMI proporciona una manera de definir objetos administrados, mientras que la MIB es la definición de los objetos mismos. Al igual que un diccionario, el cual muestra cómo se escribe una palabra y luego le da su significado o definición, la MIB define el nombre textual de un objeto gestionado y explica su significado. (Douglas & Schmidt, 2005, pág. 13)

“Todos los agentes implementan en particular la MIB-II, esta norma define variables para conocer por ejemplo estadísticas de una interfaz física o virtual como octetos enviados, octetos recibidos, MTU<sup>34</sup>, etc.” (Douglas & Schmidt, 2005, pág. 13). El objetivo principal de la MIB-II es brindar información de gestión en general TCP / IP, no cubre todos los elementos posibles que un vendedor puede desear para gestionar un dispositivo en particular.

<sup>34</sup> MTU: Máximum Transmission Unit (Unidad máxima de transferencia)



### 1.3.3.6 Introducción a la supervisión remota (RMON<sup>35</sup>)

RMON fue desarrollado para entender el funcionamiento de toda la infraestructura de red y como de forma particular los dispositivos afectan a la red vista como un todo. Se puede utilizar para controlar no sólo el tráfico LAN, sino también las interfaces WAN. RMONv1 o RMON se define en el RFC 2819, una versión mejorada de la norma, llamada RMONv2, se define en el RFC 2021. RMONv1 proporciona al NMS estadísticas a nivel de paquetes de toda una red LAN o WAN, estas estadísticas pueden ser recogidas de varias maneras, una de ellas consiste en introducir una sonda RMON en cada segmento de la red que se debe supervisar. La MIB RMON fue diseñada para permitir a una sonda RMON que funcione en un modo fuera de línea y que la sonda pueda recopilar estadísticas sobre la red que está viendo sin necesidad que un NMS esté haciendo consultas constantemente, en algún momento posterior, el NMS puede consultar la sonda para el chequeo de distintas estadísticas. Otra de las características que la mayoría de las sondas implementa es la posibilidad de establecer umbrales para diversas condiciones de error y cuando se cruza un umbral alertar con una captura de SNMP. (Douglas & Schmidt, 2005, pág. 14)

### 1.3.3.7 SNMP y UDP

El Protocolo Simple de Gestión de Red es un protocolo de nivel de aplicación que forma parte del conjunto de protocolos TCP/IP, utiliza UDP como el protocolo de transporte para pasar datos entre gestores y agentes. UDP se define en la RFC 768, fue elegido sobre TCP<sup>36</sup> ya que es no orientado a conexión, este aspecto de UDP hace que sea poco fiable ya que no hay acuse de recibo en la pérdida de datagramas a nivel de protocolo, todo depende de la solicitud SNMP para determinar si se pierden los datagramas y retransmisión si se requiere, esto se consigue normalmente con un tiempo de espera ya que el NMS envía una petición UDP al agente y espera una respuesta, la longitud del tiempo de espera del NMS

---

<sup>35</sup> RMON: Remote Network Monitoring (Monitoreo remoto de redes)

<sup>36</sup> TCP: Transmission Control Protocol (Protocolo de control de transmisión)

depende de cómo se configure. Si se alcanza el tiempo de espera y no se ha recibido respuesta del agente, se asume que el paquete fue perdido y se vuelve a transmitir la solicitud. (Douglas & Schmidt, 2005, pág. 15)

La ventaja de la naturaleza poco fiable de UDP es que requiere bajos costos, por lo que el impacto en el rendimiento de la red es reducido. “SNMP utiliza el puerto UDP 161 para el envío y recepción de solicitudes y el puerto 162 para la recepción de los trap emitidos por los dispositivos gestionados” (Douglas & Schmidt, 2005, pág. 15). La figura 10 muestra el conjunto de protocolos TCP / IP, que es la base para todas las comunicaciones. Hoy en día cualquier dispositivo que desea comunicarse a través de internet (por ejemplo, los sistemas Windows NT, Unix servidores, routers Cisco, etc.) deben utilizar este conjunto de protocolos.

SNMP se ve a menudo como una pila de protocolos, ya que cada capa utiliza la información de la capa inferior y proporciona un servicio a la capa superior.

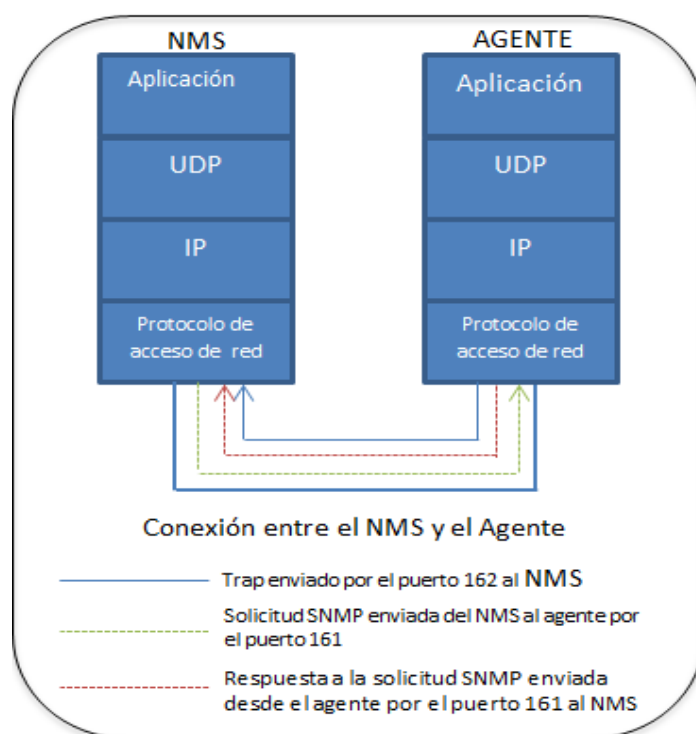


Figura 10. Modelo de comunicación TCP/IP y SNMP  
Fuente: (Douglas & Schmidt, 2005, pág. 16)

Cuando el NMS o un agente desean realizar una función SNMP (por ejemplo, una solicitud o una trampa), se producen los siguientes eventos en la pila de protocolos:

- **Aplicación:** La aplicación SNMP cumple funciones de NMS o agente, el agente se encuentra en el dispositivo administrado, tal es el caso de un router, un switch o un computador y ejecuta procesos de envío de información de administración hacia un software de gestión de red provisto por el administrador del sistema mientras que la función del NMS se define como la interfaz del administrador de red que contiene un software de gestión de todo el sistema y que mantiene una base de datos llamada MIB (Base de información de administración) con un formato SMI proporcionado por el lenguaje ASN.1.
- **UDP:** Permite la comunicación entre hosts, la cabecera UDP contiene el puerto de destino del dispositivo al que se enviará la solicitud o trap, el puerto de destino será 161 (consulta) o 162 (trap).
- **IP:** La capa IP entregará el paquete SNMP a su destino previsto especificado por su dirección IP.
- **Control de Acceso al Medio (MAC):** El evento final que debe ocurrir para que un paquete SNMP pueda llegar a su destino es pasar a la red física. La capa MAC<sup>37</sup> se compone realmente de controladores de hardware y dispositivos que ponen los datos en una pieza física, tal como una tarjeta Ethernet. La capa MAC también es responsable de recibir paquetes desde la red física y enviarlos de nuevo a la pila de protocolo para que puedan ser procesados por la capa de aplicación (SNMP, en este caso). (Douglas & Schmidt, 2005, págs. 16,17)

---

<sup>37</sup> MAC: Medium Access Control (Control de acceso al medio)

### 1.3.3.8 Comunidades SNMP

SNMPv1 y SNMPv2 utiliza la noción de las comunidades para establecer confianza entre gestores y agentes. Un agente está configurado con tres tipos de comunidad: de sólo lectura, lectura y escritura y trap. Los nombres de las comunidades son esencialmente las contraseñas, no hay verdadera diferencia entre una cadena de comunidad y la contraseña que utiliza para acceder a su cuenta en el equipo. La mayoría de los proveedores envían sus equipos con la comunidad por defecto public para el acceso de sólo lectura de la comunidad y private para la comunidad de lectura y escritura. Es importante cambiar estos valores predeterminados antes de que el dispositivo entre en funcionamiento en la red. Al configurar el agente SNMP, tendrá que configurar su destino de captura, la cual es la dirección a la que se enviará la información de gestión.

El problema con la autenticación de SNMP es que las cadenas de comunidad se envían en texto plano, lo que hace que sea fácil para los intrusos interceptarlos y usarlos en su contra. SNMPv3 aborda esto permitiendo, entre otras cosas, la autenticación segura y la comunicación entre los dispositivos SNMP (Douglas & Schmidt, 2005).

### 1.3.3.9 Estructura de gestión de la información

La Estructura de la Información de Gestión (SMIV1, RFC 1155) define con precisión cómo los objetos administrados se nombran y especifica los tipos de datos asociados. La definición de objetos gestionados puede dividirse en tres atributos.

- Nombre: El nombre o OID<sup>38</sup>, define un objeto gestionado, los nombres suelen aparecer en forma textual o en forma de números separados por puntos.
- Tipo y sintaxis: El tipo de datos de un objeto gestionado se define mediante ASN.1, que es una forma de especificar cómo se representan y se transmiten los datos entre

---

<sup>38</sup> OID: Object Identifiers (Identificador de objeto)

gestores y agentes, en el contexto de SNMP, ASN.1 es una norma para representar datos independientemente de la máquina que se esté usando y sus formas de representación internas. Esto significa que un PC con Windows NT pueden comunicarse con una máquina Sun SPARC y no tener que preocuparse acerca de cosas tales como ordenamiento de bytes.

- Codificación: Una sola instancia de un objeto gestionado se codifica en una cadena de octetos utilizando las reglas de codificación básica (BER<sup>39</sup>). BER define cómo se codifican y decodifican los objetos para que puedan ser transmitidos a través de un medio de transporte como Ethernet (Martí, 2009).

### 1.3.3.10 Designación de OID

Esta estructura es la base para el esquema de nomenclatura de SNMP. Un ID de objeto se compone de una serie de números enteros separados por puntos, aunque hay una forma legible que es más agradable que una serie de números, esta forma no es más que una serie de nombres separados por puntos, cada uno de los cuales representa un nodo del árbol SMI. La figura 11 muestra algunos niveles de este árbol. (Douglas & Schmidt, 2005, pág. 20)

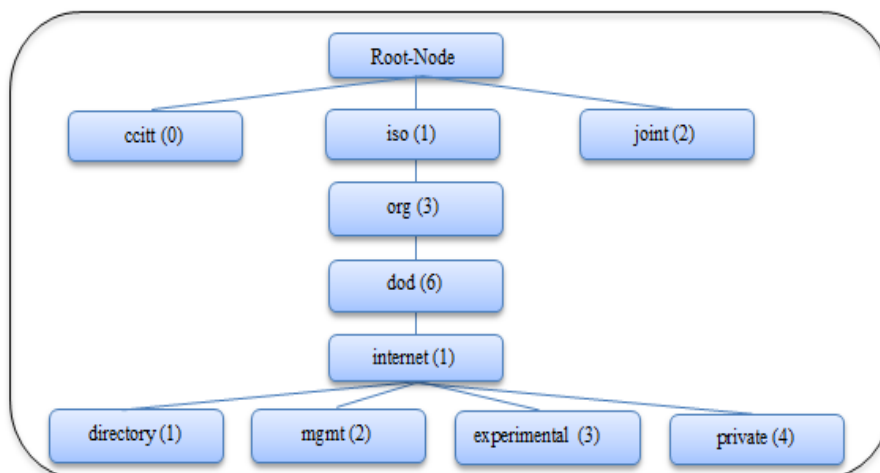


Figura 11. Árbol de Objetos SMI  
Fuente: (Douglas & Schmidt, 2005, pág. 25)

<sup>39</sup> BER: Basic Encoding Rules (Reglas de codificación básica)

La notación decimal con puntos es como el objeto se representa internamente dentro de un agente, el nombre textual evita tener que recordar largas cadenas de enteros.

La sub-rama directory (1) no se utiliza actualmente, la sub-rama mgmt (2) define un conjunto estándar de gestión de objetos de Internet, la sub-rama experimental (3) se reserva para pruebas y fines de investigación y los objetos debajo de la sub-rama private (4) se definen unilateralmente, lo que significa que los individuos y las organizaciones son los responsables de la definición de los objetos en esta rama. (Douglas & Schmidt, 2005, pág. 20)

### 1.3.3.11 Definición de OID

El atributo sintaxis proporciona las definiciones de objetos gestionados a través de ASN.1. SMIV1 define varios tipos de datos que son de suma importancia para la gestión de los dispositivos de red, estos tipos de datos son simplemente una manera de definir el tipo de información que un objeto gestionado puede contener. La tabla 3 enumera los tipos de datos soportados por SMIV1. (Douglas & Schmidt, 2005, pág. 22)

Tabla 3. Tipos de datos SMIV1  
Fuente: (Douglas & Schmidt, 2005, pág. 23)

TIPO DE DATO	DESCRIPCIÓN
INTEGER	Un número de 32 bits a menudo se utiliza para especificar algún valor dentro del contexto de un único objeto administrado. Por ejemplo, el estado de funcionamiento de la interfaz de un router que puede estar activa, inactiva o en proceso con valores enumerados, 1 representaría activa, 2 inactiva, y 3 en proceso.
OCTET STRING	Una cadena de cero o más octetos generalmente se utiliza para representar cadenas de texto, pero a veces también se utiliza para representar direcciones físicas.
COUNTER	Un número de 32 bits con un valor mínimo de 0 y máximo valor $2^{32}-1$ (4294967295). Cuando el valor máximo se alcanza, se envuelve de nuevo a cero y comienza de nuevo. Se utiliza principalmente para rastrear información como el número de octetos enviados y recibidos en una interfaz o el número de errores y los descartes vistos en una interfaz.
OBJECT IDENTIFIER	Una cadena decimal con puntos que representa un objeto administrado dentro del árbol de objetos. Por ejemplo, 1.3.6.1.4.1.9 representa un OID privado de Cisco Systems.
NULL	No se utiliza actualmente en SNMP.
SEQUENCE	Define las listas que contienen cero o más tipos de datos ASN.1.
SEQUENCE OF	Define un objeto gestionado que se compone de una secuencia de tipo ASN.1.
IPADDRESS	Representa una dirección IPv4 de 32 bits. Ni SMIV1 ni SMIV2 soporta direcciones IPv6 de 128 bits, este problema serán tratados por nuevas SMI.
NETWORKADDRESS	Igual que el tipo IpAddress, pero puede representar diferentes tipos de direcciones de red.
GAUGE	Un número de 32 bits con un valor mínimo de 0 y máximo de $2^{32}-1$ (4294967295). A diferencia de un contador, un medidor puede aumentar o disminuir a voluntad, pero nunca puede exceder su valor máximo. La velocidad de interfaz en un enrutador se mide con un medidor.
TIMETICKS	Un número de 32 bits con un valor mínimo de 0 y máximo de $2^{32}-1$ (4294967295). TimeTicks mide el tiempo en centésimas de segundo. El tiempo de actividad en un dispositivo es medido utilizando este tipo de datos.
OPAQUE	Permite cualquier otra codificación ASN.1 en un octeto.

### 1.3.3.12 MIB-II

MIB-II es un grupo de gestión muy importante, ya que cada dispositivo compatible con SNMP también debe ser compatible con MIB-II. Se define como iso.org.dod.internet.mgmt.1, o 1.3.6.1.2.1. A partir de aquí, el grupo del sistema es MIB-II (1), o 1.3.6.1.2.1.1, y así sucesivamente. La figura 12 muestra la MIB-II y el subárbol mgmt (2). La tabla 4 describe brevemente cada uno de los grupos de gestión definidos en la MIB-II (Douglas & Schmidt, 2005).

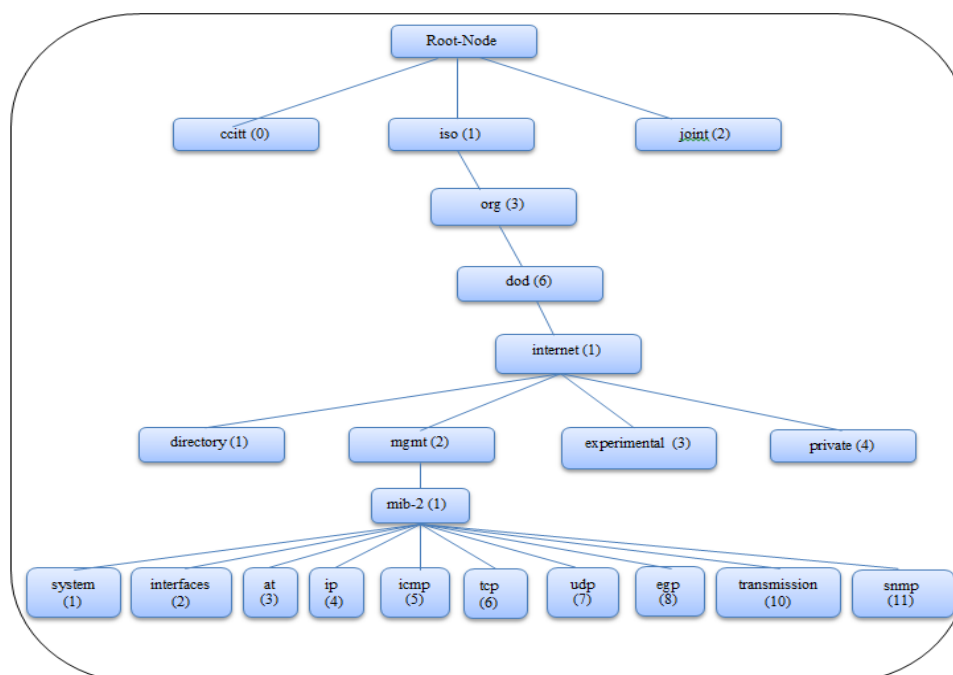


Figura 12. Árbol MIB II  
Fuente: (Douglas & Schmidt, 2005, pág. 33)

Tabla 4. Descripción de los grupos de la Mib-II  
Fuente: (Douglas & Schmidt, 2005, pág. 34)

NOMBRE SUB-ÁRBOL	OID	DESCRIPCIÓN
SYSTEM	1.3.6.1.2.1.1	Define una lista de objetos que corresponden a la operación del sistema, tal como el tiempo de actividad del sistema, sistema de contacto y el nombre del sistema.
INTERFACES	1.3.6.1.2.1.2	Realiza un seguimiento de la situación de cada interfaz en una entidad gestionada, permite conocer que interfaces están arriba o abajo así como octetos enviados, recibidos, errores, descartes, etc.
AT	1.3.6.1.2.1.3	El grupo traducción de direcciones (at) está en desuso y sólo tiene compatibilidad con versiones anteriores. Será probablemente eliminado de la MIB-III.
IP	1.3.6.1.2.1.4	Realiza un seguimiento de muchos aspectos IP, incluyendo el enrutamiento.
ICMP	1.3.6.1.2.1.5	Pistas de errores ICMP, descartes, etc.
TCP	1.3.6.1.2.1.6	Pistas del estado de la conexión TCP (por ejemplo si esta activa o no, etc.)
UDP	1.3.6.1.2.1.7	Pistas de estadísticas UDP, datagramas entrantes y salientes, etc.
EGP	1.3.6.1.2.1.8	Pistas de estadísticas sobre EGP y mantiene una tabla de vecinos EGP.
TRANSMISSION	1.3.6.1.2.1.10	Actualmente no hay objetos definidos para este grupo.
SNMP	1.3.6.1.2.1.11	Mide el rendimiento subyacente a la aplicación SNMP en la entidad gestionada y entrega pistas acerca del número de paquetes SNMP enviados y recibidos.

### 1.3.3.13 SNMPV3

El protocolo SNMPv3 define un nuevo modelo de seguridad, específicamente USM<sup>40</sup>, este modelo tiene las siguientes características:

- **Integridad del Mensaje:** Se garantiza que un mensaje no ha sido alterado al recorrer la red.
- **Autenticación:** Determina que el mensaje proviene de una fuente válida.
- **Encriptación:** El contenido del paquete es cifrado a fin de evitar que sea leído por una fuente no autorizada. (Douglas & Schmidt, 2005, pág. 280)

"En esta versión, el agente, al igual que el gestor se definen como entidades SNMP y consisten de un motor (SNMP engine) y aplicaciones SNMP, el motor SNMP consta de los siguientes componentes" (Douglas & Schmidt, 2005, pág. 281).

- **Despachador:** Envía y recibe mensajes SNMP, determina la versión de cada mensaje recibido, entrega los mensajes al subsistema de procesamiento de mensajes.
- **Subsistema de Procesado de Mensaje:** Se encarga de preparar los mensajes para ser enviados y extraer datos de los recibidos.
- **Subsistema de Seguridad:** Se encarga de la Autenticación, cifrado y descifrado de los mensajes. La autenticación puede usar tanto comunidades (SNMPv1 y SNMPv2) como USM de SNMPv3. La autenticación basada en USM emplea algoritmos MD5<sup>41</sup> y SHA<sup>42</sup> sin enviar una contraseña en texto plano, el servicio de privacidad usa el algoritmo DES para cifrar y descifrar los mensajes SNMP.

---

<sup>40</sup> USM: User-Based Security Model (Modelo de seguridad basada en usuario)

<sup>41</sup> MD5: Message-Digest Algorithm 5 (Algoritmo de resumen del mensaje 5)

<sup>42</sup> SHA: Secure Hash Algorithm (Algoritmo de hash seguro)



- Subsistema de Control de Acceso: Determina el usuario y operaciones a las cuales se les permite el acceso a los objetos administrados de la MIB (Douglas & Schmidt, 2005).

#### 1.3.3.14 Operaciones SNMP

La PDU es el formato de mensaje que gestores y agentes utilizan para enviar y recibir información, el contenido de la PDU<sup>43</sup> depende de la operación SNMP que se realice, las cuáles pueden ser:

- Get: Solicita el valor de una variable específica mediante su OID.
- Get-Next: Solicita el valor de una variable sin conocer su nombre exacto, útil para búsquedas secuenciales dentro de una rama MIB.
- Get-Bulk (SNMPv2 y SNMPv3): Solicita grandes bloques de datos, como por ejemplo varias filas de un subárbol MIB.
- Set: Almacena y altera el valor de una variable específica.
- Get-Response: Respuesta por parte del agente a las operaciones get-request, get-next-request o set-request.
- Trap: Mensaje no solicitado enviado por un agente a un gestor cuando ocurre un evento.
- Notification (SNMPv2 and SNMPv3): En un esfuerzo para estandarizar el formato de la PDU de SNMPv1-traps.
- Inform (SNMPv2 y SNMPv3): Proporciona un mecanismo que permite la comunicación entre gestores. Esta operación puede ser útil cuando surge la necesidad de más de un gestor en la red.

---

<sup>43</sup> PDU: Protocol Data Unit (Unidad de datos de protocolo)

- Report (SNMPv2 y SNMPv3): Se define en SNMPv2 pero no se ha implementado. Ahora es parte de SNMPv3 y tiene la intención de permitir que los motores de SNMP se comuniquen entre sí (sobre todo para reportar problemas con procesamiento de los mensajes SNMP). (Douglas & Schmidt, 2005, pág. 35)

## **1.4 SISTEMA DE MONITOREO DE RED**

### **1.4.1 INTRODUCCIÓN**

Las redes de computadoras se vuelven cada vez más complejas albergando un mayor número de equipos y servicios, por ello la exigencia en su nivel de disponibilidad y operación es cada vez más demandante. El monitoreo de redes es una solución ampliamente utilizada por administradores de red, es una herramienta compuesta por software y hardware que permite tener un mejor conocimiento del funcionamiento de los equipos y el tráfico de información que soportan, alertando por medio de mensajes al correo electrónico sobre cualquier acontecimiento no esperado en la infraestructura de red.

### **1.4.2 COMPARATIVA DE SOFTWARE DE MONITOREO**

Existe un gran número de herramientas para el monitoreo de una red. Las hay tanto comerciales como basadas en software libre, cada una con características propias que realzan su funcionalidad como se muestra en la tabla 5.

El sistema de monitorización debe cumplir principalmente con los siguientes requerimientos:

- Del tipo Software libre.
- Ser escalable.
- Representación de datos, alarmas y gráficos para su estudio.
- Manejo de agentes de monitoreo y el protocolo SNMP.

- Mostrar la topología de red.
- Envío de notificaciones al correo electrónico.

Se optó como herramienta, NAGIOS, por ser el primer sistema libre de monitoreo en aparecer en el mercado, su núcleo constituye la base del funcionamiento de nuevos software de monitoreo. NAGIOS puede migrar o complementarse con otros sistemas como ICINGA, CENTREON, PANDORA o LIVESTATUS con la finalidad de mejorar características propias, como frontales web más completos y vistosos o maneras de almacenar y procesar la información. Por ser el primer sistema libre de monitoreo y estar más tiempo en el mercado, cuenta con mucha documentación accesible no solo de la página oficial, si no, también de distintas comunidades como NAGIOS CHILE o NAGIOS ESPAÑA, NAGIOS permite el manejo de reportes, generación de gráficas y envío de notificaciones al correo electrónico, hace uso del protocolo SNMP para obtener información de los equipos en la red, también utiliza agentes externos para monitorear equipos Windows o LINUX.

Tabla 5. Comparativa de Sistemas de Monitoreo  
Fuente: (Nagios Core, 2012)

SISTEMA	REPORTES	AGRUPACIÓN LÓGICA	AUTO DESCUBRIMIENTO	AGENTES	SNMP	PLUGINS	ALERTAS	MONITOREO DISTRIBUIDO	PLATAFORMA	BASE DE DATOS	LICENCIA	TOPOLOGÍA
CACTI	SI	SI	NO	SI	SI	SI	SI	SI	PHP	RRDTOOL MYSQL	GPL	SI
COLLECTD	NO	NO	NO	SI	SI	SI	SI	SI	C	RRDTOOL	GPL	NO
FREENATS	SI	SI	SI	NO	NO	SI	SI	NO	PHP	MYSQL	GPL	NO
GANGLIA	NO	SI	NO	NO	SI	SI	NO	SI	C. PHP	RRDTOOL	BSD	SI
ICINGA	SI	SI	NO	SI	SI	SI	SI	SI	C	POSTGRES QL ORACLE	GPL	SI
MUNIN	NO	NO	SI	NO	SI	SI	SI	NO	PERL	RRDTOOL	GPL	SI
NAGIOS	SI	SI	NO	SI	SI	SI	SI	SI	PHP	MYSQL POSTGRES QL	GPL	SI
PRTG NETWORK MONITOR	SI	SI	SI	SI	SI	SI	SI	SI	-----	SQL	COMERCIA L	SI
WHATSUP GOLD	SI	SI	SI	SI	SI	SI	SI	SI	-----	SQL	COMERCIA L	SI
ZABBIX	SI	SI	NO	SI	SI	SI	SI	SI	C. PHP	ORACLE. MYSQL POSTGRES QL	GPL	SI

### 1.4.3 NAGIOS CORE

Es un sistema de código abierto escrito en C, utilizado por los administradores de red para tener un mejor conocimiento de cómo está estructurada la red, el tráfico que soporta y el funcionamiento de los equipos que la conforman, alertando si se produce algún cambio no esperado en los equipos o servicios entregados (Nagios Core, 2012).

Las características de NAGIOS CORE son:

- Supervisión de los servicios de red (SMTP<sup>44</sup>, POP3<sup>45</sup>, HTTP<sup>46</sup>, ICMP<sup>47</sup>, etc.)
- Seguimiento de recursos de host (carga del procesador, uso de disco, memoria, etc.)
- Diseño simple de plugin que permite a los usuarios desarrollar comprobaciones de servicios, usando BASH, C++, PERL, RUBY, PYTHON, PHP, C#.
- Chequeo de servicios paralizados.
- Capacidad para definir jerarquías de red, especificando dependencias de equipos, lo que permite la detección y distinción entre hosts que están abajo y los que son inalcanzables.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos a través del correo electrónico.
- Visualización del estado de la red en tiempo real a través de la interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados y visualización del listado de notificaciones enviadas, historial de problemas y archivos de registros (Cayuqueo, 2012).
- NAGIOS CORE incorpora un visor de reportes, en el cual se puede ver el histórico de actividad, performance de servicios y un visor de diagramas de red con el estado

---

<sup>44</sup> SMTP: Simple Mail Transfer Protocol (Protocolo para la transferencia simple de correo electrónico)

<sup>45</sup> POP3: Post Office Protocol (Protocolo de oficina de correo)

<sup>46</sup> HTTP: Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto)

<sup>47</sup> ICMP: Internet Control Message Protocol (Protocolo de mensajes de control de internet)

actual de cada equipo. NAGIOS está constituido por un núcleo que construye la interfaz de usuario y por plugin con los cuales se encarga de recopilar información bajo configuración, los mismos pueden estar programados en diversos lenguajes como C, C++, PYTHON, PERL, PHP, JAVA y BASH ya que NAGIOS es independiente del lenguaje en el cual se desarrolle el plugin y solo procesa los datos recibidos de este, para la posterior elaboración y envío de notificaciones a los encargados de la administración del sistema (Nagios Core, 2012).

#### **1.4.4 LICENCIAS**

NAGIOS CORE está disponible bajo los términos de la Licencia Pública General GNU versión 2, publicada por la Free Software Foundation, esto otorga permisos legales para copiar, distribuir y modificar NAGIOS (Nagios Core, 2012).

#### **1.4.5 OBJETIVOS Y NECESIDADES**

NAGIOS CORE permite conocer el estado de diferentes servicios brindados por equipos como servidores o hosts con distintos sistemas operativos, routers y switches, obteniendo información de los mismos como su estado en la red, servicios y procesos corriendo, carga de CPU, carga de memoria física, carga de memoria virtual, espacio en disco e interfaces de red activas.

Es posible conocer los estados y datos de estos diferentes equipos para una posterior elaboración de reportes, por medio del testeo de paquetes de red, o haciendo uso de diferentes funciones que provee el protocolo SNMP que permite gestionar y supervisar datos de diferentes elementos y componentes de la red, con lo cual se puede concluir si la infraestructura de red lleva a cabo eficazmente su finalidad y utiliza eficientemente los recursos (Nagios Core, 2012).

## 1.4.6 DEPENDENCIAS

“Para una correcta instalación de NAGIOS con todas sus características es necesario instalar ciertos paquetes de software en el sistema, la instalación puede variar según la distribución de LINUX que se elija” (Cayuqueo, 2012). La tabla 5 muestra las dependencias utilizadas por NAGIOS.

Tabla 6. Dependencias de software utilizadas por NAGIOS  
Fuente: Cayu. Monitoreo de red con NAGIOS, recuperado de:  
<http://wiki.cayu.com.ar/doku.php?id=manuales:nagios>

PAQUETE	DESCRIPCIÓN	SITIO WEB
PERL	Interprete para el lenguaje de script Perl	<a href="http://www.perl.org">http://www.perl.org</a>
NET::SNMP	Módulo de Perl para consultas SNMP	<a href="http://search.cpan.org/dist/Net-SNMP">http://search.cpan.org/dist/Net-SNMP</a>
RRDTOOL	Utilitario para generación de gráficas de red y además su módulo de integración con el lenguaje Perl	<a href="http://oss.oetiker.ch/rrdtool">http://oss.oetiker.ch/rrdtool</a>
ZLIB	Librería de compresión utilizada por las utilidades graficas	<a href="http://www.gzip.org/zlib/">http://www.gzip.org/zlib/</a>
LIBJPEG	Librería para exportación jpg	<a href="http://www.ijg.org/">http://www.ijg.org/</a>
LIBPNG	Librería para exportación png	<a href="http://www.libpng.org/pub/png/">http://www.libpng.org/pub/png/</a>
APACHE 2	Servidor Web	<a href="http://httpd.apache.org/">http://httpd.apache.org/</a>
PHP	Interprete de lenguaje de script	<a href="http://www.php.net">http://www.php.net</a>
MYSQL	Sistema de base de datos	<a href="http://www.mysql.com">http://www.mysql.com</a>
POSTFIX	SMTP para enviar mail	<a href="http://www.postfix.org/">http://www.postfix.org/</a>
GD	Librería para generación de formatos gráficos	<a href="http://www.libgd.org/">http://www.libgd.org/</a>
PNP4NAGIOS	Aditivo para la generación de gráficos estadísticos y reportes visuales	<a href="http://www.pnp4nagios.org/">http://www.pnp4nagios.org/</a>
NDO	Agregado para articular NAGIOS con MYSQL	<a href="http://www.nagios.org">http://www.nagios.org</a>
PLUGINS	Plugins de chequeo estándar de NAGIOS	<a href="http://www.nagios.org">http://www.nagios.org</a>
SNMP PLUGINS	Plugins para la integración de chequeos SNMP de NAGIOS	<a href="http://nagios.manubulon.com/">http://nagios.manubulon.com/</a>
NAGIOS	Sistema de monitoreo	<a href="http://www.nagios.org">http://www.nagios.org</a>
NAGIOSQL	Herramienta visual de configuración de NAGIOS vía Web	<a href="http://www.nagiosql.org/">http://www.nagiosql.org/</a>

Puntos básicos previos a la instalación:

- **PATH:** Esta es la ruta de instalación, por defecto es `/usr/local/nagios`.
- **Usuario:** Se crea con `adduser` y se especifica la dirección de NAGIOS como su directorio `home` de inicio, usualmente llamado NAGIOS y debe estar dentro del grupo NAGIOS.
- **Grupo:** Este grupo tendrá permisos sobre todos los ficheros y directorios de NAGIOS, por defecto lleva el mismo nombre y puede crearse con `groupadd`.

- URL: NAGIOS utiliza una interfaz web para ejecutarse, esta URL determina cuál va a ser el directorio virtual que debe usar para instalarse. Por defecto /nagios, es decir, las peticiones irán dirigidas a `http://host/nagios` (Nagios, 2012).

#### 1.4.7 ESTRUCTURA DE ARCHIVOS

Después de compilar e instalar el paquete NAGIOS, se crea la ruta de instalación del sistema `/usr/local/nagios`, la cual tiene la siguiente nomenclatura de directorios:

- bin: Almacenan los binarios ejecutables, dentro de este directorio se encuentran los ejecutable principales, como el binario-NAGIOS que se ejecuta como proceso en segundo plano, el objeto `ndomod.o` que es el módulo que se encarga de traducir las estadísticas de NAGIOS en formato de consultas MySQL y `ndo2db` que es el proceso que se conecta con la base de datos para posteriormente ejecutar consultas.
- etc: Este directorio guarda la configuración de NAGIOS, sus componentes, hosts/servicios a chequear, comandos de ejecución, contactos de notificación e intervalos de chequeos.
- libexec: Contiene los plugin (archivos ejecutables) que efectúan los chequeos SNMP, sbin: Dentro de este directorio se almacenan los ejecutables cgi para la visualización web.
- share: Este directorio contiene iconos, imágenes, logos y aditivos que se necesitan para la visualización web.
- var: Guarda los datos de ejecución del monitoreo, estado de servicios, hosts y logs, almacena los datos internos de NAGIOS, estadísticas de los chequeos e información de ejecución actual (Nagios, 2012).



## 1.4.8 ARCHIVOS DE CONFIGURACIÓN

Es sistema de monitoreo está compuesto por distintos directorios que albergan la configuración e información específica necesaria para el correcto funcionamiento del sistema, a continuación se detalla el contenido de cada directorio.

### 1.4.8.1 nagios/etc

Este directorio contiene algunos de los archivos más importantes en la configuración del servidor NAGIOS, donde es posible habilitar la autenticación así como los usuarios para acceder al servicio, especificar las rutas de los directorios y archivos extras utilizados y tiempos de actualización del sistema (Cayuqueo, 2012). A continuación se describen los archivos contenidos:

- `cgi.cfg`: Permite definir la ruta del archivo de configuración principal de NAGIOS así como la configuración de los parámetros de la interfaz web, contraseñas y usuarios para acceder al servicio de monitoreo, la tabla 6 describe cada línea de configuración.

Tabla 7. Contenido del archivo `cgi.cfg` - NAGIOS CORE  
Fuente: Cayu. Monitoreo de red con NAGIOS, 2012, recuperado de:  
<http://wiki.cayu.com.ar/doku.php?id=manuales:nagios>

LÍNEA DE CONFIGURACIÓN	DESCRIPCIÓN
<code>main_config_file=/usr/local/nagios/etc/nagios.cfg</code>	Definir archivo de configuración principal de sistema
<code>physical_html_path=/usr/local/nagios/share</code>	Ruta donde se ubican los archivos a mostrar vía web
<code>url_html_path=/nagios</code>	Ruta del url a donde ubicar NAGIOS desde el navegador
<code>show_context_help=0</code>	Mostrar o no el icono de ayuda en la interfaz web
<code>use_pending_states=1</code>	Mostrar objetos pendientes de chequeo
<code>use_authentication=1</code>	Usar autenticación para acceder al sistema
<code>#default_user_name=guest</code>	Tener usuario logueado por default (no recomendado, dejar comentado)
<code>authorized_for_system_information=nagiosadmin</code>	Usuarios con acceso permitido para ver la información de objetos (separados por comas)
<code>authorized_for_configuration_information=nagiosadmin</code>	Usuarios con acceso permitido para ver la información de configuración (separados por comas)
<code>authorized_for_system_commands=nagiosadmin</code>	Usuarios con acceso permitido para la ejecución de comandos NAGIOS (separados por comas)
<code>authorized_for_all_services=nagiosadmin</code> <code>authorized_for_all_hosts=nagiosadmin</code>	Usuarios permitidos a ver información de hosts y servicios (separados por comas)
<code>authorized_for_all_service_commands=nagiosadmin</code> <code>authorized_for_all_host_commands=nagiosadmin</code>	Usuarios permitidos para ejecutar comandos sobre hosts y servicios (separados por comas)
Tasa de refresco para la interfaz web en segundos	<code>refresh_rate=90</code>

- `htpasswd.users`: Archivo que contiene todas las contraseñas encriptadas de los usuarios que se autentifican vía web.
- `nagios.cfg`: Archivo de configuración principal de NAGIOS, especifica los directorios de trabajo e incluye los archivos de configuración extra a utilizar, la tabla 7 describe cada línea de configuración.

*Tabla 8.* Contenido del archivo `nagios.cfg` - NAGIOS CORE  
Fuente: Cayu. Monitoreo de red con NAGIOS, 2012, recuperado de:  
<http://wiki.cayu.com.ar/doku.php?id=manuales:nagios>

LÍNEA DE CONFIGURACIÓN	DESCRIPCIÓN
<code>log_file</code>	Especifica el archivo de log a utilizar por NAGIOS
<code>cfg_file</code>	Especifica archivos de configuración extras a incluir en la ejecución del sistema.
<code>cfg_dir</code>	Especifica un directorio con archivos de configuración extras a incluir recursivamente en la ejecución del sistema
<code>log_archive_path</code>	Dirección donde se ubicaran los archivos de log

- `ndo2db.cfg`: Archivo de configuración del demonio que se encarga de introducir las consultas generadas por el módulo `ndomod`.
- `ndomod.cfg`: Módulo que se encarga de traducir la información de ejecución de Nagios en consultas MySQL, disponiéndolas por medio de un socket.
- `resource.cfg`: Archivo de configuración donde se definen los macros de ejecución (Cayuqueo, 2012).

#### 1.4.8.2 `nagios/etc/objects`

Este directorio contiene plantillas con información de comandos, contactos y equipos que son utilizados por NAGIOS para poder monitorear la red, la tabla 8 describe cada plantilla (Nagios Core, 2012).

*Tabla 9.* Contenido del directorio `objects` - NAGIOS CORE  
Fuente: Nagios Core – Nagios Documentation, 2012, recuperado de:  
[http://nagios.sourceforge.net/docs/3\\_0/about.html#whatis](http://nagios.sourceforge.net/docs/3_0/about.html#whatis)

PLANTILLA	DESCRIPCIÓN
<code>objects/commands.cfg</code>	Define los comandos de ejecución por default con los alias que se utilizarán.
<code>objects/contacts.cfg</code>	Define los contactos a los que se enviarán notificaciones
<code>objects/localhost.cfg</code>	Plantilla inicial para el chequeo del host local

objects/printer.cfg	Plantilla de ejemplo para el chequeo de impresoras por SNMP
objects/switch.cfg	Plantilla de ejemplo para el chequeo de switches por SNMP
objects/templates.cfg	Plantillas generales de host, contactos, y servicios
objects/timeperiods.cfg	Plantilla inicial para definir periodos de chequeos, aquí se definen los rangos de tiempo donde son válidos el envío de alertas y las verificaciones de los servicios que están funcionando
objects/windows.cfg	Plantilla de ejemplo de chequeo de equipos Windows

### 1.4.8.3 nagios/var/rw

Este directorio contiene el archivo nagios.cmd el cual realiza la comunicación de los comandos y órdenes de la interfaz web hacia el núcleo NAGIOS (Nagios Core, 2012).

## CAPITULO II

### PLANEACIÓN EN LA RED DE DATOS DE LA UNIVERSIDAD

#### TÉCNICA DEL NORTE “SITUACIÓN ACTUAL”

##### 2.1 INTRODUCCIÓN

La red de datos de la UTN<sup>48</sup> está conformada por tres capas, la capa de core ubicada en el edificio central la cual cuenta con un router Cisco 7604 como equipo de borde entregado por la empresa proveedora del servicio de internet, un firewall Asa 5520 de Cisco que permite administrar la seguridad en la red interna de la universidad y un switch Cisco 3750 que es utilizado como concentrador para la capa de distribución.

La capa de distribución dispone de dos equipos Cisco 4506-E que permiten la propagación de VLAN a la capa de acceso, uno se encuentra ubicado en el Ed. Central y el otro en la FICA<sup>49</sup>.

La capa de acceso en la FICA está compuesta por diez switches Cisco ubicados en cada laboratorio y salas de la facultad, en conjunto con los servidores de monitoreo, encuestas, ambiente educativo, DHCP y puntos de acceso inalámbricos están conectados al equipo de core de la facultad. La capa de acceso de las facultades FECYT<sup>50</sup>, FACAE<sup>51</sup>, FICAYA, SALUD, POSTGRADO, ED. FÍSICA Y LA BIBLIOTECA tienen conectividad hacia la nube de internet a través de enlaces de fibra óptica que llegan desde el equipo de core ubicado en el Ed. Central y mantienen enlaces de fibra redundantes a través del equipo de core ubicado en la FICA por medio del protocolo STP<sup>52</sup>, cabe recalcar que únicamente el equipo de core ubicado en el ED. Central tiene salida hacia la nube de internet, por lo que si

---

<sup>48</sup> UTN: Universidad Técnica del Norte.

<sup>49</sup> FICA: Facultad de Ingeniería en Ciencias Aplicadas.

<sup>50</sup> FECYT: Facultad de Educación Ciencia y Tecnología.

<sup>51</sup> FACAE: Facultad de Ciencias Administrativas y Económicas.

<sup>52</sup> STP: Spanning Tree Protocol (Protocolo de Árbol de Extensión)

se llega a tener algún problema con este equipo se perdería conexión hacia la nube de internet desde toda la red de la UTN

Se realizó la inspección a cada facultad y edificación de la UTN con la finalidad de conocer de manera general como se encuentra la infraestructura de red, identificando los rack y equipos albergados así como la ubicación de los puntos de red en las distintas localidades dentro de la universidad. La figura 13 detalla la infraestructura de red albergada en la UTN.

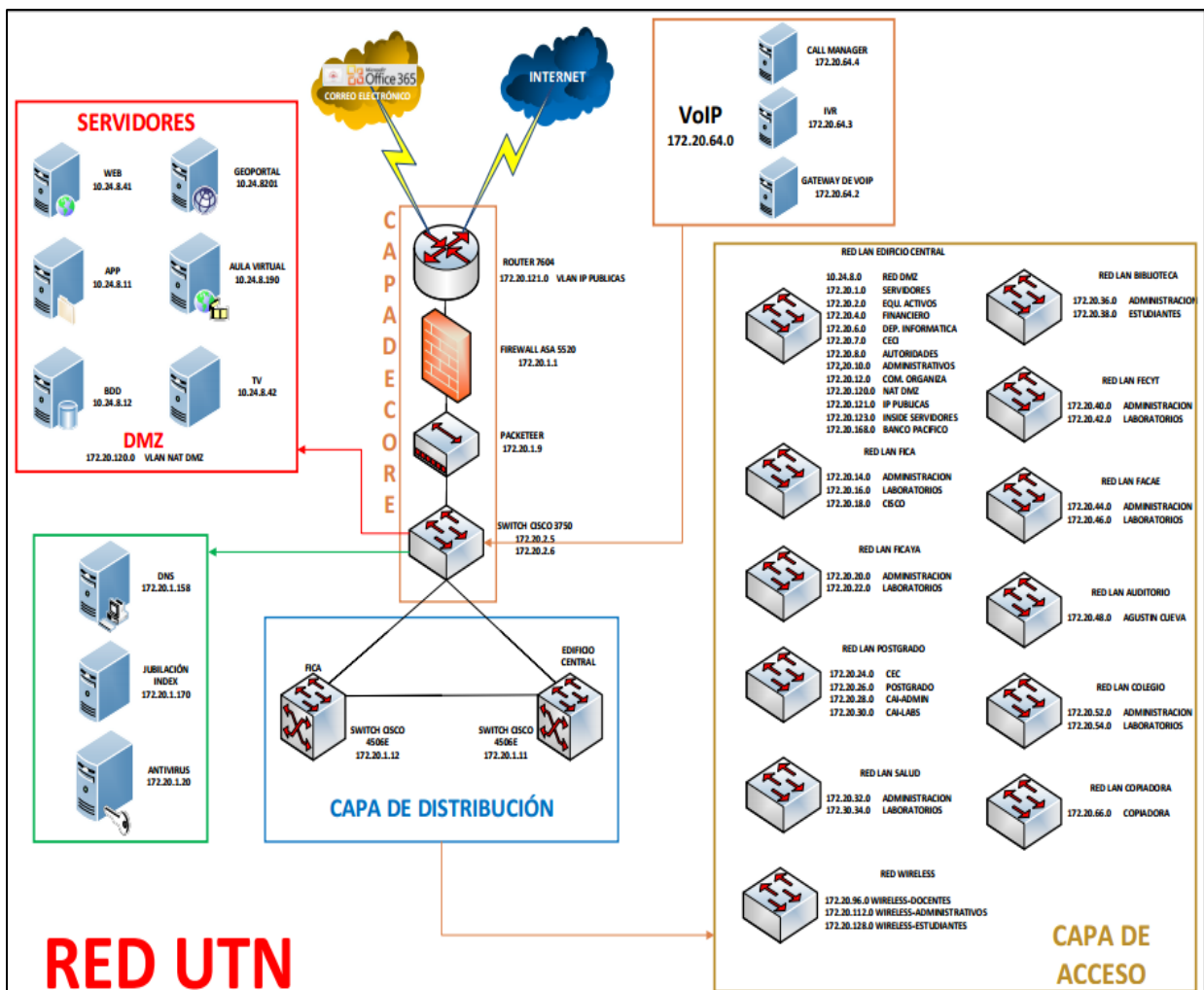


Figura 13. Topología Lógica UTN  
Fuente: Departamento de Informática-UTN

## **2.2 FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS**

### **2.2.1 INTRODUCCIÓN**

Para conocer cómo se encuentran conectados los equipos de conmutación, hosts, servidores y puntos de acceso dentro de la FICA, se identificó cada rack de telecomunicaciones así como todos los equipos comprendidos en los mismos, se realizó el mapeo del cableado estructurado para tener conocimiento de que puertos en los switches de acceso en cada laboratorio permiten la interconexión de hosts o puntos de acceso inalámbricos y cuales permiten la interconexión en cascada hacia otros switches, sean estos de acceso ubicados en otros laboratorios o directamente al switch de core de la facultad, se recopiló información acerca del uso de los laboratorios y aplicaciones instaladas necesarias para cada carrera, en este proceso se verificó que todos los equipos de conmutación dentro de la FICA son switches CISCO los cuales incorporan un agente SNMP versión I, II y III en el IOS<sup>53</sup>, basta con habilitar el agente para poder utilizar SNMP en el equipo, también se determinó que el sistema operativo utilizado en los laboratorios de la FICA es Windows 7 debido a las licencias que se manejan en la UTN<sup>54</sup>, Windows 7 incorpora un agente SNMP V2 y es necesario activarlo y configurarlo si se lo desea utilizar.

### **2.2.2 LABORATORIO DE COMPUTACIÓN I**

#### **2.2.2.1 Equipos de cómputo**

El laboratorio I, se encuentra ubicado en el segundo piso de la FICA y está provisto de equipos de cómputo que se detallan en la tabla 10.

---

<sup>53</sup> IOS: Internetwork Operating System (Sistema operativo en la red)

Tabla 10. Equipos de cómputo - Laboratorio I - FICA  
Fuente: Laboratorio I – FICA

LISTA DE EQUIPOS Y HERRAMIENTAS	MARCA	CANTIDAD	FECHA DE COMPRA	PRECIO UNIT. (USD)	ESTADO			VIDA ÚTIL (AÑOS)
					Bueno	Regular	Malo	
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE I5 DE 3.2 GHZ, TARJETA MADRE INTEL, RAM 4GB, DISCO DURO 1TB, DVD-RW, PANTALLA PLANA 18.5", MOUSE, TECLADO, PARLANTE, REGULADOR/UPS	CLON	20	14/09/2011	672.00	X			6
COMPUTADORAS PORTATILES: PROCESADOR INTEL CORE 2 DUO 2.0 GHZ, RAM 4GB, DISCO DURO 250 GB, DVD-RW, PANTALLA 15.4", MOUSE, CARGADOR DE BATERÍAS	DELL	7	23/03/2009	1,108.00	X			6

### 2.2.2.2 Equipos de telecomunicaciones

El laboratorio I alberga su propio rack de telecomunicaciones, el cual contiene los equipos de acceso que permiten la conectividad de cada equipo de cómputo. La tabla 11 detalla los equipos alojados en el rack.

Tabla 11. Equipos de telecomunicaciones - Laboratorio I - FICA  
Fuente: Laboratorio I – FICA

EQUIPOS DE TELECOMUNICACIONES	MARCA	NOMBRE	DIRECCIÓN IP	CANT. #	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
							Bueno	Regular	Malo	
RACK DE PARED DE 19"	PANDUIT	-----	-----	1	31/05/2011	373.50	X			10
PATCH PANEL DE 48 PUERTOS CAT. 6.	NEWLINK	-----	-----	1	31/05/2011	230.00	X			10
SWITCH DE 48 PUERTOS	CISCO CATALYST 2960	SW-FICA-LAB1-01	172.20.2.31	1	31/05/2011	3,399.34	X			10

### 2.2.2.3 Utilización del laboratorio y software instalado

El laboratorio I tiene distintos requerimientos de software así como distintos horarios de uso a lo largo del día, la tabla 12 detalla la utilización y los requerimientos de software del laboratorio.

Tabla 12. Utilización y software instalado - Laboratorio I – FICA  
Fuente: Laboratorio I – FICA

MATERIA	NIVEL	ESCUELA	SOFTWARE REQUERIDO PARA CLASES
COMPILADORES	7	CISIC	MICROSOFT .NET, EXPRESSION BLEND
DIBUJO MECÁNICO 1	4	CINDU	AUTOCAD
ING. DE SOFTWARE 1	7	CISIC	VIRTUAL BOX
COMPILADORES	7	CISIC	MICROSOFT .NET, EXPRESSION BLEND
TRABAJO DE GRADO 2	10	CISIC	MICROSOFT OFFICE, MSTUDIO, INTERNET
ARQUITECTURA DE SOFTWARE	8	CISIC	VIRTUAL BOX

PROGRAMACIÓN 2	3	CIERCOM	C++
ING. ECONÓMICA	5	CIME-CIERCOM	MICROSOFT EXCEL , PPT, INTERNET
BASE DE DATOS 3	6	CISIC	SQL SERVER 2008 R2
PROGRAMACIÓN 2	3	CIERCOM	C++
DIBUJO MECÁNICO 1	2	CIME	AUTOCAD-INVENTOR
OPTATIVA 1	8	CISIC	SQL SERVER 2008 R2 BIDS
BASE DE DATOS 3	6	CISIC	SQL SERVER 2008 R2
ING. DE SOFTWARE 2	7	CISIC	VIRTUAL BOX
DIBUJO MECÁNICO 1	2	CIME	AUTOCAD-INVENTOR
DIBUJO MECÁNICO 2	6	CINDU	AUTOCAD
Base de Datos 1	4	CISIC	BDD ORACLE XE Y SQL DEVELOPER
OPTATIVA 1	8	CISIC	SQL SERVER 2008 R2 BIDS

#### 2.2.2.4 Cableado estructurado

Actualmente este laboratorio cuenta con el etiquetado de los puntos de red pero no existe documentación con información del mapeo de la red, por ello se verificó la integridad del etiquetado de cada punto hacia el switch de acceso así como también su conexión hacia el switch de core de la FICA, utilizando un testeador de red. Como se muestra en la tabla 11, el switch de acceso es un equipo cisco Catalyst 2960 de 48 puertos el cual brinda conectividad a la red por medio de una conexión cruzada hacia un patch panel Newlink cat.6 de 48 puertos, la conexión cruzada desde el switch de core de la FICA llega a través del puerto 48 del patch panel A al puerto GigabitEthernet 1 del switch 1, la figura 14 detalla el mapeo de la red.



NC : NO CONECTADO		CONEX. SW CORE-FICA		
----- : NULO		SW-CORE (2º-PISO)	PATCH PANEL	
EQUIPOS		PPE -PUERTO	PPA-PUERTO	
PATCH PANEL NEWLINK CAT 6 (48 P)		18	48	
SWITCH CATALYST 2960 (48 P)		SW1		
CONEX. CRUZ. SW1- PPA.		DESTINO		
SW1-PUERTO	PUERTO	PPA-PUERTO	ETIQUETA	UBICACIÓN
1	1	1	R.LAB1 PPA-01	LAB.1
2	2	2	R.LAB1 PPA-02	LAB.1
3	3	3	R.LAB1 PPA-03	LAB.1
4	4	4	R.LAB1 PPA-04	LAB.1
5	5	5	R.LAB1 PPA-05	LAB.1
6	6	6	R.LAB1 PPA-06	LAB.1
7	7	7	R.LAB1 PPA-07	LAB.1
8	8	8	R.LAB1 PPA-08	LAB.1
9	9	9	R.LAB1 PPA-09	LAB.1
10	10	10	R.LAB1 PPA-10	LAB.1
11	11	11	R.LAB1 PPA-11	LAB.1
12	12	12	R.LAB1 PPA-12	LAB.1
13	13	13	R.LAB1 PPA-13	LAB.1
14	14	14	R.LAB1 PPA-14	LAB.1
15	15	15	R.LAB1 PPA-15	LAB.1
16	16	16	R.LAB1 PPA-16	LAB.1
17	17	17	R.LAB1 PPA-17	LAB.1
18	18	18	R.LAB1 PPA-18	LAB.1
19	19	19	R.LAB1 PPA-19	LAB.1
20	20	20	R.LAB1 PPA-20	LAB.1
21	21	21	R.LAB1 PPA-21	LAB.1
22	22	22	R.LAB1 PPA-22	LAB.1
23	23	23	R.LAB1 PPA-23	LAB.1
24	24	24	R.LAB1 PPA-24	LAB.1
25	25	25	R.LAB1 PPA-25	LAB.1
26	26	26	R.LAB1 PPA-26	LAB.1
27	27	27	R.LAB1 PPA-27	LAB.1
28	28	28	R.LAB1 PPA-28	LAB.1
29	29	29	R.LAB1 PPA-29	LAB.1
30	30	30	R.LAB1 PPA-30	LAB.1
31	31	31	R.LAB1 PPA-31	LAB.1
32	32	32	R.LAB1 PPA-32	LAB.1
33	33	33	R.LAB1 PPA-33	LAB.1
34	34	34	R.LAB1 PPA-34	LAB.1
35	35	35	R.LAB1 PPA-35	LAB.1
36	36	36	R.LAB1 PPA-36	LAB.1
37	37	37	R.LAB1 PPA-37	LAB.1
38	38	38	R.LAB1 PPA-38	LAB.1
39	39	39	R.LAB1 PPA-39	LAB.1
40	40	40	R.LAB1 PPA-40	LAB.1
41	41	41	R.LAB1 PPA-41	LAB.1
42	42	42	R.LAB1 PPA-42	LAB.1
43	43	43	R.LAB1 PPA-43	LAB.1
44	44	44	R.LAB1 PPA-44	LAB.1
45	45	45	R.LAB1 PPA-45	LAB.1
46	46	46	R.LAB1 PPA-46	LAB.1
47	47	47	R.LAB1 PPA-47	LAB.1
48 (NC)	-----			
GIGABIT 1	48			

Figura 14. Mapeo de red - Laboratorio I – FICA

Fuente: Laboratorio I – FICA

## 2.2.3 LABORATORIO DE COMPUTACIÓN II

### 2.2.3.1 Equipos de cómputo

El laboratorio II, se encuentra ubicado en el segundo piso de la FICA y está provisto de equipos de cómputo que se detallan en la tabla 13.

Tabla 13. Equipos de cómputo - Laboratorio II - FICA  
Fuente: Laboratorio II – FICA

LISTA DE EQUIPOS Y HERRAMIENTAS	MARCA	CANTIDAD	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
					Bueno	Regular	Malo	
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE 2 QUAD DE 2.4 GHZ, TARJETA MADRE INTEL, RAM 2GB, DISCO DURO 250GB, DVD-RW, PANTALLA PLANA 17", MOUSE, TECLADO, PARLANTE, REGULADOR/UPS.	CLON	20	31/10/2008	675.00	X			6
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE I5 DE 3.2 GHZ, TARJETA MADRE INTEL, RAM 4GB, DISCO DURO 1TB, DVD-RW, PANTALLA PLANA 18.5", MOUSE, TECLADO, PARLANTE, REGULADOR/UPS.	CLON	2	14/09/2011	672.00	X			6

### 2.2.3.2 Equipos de telecomunicaciones

Este laboratorio alberga su propio rack de telecomunicaciones, el cual contiene los equipos de acceso que permiten la conectividad de cada equipo de cómputo. La tabla 14 detalla los equipos alojados en el rack.

Tabla 14. Equipos de telecomunicaciones - Laboratorio II - FICA  
Fuente: Laboratorio II – FICA

EQUIPOS DE TELECOMUNICACIONES	MARCA	NOMBRE	DIRECCIÓN IP	CANT. #	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
							Bueno	Regular	Malo	
RACKS DE PARED DE 19"	PANDUIT	-----	-----	1	31/05/2011	180.00	X			10
PATCH PANEL DE 48 PUERTOS CAT. 6	NEWLINK	-----	-----	1	31/05/2011	230.00	X			10
SWITCH DE 48 PUERTOS	CISCO CATALYS T 2960	SW-FICA-LAB2-01	172.20.2.32	1	31/05/2011	3,399.34	X			10

### 2.2.3.3 Utilización del laboratorio y software instalado

El laboratorio tiene distintos requerimientos de software así como distintos horarios de uso a lo largo del día, la tabla 15 detalla la utilización y los requerimientos de software del laboratorio.

Tabla 15. Utilización y software instalado - Laboratorio II – FICA  
Fuente: Laboratorio II – FICA

MATERIA	NIVEL	ESCUELA	SOFTWARE REQUERIDO PARA CLASES
SISTEMAS MICROPROCESADOS	6	CIERCOM	PIC CCS COMPILER
BASE DE DATOS	4	CIERCOM	POSTGRESQL, OFFICE, INTERNET
PROGRAMACIÓN 1	2	CIERCOM	VISUAL STUDIO 2010, NETBEANS 7.1
ESTRUCTURA DE DATOS I	3A	CISIC	JAVA 1.6.X, NETBEANS 7.1
PRODUCCIÓN DE AUDIO Y VIDEO	2B	CISIC	ADOBE CS5
SISTEMAS MICROPROCESADOS	6	CIME	PICC - PROTEUS BASCOM

SISTEMAS MICROPROCESADOS	6	CIERCOM	PROTEUS
PROGRAMACIÓN II	2B	CISIC	JAVA 1.6.X, NETBEANS 7.1
SISTEMAS MULTIMEDIA	3B	CISIC	ADOBE CS5
SISTEMAS MICROPROCESADOS	6	CIERCOM	
BASE DE DATOS I	4	CISIC	BDD ORACLE XE Y SQL DEVELOPER
PROGRAMACIÓN IV	4	CISIC	NAVEGADORES
SISTEMAS MICROPROCESADOS	6	CIME	PICC - PROTEUS BASCOM
EMPRENDIMIENTO	5	CIME	MICROSOFT EXCEL , PPT, INTERNET
ING. ECONÓMICA	5	CIME-CIERCOM	MICROSOFT EXCEL , PPT, INTERNET
PROGRAMACIÓN 5	5	CISIC	NETBEANS 7.1 / VISUAL STUDIO .NET 2010 / POSTGRES / MYSQL / JDEVELOPER 11G
PRODUCCIÓN DE AUDIO Y VIDEO	2	CISIC	ADOBE CS5
PROGRAMACIÓN 2	3	CIERCOM	C++
GRAFICACION Y ANIMACIÓN	2	CISIC	GIMP, 2 INKSCAPE, BLENDER
ESTRUCTURA DE DATOS I	3A	CISIC	NETBEANS 7.1.1
PROGRAMACIÓN 5	5A	CISIC	POSTGRES,MYSQL,NETBEANS 7.1.1,VISUAL STUDIO,ECLIPSE,MATLAB

### 2.2.3.4 Cableado estructurado

Actualmente este laboratorio cuenta con el etiquetado de los puntos de red pero no existe documentación con información del mapeo de la red, por ello se verificó la integridad del etiquetado de cada punto hacia el switch de acceso así como también su conexión hacia el switch de core de la FICA, utilizando un testeador de red, el switch de acceso es un equipo cisco Catalyst 2960 de 48 puertos el cual brinda conectividad a la red por medio de una conexión cruzada hacia un patch panel Newlink cat.6 de 48 puertos. La conexión cruzada desde el switch de core de la FICA llega a través del puerto 48 del patch panel A al puerto GigabitEthernet 1 del switch 1, la figura 15 detalla el mapeo de la red.

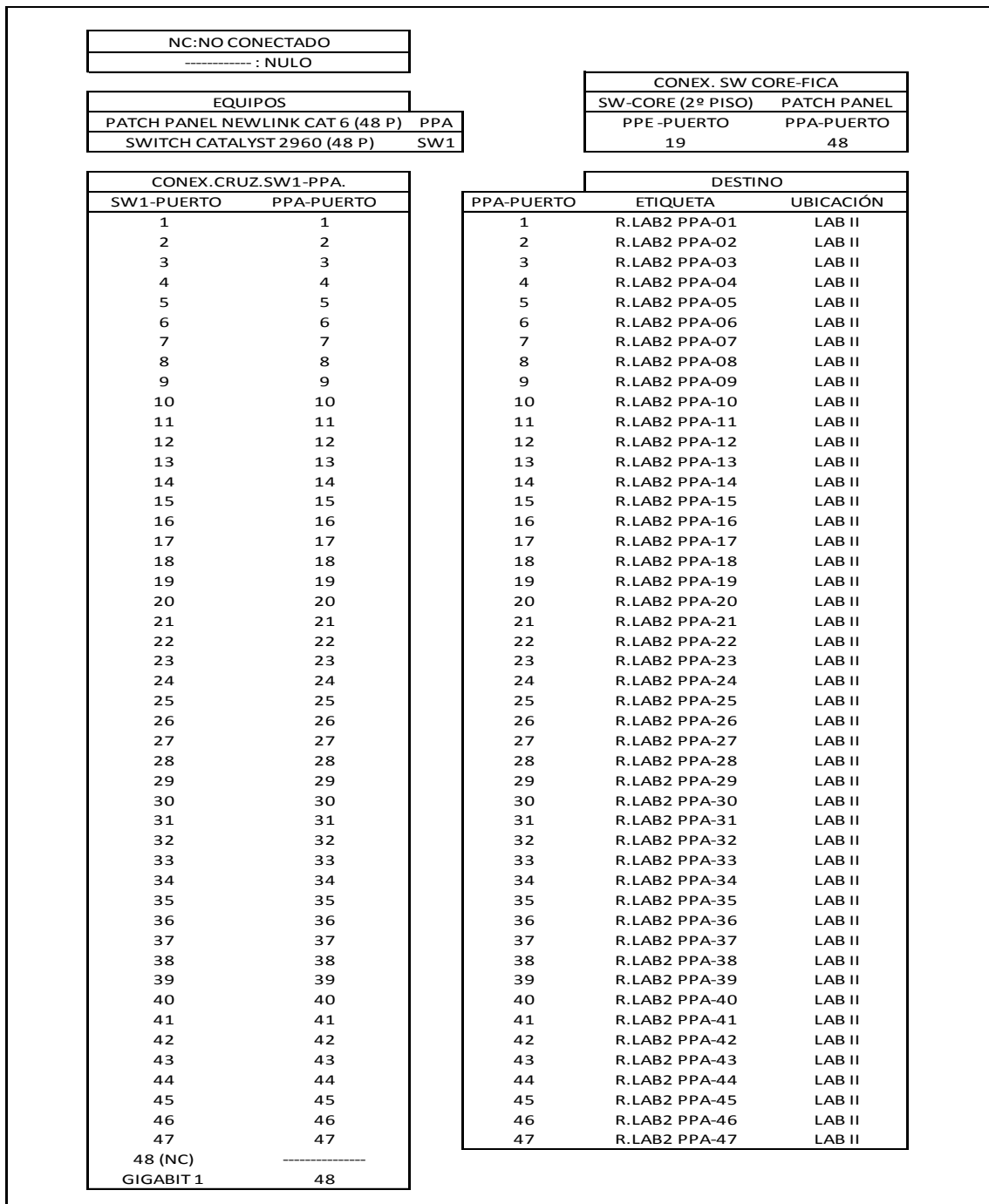


Figura 15. Mapeo de red - Laboratorio II – FICA  
 Fuente: Laboratorio II – FICA

## 2.2.4 LABORATORIO DE COMPUTACIÓN III Y LABORATORIO DE COMPUTACIÓN V

El Laboratorio de computación III alberga su propio rack de telecomunicaciones el cual contiene los switches de acceso que permiten la conectividad de los equipos de cómputo del mismo laboratorio como a los equipos del laboratorio V.

### 2.2.4.1 Equipos de cómputo

El laboratorio III y el laboratorio V, se encuentran ubicados en el segundo piso de la FICA y están provistos de equipos de cómputo que se detallan en la tabla 16 y 17 respectivamente.

Tabla 16. Equipos de cómputo - Laboratorio III – FICA  
Fuente: Laboratorio III – FICA

LISTA DE EQUIPOS Y HERRAMIENTAS	MARCA	CANTIDAD	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
					Bueno	Regular	Malo	
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE 2 QUAD DE 2.4GHZ , TARJETA MADRE INTEL, RAM 2GB, DISCO DURO 250GB, DVD-RW, PANTALLA PLANA 17", MOUSE, TECLADO, PARLANTES, REGULADOR/UPS	CLON	20	31/10/2008	675.00	X			6

Tabla 17. Equipos de cómputo - Laboratorio V – FICA  
Fuente: Laboratorio V – FICA

LISTA DE EQUIPOS Y HERRAMIENTAS	MARCA	CANTIDAD	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
					Bueno	Regular	Malo	
COMPUTADORAS IMAC: PROCESADOR INTEL CORE 2 DUO 2.66 GHZ, RAM 2GB, DISCO DURO 320 GB, DVD-RW, PANTALLA 21", MOUSE, TECLADO	APPLE	10	22/12/2008	1,568.67	x			7

### 2.2.4.2 Equipos de telecomunicaciones

El laboratorio de computación III alberga un rack de telecomunicaciones, la tabla 81 describe los equipos contenidos. El laboratorio V no alberga ningún rack de telecomunicaciones y utiliza los equipos de acceso alojados en el laboratorio III para tener conectividad en la red.

Tabla 18. Equipos de telecomunicaciones - Laboratorio III - FICA  
Fuente: Laboratorio III - FICA

EQUIPOS DE TELECOMUNICACIONES	MARCA	NOMBRE	DIRECCIÓN IP	CANT. #	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
							Bueno	Regular	Malo	
RACK DE PARED DE 19"	PANDUIT	-----	-----	1	31/05/2011	373.50	X			10
PATCH PANEL DE 24 PUERTOS CAT. 6	NEWLINK	-----	-----	3	31/05/2011	147.00	X			10
SWITCH DE 48 PUERTOS	CISCO CATALYST 2960	SW-FICA-LAB3-01	172.20.2.33	1	31/05/2011	3,399.34	X			10
SWITCH DE 24 PUERTOS	CISCO CATALYST 2960	SW-FICA-LAB3-02	172.20.2.34	1	31/05/2011	1,800.00	X			10

### 2.2.4.3 Utilización de los laboratorios y software instalado

Los laboratorios tienen distintos requerimientos de software así como distintos horarios de uso a lo largo del día, la tabla 19 y 20 detalla la utilización y los requerimientos de software de cada laboratorio.

Tabla 19. Utilización y software instalado - Laboratorio III - FICA  
Fuente: Laboratorio III – FICA

MATERIA	NIVEL	ESCUELA	SOFTWARE REQUERIDO PARA CLASES
SISTEMAS OPERATIVOS	3	CIERCOM	WINDOWS, VIRTUAL BOX, INTERNET, LINUX, OSX
PROGRAMACIÓN 1	2	CIME	NETBEANS 7.01-C#
PROGRAMACIÓN 2	2	CISIC	NETBEANS 7.1
MATEMÁTICAS DISCRETAS	5	CISIC	VISUAL STUDIO 2010, NETBEANS 7.1
ESTRUCTURA DE DATOS 1	3	CISIC	VISUAL STUDIO 2010, NETBEANS 7.1
EMPRENDIMIENTO	5	CIME	MICROSOFT EXCEL , PPT, INTERNET
BASE DE DATOS	4	CIERCOM	POSTGRESQL, OFFICE, INTERNET
PROGRAMACIÓN 1	2	CIERCOM	VISUAL STUDIO 2010, NETBEANS 7.1
ESTRUCTURA DE DATOS 1	3	CISIC	VISUAL STUDIO 2010, NETBEANS 7.1
ESTRUCTURA DE DATOS 2	4	CISIC	VISUAL STUDIO 2010, NETBEANS 7.1
TESIS	9	CISIC	INTERNET-NAVEGADORES
PROGRAMACIÓN 3	3	CISIC	NETBEANS .NET/VISUAL STUDIO
PROGRAMACIÓN 2	3	CIERCOM	VISUAL STUDIO 2010, NETBEANS 7.1
ANÁLISIS NUMÉRICO	3	CISIC	VISUAL STUDIO 2010, NETBEANS 7.1
MATEMÁTICAS DISCRETAS	5	CISIC	VISUAL STUDIO 2010, NETBEANS 7.1
ING. DE SOFTWARE 1	6	CISIC	VIRTUAL BOX
PROGRAMACIÓN 2	3	CIERCOM	VISUAL STUDIO 2010, NETBEANS 7.1
PROGRAMACIÓN 1	4	CISIC	NETBEANS .NET
ANÁLISIS NUMÉRICO	3	CISIC	VISUAL STUDIO 2010, NETBEANS 7.1
PROGRAMACIÓN 4	4	CISIC	NAVEGADORES
PROGRAMACIÓN 3	3	CISIC	NETBEANS 7.01-C#
PROGRAMACIÓN 2	3	CIERCOM	VISUAL STUDIO 2010, NETBEANS 7.1
COSTOS	4	CISIC	MICROSOFT EXCEL , PPT, INTERNET
COSTOS	5	CIERCOM	MICROSOFT EXCEL , PPT, INTERNET
PROGRAMACIÓN 1	7	CISIC	NAVEGADORES, INTERNET, SIMFONY, SERVIDOR WEB
PROGRAMACIÓN 4	4	CISIC	NAVEGADORES
OPTATIVA 2	8	CISIC	.NET 201

Tabla 20. Utilización y software instalado - Laboratorio V – FICA  
Fuente: Laboratorio V – FICA

MATERIA	NIVEL	ESCUELA	SOFTWARE REQUERIDO PARA CLASES
MULTIMEDIA	5	CIERCOM	WINDOWS, VIRTUAL BOX, INTERNET, LINUX, OSX
TRABAJO DE GRADO 2	10	CISIC	MICROSOFT OFFICE, M STUDIO, INTERNET
MULTIMEDIA	5	CIERCOM	WINDOWS, VIRTUAL BOX, INTERNET, LINUX, OSX
SISTEMAS OPERATIVOS	3	CIERCOM	WINDOWS, VIRTUAL BOX, INTERNET, LINUX, OSX
ARQUITECTURA DE SOFTWARE	8	CISIC	VIRTUAL BOX
SISTEMAS MULTIMEDIA	3B	CISIC	ADOBE CS5
ING. DE SOFTWARE 1	6	CISIC	VIRTUAL BOX

### 2.2.4.4 Cableado estructurado

Actualmente el laboratorio III como el laboratorio V de computación cuentan con el etiquetado de los puntos de red pero no existe documentación con información del mapeo de la red, por ello se verificó la integridad del etiquetado de cada punto hacia el switch de acceso así como también su conexión hacia el switch de core de la FICA, utilizando un testeador de red, el laboratorio III utiliza como equipo de acceso un switch cisco Catalyst 2960 de 48

puertos para dar conectividad a la red por medio de una conexión cruzada hacia dos patch panel Newlink cat.6 de 24 puertos mientras que el switch cisco Catalyst 2960 de 24 puertos es utilizado para brindar conectividad al laboratorio V, a través de una conexión cruzada con un patch panel Newlink cat.6 de 24 puertos. La conexión cruzada desde el switch de core de la FICA llega a través del puerto 24 del patch panel B al puerto GigabitEthernet 1 del switch 1, mientras que la conexión en cascada hacia el laboratorio V va desde el puerto GigabitEthernet 2 del switch 1 al puerto GigabitEthernet 1 del switch 2, la figura 16 y 17 detalla el mapeo de la red.

CONEX. CRUZ. SW2-PP.		DESTINO		
SW2-PUERTO	PP-PUERTO	PP-PUERTO	DEST. ETIQUETA	UBICACIÓN
1	PPC-1	PPC-1	R.LAB3 PPC-01	LAB. V
2	PPC-2	PPC-2	R.LAB3 PPC-02	LAB. V
3	PPC-3	PPC-3	R.LAB3 PPC-03	LAB. V
4	PPC-4	PPC-4	R.LAB3 PPC-04	LAB. V
5	PPC-5	PPC-5	R.LAB3 PPC-05	LAB. V
6	PPC-6	PPC-6	R.LAB3 PPC-06	LAB. V
7	PPC-7	PPC-7	R.LAB3 PPC-07	LAB. V
8	PPC-8	PPC-8	R.LAB3 PPC-08	LAB. V
9	PPC-9	PPC-9	R.LAB3 PPC-09	LAB. V
10	PPC-10	PPC-10	R.LAB3 PPC-10	LAB. V
11	PPC-11	PPC-11	R.LAB3 PPC-11	LAB. V
12	PPC-12	PPC-12	R.LAB3 PPC-12	LAB. V
13	PPC-13	PPC-13	R.LAB3 PPC-13	LAB. V
14	PPC-14	PPC-14	R.LAB3 PPC-14	LAB. V
15	PPC-15	PPC-15	R.LAB3 PPC-15	LAB. V
16	PPC-16	PPC-16	R.LAB3 PPC-16	LAB. V
17	PPC-17	PPC-17	R.LAB3 PPC-17	LAB. V
18	PPC-18	PPC-18	R.LAB3 PPC-18	LAB. V
19	PPC-19	PPC-19	R.LAB3 PPC-19	LAB. V
20	PPC-20	PPC-20	R.LAB3 PPC-20	LAB. V
21	PPC-21	PPC-21	R.LAB3 PPC-21	LAB. V
22	PPC-22	PPC-22	R.LAB3 PPC-22	LAB. V
23	PPC-23	PPC-23	R.LAB3 PPC-23	LAB. V
24 (NC)	PPC-24 (NC)	PPC-24 (NC)	-----	-----
GIGABIT 1	SW1-GIGABIT 2			

Figura 16. Mapeo de red - Laboratorio V – FICA  
Fuente: Laboratorio V – FICA

NC: NO CONECTADO		
----- : NULO		
EQUIPOS		
PATCH PANEL NEWLINK CAT 6 (24 P)	PPA	
SWITCH CATALYST 2960 (48 P)	SW1	
PATCH PANEL NEWLINK CAT 6 (24 P)	PPB	
SWITCH CATALYST 2960 (24 P)	SW2	
PATCH PANEL NEWLINK CAT 6 (24 P)	PPC	
CONEX. SW CORE-FICA		
SW - CORE(2ºPISO)	PATCH PANEL	
PPE -PUERTO	PPB-PUERTO	
20	24	
CONEX. CRUZ. SW1-PP.		
SW1-PUERTO	PP-PUERTO	
1	PPA-1	
2	PPA-2	
3	PPA-3	
4	PPA-4	
5	PPA-5	
6	PPA-6	
7	PPA-7	
8	PPA-8	
9	PPA-9	
10	PPA-10	
11	PPA-11	
12	PPA-12	
13	PPA-13	
14	PPA-14	
15	PPA-15	
16	PPA-16	
17	PPA-17	
18	PPA-18	
19	PPA-19	
20	PPA-20	
21	PPA-21	
22	PPA-22	
23	PPA-23	
24	PPA-24	
25	PPB-1	
26	PPB-2	
27	PPB-3	
28	PPB-4	
29	PPB-5	
30	PPB-6	
31	PPB-7	
32	PPB-8	
33	PPB-9	
34	PPB-10	
35	PPB-11	
36	PPB-12	
37	PPB-13	
38	PPB-14	
39	PPB-15	
40	PPB-16	
41	PPB-17	
42	PPB-18	
43	PPB-19	
44 (NC)	PPB-20 (NC)	
45 (NC)	PPB-21 (NC)	
46 (NC)	PPB-22 (NC)	
47 (NC)	PPB-23 (NC)	
48 (NC)	-----	
GIGABIT 1	PPB-24	
GIGABIT 2	SW2-GIGABIT 1	
DESTINO		
PP-PUERTO	ETIQUETA	UBICACIÓN
PPA-1	R.LAB3 PPA-01	LAB .III
PPA-2	R.LAB3 PPA-02	LAB .III
PPA-3	R.LAB3 PPA-03	LAB .III
PPA-4	R.LAB3 PPA-04	LAB .III
PPA-5	R.LAB3 PPA-05	LAB .III
PPA-6	R.LAB3 PPA-06	LAB .III
PPA-7	R.LAB3 PPA-07	LAB .III
PPA-8	R.LAB3 PPA-08	LAB .III
PPA-9	R.LAB3 PPA-09	LAB .III
PPA-10	R.LAB3 PPA-10	LAB .III
PPA-11	R.LAB3 PPA-11	LAB .III
PPA-12	R.LAB3 PPA-12	LAB .III
PPA-13	R.LAB3 PPA-13	LAB .III
PPA-14	R.LAB3 PPA-14	LAB .III
PPA-15	R.LAB3 PPA-15	LAB .III
PPA-16	R.LAB3 PPA-16	LAB .III
PPA-17	R.LAB3 PPA-17	LAB .III
PPA-18	R.LAB3 PPA-18	LAB .III
PPA-19	R.LAB3 PPA-19	LAB .III
PPA-20	R.LAB3 PPA-20	LAB .III
PPA-21	R.LAB3 PPA-21	LAB .III
PPA-22	R.LAB3 PPA-22	LAB .III
PPA-23	R.LAB3 PPA-23	LAB .III
PPA-24	R.LAB3 PPA-24	LAB .III
PPB-1	R.LAB3 PPB-1	LAB .III
PPB-2	R.LAB3 PPB-2	LAB .III
PPB-3	R.LAB3 PPB-3	LAB .III
PPB-4	R.LAB3 PPB-4	LAB .III
PPB-5	R.LAB3 PPB-5	LAB .III
PPB-6	R.LAB3 PPB-6	LAB .III
PPB-7	R.LAB3 PPB-7	LAB .III
PPB-8	R.LAB3 PPB-8	LAB .III
PPB-9	R.LAB3 PPB-9	LAB .III
PPB-10	R.LAB3 PPB-10	LAB .III
PPB-11	R.LAB3 PPB-11	LAB .III
PPB-12	R.LAB3 PPB-12	LAB .III
PPB-13	R.LAB3 PPB-13	LAB .III
PPB-14	R.LAB3 PPB-14	LAB .III
PPB-15	R.LAB3 PPB-15	LAB .III
PPB-16	R.LAB3 PPB-16	LAB .III
PPB-17	R.LAB3 PPB-17	LAB .III
PPB-18	R.LAB3 PPB-18	LAB .III
PPB-19	R.LAB3 PPB-19	LAB .III
PPB-20 (NC)	-----	-----
PPB-21 (NC)	-----	-----
PPB-22 (NC)	-----	-----
PPB-23 (NC)	-----	-----

Figura 17. Mapeo de red - Laboratorio III – FICA  
Fuente: Laboratorio III – FICA

## 2.2.5 LABORATORIO DE COMPUTACIÓN IV

### 2.2.5.1 Equipos de cómputo

El laboratorio IV, se encuentra ubicado en el segundo piso de la FICA y está provisto de equipos de cómputo que se detallan en la tabla 21.



Tabla 21. Equipos de cómputo - Laboratorio IV– FICA  
Fuente: Laboratorio IV – FICA

LISTA DE EQUIPOS Y HERRAMIENTAS	MARCA	CANTIDAD	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
					Bueno	Regular	Malo	
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL DUAL CORE DE 3.4 GHZ , TARJETA MADRE INTEL, RAM 2GB, DISCO DURO 250GB, DVD-RW, PANTALLA PLANA 17", MOUSE, TECLADO, PARLANTES, REGULADOR/UPS	CLON	12	28/02/2007	847.00		x		7
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE 2 DUO DE 2.13 GHZ , TARJETA MADRE INTEL, RAM 2GB, DISCO DURO 500GB, DVD- RW, PANTALLA PLANA 17", MOUSE, TECLADO, REGULADOR/UPS	CLON	2	04/10/2007	739.00		x		7
COMPUTADORAS PORTATILES: PROCESADOR INTEL CORE I5 DE 267 GHZ, RAM 4GB, DISCO DURO 640 GB, DVD-RW, PANTALLA 14.5", MOUSE, CARGADOR DE BATERÍAS	HP	6	14/09/2011	905.00	x			6

### 2.2.5.2 Equipos de telecomunicaciones

Este laboratorio alberga su propio rack de telecomunicaciones, el cual contiene los equipos de acceso que permiten la conectividad de cada equipo de cómputo. La tabla 22 detalla los equipos alojados en el rack.

Tabla 22. Equipos de telecomunicaciones - Laboratorio IV – FICA  
Fuente: Laboratorio IV – FICA

EQUIPOS DE TELECOMUNICACIONES	MARCA	CANTIDAD	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
					Bueno	Regular	Malo	
RACK DE 19 " DE ANCHO - 24 UR	PANDUIT	1	31/05/2011	373.50	x			10
SWITCH DE 48 PUERTOS.	CISCO 2960	2	31/05/2011	3,399.34	x			10
PATCH PANEL DE 24 PUERTOS CAT. 6	NEWLINK	3	31/05/2011	147.00	x			10

### 2.2.5.3 Utilización de los laboratorios y software instalado

El laboratorio tiene distintos requerimientos de software así como distintos horarios de uso a lo largo del día, la tabla 23 detalla la utilización y los requerimientos de software del laboratorio.

Tabla 23. Utilización y software instalado - Laboratorio IV – FICA  
Fuente: Laboratorio IV – FICA

MATERIA	NIVEL	ESCUELA	SOFTWARE REQUERIDO PARA CLASES
REDES I	4	CISIC	PACKET TRACERT 5.3
REDES II	5	CISIC	VMWARE
NETWORKING 2	8	CIERCOM	PACKET TRACERT 5.3.3 - GNS3
TESIS	9	CIERCOM	

NETWORKING 3	9	CIERCOM	PACKET TRACERT 5.3.3 - GNS3
REDES II	4	CISIC	PACKET TRACERT 5.3
REDES I	5	CISIC	VMWARE
PROGRAMACIÓN 2	4	CISIC	NETBEANS .NET
PROGRAMACIÓN 5	5	CISIC	NETBEANS 7.1 / VISUAL STUDIO .NET 2010 / POSTGRES / MYSQL / JDEVELOPER 11G
NETWORKING 3	9	CIERCOM	PACKET TRACERT 5.3.3 - GNS3
NETWORKING 2	8	CIERCOM	PACKET TRACERT 5.3.3 - GNS3
PROGRAMACIÓN 2	3	CISIC	NETBEANS 7.1.1,VISUAL STUDIO 2010
SEGURIDAD DE REDES	9	CIERCOM	GNS 3, PACKET TRACER
PROGRAMACIÓN 2	3	CISIC	NETBEANS 7.1 / MATLAB
PROGRAMACIÓN V	5	CISIC	NETBEANS, VISUAL STUDIO, POSTGRESQL, MYSQL
PROGRAMACIÓN IV	4	CISIC	NAVEGADORES
ADMINISTRACIÓN Y	9	CIERCOM	MRTG, WHATSUP
GESTIÓN REDES			

#### 2.2.5.4 Cableado estructurado

Actualmente este laboratorio cuenta con el etiquetado de los puntos de red pero no existe documentación con información del mapeo de la red, por ello se verificó la integridad del etiquetado de cada punto hacia el switch de acceso así como también su conexión hacia el switch de core de la FICA, utilizando un testeador de red. Se utiliza como equipo de acceso un switch cisco Catalyst 2960 de 48 puertos para dar conectividad a la red por medio de una conexión cruzada hacia dos patch panel Newlink cat.6 de 24 puertos, en el rack de telecomunicaciones se encuentra también un switch cisco Catalyst 2960 de 48 puertos sin utilizar como se muestra en la tabla 18 y 19. La conexión cruzada desde el switch de core de la FICA llega a través del puerto 24 del patch panel B al puerto GigabitEthernet 1 del switch 1, mientras que la conexión en cascada hacia el switch 2 va desde el puerto GigabitEthernet 2 del switch 1 al puerto GigabitEthernet 1 del switch 2, la figura 18 y 19 detalla el mapeo de la red.

NC : NO CONECTADO	
----- : NULO	

EQUIPOS	
PATCH PANEL NEWLINK CAT 6 (24 P)	PPA
SWITCH CATALYST 2960 (48 P)	SW1
PATCH PANEL NEWLINK CAT 6 (24 P)	PPB
PATCH PANEL NEWLINK CAT 6 (24 P)	PPC
SWITCH CATALYST 2960 (48 P)	SW2

CONEX. SW CORE - FICA	
SW-CORE (2º PISO)	PATCH PANEL
PPE -PUERTO	PPB-PUERTO
21	24

CONEX. CRUZ. SW1-PP.	
SW1-PUERTO	PP-PUERTO
1	PPA-1
2	PPA-2
3	PPA-3
4	PPA-4
5	PPA-5
6	PPA-6
7	PPA-7
8	PPA-8
9	PPA-9
10	PPA-10
11	PPA-11
12	PPA-12
13	PPA-13
14	PPA-14
15	PPA-15
16	PPA-16
17	PPA-17
18	PPA-18
19	PPA-19
20	PPA-20
21	PPA-21
22	PPA-22
23	PPA-23
24	PPA-24
25	PPB-1
26	PPB-2
27	PPB-3
28	PPB-4
29	PPB-5
30	PPB-6
31	PPB-7
32	PPB-8
33	PPB-9
34	PPB-10
35	PPB-11
36	PPB-12
37	PPB-13
38	PPB-14
39	PPB-15
40	PPB-16
41	PPB-17
42	PPB-18
43	PPB-19
44 (NC)	PPB-20 (NC)
45 (NC)	PPB-21 (NC)
46 (NC)	PPB-22 (NC)
47 (NC)	PPB-23 (NC)
48 (NC)	-----
GIGABIT 1	PPB-24
GIGABIT 2	SW2-GIGABIT 1

DESTINO		
PP-PUERTO	ETIQUETA	UBICACIÓN
PPA-1	R.LAB4 PPA-01	LAB. IV
PPA-2	R.LAB4 PPA-02	LAB. IV
PPA-3	R.LAB4 PPA-03	LAB. IV
PPA-4	R.LAB4 PPA-04	LAB. IV
PPA-5	R.LAB4 PPA-05	LAB. IV
PPA-6	R.LAB4 PPA-06	LAB. IV
PPA-7	R.LAB4 PPA-07	LAB. IV
PPA-8	R.LAB4 PPA-08	LAB. IV
PPA-9	R.LAB4 PPA-09	LAB. IV
PPA-10	R.LAB4 PPA-10	LAB. IV
PPA-11	R.LAB4 PPA-11	LAB. IV
PPA-12	R.LAB4 PPA-12	LAB. IV
PPA-13	R.LAB4 PPA-13	LAB. IV
PPA-14	R.LAB4 PPA-14	LAB. IV
PPA-15	R.LAB4 PPA-15	LAB. IV
PPA-16	R.LAB4 PPA-16	LAB. IV
PPA-17	R.LAB4 PPA-17	LAB. IV
PPA-18	R.LAB4 PPA-18	LAB. IV
PPA-19	R.LAB4 PPA-19	LAB. IV
PPA-20	R.LAB4 PPA-20	LAB. IV
PPA-21	R.LAB4 PPA-21	LAB. IV
PPA-22	R.LAB4 PPA-22	LAB. IV
PPA-23	R.LAB4 PPA-23	LAB. IV
PPA-24	R.LAB4 PPA-24	LAB. IV
PPB-1	R.LAB4 PPB-1	LAB. IV
PPB-2	R.LAB4 PPB-2	LAB. IV
PPB-3	R.LAB4 PPB-3	LAB. IV
PPB-4	R.LAB4 PPB-4	LAB. IV
PPB-5	R.LAB4 PPB-5	LAB. IV
PPB-6	R.LAB4 PPB-6	LAB. IV
PPB-7	R.LAB4 PPB-7	LAB. IV
PPB-8	R.LAB4 PPB-8	LAB. IV
PPB-9	R.LAB4 PPB-9	LAB. IV
PPB-10	R.LAB4 PPB-10	LAB. IV
PPB-11	R.LAB4 PPB-11	LAB. IV
PPB-12	R.LAB4 PPB-12	LAB. IV
PPB-13	R.LAB4 PPB-13	LAB. IV
PPB-14	R.LAB4 PPB-14	LAB. IV
PPB-15	R.LAB4 PPB-15	LAB. IV
PPB-16	R.LAB4 PPB-16	LAB. IV
PPB-17	R.LAB4 PPB-17	LAB. IV
PPB-18	R.LAB4 PPB-18	LAB. IV
PPB-19	R.LAB4 PPB-19	LAB. IV
PPB-20 (NC)	-----	-----
PPB-21 (NC)	-----	-----
PPB-22 (NC)	-----	-----
PPB-23 (NC)	-----	-----

Figura 18. Mapeo de red - Lab IV – FICA  
 Fuente: Laboratorio IV – FICA

CONEX.CRUIZ.SW2-PP.		DESTINO		
SW2-PUERTO	PP-PUERTO	PP-PUERTO	ETIQUETA	UBICACIÓN
1	PPC-1	PPC-1	NO ETIQUETADO	NC
2	PPC-2	PPC-2	NO ETIQUETADO	NC
3	PPC-3	PPC-3	NO ETIQUETADO	NC
4	PPC-4	PPC-4	NO ETIQUETADO	NC
5	PPC-5	PPC-5	NO ETIQUETADO	NC
6	PPC-6	PPC-6	NO ETIQUETADO	NC
7	PPC-7	PPC-7	NO ETIQUETADO	NC
8	PPC-8	PPC-8	NO ETIQUETADO	NC
9	PPC-9	PPC-9	NO ETIQUETADO	NC
10	PPC-10	PPC-10	NO ETIQUETADO	NC
11	PPC-11	PPC-11	NO ETIQUETADO	NC
12	PPC-12	PPC-12	NO ETIQUETADO	NC
13	PPC-13	PPC-13	NO ETIQUETADO	NC
14	PPC-14	PPC-14	NO ETIQUETADO	NC
15	PPC-15	PPC-15	NO ETIQUETADO	NC
16	PPC-16	PPC-16	NO ETIQUETADO	NC
17	PPC-17	PPC-17	NO ETIQUETADO	NC
18	PPC-18	PPC-18	NO ETIQUETADO	NC
19	PPC-19	PPC-19	NO ETIQUETADO	NC
20	PPC-20	PPC-20	NO ETIQUETADO	NC
21	PPC-21	PPC-21	NO ETIQUETADO	NC
22	PPC-22	PPC-22	NO ETIQUETADO	NC
23	PPC-23	PPC-23	NO ETIQUETADO	NC
24 (NC)	PPC-24 (NC)	PPC-24 (NC)	-----	-----
25 (NC)	-----			
26 (NC)	-----			
27 (NC)	-----			
28 (NC)	-----			
29 (NC)	-----			
30 (NC)	-----			
31 (NC)	-----			
32 (NC)	-----			
33 (NC)	-----			
34 (NC)	-----			
35 (NC)	-----			
36 (NC)	-----			
37 (NC)	-----			
38 (NC)	-----			
39 (NC)	-----			
40 (NC)	-----			
41 (NC)	-----			
42 (NC)	-----			
43 (NC)	-----			
44 (NC)	-----			
45 (NC)	-----			
46 (NC)	-----			
47 (NC)	-----			
48 (NC)	-----			
GIGABIT 1	SW1-GIGABIT 2			

Figura 19. Mapeo de red - Laboratorio IV  
Fuente: Laboratorio IV - FICA

## 2.2.6 LABORATORIO DE COMPUTACIÓN VI Y LABORATORIO DE COMPUTACIÓN VII

El Laboratorio de computación VII alberga su propio rack de telecomunicaciones el cual contiene los switches de acceso que permiten la conectividad de los equipos de cómputo del mismo laboratorio como a los equipos del laboratorio VI.

### 2.2.6.1 Equipos de cómputo

El laboratorio VII y el laboratorio VI, se encuentran ubicados en el último piso de la FICA y están provistos de equipos de cómputo que se detallan en la tabla 24 y 25 respectivamente.

Tabla 24. Equipos de cómputo - Laboratorio VII – FICA  
Fuente: Laboratorio VII – FICA

LISTA DE EQUIPOS Y HERRAMIENTAS	MARCA	CANTIDAD	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
					Bueno	Regular	Malo	
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL DUAL CORE DE 3.4 GHZ , TARJETA MADRE INTEL, RAM 2GB, DISCO DURO 250GB, DVD-RW, PANTALLA PLANA 17", MOUSE, TECLADO, PARLANTE, REGULADOR/UPS	CLON	3	28/02/2007	847.00		x		7
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE 2 DUO DE 2.13 GHZ , TARJETA MADRE INTEL, RAM 2GB, DISCO DURO 500GB, DVD-RW, PANTALLA PLANA 17", MOUSE, TECLADO, PARLANTE, REGULADOR/UPS	CLON	2	22/12/2008	739.00		x		6
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE 2 DUO DE 2.65 GHZ , TARJETA MADRE INTEL, RAM 2GB, DISCO DURO 500GB, DVD-RW, PANTALLA PLANA 17", MOUSE, TECLADO, PARLANTE, REGULADOR/UPS	CLON	8	01/01/2009	650.00	x			10
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE 2 QUAD DE 2.67 GHZ , TARJETA MADRE INTEL, RAM 4GB, DISCO DURO 500GB, DVD-RW, PANTALLA PLANA 17", MOUSE, TECLADO, REGULADOR/UPS	CLON	6	2011	665.00	x			6
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE i5 DE 3.2 GHZ , TARJETA MADRE INTEL, RAM 4GB, DISCO DURO 1TB, DVD- RW, PANTALLA PLANA 22", MOUSE, TECLADO, REGULADOR/UPS	CLON	1	2011	626.00	x			6

Tabla 25. Equipos de cómputo - Laboratorio VI – FICA  
Fuente: Laboratorio VI – FICA

LISTA EQUIPOS Y HERRAMIENTAS	MARCA	CANTIDAD	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
					Bueno	Regular	Malo	
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE i5 DE 3.2 GHZ , TARJETA MADRE INTEL, RAM 4GB, DISCO DURO 1TB, DVD-RW, PANTALLA PLANA 22", MOUSE, TECLADO, PARLANTE, REGULADOR/UPS	CLON	14	2011	626.00		X		6
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE 2 QUAD DE 2.67 GHZ , TARJETA MADRE INTEL, RAM 4GB, DISCO DURO 500GB, DVD-RW, PANTALLA PLANA 17", MOUSE, TECLADO, REGULADOR/UPS	CLON	1	2011	665.00		X		6

COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL CORE i3 DE 2.93 GHZ, TARJETA MADRE INTEL, RAM 2GB, DISCO DURO 500GB, DVD-RW, PANTALLA PLANA 18.5", MOUSE, TECLADO, PARLANTES, REGULADOR/UPS	CLON	2	22/06/2010	595.00	X	6
COMPUTADORAS DE ESCRITORIO: PROCESADOR INTEL DUAL CORE DE 3.4 GHZ, TARJETA MADRE INTEL, RAM 2GB, DISCO DURO 320GB, DVD-RW, PANTALLA PLANA 18.5", MOUSE, TECLADO, REGULADOR/UPS	CLON	2	28/02/2007	847.00	X	7

### 2.2.6.2 Equipos de telecomunicaciones

Solo el laboratorio de computación VII alberga un rack de telecomunicaciones, la tabla 26 describe los equipos contenidos. El laboratorio VI no alberga ningún rack de telecomunicaciones y utiliza los equipos de acceso alojados en el laboratorio VII para tener conectividad en la red.

Tabla 26. Equipos de telecomunicaciones - Laboratorio VII – FICA  
Fuente: Laboratorio VII – FICA

EQUIPOS DE TELECOMUNICACIONES	MARCA	NOMBRE	DIRECCIÓN IP	CANT. #	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
							Bueno	Regular	Malo	
RACKS DE 19" DE ANCHO - 36UR	PANDUIT	-----	-----	1	31/05/2011	754.00	X			10
PATCH PANEL DE 24 PUERTOS CAT. 6	NEWLINK	-----	-----	4	31/05/2011	230.00	X			10
NFO-5000	QUEST	-----	-----	1	31/05/2012	60.00	X			10
SWITCH DE 48 PUERTOS	CISCO CATALYST 2960	SW-FICA- LABCISCO-01	172.20.2.37	1	31/05/2011	3,399.34	X			10
SWITCH DE 48 PUERTOS	CISCO CATALYST 2960	SW-FICA- LABCISCO-02	172.20.2.38	1	31/05/2011	3,399.34	X			10

### 2.2.6.3 Utilización de los laboratorios y software instalado

Los laboratorios tienen distintos requerimientos de software así como distintos horarios de uso a lo largo del día, la tabla 27 y 28 detalla la utilización y los requerimientos de software de cada laboratorio.

Tabla 27. Utilización y software instalado - Laboratorio VII – FICA  
Fuente: Laboratorio VII – FICA

MATERIA	NIVEL	ESCUELA	SOFTWARE REQUERIDO PARA CLASES
SISTEMAS OPERATIVOS	3	CISIC	SONY VEGAS, ADOBE PREMIER CS4, WINDVD CREATOR, ADOBE AUDITION CS5
PROGRAMACIÓN 4	4	CISIC	NAVEGADORES
MULTIMEDIA	3	CISIC	MAQUINA VIRTUAL(XP)
BASE DE DATOS 2	5	CISIC	SQL SERVER 2008 R2
SISTEMAS OPERATIVOS	3	CISIC	ADOBE CS4-AUDICION CS5-VISUAL .NET 2010-WAV EDITOR-SONY VEGAS 11-ADOBE PREMIER
BASE DE DATOS 2	5	CISIC	SQL SERVER 2008 R2
COSTOS	4	CISIC	MICROSOFT EXCEL , PPT, INTERNET
COSTOS	5	CIERCOM	MICROSOFT EXCEL , PPT, INTERNET
ESTRUCTURA DE DATOS 2	4	CISIC	VISUAL STUDIO 2010, NETBEANS 7.1
ARQUITECTURA DE COMPUTADORAS	5	CISIC	ADOBE CS4-AUDICION CS5-VISUAL .NET 2010-WAV EDITOR-SONY VEGAS 11-ADOBE PREMIER
MULTIMEDIA	3	CISIC	ADOBE CS4-AUDICION CS5-VISUAL .NET 2010-WAV EDITOR-SONY VEGAS 11-ADOBE PREMIER

Tabla 28. Utilización y software instalado - Laboratorio VI – FICA  
Fuente: Laboratorio VI – FICA

MATERIA	NIVEL	ESCUELA	SOFTWARE REQUERIDO PARA CLASES
DISEÑO MECÁNICO 2	7	CIME	INVENTOR, SIMULATION MULTIPHYSICS
DIBUJO MECÁNICO 2	3B	CIME	INVENTOR
DIBUJO MECÁNICO 2	3A	CIME	INVENTOR
PROGRAMACIÓN V	5	CISIC	NETBEANS 7.2, VISUAL STUDIO 2010, POSTGRESQL 9.1, MYSQL 5
DISEÑO MECÁNICO 2	7	CIME	AUTOCAD 2012, INVENTOR
DIBUJO MECÁNICO 2	3B	CIME	INVENTOR 2012
PROGRAMACIÓN 6	6	CISIC	.NET 2010, SQL SERVER
GRAFICACION Y ANIMACIÓN	2	CISIC	GIMP, 2 INSCAPE, BLENDER
NEUMÁTICA	6	CIME	FLUID SIM 1.6
TESIS	9	CIERCOM	
APLICACIONES INF. 1	7	CISIC	NAVEGADORES, INTERNET, SIMFONY, SERVIDOR WEB
MECANISMO	4	CIME	AUTOCAD, INVENTOR 2012
PROGRAMACIÓN I	1	CIME	NETBEANS 6-7.01
ADMINISTRACIÓN DE SISTEMAS I	6	CISIC	VMWARE WINSERVER2008
PROGRAMACIÓN II	2	CIME	CODEBLOCKS
MECANISMO	4	CIME	AUTOCAD, INVENTOR 2012
PROGRAMACIÓN I	1	CIME	NETBEANS .NET
ADMINISTRACIÓN DE SISTEMAS I	6	CISIC	VMWARE WINSERVER2008
PROGRAMACIÓN II	2	CIME	NETBEANS .NET
PROGRAMACIÓN 6	6	CISIC	.NET 2010, SQL SERVER

#### 2.2.6.4 Cableado estructurado

El laboratorio VII cuenta con el etiquetado de los puntos de red mientras que el laboratorio VI no, ya que no existe documentación con información del mapeo de la red se verificó la integridad del etiquetado y la conexión de cada punto hacia el switch de acceso así como también su conexión hacia el switch de core de la FICA. El laboratorio VII utiliza como equipo de acceso un switch cisco Catalyst 2960 de 48 puertos para dar conectividad a la red por medio de una conexión cruzada hacia dos patch panel Newlink cat.6 de 24 puertos mientras que el otro switch cisco Catalyst 2960 de 48 puertos es utilizado para brindar conectividad al laboratorio VI, a través de una conexión cruzada con dos patch panel

Newlink cat.6 de 24. La conexión cruzada desde el switch de core de la FICA llega a través del módulo 7 de fibra óptica del QUEST al puerto SFP 1 del switch 1, mientras que la conexión en cascada hacia el switch 2 va desde el puerto GigabitEthernet 2 del switch 1 al puerto GigabitEthernet 1 del switch 2, la figura 20 y 21 detalla el mapeo de la red.

NC: NO CONECTADO	
----- : NULO	
EQUIPOS	
QUEST NFO-5000	FO
PATCH PANEL NEWLINK CAT 6 (24 P)	PPA
SWITCH CATALYST 2960 (48 P)	SW1
PATCH PANEL NEWLINK CAT 6 (24 P)	PPB
PATCH PANEL NEWLINK CAT 6 (24 P)	PPC
SWITCH CATALYST 2960 (48 P)	SW2
PATCH PANEL NEWLINK CAT 6 (24 P)	PPD
SERVIDOR DE VIDEO	SV

CONEX. SW CORE - FICA	
SW - CORE (2ºPISO)	FO-MODULO
HUBBEL-FO-07	1-2

CONEX. CRUZ. SW1-PP	
SW1-PUERTO	PP-PUERTO
1	PPA-1
2	PPA-2
3	PPA-3
4	PPA-4
5	PPA-5
6	PPA-6
7	PPA-7
8	PPA-8
9	PPA-9
10	PPA-10
11	PPA-11
12	PPA-12
13	PPA-13
14	PPA-14
15	PPA-15
16	PPA-16
17	PPA-17
18	PPA-18
19	PPA-19
20	PPA-20
21	PPA-21
22	PPA-22
23	PPA-23
24	PPA-24
25	PPB-1
26	PPB-2
27	PPB-3
28	PPB-4
29	PPB-5
30	PPB-6
31	PPB-7
32	PPB-8
33	PPB-9
34	PPB-10
35	PPB-11
36	PPB-12
37	PPB-13
38	PPB-14
39	PPB-15
40	PPB-16
41	PPB-17
42	PPB-18
43	PPB-19
44	PPB-20
45	PPB-21
46	PPB-22
47	PPB-23
48 (NC)	PPB-24 (NC)
GIGABIT 2	SW2-GIGABIT 1
SFP 1	FO-MODULO 1-2

DESTINO		
PP-PUERTO	ETIQUETA	UBICACIÓN
PPA-1	R.LAB.C2 PPA-01	LAB.VII
PPA-2	R.LAB.C2 PPA-02	LAB.VII
PPA-3	R.LAB.C2 PPA-03	LAB.VII
PPA-4	R.LAB.C2 PPA-04	LAB.VII
PPA-5	R.LAB.C2 PPA-05	LAB.VII
PPA-6	R.LAB.C2 PPA-06	LAB.VII
PPA-7	R.LAB.C2 PPA-07	LAB.VII
PPA-8	R.LAB.C2 PPA-08	LAB.VII
PPA-9	R.LAB.C2 PPA-09	LAB.VII
PPA-10	R.LAB.C2 PPA-10	LAB.VII
PPA-11	R.LAB.C2 PPA-11	LAB.VII
PPA-12	R.LAB.C2 PPA-12	LAB.VII
PPA-13	R.LAB.C2 PPA-13	LAB.VII
PPA-14	R.LAB.C2 PPA-14	LAB.VII
PPA-15	R.LAB.C2 PPA-15	LAB.VII
PPA-16	R.LAB.C2 PPA-16	LAB.VII
PPA-17	R.LAB.C2 PPA-17	LAB.VII
PPA-18	R.LAB.C2 PPA-18	LAB.VII
PPA-19	R.LAB.C2 PPA-19	LAB.VII
PPA-20	R.LAB.C2 PPA-20	LAB.VII
PPA-21	R.LAB.C2 PPA-21	LAB.VII
PPA-22	R.LAB.C2 PPA-22	LAB.VII
PPA-23	R.LAB.C2 PPA-23	LAB.VII
PPA-24	R.LAB.C2 PPA-24	LAB.VII
PPB-1	R.LAB.C2 PPB-1	LAB.VII
PPB-2	R.LAB.C2 PPB-2	LAB.VII
PPB-3	R.LAB.C2 PPB-3	LAB.VII
PPB-4	R.LAB.C2 PPB-4	LAB.VII
PPB-5	R.LAB.C2 PPB-5	LAB.VII
PPB-6	R.LAB.C2 PPB-6	LAB.VII
PPB-7	R.LAB.C2 PPB-7	LAB.VII
PPB-8	R.LAB.C2 PPB-8	LAB.VII
PPB-9	R.LAB.C2 PPB-9	LAB.VII
PPB-10	R.LAB.C2 PPB-10	LAB.VII
PPB-11	R.LAB.C2 PPB-11	LAB.VII
PPB-12	R.LAB.C2 PPB-12	LAB.VII
PPB-13	R.LAB.C2 PPB-13	LAB.VII
PPB-14	R.LAB.C2 PPB-14	LAB.VII
PPB-15	R.LAB.C2 PPB-15	LAB.VII
PPB-16	R.LAB.C2 PPB-16	LAB.VII
PPB-17	R.LAB.C2 PPB-17	LAB.VII
PPB-18	R.LAB.C2 PPB-18	LAB.VII
PPB-19	R.LAB.C2 PPB-19	LAB.VII
PPB-20	R.LAB.C2 PPB-20	LAB.VII
PPB-21	R.LAB.C2 PPB-21	LAB.VII
PPB-22	R.LAB.C2 PPB-22	LAB.VII
PPB-23	R.LAB.C2 PPB-23	LAB.VII
PPB-24 (NC)	-----	-----

Figura 20. Mapeo de red - Laboratorio VII – FICA  
Fuente: Laboratorio VII – FICA



CONEX.CRUZ.SW2-PP		DESTINO		
SW2-PUERTO	PP-PUERTO	PP-PUERTO	ETIQUETA	UBICACIÓN
1	PPC-1	PPC-1	NO-ETIQUETADO	LAB VI
2	PPC-2	PPC-2	NO-ETIQUETADO	LAB VI
3	PPC-3	PPC-3	NO-ETIQUETADO	LAB VI
4	PPC-4	PPC-4	NO-ETIQUETADO	LAB VI
5	PPC-5	PPC-5	NO-ETIQUETADO	LAB VI
6	PPC-6	PPC-6	NO-ETIQUETADO	LAB VI
7	PPC-7	PPC-7	NO-ETIQUETADO	LAB VI
8	PPC-8	PPC-8	NO-ETIQUETADO	LAB VI
9	PPC-9	PPC-9	NO-ETIQUETADO	LAB VI
10	PPC-10	PPC-10	NO-ETIQUETADO	LAB VI
11	PPC-11	PPC-11	NO-ETIQUETADO	LAB VI
12	PPC-12	PPC-12	NO-ETIQUETADO	LAB VI
13	PPC-13	PPC-13	NO-ETIQUETADO	LAB VI
14	PPC-14	PPC-14	NO-ETIQUETADO	LAB VI
15	PPC-15	PPC-15	NO-ETIQUETADO	LAB VI
16	PPC-16	PPC-16	NO-ETIQUETADO	LAB VI
17	PPC-17	PPC-17	NO-ETIQUETADO	LAB VI
18	PPC-18	PPC-18	NO-ETIQUETADO	LAB VI
19	PPC-19	PPC-19	NO-ETIQUETADO	LAB VI
20	PPC-20	PPC-20	NO-ETIQUETADO	LAB VI
21	PPC-21	PPC-21	NO-ETIQUETADO	LAB VI
22	PPC-22	PPC-22	NO-ETIQUETADO	LAB VI
23	PPC-23	PPC-23	NO-ETIQUETADO	LAB VI
24	PPC-24	PPC-24	NO-ETIQUETADO	LAB VI
25	PPD-1	PPD-1	NO-ETIQUETADO	LAB VI
26	PPD-2	PPD-2	NO-ETIQUETADO	LAB VI
27	PPD-3	PPD-3	NO-ETIQUETADO	LAB VI
28	PPD-4	PPD-4	NO-ETIQUETADO	LAB VI
29	PPD-5	PPD-5	NO-ETIQUETADO	LAB VI
30	PPD-6	PPD-6	NO-ETIQUETADO	LAB VI
31	PPD-7	PPD-7	NO-ETIQUETADO	LAB VI
32	PPD-8	PPD-8	NO-ETIQUETADO	LAB VI
33	PPD-9	PPD-9	NO-ETIQUETADO	LAB VI
34	PPD-10	PPD-10	NO-ETIQUETADO	LAB VI
35	PPD-11	PPD-11	NO-ETIQUETADO	LAB VI
36	PPD-12	PPD-12	NO-ETIQUETADO	LAB VI
37	PPD-13	PPD-13	NO-ETIQUETADO	LAB VI
38	PPD-14	PPD-14	NO-ETIQUETADO	LAB VI
39	PPD-15	PPD-15	NO-ETIQUETADO	LAB VI
40	PPD-16	PPD-16	NO-ETIQUETADO	LAB VI
41	PPD-17	PPD-17	NO-ETIQUETADO	LAB VI
42	PPD-18	PPD-18	NO-ETIQUETADO	LAB VI
43	PPD-19	PPD-19	NO-ETIQUETADO	LAB VI
44	PPD-20	PPD-20	NO-ETIQUETADO	LAB VI
45	PPD-21	PPD-21	NO-ETIQUETADO	LAB VI
46	PPD-22	PPD-22	NO-ETIQUETADO	LAB VI
47	PPD-23	PPD-23	NO-ETIQUETADO	LAB VI
-----	PPD-24 (NC)	PPD-24 (NC)	-----	LAB VI
48	SV			
GIGABIT 1	SW1-GIGABIT 2			

Figura 21. Mapeo de red - Laboratorio VI – FICA  
Fuente: Laboratorio VI – FICA

## 2.2.7 CUBÍCULOS PROFESORES

### 2.2.7.1 Equipos de telecomunicaciones

Esta sala ubicada en el último piso de la facultad alberga su propio rack de telecomunicaciones, el cual contiene los equipos de acceso que permiten la conectividad de cada equipo de cómputo. La tabla 31 detalla los equipos alojados en el rack.

Tabla 29. Equipos de telecomunicaciones - Cubículos Profesores – FICA  
Fuente: Cubículos Profesores – FICA

EQUIPOS DE TELECOMUNICACIONES	MARCA	NOMBRE	DIRECCIÓN IP	CANT. #	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
							Bueno	Regular	Malo	
RACKS DE PARED DE 19"	PANDUIT	-----	-----	1	31/05/2011	373.50	X			10
PATCH PANEL DE 24 PUERTOS CAT. 6	NEWLINK	-----	-----	2	31/05/2011	230.00	X			10
SWITCH DE 48 PUERTOS	CISCO CATALYST 2960	SW-FICA-SALAINVESTIGACION-01	172.20.2.39	1	31/05/2011	3,399.34	X			10

### 2.2.7.2 Cableado estructurado

Esta sala ubicada en el último piso de la facultad cuenta con el etiquetado de los puntos de red pero no existe documentación con información del mapeo de la red, por ello se verificó la integridad del etiquetado de cada punto hacia el switch de acceso así como también su conexión hacia el switch de core de la FICA, esta sala utiliza como equipo de acceso un switch cisco Catalyst 2960 de 48 puertos para dar conectividad a la red por medio de una conexión cruzada hacia dos patch panel Newlink cat.6 de 24 puertos. La conexión cruzada desde el switch de core de la FICA llega a través del puerto 24 del patch panel B al puerto GigabitEthernet-1 del switch 1, la figura 22 detalla el mapeo de la red.

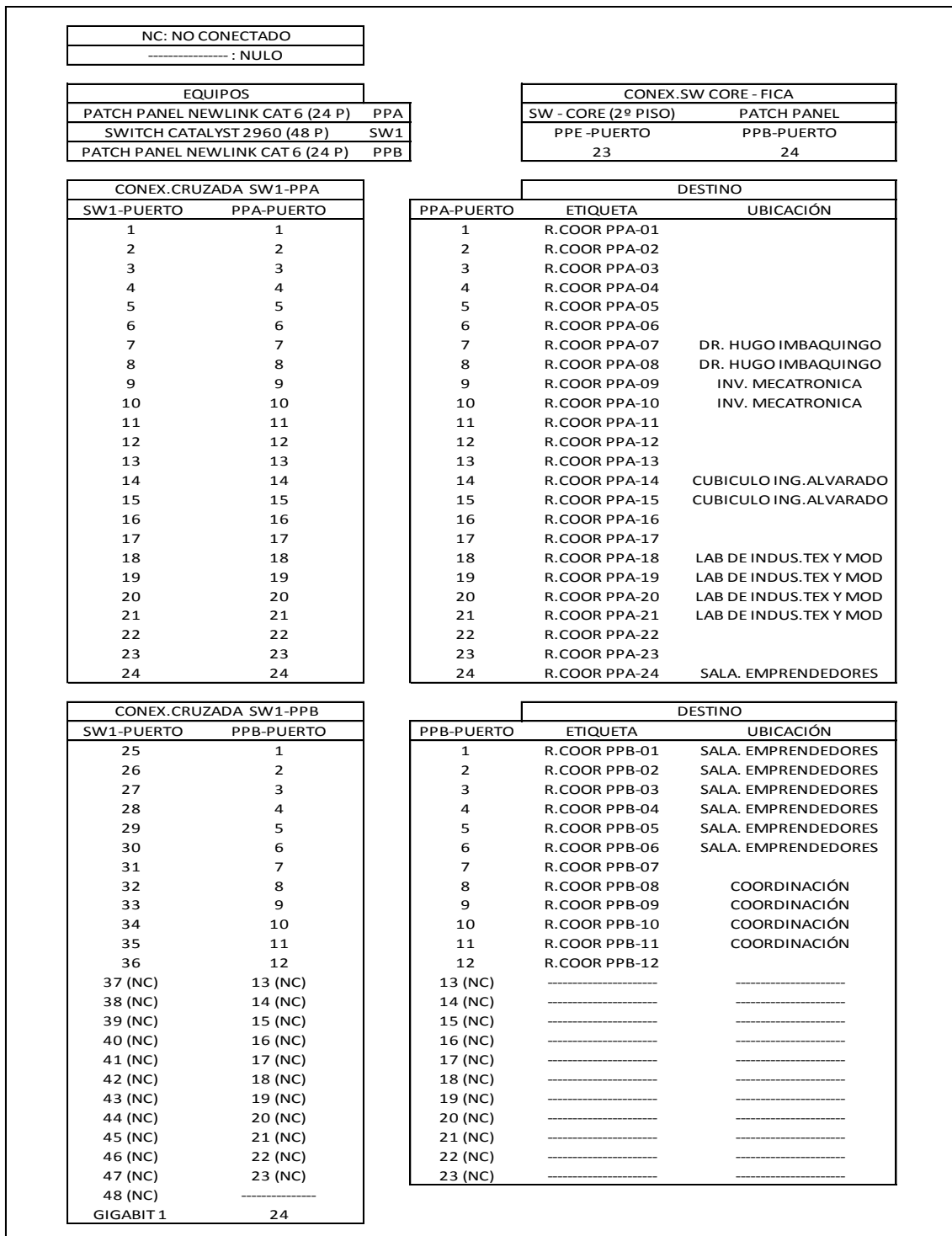


Figura 22. Mapeo de red - Cubículos Profesores – FICA  
 Fuente: Cubículos Profesores – FICA

## 2.2.8 SALA DE PROFESORES

### 2.2.8.1 Equipos de telecomunicaciones

Esta sala alberga su propio rack de telecomunicaciones, el cual contiene los equipos de acceso que permiten la conectividad de cada equipo de cómputo. La tabla 33 detalla los equipos alojados en el rack.

Tabla 30. Equipos de telecomunicaciones - Sala de Profesores – FICA  
Fuente: Sala de Profesores – FICA

EQUIPOS DE TELECOMUNICACIONES	MARCA	NOMBRE	DIRECCIÓN IP	CANT. #	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
							Bueno	Regular	Malo	
RACKS DE PARED DE 19"	PANDUIT	-----	-----	1	31/05/2011	373.50	X			10
PATCH PANEL DE 24 PUERTOS CAT. 6	NEWLINK	-----	-----	1	31/05/2011	230.00	X			10
SWITCH DE 24 PUERTOS.	CISCO CATALYST 2960	SW-FICA-ASOPROFESORES-01	172.20.2.40	1	31/05/2011	3,399.34	X			10

### 2.2.8.2 Cableado estructurado

Esta sala cuenta con el etiquetado de los puntos de red pero no existe documentación con información del mapeo de la red, por ello se verificó la integridad del etiquetado de cada punto hacia el switch de acceso así como también su conexión hacia el switch de core de la FICA, utilizando un testeador de red. La tabla 49 muestra los resultados obtenidos por medio del testeado de todos los puntos de red de este laboratorio, se utiliza como equipo de acceso un switch cisco Catalyst 2960 de 24 puertos para dar conectividad a la red por medio de una conexión cruzada hacia un patch panel Newlink cat.6 de 24 puertos. La conexión cruzada desde el switch de core de la FICA llega a través del puerto 24 del patch panel A al puerto GigabitEthernet-1 del switch 1, la figura 23 detalla el mapeo de la red.

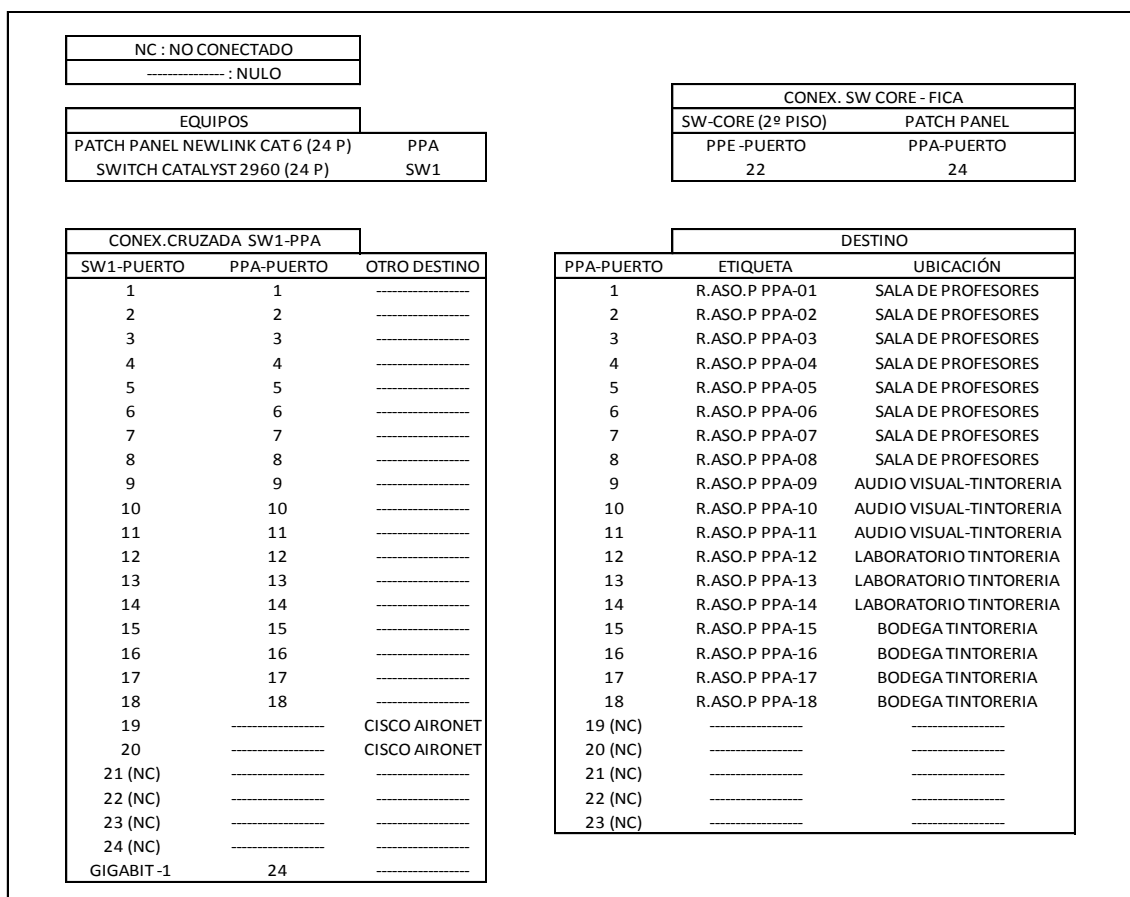


Figura 23. Mapeo de red - Sala de Profesores – FICA  
Fuente: Sala de Profesores – FICA

## 2.2.9 CUARTO DE EQUIPOS FICA

### 2.2.9.1 Servidores

El cuarto de equipos de telecomunicaciones de la Facultad de Ingeniería en Ciencias Aplicadas ubicado en el segundo piso dispone de cinco servidores, los cuales entregan los servicios de encuestas, monitoreo, DHCP y ambiente educativo, la tabla 31 muestra información de estos equipos.

Tabla 31. Servidores – FICA  
Fuente: FICA-UTN

EQUIPO	SERVICIO	SISTEMA OPERATIVO
PROLIANT ML150 G5	OPINA-SERVIDOR DE ENCUESTAS	UBUNTU-SERVER 12.10
IBM SYSTEM X3500 M4	MOODLE-AMBIENTE EDUCATIVO	CENTOS 6.4
IBM SYSTEM X3200 M2	SERVIDOR-DHCP	CENTOS 5.7

### 2.2.9.2 Equipos de telecomunicaciones

El cuarto de equipos alberga el rack principal de telecomunicaciones el cual contiene al switch de core de la facultad que interconecta a los switches de acceso alojados en los laboratorios, brinda conectividad a los equipos del área administrativa, puntos de acceso inalámbricos y otras dependencias, además brinda redundancia en la red de la UTN por medio de enlaces de fibra hacia la capa de acceso de las facultades FECYT<sup>55</sup>, FACAE<sup>56</sup>, FICAYA, SALUD, POSTGRADO Y BIBLIOTECA por medio de STP, estas facultades tienen conectividad hacia la nube de internet a través de enlaces de fibra óptica que llegan desde el equipo de core ubicado en el Ed. Central, cabe recalcar que únicamente el equipo de core ubicado en el ED. Central tiene salida hacia la nube de internet, por lo que si se llega a tener algún problema con este equipo se perdería la salida hacia la nube de internet desde toda la red de la UTN, la tabla 32 describe el contenido del rack principal de telecomunicaciones de la facultad.

Tabla 32. Equipos de telecomunicaciones – Cuarto de Equipos FICA  
Fuente: FICA-UTN

EQUIPOS DE TELECOMUNICACIONES	MARCA	NOMBRE	DIRECCIÓN IP	CANT. #	FECHA DE COMPRA	PRECIO UNIT.	ESTADO			VIDA ÚTIL (AÑOS)
							Bueno	Regular	Malo	
RACKS DE 19" DE ANCHO - 36UR.	PANDUIT	-----	-----	1	31/05/2011	373.50	X			10
PATCH PANEL DE 24 PUERTOS CAT. 6.	NEWLINK	-----	-----	6	31/05/2011	230.00	X			10
SWITCH DE CAPA 3	CISCO CATALYST 4506-E	SW-FICA	172.20.1.12	1	31/05/2011	14,737.29	X			10

### 2.2.9.3 Cableado estructurado

El switch de core de la facultad es un equipo CISCO CATALYST 4506-E cuenta con tres módulos de 48 puertos 10/100/1000 los cuales se distinguen con los nombres SW4, SW5 y SW6 y tienen una conexión cruzada hacia 6 patch panel de 24 puertos cat.6, se cuenta con el etiquetado de los puntos pero no existe documentación con información del mapeo de la red,

<sup>55</sup> FECYT: Facultad de Educación Ciencia y Tecnología.

<sup>56</sup> FACAE: Facultad de Ciencias Administrativas y Económicas.

como se muestra en las figuras 24 y 25, los switches de acceso de la facultad están conectados al patch panel E, los puntos de acceso inalámbricos a los patch panel E, F y C y los servidores directamente al switch de core, las figuras 24,25 y 26 detallan el mapeo de la red dividido en la interconexión de los switches SW4, SW5 y SW6.

EQUIPOS		NC : NO CONECTADO		
SWITCH 4 (48 P)	SW4	----- : NULO		
SWITCH 5 (48 P)	SW5			
SWITCH 6 (48 P)	SW6			
PATCH PANEL NEWLINK CAT 6 (24 P)	PPA			
PATCH PANEL NEWLINK CAT 6 (24 P)	PPB			
PATCH PANEL NEWLINK CAT 6 (24 P)	PPC			
PATCH PANEL NEWLINK CAT 6 (24 P)	PPD			
PATCH PANEL NEWLINK CAT 6 (24 P)	PPE			
PATCH PANEL NEWLINK CAT 6 (24 P)	PPF			

CONEXIÓN CRUZADA			DESTINO		
SW4-PUERTO	PP-PUERTO	OTRO DEST.	PP-PUERTO	ETIQUETA	UBICACION
1	PPE-1	-----	PPE-1	R.PISO2 PPE-1	ENTRADA LABORATORIO
2	PPE-2	-----	PPE-2	R.PISO2 PPE-2	ENTRADA LABORATORIO
3	PPE-3	-----	PPE-3	R.PISO2 PPE-3	ENTRADA LABORATORIO
4	PPE-4	-----	PPE-4	R.PISO2 PPE-4	ENTRADA LABORATORIO
5	PPE-5	-----	PPE-5	R.PISO2 PPE-5	SAL. DE CONFERENCIAS
6	PPE-6	-----	PPE-6	R.PISO2 PPE-6	SAL. DE CONFERENCIAS
7	PPE-7	-----	PPE-7	R.PISO2 PPE-7	SAL. DE CONFERENCIAS
8	PPE-8	-----	PPE-8	R.PISO2 PPE-8	SAL. DE CONFERENCIAS
9	PPE-9	-----	PPE-9	DESCONOCIDO	DESCONOCIDO
10	PPE-10	-----	PPE-10	AP-FICA-PA2D	AP - FICA
11	PPE-11	-----	PPE-11	DESCONOCIDO	DESCONOCIDO
12	PPE-12	-----	PPE-12	DESCONOCIDO	DESCONOCIDO
13	PPE-13	-----	PPE-13	DESCONOCIDO	DESCONOCIDO
14	PPE-14	-----	PPE-14	AP-FICA-PA2I	AP - FICA
15	-----	CONTROL ACCESO LAB	PPE-15 (NC)	-----	-----
16	-----	CONTEOL ACCESO LAB	PPE-16 (NC)	-----	-----
17	-----	SERV. DE MONITOREO	PPE-17 (NC)	-----	-----
18 (NC)	-----	-----	-----	-----	-----
19 (NC)	-----	-----	-----	-----	-----
20 (NC)	-----	-----	-----	-----	-----
21 (NC)	-----	-----	-----	-----	-----
22 (NC)	-----	-----	-----	-----	-----
23	-----	SERV.SISTEMAS	-----	-----	-----
24 (NC)	-----	-----	-----	-----	-----
25 (NC)	-----	-----	-----	-----	-----
26 (NC)	-----	-----	-----	-----	-----
27 (NC)	-----	-----	-----	-----	-----
28	-----	-----	-----	-----	-----
29 (NC)	-----	-----	-----	-----	-----
30	-----	SERV. MOODLE/OPINA	-----	-----	-----
31	PPF-1	-----	PPF-1	DESCONOCIDO	DESCONOCIDO
32	PPF-2	-----	PPF-2	DESCONOCIDO	DESCONOCIDO
33	PPF-3	-----	PPF-3	DESCONOCIDO	DESCONOCIDO
34	PPF-4	-----	PPF-4	DESCONOCIDO	DESCONOCIDO
35	PPF-5	-----	PPF-5	DESCONOCIDO	DESCONOCIDO
36	PPF-6	-----	PPF-6	DESCONOCIDO	DESCONOCIDO
37	PPF-7	-----	PPF-7	AP-FICA-PA4	AP - FICA
38	PPF-8	-----	PPF-8	DESCONOCIDO	DESCONOCIDO
39	PPF-9	-----	PPF-9	AP-FICA-PA3D	AP - FICA
40	PPF-10	-----	PPF-10	AP-FICA-PA3I	AP - FICA
41	PPF-11	-----	PPF-11	NO ETIQUETADO	ASO. IND-TEX (P. DER.)
42	PPF-12	-----	PPF-12	NO ETIQUETADO	ASO. IND-TEX (P. IZQ.)
-----	-----	-----	PPF-13 (NC)	-----	-----
-----	-----	-----	PPF-14 (NC)	-----	-----
-----	-----	-----	PPF-15 (NC)	-----	-----
-----	-----	-----	PPF-16 (NC)	-----	-----
-----	-----	-----	PPF-17 (NC)	-----	-----
-----	-----	-----	PPF-18 (NC)	-----	-----
-----	-----	-----	PPF-19 (NC)	-----	-----
-----	-----	-----	PPF-20 (NC)	-----	-----
-----	-----	-----	PPF-21 (NC)	-----	-----
-----	-----	-----	PPF-22 (NC)	-----	-----
-----	-----	-----	PPF-23 (NC)	-----	-----
-----	-----	-----	PPF-24 (NC)	-----	-----
43	PPE-18	-----	PPE-18	PPA-48	LABORATORIO I
44	PPE-19	-----	PPE-19	PPA-48	LABORATORIO II
45	PPE-20	-----	PPE-20	PPB-24	LABORATORIO III
46	PPE-21	-----	PPE-21	PPB-24	LABORATORIO IV
47	PPE-22	-----	PPE-22	PPA-24	SAL. PROF.ULT- PISO
48	PPE-23	-----	PPE-23	PPB-24	CUBILO PROF.
-----	-----	-----	PPE-24(NC)	-----	-----

Figura 24. Mapeo de red - Cuarto de Equipos FICA – Switch 4  
Fuente: Cuarto de equipos – FICA



CONEXIÓN CRUZADA		DESTINO		
SW5-PUERTO	PP-PUERTO	PPC-PUERTO	ETIQUETA	UBICACIÓN
1	PPC-1	PPC-1	R.PISO2 PPC-1	SALA DE GRADOS
2	PPC-2	PPC-2	DESCONOCIDO	DESCONOCIDO
3	PPC-3	PPC-3	R.PISO2 PPC-3	SECRET. DECANATO
4	PPC-4	PPC-4	R.PISO2 PPC-4	SECRET. DECANATO
5	PPC-5	PPC-5	R.PISO2 PPC-5	SECRET. DECANATO
6	PPC-6	PPC-6	R.PISO2 PPC-6	SECRET. DECANATO
7	PPC-7	PPC-7	R.PISO2 PPC-7	SECRET. DECANATO
8	PPC-8	PPC-8	R.PISO2 PPC-8	SECRET. DECANATO
9	PPC-9	PPC-9	R.PISO2 PPC-9	SECRET. DECANATO
10	PPC-10	PPC-10	R.PISO2 PPC-10	SECRET. DECANATO
11	PPC-11	PPC-11	R.PISO2 PPC-11	SECRET. CIME
12	PPC-12	PPC-12	R.PISO2 PPC-12	SECRET. CIME
13	PPC-13	PPC-13	R.PISO2 PPC-13	SECRET. CIME
14	PPC-14	PPC-14	R.PISO2 PPC-14	SECRET. CIME
15	PPC-15	PPC-15	R.PISO2 PPC-15	SECRET. CIME
16	PPC-16	PPC-16	R.PISO2 PPC-16	SECRET. CIME
17	PPC-17	PPC-17	R.PISO2 PPC-17	SECRET. CISIC
18	PPC-18	PPC-18	R.PISO2 PPC-18	SECRET. CISIC
19	PPC-19	PPC-19	R.PISO2 PPC-19	SECRET. CISIC
20	PPC-20	PPC-20	R.PISO2 PPC-20	SECRET. CISIC
21	PPC-21	PPC-21	R.PISO2 PPC-21	SECRET. CISIC
22	PPC-22	PPC-22	R.PISO2 PPC-22	SECRET. CISIC
23	PPC-23	PPC-23	AP-FICA-PB	AP - FICA
24	PPC-24	PPC-24	DESCONOCIDO	DESCONOCIDO
25	PPD-1	PPD-1	R.PISO2 PPD-1	LABORATORIO
26	PPD-2	PPD-2	R.PISO2 PPD-2	LABORATORIO
27	PPD-3	PPD-3	R.PISO2 PPD-3	LABORATORIO
28	PPD-4	PPD-4	R.PISO2 PPD-4	LABORATORIO
29	PPD-5	PPD-5	R.PISO2 PPD-5	LABORATORIO
30	PPD-6	PPD-6	R.PISO2 PPD-6	LABORATORIO
31	PPD-7	PPD-7	R.PISO2 PPD-7	LABORATORIO
32	PPD-8	PPD-8	R.PISO2 PPD-8	LABORATORIO
33	PPD-9	PPD-9	R.PISO2 PPD-9	LABORATORIO
34	PPD-10	PPD-10	R.PISO2 PPD-10	LABORATORIO
35	PPD-11	PPD-11	R.PISO2 PPD-11	LABORATORIO
36	PPD-12	PPD-12	R.PISO2 PPD-12	LABORATORIO
37	PPD-13	PPD-13	R.PISO2 PPD-13	LABORATORIO
38	PPD-14	PPD-14	R.PISO2 PPD-14	LABORATORIO
39	PPD-15	PPD-15	R.PISO2 PPD-15	LABORATORIO
40	PPD-16	PPD-16	R.PISO2 PPD-16	LABORATORIO
41	PPD-17	PPD-17	R.PISO2 PPD-17	LABORATORIO
42	PPD-18	PPD-18	R.PISO2 PPD-18	LABORATORIO
43	PPD-19	PPD-19	R.PISO2 PPD-19	LABORATORIO
44	PPD-20	PPD-20	R.PISO2 PPD-20	LABORATORIO
45	PPD-21	PPD-21	R.PISO2 PPD-21	LABORATORIO
46	PPD-22	PPD-22	R.PISO2 PPD-22	LABORATORIO
47	PPD-23	PPD-23	R.PISO2 PPD-24	LABORATORIO
48	PPD-24	PPD-24	R.PISO2 PPD-23	LABORATORIO

Figura 25. Mapeo de red - Cuarto de Equipos FICA – Switch 5  
Fuente: Cuarto de equipos – FICA

CONEXIÓN CRUZADA		DESTINO		
SW6-PUERTO	PP-PUERTO	PPA-PUERTO	ETIQUETA	UBICACIÓN
1	PPA-1	PPA-1	R.PISO2 PPA-01	SECRET. CIERCOM
2	PPA-2	PPA-2	R.PISO2 PPA-02	SECRET. CIERCOM
3	PPA-3	PPA-3	DESCONOCIDO	DESCONOCIDO
4	PPA-4	PPA-4	DESCONOCIDO	DESCONOCIDO
5	PPA-5	PPA-5	R.PISO2 PPA-05	SECRET. CIERCOM
6	PPA-6	PPA-6	R.PISO2 PPA-06	SECRET. CIERCOM
7	PPA-7	PPA-7	R.PISO2 PPA-07	SECRET. TEXTIL
8	PPA-8	PPA-8	R.PISO2 PPA-08	SECRET. TEXTIL
9	PPA-9	PPA-9	R.PISO2 PPA-09	SECRET. TEXTIL
10	PPA-10	PPA-10	R.PISO2 PPA-10	SECRET. TEXTIL
11	PPA-11	PPA-11	R.PISO2 PPA-11	SECRET. TEXTIL
12	PPA-12	PPA-12	R.PISO2 PPA-12	SECRET. TEXTIL
13	PPA-13	PPA-13	R.PISO2 PPA-13	SECRET. TEXTIL
14	PPA-14	PPA-14	R.PISO2 PPA-14	SECRET. TEXTIL
15	PPA-15	PPA-15	R.PISO2 PPA-15	CENT. CAP.CONT.
16	PPA-16	PPA-16	R.PISO2 PPA-16	CENT. CAP.CONT.
17	PPA-17	PPA-17	R.PISO2 PPA-17	SALA DE PROFESORES
18	PPA-18	PPA-18	R.PISO2 PPA-18	SALA DE PROFESORES
19	PPA-19	PPA-19	R.PISO2 PPA-19	SALA DE PROFESORES
20	PPA-20	PPA-20	R.PISO2 PPA-20	SALA DE PROFESORES
21	PPA-21	PPA-21	R.PISO2 PPA-22	SALA DE PROFESORES
22	PPA-22	PPA-22	R.PISO2 PPA-21	SALA DE PROFESORES
23	PPA-23	PPA-23	R.PISO2 PPA-22	SECRETARIO ABOGADO
24	PPA-24	PPA-24	R.PISO2 PPA-23	SECRETARIO ABOGADO
25	PPB-1	PPB-1	R.PISO2 PPA-01	SECRETARIO ABOGADO
26	PPB-2	PPB-2	R.PISO2 PPA-02	SECRETARIO ABOGADO
27	PPB-3	PPB-3	R.PISO2 PPA-03	SECRETARIO ABOGADO
28	PPB-4	PPB-4	R.PISO2 PPA-04	SECRETARIO ABOGADO
29	PPB-5	PPB-5	R.PISO2 PPA-05	COPIAS - PLANTA BAJA
30	PPB-6	PPB-6	R.PISO2 PPA-06	COPIAS - PLANTA BAJA
31	PPB-7	PPB-7	R.PISO2 PPB-07	DIRECCION - EITEX
32	PPB-8	PPB-8	R.PISO2 PPB-08	DIRECCION - EITEX
33	PPB-9	PPB-9	R.PISO2 PPB-09	DIRECCION - EITEX
34	PPB-10	PPB-10	R.PISO2 PPB-10	DIRECCION - EITEX
35	PPB-11	PPB-11	R.PISO2 PPB-11	DIRECCION - EITEX
36	PPB-12	PPB-12	R.PISO2 PPB-12	DIRECCION - EITEX
37	PPB-13	PPB-13	R.PISO2 PPB-13	SECRET. SUBDECANATO
38	PPB-14	PPB-14	R.PISO2 PPB-14	SECRET. SUBDECANATO
39	PPB-15	PPB-15	R.PISO2 PPB-15	SECRET. SUBDECANATO
40	PPB-16	PPB-16	R.PISO2 PPB-16	SECRET. SUBDECANATO
41	PPB-17	PPB-17	R.PISO2 PPB-17	DECANATO
42	PPB-18	PPB-18	R.PISO2 PPB-18	DECANATO
43	PPB-19	PPB-19	R.PISO2 PPB-19	DECANATO
44	PPB-20	PPB-20	R.PISO2 PPB-20	DECANATO
45	PPB-21	PPB-21	R.PISO2 PPB-21	SALA DE GRADOS
46	PPB-22	PPB-22	R.PISO2 PPB-22	SALA DE GRADOS
47	PPB-23	PPB-23	R.PISO2 PPB-23	SALA DE GRADOS
48	PPB-24	PPB-24	R.PISO2 PPB-24	SALA DE GRADOS

Figura 26. Mapeo de red - Cuarto de Equipos FICA – Switch 6

Fuente: Cuarto de Equipos - FICA

## 2.3 FACULTAD DE INGENIERÍA EN CIENCIAS AGROPECUARIAS Y AMBIENTALES

La tabla 33 muestra los equipos localizados en el rack de comunicaciones de la facultad y la ubicación de los puntos de red se muestra en la tabla 34.

Tabla 33. Equipos de telecomunicaciones - FICAYA  
Fuente: FICAYA-UTN

N°	EQUIPOS	# PUERTOS
1	CONVERTIDOR FO-UTP	
2	SWITCH CISCO LINKSYS SRW2024	24
3	SWITCH CISCO SLM 2024 GIGANT	24
4	SWITCH 3COM 4228G 3C17304 SS3	24
5	SWITCH 3COM 4400 3C17203 SS3	24
6	SWITCH CISCO LINKSYS SR224	24
7	PATCH PANEL HUBBELL	24
8	PATCH PANEL IBM	48
9	PATCH PANEL QUEST	48

Tabla 34. Ubicación de puntos de red – FICAYA  
Fuente: FICAYA -UTN

N°	DEPARTAMENTO - OFICINA	# PUNTOS	#TELF
1	DECANATO	8	2
2	SUB-DECANATO	2	1
3	SECRETARIA SUB-DECANATO	2	1
4	SECRETARIO ABOGADO	2	2
5	OFICINA DE AGROPECUARIA	2	1
6	OFICINA DE FORESTAL	2	1
7	OFICINA DE AGROINDUSTRIAL	2	1
8	OFICINA DE AGRONEGOCIOS	4	1
9	OFICINA DE RECURSOS NATURALES	2	1
10	SALA DE TUTORÍAS	5	NO
11	SALA DE CONFERENCIAS	1	NO
12	SALA DE PROFESORES	2	NO
13	LABORATORIO SALA A	26	1
14	LABORATORIO SALA B	31	NO
15	LABORATORIO DE LIMNOLOGÍA	1	NO
16	LABORATORIO DE ENTOMOLOGÍA	1	NO
17	LABORATORIO DE GEOLOGÍA	1	NO
18	LABORATORIO DE USO MÚLTIPLE	2	NO
19	HERBARIO	1	NO
20	MUSEO	1	NO
21	CLUB ECOLÓGICO	1	NO
22	ASO. EST. ING. FORESTAL	1	NO
23	ASO. EST. ING. AGROINDUSTRIAL	1	NO
24	ASO. EST. ING. RECURSOS NATURALES	1	NO
25	PUNTO DE VENTA	2	NO
26	COPIADORA	2	NO
27	AP INTERNOS	3	NO
	TOTAL PUNTOS DE RED Y TELÉFONOS	109	12

## 2.4 FACULTAD DE CIENCIAS ADMINISTRATIVAS Y ECONÓMICAS

Los equipos localizados en el rack de comunicaciones de esta facultad se describen en la tabla 35 y la ubicación de los puntos de red se muestra en la tabla 36.

Tabla 35. Equipos de telecomunicaciones – FACAE  
Fuente: UTN- FACAE

N°	EQUIPOS	# PUERTOS
1	CONVERTIDOR FO-UTP HUBBELL	12
2	SWITCH 3COM 4400SE	24
3	SWITCH 3COM 4400	24
4	SWITCH 3COM 2816 SFP	16
5	SWITCH 3COM 4400SE	24
6	SWITCH 3COM 5500G	48
7	SWITCH TPLINK TLSG22 24 WEP	24
8	SWITCH TPLINK TLSG22 24 WEP	24
9	PATCH PANEL IBM	48
10	PATCH PANEL UNICOM	24
11	PATCH PANEL NEXTT	24
12	PATCH PANEL QUEST	48
13	PATCH PANEL PANDUIT	24
14	PATCH PANEL PANDUIT	24
15	PATCH PANEL PANDUIT	24
16	SWITCH CATALYS 2960G (LAB 4)	48
17	PATCH PANEL HUBBELL (LAB 4)	24
18	PATCH PANEL HUBBELL (LAB 4)	24

Tabla 36. Ubicación de puntos de red – FACAE  
Fuente: UTN- FACAE

N°	DEPARTAMENTO - OFICINA	# PUNTOS	#TELEF
1	DECANO	1	1
2	SECRETARIA DECANATO	1	1
3	SUB-DECANO	1	1
4	SECRETARIA SUB-DECANATO	3	1
5	SECRETARIO ABOGADO	2	1
6	ASESORÍA DE TESIS	3	NO
7	COORDINADORA MERCADOTECNIA	1	1
8	SECRETARIA ING. MERCADOTECNIA	1	1
9	COORDINADOR CONTABILIDAD	1	1
10	SECRETARIA ING. CONTABILIDAD	1	1
11	SECRETARIA ING. CONTABILIDAD SEMI-PRESENCIAL	1	1
12	COORDINADOR ECONOMÍA	1	1
13	SECRETARIA ING. ECONOMÍA	1	1
14	COORDINADOR COMERCIAL	1	1
15	SECRETARIA ING. COMERCIAL	1	1
16	SALA DE GRADOS	1	NO
17	AUDITORIO	2	NO
18	SALA DE PROFESORES	1	NO
19	OFICINA DE LABORATORIOS	10	1
20	LABORATORIO I	32	NO
21	LABORATORIO II	42	NO
22	LABORATORIO III	52	NO
23	LABORATORIO IV	36	NO
24	LABORATORIO DE PUBLICIDAD I	5	NO
25	LABORATORIO DE PUBLICIDAD II	5	NO
26	AULA 103	2	NO
27	AP'S INTERNOS	3	NO
28	AP'S EXTERNOS	2	NO
	TOTAL PUNTOS DE RED Y TELÉFONOS	213	15

## 2.5 FACULTAD DE EDUCACIÓN CIENCIA Y TECNOLOGÍA

El rack de comunicaciones de esta facultad contiene los equipos descritos en la tabla 37 y la tabla 38 muestra la ubicación de los puntos de red.

Tabla 37. Equipos de telecomunicaciones - FECYT  
Fuente: UTN – FECYT

N°	EQUIPOS	# PUERTOS
1	TRANSDUCTOR FFOO	4
2	SWITCH CATALYST 2960	48
3	SWITCH CATALYST 2960	48
4	SWITCH CATALYST 2960	24
5	PATCH PANNEL	24
6	PATCH PANNEL	24

7	PATCH PANNEL	24
8	PATCH PANNEL	24
9	PATCH PANNEL	24
10	SWITCH CATALYST 2960 (LAB 1)	48
11	PATCH PANNEL NEWLINK CAT6 (LAB 1)	48
12	SWITCH CATALYST 2960 (LAB 2)	48
13	PATCH PANNEL NEWLINK CAT6 (LAB 2)	48
14	SWITCH CATALYST 2960 (LAB 4)	48
15	PATCH PANNEL (LAB 4)	24
16	SWITCH CATALYST 2960 (COORD)	24
17	PATCH PANNEL (COORD)	24

Tabla 38. Ubicación de puntos de red – FECYT  
Fuente: UTN- FECYT

N°	DEPARTAMENTO - OFICINA	# PUNTOS
1	DECANO	5
2	SECRETARIA DECANATO	5
3	SUB-DECANO	4
4	SECRETARIA SUB-DECANATO	2
5	SECRETARIO ABOGADO	4
6	AUDITORIO	4
7	PLAN DE CONTINGENCIA	8
8	SEMPRESENCIAL	5
9	COORDINACIONES	16
10	OFICINA DE CARRERAS	5
11	SECRETARIAS DE CARRERA	3
12	COOR. GESTIÓN Y DESARROLLO	2
13	COOR. CONTABILIDAD	2
14	AUDIOVISUALES	10
15	CLUB DE TURISMO	2
16	BODEGA	1
17	LAB. PSICOLOGÍA	4
18	LABORATORIO 1	48
19	LABORATORIO 2	32
20	LABORATORIO 4	22
21	LABORATORIO DE INGLÉS	45
22	AP INTERIORES	3
23	AP EXTERIORES	1
	TOTAL PUNTOS DE RED Y TELÉFONOS	233

## 2.6 FACULTAD DE CIENCIAS DE LA SALUD

La tabla 39 describe los equipos localizados en el rack de comunicaciones de la facultad y la ubicación de los puntos de red se muestra en la tabla 40.

Tabla 39. Equipos de telecomunicaciones - SALUD  
Fuente: UTN- CIENCIAS DE LA SALUD

N°	EQUIPOS	# PUERTOS
1	CONVERTIDOR FO-UTP HUBBELL	12
2	SWITCH 3COM 4400	48
3	SWITCH 3COM 4400	48
4	PATCH PANEL NEXTT	24
5	PATCH PANEL NEXTT	24
6	PATCH PANEL NEXTT	24
7	PATCH PANEL NEXTT	24
8	PATCH PANEL NEXTT	24
9	PATCH PANEL NEXTT	24
10	PATCH PANEL NEXTT	24
11	PATCH PANEL NEXTT	24
12	PATCH PANEL NEXTT	24

Tabla 40. Ubicación de puntos de red – SALUD  
Fuente: UTN- CIENCIAS DE LA SALUD

N°	DEPARTAMENTO - OFICINA	# PUNTOS
1	DECANO	2
2	SECRETARIA DECANATO	2
3	SUB-DECANO	2

4	SECRETARIA SUB-DECANATO	2
5	SECRETARIO ABOGADO	4
6	SALA DEL HCD	4
7	SALA DE GRADOS	2
8	TUTORÍAS ENFERMERÍA (PB)	4
9	TUTORÍAS NUTRICIÓN	4
10	TUTORÍAS ENFERMERÍA	2
11	AULA DE DEMOSTRACIÓN	1
12	PROYECTOS ENFERMERÍA	2
13	DIRECCIÓN NUTRICIÓN	6
14	DIRECCIÓN ENFERMERÍA	2
15	CUBÍCULOS DE PROFESORES	20
16	SALA DE INTERNET	30
17	LABORATORIO DE NUTRICIÓN	1
18	LABORATORIO DE ESTÉTICA	1
19	LABORATORIO DE INFORMÁTICA I	18
20	LABORATORIO DE ENFERMERÍA	2
21	LABORATORIO DE MORFOFISIOLOGÍA	3
22	INVESTIGACIÓN Y PUBLICACIÓN	1
23	ARCHIVO	2
24	FEUE	4
25	AULA 309	2
26	AULA 307	1
27	AULA 306	1
28	AULA TERRAZA	1
29	AULA EXTERIOR	2
25	AP'S INTERNOS	3
	TOTAL PUNTOS DE RED Y TELÉFONOS	127

## 2.7 AUDITORIO AGUSTÍN CUEVA

Los equipos ubicados en el rack de comunicaciones del auditorio se muestran en la tabla 41 y la ubicación de los puntos de red se muestra en la tabla 42.

*Tabla 41.* Equipos de telecomunicaciones - AUDITORIO AGUSTÍN CUEVA  
Fuente: UTN- AUDITORIO AGUSTÍN CUEVA

N°	EQUIPOS	# PUERTOS
1	SWITCH 3COM 4400SE	24
2	PATCH PANEL	24
3	TERMINAL HUBBELL DE FO	12
4	CONVERTIDOR FO-UTP	
5	CONVERTIDOR COAXIAL-UTP	

*Tabla 42.* Ubicación de puntos de red - AGUSTÍN CUEVA  
Fuente: UTN- AUDITORIO AGUSTÍN CUEVA

N°	DEPARTAMENTO - OFICINA	# PUNTOS	#TELEF.
1	CUARTO DE MANTENIMIENTO	2	NO
2	CUARTO SUPERIOR (SWITCH DE ENERGÍA)	2	NO
3	SALÓN	2	NO
4	CUARTO DE EQUIPOS DE AUDIO-VIDEO	2	NO
5	SALA DE TEATRO	2	NO
6	SALA SUPERIOR IZQUIERDA (ASIENTOS)	1	NO
7	DEPARTAMENTO DE MÚSICA	1	NO
8	DEPARTAMENTO DE DANZA	2	NO
9	ESCENARIO	4	NO
10	AP INTERNO	1	NO
11	AP EXTERNOS	2	NO
	TOTAL PUNTOS DE RED Y TELÉFONOS	21	0

## 2.8 EDIFICIO DE POSTGRADO

El rack de comunicaciones de la facultad contiene los equipos que se muestran en la tabla 43 y la ubicación de los puntos de red se muestra en la tabla 44.

Tabla 43. Equipos de telecomunicaciones – POSGRADO  
Fuente: UTN- POSGRADO

N°	EQUIPO	# PUERTOS
1	TRANCIVER FFOO – COAXIAL	
2	SWITCH LINKSYS SRW2048	48
3	SWITCH LINKSYS SRW2024 V1.2	24
4	PATCH PANNEL TEKDATA	48
5	PATCH PANNEL HUBBELL	24
6	PATCH PANNEL HUBBELL	24
7	PATCH PANNEL HUBBELL	24
8	PATCH PANNEL FFOO (TERCER PISO)	
9	SWITCH LINKSYS SRW2048 (TERCER PISO)	48
10	SWITCH LINKSYS SRW2048 (TERCER PISO)	48
11	SWITCH 3COM 3C17304A 4200 (TERCER PISO)	24
12	SWITCH 3COM 3C17304A 4200 (TERCER PISO)	24
13	PATCH PANNEL HUBBELL (TERCER PISO)	24
14	PATCH PANNEL HUBBELL (TERCER PISO)	24
15	PATCH PANNEL HUBBELL (TERCER PISO)	24
16	PATCH PANNEL HUBBELL (TERCER PISO)	24
17	PATCH PANNEL HUBBELL (TERCER PISO)	24
18	PATCH PANNEL HUBBELL (TERCER PISO)	24

Tabla 44. Ubicación de puntos de red - POSGRADO  
Fuente: UTN- POSGRADO

N°	DEPARTAMENTO - OFICINA	# PUNTOS
1	DIRECTOR CAI	4
2	SECRETARÍA CAI	4
3	VIRTUAL ROOM	2
4	LABORATORIO DE INGLÉS	6
5	LABORATORY OFFICE	4
6	LABORATORIO DE GEOMÁTICA	2
7	CENTRO DE BIOLOGÍA	2
8	AULA DE BIOLOGÍA	16
9	CENTRO DE FÍSICA	2
10	BODEGA DE FÍSICA	2
11	AULA DE FÍSICA	12
12	CENTRO DE QUÍMICA	2
13	AULA DE QUÍMICA	10
14	COORDINACIONES	6
15	CEC	4
16	CENTRO DE COMPUTO	18
17	SALA SEGUNDO PISO	6
18	DIRECTOR	4
19	BIBLIOTECA	4
20	AUDITORIO ANTONIO POSSO	6
21	EVALUACIÓN Y ACREDITACIÓN	4
22	SENAGUA	4
23	SALA DE REUNIONES SENAGUA	10
24	CONTABILIDAD	4
25	AULA 1	14
26	AULA 2	14
27	AULA 3	14
28	AULA 4	14
29	OFICINA LAB. FICA	4
30	LAB. ELECTRÓNICA	8
31	LAB. MECATRÓNICA	4
32	AP INTERNOS	3
33	AP EXTERNOS	1
	TOTAL PUNTOS DE RED Y TELÉFONOS	214

## 2.9 EDUCACIÓN FÍSICA

La tabla 45 y 46 describen los equipos localizados en el rack de comunicaciones de la facultad y la ubicación de los puntos de red respectivamente.

Tabla 45. Equipos de telecomunicaciones - EDUCACIÓN FÍSICA  
Fuente: UTN - EDUCACIÓN FÍSICA

N°	EQUIPO	# PUERTOS
1	SWITCH 3COM 3C17304 SUPERSTACK3 4228G	24
2	PATCH PANEL AMP NETCONNECT	24
3	PATCH PANEL HUBBELL DE FO	12

Tabla 46. Ubicación de puntos de red - EDUCACIÓN FÍSICA  
Fuente: UTN - EDUCACIÓN FÍSICA

Nº	DEPARTAMENTO - OFICINA	# PUNTOS	#TELEF.
1	AULA 101	1	NO
2	AULA 102	1	NO
3	AULA 103	1	NO
4	AULA 104	1	NO
5	AULA 107	2	NO
6	AULA 108	1	NO
7	AULA 109	1	NO
8	DIRECCIÓN DE EDUCACIÓN FÍSICA	1	1
9	SECRETARÍA DE EDUCACIÓN FÍSICA	2	1
10	SALA DE CONFERENCIAS EDUCACIÓN FÍSICA	2	NO
11	DIRECCIÓN COORDINACIÓN SENESCYT	2	1
12	SECRETARÍA COORDINACIÓN SENESCYT	2	1
13	SALA DE REUNIONES SENESCYT	2	NO
14	BODEGA Y CUARTO DE EQUIPOS	2	NO
15	AP EXTERNO	1	NO
	TOTAL PUNTOS DE RED Y TELÉFONOS	22	4

## 2.10 BIBLIOTECA

La tabla 47 describe los equipos alojados en el rack de comunicaciones de la biblioteca y la ubicación de los puntos de red se muestra en la tabla 48.

Tabla 47. Equipos de telecomunicaciones -BIBLIOTECA  
Fuente: UTN-BIBLIOTECA

Nº	EQUIPO	# PUERTOS
1	TRANSDUCTOR FFOO	4
2	PATCH PANNEL FFOO	
3	SWITCH CATALYST 2960	48
4	SWITCH SG 300-52	48
5	SWITCH SG 200-18	18
6	SWITCH CÁMARAS	
7	SWITCH 3COM 3C17304 4228G	24
8	SWITCH 3COM 3C16792A (HEMEROTECA)	16
9	PATCH PANNEL TEKDATA	24
10	PATCH PANNEL TEKDATA	24
11	PATCH PANNEL TEKDATA	24
12	PATCH PANNEL TEKDATA	24
13	PATCH PANNEL TEKDATA	24
14	PATCH PANNEL TEKDATA	24
15	PATCH PANNEL FFOO (IC3)	
16	SWITCH CISCO SG200-50 (IC3)	48
17	SWITCH CISCO SG200-50 (IC3)	48
18	PATCH PANNEL DIGILINK (IC3)	24
19	PATCH PANNEL DIGILINK (IC3)	24
20	PATCH PANNEL DIGILINK (IC3)	24

Tabla 48. Ubicación de puntos de red – BIBLIOTECA  
Fuente: UTN– BIBLIOTECA

Nº	DEPARTAMENTO - OFICINA	# PUNTOS
1	CÁMARAS	12
2	PRESTAMOS LIBROS	16
3	CATÁLOGO EN LÍNEA	6
4	ÁREA VIRTUAL	15
5	EQUIPOS PORTÁTILES	6
6	NO VIDENTES	4
7	HEMEROTECA	14
8	DIRECCIÓN BIBLIOTECA	10
9	PROCESOS TÉCNICOS	6
10	VIDEOTECA	8
11	SALA DE PROYECTOS	2
12	INFORMÁTICA	4
13	AUDIO Y VIDEO	2
14	INSTITUTO DE ALTOS ESTUDIOS	4
15	FJI	4
16	UNIDAD AUDITORIA INTERNA	8
17	EX CLUB DE ROBÓTICA	2
18	ASO. GENERAL PROFESORES	4



19	CLUB ROBÓTICA	4
20	ÁREA IC3	14
21	CAPACITACIÓN INTER	2
22	LABORATORIO EXÁMENES	8
23	LABORATORIO 1	16
24	LABORATORIO 2	16
25	LABORATORIO 3	8
26	ARCHIVO 1	16
27	ARCHIVO 2	16
	TOTAL PUNTOS DE RED Y TELÉFONOS	227

## 2.11 GARITA

Los equipos localizados en el rack de comunicaciones de la garita se muestran en la tabla 49 y la ubicación de los puntos de red se muestra en la tabla 50.

*Tabla 49.* Equipos de telecomunicaciones - GARITA  
Fuente: UTN - GARITA

N°	EQUIPO	# PUERTOS
1	TRANSEIVER FFOO – UTP	
2	PATCH PANNEL FFOO	
3	SWITCH 3COM 3C17206 4400SE	24
4	PATCH PANNEL	24

*Tabla 50.* Ubicación de puntos de red – GARITA  
Fuente: UTN- GARITA

N°	DEPARTAMENTO - OFICINA	# PUNTOS
1	RADIO ENLACE	1
2	CONTROLADORA DE ACCESO	1
3	GARITA	1
4	AP INTERNOS	4
5	AP EXTERIORES	1
	TOTAL PUNTOS DE RED Y TELÉFONOS	8

## 2.12 DEFINICIÓN DE EQUIPOS MONITOREADOS

Con la finalidad de conocer el rendimiento en la red de datos de la UTN se realizó un monitoreo en los equipos tanto de la capa de acceso como de la capa de distribución, en los mismos se observa el consumo de recursos de hardware como la utilización de enlaces físicos o lógicos que soportan, los equipos monitoreados se consideraron en base al impacto que podría ocasionar su mal funcionamiento dentro de la universidad, con la finalidad de conocer el rendimiento de la capa de acceso, se agregaron al sistema NAGIOS los switches que permiten conectividad a todos los dispositivos finales o host alojados en los distintos laboratorios y áreas administrativas dentro de la universidad.

Para conocer el rendimiento de la capa de distribución se agregaron los switches que soportan los enlaces troncales hacia las distintas facultades de la UTN, que además proporcionan mecanismos de redundancia en la red por medio del protocolo STP y permitan la propagación de VLAN a la capa de acceso de la UTN.

Para conocer el número de usuarios conectados así como el ancho de banda requerido en la red inalámbrica de la UTN se agregaron al sistema NAGIOS los puntos de acceso inalámbricos instalados en la universidad, también se agregaron al sistema los servidores de encuestas, ambiente educativo y DHCP alojados en FICA con la finalidad de conocer su rendimiento en la red, actualmente en el edificio central se albergan otros servidores como el de aplicaciones, geo portal, aula virtual y base de datos que no están incluidos en el sistema Nagios debido a que son equipos prioritarios para la UTN en los que no se puede realizar ningún tipo de manipulación debido a los requerimientos de disponibilidad en los mismos.

A continuación se detallan los switches monitoreados por cada facultad o edificación dentro de universidad, así como los puntos de acceso inalámbricos y servidores.

*Tabla 51.* Equipos de conmutación alojados en el Edificio Central  
Fuente: Switches instalados en el Edificio Central-UTN

NOMBRE	UBICACIÓN	DESCRIPCIÓN	MARCA	MODELO
SW-ZEUS	DATA CENTER	CORE	CISCO	WS-C4506-E L3
SW-AFRODITA	DATA CENTER	CHASIS BLADE 01	CISCO	WS-CBS3020-HPQ
SW-APOLO	DATA CENTER	CHASIS BLADE 02	CISCO	WS-CBS3020-HPQ
SW-ARES	DATA CENTER	CONCENTRADOR02	CISCO	WS-C3750X-24
SW-ATENEA	PLANTA BAJA	RACKDERECHO01	CISCO	WS-C2960-48TC-L
SW-CRATOS	PRIMER PISO	RACKPISO2-01	CISCO	WS-C2960-48TC-L
SW-CRONOS	PRIMER PISO	RACKPISO2-02	CISCO	WS-C2960-24TC-L
SW-ERIS	AUDITORIO JOSÉ MARTÍ	RACKJOSEMARTI01	CISCO	WS-C2960-48TC-L
SW-EROS	AUDITORIO JOSÉ MARTÍ	RACKJOSEMARTI02	CISCO	WS-C2960-48TC-L
SW-HADES	CANAL UNIVERSITARIO	UTV01	CISCO	WS-C2960-48TC-L
SW-HERA	TERRAZA	TERRAZA01	CISCO	WS-C2960-48TC-L
SW-HERACLES	TERRAZA	TERRAZA02	3COM	SS3 SW 4400 SE
SW-PERSEO	GARITA		3COM	SS3 SW 4400 SE
SW-IRIS	BIENESTAR-ESTUDIANTIL	BIENESTARRACK0101	CISCO	WS-C2960X-48TS-LL
SW-MORFEO	BIENESTAR-ESTUDIANTIL	BIENESTARRACK0102	CISCO	WS-C2960X-48TS-LL
SW-NÉMESIS	BIENESTAR-ESTUDIANTIL	BIENESTARRACK0201	CISCO	WS-C2960X-48TS-LL
SW-NIX	BIENESTAR-ESTUDIANTIL	BIENESTARRACK0202	CISCO	WS-C2960X-48TS-LL
SW-ODÍN	BIENESTAR-ESTUDIANTIL		3COM	SS3 SW 4400 SE
SW-POSEIDÓN	AUDITORIO AGUSTÍN CUEVA		3COM	SS3 SW 4400 SE
	GIMNASIO	GIMNASIO-UTN	3COM	SS3 SW 4400 SE

Tabla 52. Equipos de conmutación alojados en la FICA

Fuente: Switches instalados en la FICA-UTN

NOMBRE	UBICACIÓN	DESCRIPCIÓN	MARCA	MODELO
SW-ARISTÓTELES	CUARTO DE EQUIPOS	DISTFICA	CISCO	WS-C4506-E L3
SW-ARQUÍMEDES	LABORATORIO I	FICALAB101	CISCO	WS-C2960-48TC-L
SW-BERNOULLI	LABORATORIO II	FICALAB201	CISCO	WS-C2960-48TC-L
SW-COPÉRNICO	LABORATORIO III	FICALAB301	CISCO	WS-C2960-48TC-L
SW-COULOMB	LABORATORIO III	FICALAB302	CISCO	WS-C2960-24TC-L
SW-DESCARTES	LABORATORIO IV	FICALAB401	CISCO	WS-C2960-48TC-L
SW-EINSTEIN	LABORATORIO IV	FICALAB402	CISCO	WS-C2960-48TC-L
SW-EUCLIDES	LABORATORIO CISCO	FICALABCISCO01	CISCO	WS-C2960-48TC-L
SW-EULER	LABORATORIO CISCO	FICALABCISCO02	CISCO	WS-C2960-48TC-L
SW-FOURIER	SALA DE INVESTIGACIÓN	SALAINVESTIGACION01	CISCO	WS-C2960-48TC-L
SW-GALILEO	SALA DE PROFESORES	ASOPROFESORES01	CISCO	WS-C2960-24TC-L

Tabla 53. Equipos de conmutación alojados en la FICAYA

Fuente: Switches instalados en la FICAYA -UTN

NOMBRE	UBICACIÓN	DESCRIPCIÓN	MARCA	MODELO
SW-BATMAN	CUARTO DE EQUIPOS	FICAYA01	CISCO LYNKSYS	SRW2024
SW-CÍCLOPE	CUARTO DE EQUIPOS	FICAYA02	CISCO	SLM2024
SW-COLOSUS	CUARTO DE EQUIPOS	SW 6 RAKDERECHOPLANTAC	3COM	SS3 SW 4200
SW-DAREDEVIL	CUARTO DE EQUIPOS	SW 3 RACKIZQUIERDO	3COM	SS3 SW 4400
SW-ELEKTRA	CUARTO DE EQUIPOS	FICAYA05	CISCO LYNKSYS	SR224
SW-FALCON	LA PRADERA	LAPRADERA01	CISCO LYNKSYS	SRW248G4
SW-GHOST-RIDER	YUYUCOCHA	YUYUCOCHA01	CISCO	SG 300-28

Tabla 54. Equipos de conmutación alojados en la FECYT

Fuente: Switches instalados en la FECYT -UTN

NOMBRE	UBICACIÓN	DESCRIPCIÓN	MARCA	MODELO
SW-AC-DC	CUARTO DE EQUIPOS	RACKPRINCIPAL01	CISCO	WS-C2960-48TC-L
SW- AEROSMITH	CUARTO DE EQUIPOS	RACKPRINCIPAL02	CISCO	WS-C2960-48TC-L
SW-BEATLES	CUARTO DE EQUIPOS	RACKPRINCIPAL03	CISCO	WS-C2960-24TC-L
SW-CHICAGO	LABORATORIO 1	FECYTLA101	CISCO	WS-C2960-48TC-L
SW-CINDERELLA	LABORATORIO 2	FECYTLA201	CISCO	WS-C2960-48TC-L
SW-EUROPE	LABORATORIO MAC	FECYTLABMAC01	CISCO	WS-C2960-48TC-L
SW-JACKSON	COORDINACIÓN DE CARRERAS	FECYTCOORDINACIONES01	CISCO	WS-C2960-24TC-L
SW-KISS	INST. EDUCACIÓN FÍSICA	ED-FISICA	CISCO	WS-C2960S-24TS-S
SW-METALLICA	PISCINA	SW5RACKDERECHOPLANTAC	3COM	SS3 SW 4200

Tabla 55. Equipos de conmutación alojados en la FACAE

Fuente: Switches instalados en la FACAE -UTN

NOMBRE	UBICACIÓN	DESCRIPCIÓN	MARCA	MODELO
SW-ALEXANDRA	CUARTO DE EQUIPOS		3COM	SS3 SW 4400 SE
SW-ANDREA	CUARTO DE EQUIPOS		3COM	SS3 SW 4400
SW-CAROLINA	CUARTO DE EQUIPOS		3COM	SS3 SW 4400 SE
SW-CATALINA	CUARTO DE EQUIPOS		3COM	5500G-EI
SW-DIANA	CUARTO DE EQUIPOS		TP-LINK	TL-SG2224WEB
SW-EDUARDA	CUARTO DE EQUIPOS		TP-LINK	TL-SG2224WEB
ELIZABETH	LABORATORIO IV	LAB4FACAE	CISCO	WS-C2960G-248TC-L

Tabla 56. Equipos de conmutación alojados en la FCCSS

Fuente: Switches instalados en la FCCSS -UTN

NOMBRE	UBICACIÓN	DESCRIPCIÓN	MARCA	MODELO
SW-FLEMING	CUARTO DE EQUIPOS	SWITCH 1 FCCSS	3COM	SS3 SW 4400
SW- PASTEUR	CUARTO DE EQUIPOS	SWITCH 2 FCCSS	CISCO	
SW-JENNER	ANTIGUO HSVP	HSVP-01	TP-LINK	TL-SG2216WEB
SW-ESKOLA	ANTIGUO HSVP	HSVP-02	TP-LINK	TL-SF1024

Tabla 57. Equipos de conmutación alojados en el CAI

Fuente: Switches instalados en el CAI -UTN

NOMBRE	UBICACIÓN	DESCRIPCIÓN	MARCA	MODELO
ALEMÁN	PLANTA BAJA	SWITCHPRINCIPAL	CISCO LINKSYS	SRW2048
ÁRABE	PLANTA BAJA	SWITCH02	CISCO LINKSYS	SRW2024
BÚLGARO	SEGUNDO PISO	SWITCHRACK0201	CISCO LINKSYS	SRW2048
CHINO	SEGUNDO PISO	SWITCHRACK0202	CISCO LINKSYS	SRW2048
SW-COREANO	SEGUNDO PISO	SWITCHRACK0203	3COM	SS3 SW 4200
FINLANDÉS	SEGUNDO PISO	SWITCHRACK0204	3COM	SS3 SW 4200

Tabla 58. Equipos de conmutación alojados en POSTGRADO

Fuente: Switches instalados en POSTGRADO -UTN

NOMBRE	UBICACIÓN	DESCRIPCIÓN	MARCA	MODELO
SW-GOKU	CUARTO DE EQUIPOS	COREPOSTGRADO	CISCO	WS-C4503-E L3
SW-BILLS	CUARTO DE EQUIPOS	POSTGRADORACK0102	CISCO	WS-C2960S-48TS-S
SW-BOO	CUARTO DE EQUIPOS	POSTGRADORACK0103	CISCO	WS-C2960S-48TS-S
SW-BROLY	SEGUNDO PISO	POSTGRADORACK0201	CISCO	WS-C2960S-48TD-L
SW-BULMA	SEGUNDO PISO	POSTGRADORACK0202	CISCO	WS-C2960S-48TS-S
SW-CELL	SEGUNDO PISO	POSTGRADORACK0203	CISCO	WS-C2960S-48TS-S
SW-DABURA	SEGUNDO PISO	POSTGRADORACK0204	CISCO	WS-C2960S-24PS-S

Tabla 59. Equipos de conmutación alojados en la BIBLIOTECA

Fuente: Switches instalados en la BIBLIOTECA -UTN

NOMBRE	UBICACIÓN	DESCRIPCIÓN	MARCA	MODELO
CERVANTES	CUARTO DE EQUIPOS	BIBLIOTECA01	CISCO	WS-C2960-48TC-L
ALAN-POE	CUARTO DE EQUIPOS		CISCO	SG-300-52
ALMAGRO	CUARTO DE EQUIPOS		CISCO	SG-200-18
BENEDETTI	HEMEROTECA		3COM	3C16792A
BERNE	IC3		CISCO	SG 200-50
BORGES	IC3		CISCO	SG 200-50

Tabla 60. Puntos de acceso inalámbrico alojados en el Edificio Central

Fuente: Puntos de acceso inalámbrico instalados en el Edificio Central -UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
WLC-UTN	DATA CENTER //EDIFICIO CENTRAL	CISCO	AIR-CT5508-K9
AP-CENTRAL-PB	PLANTA BAJA EDIFICIO CENTRAL	CISCO	AIR-LAP1262N-A-K9
AP-CENTRAL-PA2	PLANTA ALTA 2 EDIFICIO CENTRAL	CISCO	AIR-LAP1262N-A-K9

Tabla 61. Puntos de acceso inalámbrico alojados en la FICA

Fuente: Puntos de acceso inalámbrico instalados en la FICA -UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-FICA-PB	PLANTA BAJA FICA	CISCO	AIR-LAP1262N-A-K9
AP-FICA-PA2D	PLANTA ALTA 2 DERECHA FICA	CISCO	AIR-LAP1262N-A-K9
AP-FICA-PA2I	PLANTA ALTA 2 IZQUIERDA FICA	CISCO	AIR-LAP1262N-A-K9
AP-FICA-PA3D	PLANTA ALTA 3 DERECHA FICA	CISCO	AIR-LAP1262N-A-K9
AP-FICA-PA3I	PLANTA ALTA 3 IZQUIERDA FICA	CISCO	AIR-LAP1262N-A-K9
AP-FICA-PA4	PLANTA ALTA 4 FICA	CISCO	AIR-LAP1262N-A-K9

Tabla 62. Puntos de acceso inalámbrico alojados en la FACAE

Fuente: Puntos de acceso inalámbrico instalados en la FACAE -UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-FACAE-PA1	PLANTA ALTA 1 FACAE	CISCO	AIR-LAP1262N-A-K9
AP-FACAE-PA2	PLANTA ALTA 2 FACAE	CISCO	AIR-LAP1262N-A-K9
AP-FACAE-PA3	PLANTA ALTA 3 FACAE	CISCO	AIR-LAP1262N-A-K9

Tabla 63. Puntos de acceso inalámbrico alojados en la FECYT

Fuente: Puntos de acceso inalámbrico instalados en la FECYT -UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-FECYT-PA1	PLANTA ALTA 1 FECYT	CISCO	AIR-LAP1262N-A-K9
AP-FECYT-PA2	PLANTA ALTA 2 FECYT	CISCO	AIR-LAP1262N-A-K9
AP-FECYT-PA3	PLANTA ALTA 3 FECYT	CISCO	AIR-LAP1262N-A-K9

Tabla 64. Puntos de acceso inalámbrico alojados en Bienestar Universitario

Fuente: Puntos de acceso inalámbrico instalados en Bienestar Universitario -UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-BIENESTAR-PB	PLANTA BAJA BIENESTAR	CISCO	AIR-LAP1262N-A-K9
AP-BIENESTAR-PA1	PLANTA ALTA 1 BIENESTAR	CISCO	AIR-LAP1262N-A-K9
AP-BIENESTAR-PA2	PLANTA ALTA 2 BIENESTAR	CISCO	AIR-LAP1262N-A-K9
AP-BIENESTAR-PA3	PLANTA ALTA 3 BIENESTAR	CISCO	AIR-LAP1262N-A-K9

Tabla 65. Puntos de acceso inalámbrico alojados en exteriores  
Fuente: Puntos de acceso inalámbrico instalados en exteriores -UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-UTN-FICA-FICAYA	TERRAZA ENTRE FICA - FICAYA	CISCO	AIR-LAP1310G-A-K9
AP-UTN-CAI-FICAYA	TERRAZA ENTRE CAI-FICAYA	CISCO	AIR-BR1310G-A-K9-R
AP-UTN-FICA-FCCSS	TERRAZA ENTRE FICA - FCCSS	CISCO	AIR-LAP1310G-A-K9
AP-UTN-EDFISICA	ESTE - INSTITUTO EDUCACIÓN FÍSICA	CISCO	AIR-BR1310G-A-K9-R
AP-UTN-ESTE-AUDITORIO	ESTE - AUDITORIO AGUSTÍN CUEVA	CISCO	AIR-BR1310G-A-K9-R
AP-UTN-NORTE-AUDITORIO	NORTE - AUDITORIO AGUSTÍN CUEVA	CISCO	AIR-LAP1310G-A-K9
AP-UTN-SUR-CENTRAL	TERRAZA PLANTA CENTRAL SUR	CISCO	AIR-LAP1310G-A-K9
AP-UTN-NORTE-CENTRAL	TERRAZA PLANTA CENTRAL NORTE	CISCO	AIR-BR1310G-A-K9-R
AP-UTN-CAI-TERRAZA	TERRAZA CAI	CISCO	AIR-LAP1310G-A-K9
AP-UTN-SUR-FACAE	TERRAZA PLANTA 1 SUR FACAE	CISCO	AIR-BR1310G-A-K9-R
AP-UTN-NORTE-FACAE	TERRAZA PLANTA 1 NORTE FACAE	CISCO	AIR-BR1310G-A-K9-R
AP-UTN-FECYT	TERRAZA PLANTA 1 NORESTE FECYT	CISCO	AIR-BR1310G-A-K9-R
AP-UTN-OESTE-CENTRAL	TERRAZA PLANTA 1 OESTE EDIFICIO CENTRAL	CISCO	AIR-BR1310G-A-K9-R
AP-UTN-NORTE-ENTRADA	ENTRADA NORTE	CISCO	AIR-BR1310G-A-K9-R
AP-UTN-PISCINA	EXTERIOR COMPLEJO ACUÁTICO	CISCO	AIR-LAP1310G-A-K9

Tabla 66. Puntos de acceso inalámbrico alojados en la FICAYA  
Fuente: Puntos de acceso inalámbrico instalados en la FICAYA -UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-FICAYA-PA1	PLANTA ALTA 1 FICAYA	CISCO	AIR-LAP1262N-A-K9
AP-FICAYA-PA2	PLANTA ALTA 2 FICAYA	CISCO	AIR-LAP1262N-A-K9
AP-FICAYA-PA3	PLANTA ALTA 3 FICAYA	CISCO	AIR-LAP1262N-A-K9

Tabla 67. Puntos de acceso inalámbrico alojados en la FCCSS  
Fuente: Puntos de acceso inalámbrico instalados en la FCCSS –UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-FCCSS-PA1	PLANTA ALTA 1 FCCSS	CISCO	AIR-LAP1262N-A-K9
AP-FCCSS-PA2	PLANTA ALTA 2 FCCSS	CISCO	AIR-LAP1262N-A-K9
AP-FCCSS-PA3	PLANTA ALTA 3 FCCSS	CISCO	AIR-LAP1262N-A-K9

Tabla 68. Puntos de acceso inalámbrico alojados en el CAI  
Fuente: Puntos de acceso inalámbrico instalados en el CAI- UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-CAI-PA1	PLANTA ALTA 1 CAI	CISCO	AIR-LAP1262N-A-K9
AP-CAI-PA2	PLANTA ALTA 2 CAI	CISCO	AIR-LAP1262N-A-K9
AP-CAI-PA3	PLANTA ALTA 3 CAI	CISCO	AIR-LAP1262N-A-K9

Tabla 69. Puntos de acceso inalámbrico alojados en Postgrado  
Fuente: Puntos de acceso inalámbrico instalados en Postgrado-UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-POSTGRADO-PB1	PLANTA BAJA POSTGRADO CUBÍCULOS	CISCO	AIR-LAP1262N-A-K9
AP-POSTGRADO-PB2	PLANTA BAJA POSTGRADO	CISCO	AIR-LAP1262N-A-K9
AP-POSTGRADO-PB-AUDITORIO	PLANTA BAJA AUDITORIO POSTGRADO	CISCO	AIR-LAP1262N-A-K9
AP-POSTGRADO-PA1	PLANTA ALTA 1 POSTGRADO	CISCO	AIR-LAP1262N-A-K9
AP-POSTGRADO-PA2	PLANTA ALTA 2 POSTGRADO	CISCO	AIR-LAP1262N-A-K9

Tabla 70. Puntos de acceso inalámbrico Autónomos  
Fuente: Puntos de acceso inalámbrico Autónomos –UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-DDTI-UTN	DDTI EDIFICIO CENTRAL	CISCO	AIR-LAP1262N-A-K9
AP8	DDTI EDIFICIO CENTRAL	CISCO	AIR-LAP1262N-A-K9
AP11	DDTI EDIFICIO CENTRAL	CISCO	AIR-LAP1262N-A-K9

Tabla 71. Puntos de acceso inalámbrico alojados en áreas públicas  
Fuente: Puntos de acceso inalámbrico áreas públicas –UTN

NOMBRE	UBICACIÓN	MARCA	MODELO
AP-AUDITORIO-INTERIOR	AUDITORIO AGUSTÍN CUEVA (INTERIOR)	CISCO	AIR-LAP1262N-A-K9
AP-PISCINA-INTERIOR	INTERIOR COMPLEJO ACUÁTICO	CISCO	AIR-LAP1262N-A-K9
AP-POLIDEPORTIVO	POLIDEPORTIVO UTN	CISCO	AIR-LAP1262N-A-K9

## CAPITULO III

### ADMINISTRACIÓN DE SOFTWARE

#### 3.1 POLÍTICAS PARA MONITOREAR EQUIPOS LINUX

- Instalar el agente de monitoreo NRPE en el equipo LINUX para conocer sus características.
- Configurar el archivo `/etc/xinetd.d/nrpe` indicando la ip del servidor NAGIOS al cual se devolverá la información de los recursos del equipo.
- Configurar el archivo `/usr/local/nagios/etc/nrpe.cfg` con los comandos que ejecutaran los plugins que recogerán información del equipo y las condiciones para el envío de notificaciones.
- Configurar los comandos que ejecutarán los plugins en el archivo de configuración `/usr/local/nagios/etc/objects/commands.cfg` en el servidor NAGIOS.
- Definir los equipos y los servicios a monitorear desde el sistema NAGIOS en el directorio `/usr/local/nagios/etc/objects/hosts`.
- Seleccionar los grupos a los que pertenecerán cada equipo en la red y configurar las condiciones en las que se recibirán notificaciones del dispositivo en el directorio `/usr/local/nagios/etc/objects/`
- Configurar las cuentas de correo que recibirán las notificaciones emitidas por NAGIOS en el archivo `/usr/local/nagios/etc/objects/contacts`.
- Ejecutar el comando de comprobación de configuración `/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg` en el sistema NAGIOS, si los resultados son positivos reiniciar el servidor de monitoreo `/etc/init.d/nagios start`.

### 3.1.1 CONFIGURACIÓN DEL AGENTE DE MONITOREO

Antes de monitorear servicios privados y atributos de equipos LINUX se necesita instalar un agente de monitoreo llamado NRPE, que puede ser localizado en <http://exchange.nagios.org/directory/Addons/Monitoring-Agents/NRPE--2D-Nagios-Remote-Plugin-Executor/details>, de modo que el servidor NAGIOS con el plugin `check_nrpe` pueda recoger información del agente NRPE instalado en el equipo que se desea monitorear, véase la figura 27.

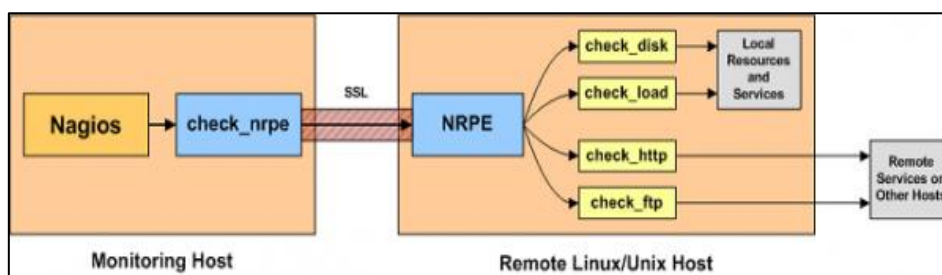


Figura 27. Funcionamiento del agente NRPE

Fuente: <http://nagios.sourceforge.net/docs/nagioscore/4/en/addons.html#nrpe>

Los equipos LINUX a monitorear deben tener instalados los plugin de modo que el agente devuelva al servidor NAGIOS la información obtenida con la ejecución de cada plugin.

En el archivo de configuración `/etc/xinetd.d/nrpe` en la línea `only_from` se debe indicar la dirección ip del servidor NAGIOS como se muestra en la figura 28 y en el archivo `/usr/local/nagios/etc/nrpe.cfg` se definen los comandos utilizados para los chequeos, cada línea representa la ejecución de un plugin que recogerá información específica del equipo LINUX, véase la figura 29, la tabla 72 describe la ejecución de cada plugin en los servidores LINUX monitoreados y las condiciones en las que se mostrarán mensajes de advertencia o peligro desde la web que posteriormente serán enviadas al correo electrónico del administrador de la red, esta configuración se debe utilizar en los nuevos equipos que se agreguen al sistema o modificarla según los nuevos requerimientos impuestos por el administrador.

```

# default: on
# description: NRPE (Nagios Remote Plugin Executor)
service nrpe

flags = REUSE
socket_type = stream
port = 5666
wait = no
user = nagios
group = nagios
server = /usr/local/nagios/bin/nrpe
server_args = -c /usr/local/nagios/etc/nrpe.cfg --inetd
log_on_failure += USERID
disable = no
only_from = 172.20.1.172

```

Figura 28. Archivo de configuración del agente NRPE  
Fuente: Configuración del agente en el servidor MOODLE

```

# The following examples use hardcoded command arguments...

command[check_users]=usr/lib64/nagios/plugins/check_users -w 5 -c 10
command[check_load]=usr/lib64/nagios/plugins/check_load -w 15,10,5 -c 30,25,20
command[check_disk]=usr/lib64/nagios/plugins/check_disk -w 20% -c 10% -p /dev/sda
command[check_zombie_procs]=usr/lib64/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_procs]=usr/lib64/nagios/plugins/check_procs -w 350 -c 450
command[check_ssh]=usr/local/nagios/libexec/check_ssh 127.0.0.1
command[check_swap]=usr/local/nagios/libexec/check_swap -w 50% -c 0%
command[check_tcptraffice]=usr/lib/nagios/plugins/contrib/check_tcptraffice -i eth0 -s 100 -w 1310720 -c 1835008
command[check_lm_sensors]=usr/local/nagios/libexec/check_lm_sensors --high 'Core 0'=60,80 --high 'Core 1'=60,80
command[check_linux_stats.pl]=usr/local/nagios/libexec/check_linux_stats.pl -C -w 60 -c 80
command[check_mem]=usr/local/nagios/libexec/check_mem -w 60 -c 80
command[check_http]=usr/local/nagios/libexec/check_http -H 172.20.1.240 -p 888 -u http://172.20.1.240:888/fica/moodle/
command[check_http_internet]=usr/local/nagios/libexec/check_http_internet -H youtube.com -u http://www.youtube.com

```

Figura 29. Archivo de configuración nrpe.cfg  
Fuente: Configuración del agente en el servidor MOODLE

Tabla 72. Descripción de la ejecución de plugin en el agente NRPE  
Fuente: Plugin instalados en el servidor MOODLE

EJECUCIÓN DE PLUGIN	DESCRIPCIÓN
check_users -w 5 -c 10	Chequea el número de usuarios logueados en el sistema, muestra un mensaje de advertencia si el número de usuarios supera los 5 y un crítico si supera los 10.
check_ping!100.0,20%!500.0,60%	Chequea el estado del equipo en base a paquetes ICMP, muestra un mensaje de advertencia si el tiempo promedio de ida y vuelta es mayor a 200 ms o la pérdida de paquetes es mayor al 20 % y un crítico si el tiempo promedio de ida y vuelta es mayor a 600 ms o la pérdida de paquetes es mayor al 60 %
check_load -w 15,10,5 -c 30,25,20	Chequea la carga de la CPU en el minuto 1,5 y 15, muestra un mensaje de advertencia si la carga supera los valores 15,10,5 y un crítico si supera los valores 30,25,20.
check_disk -w 10% -c 5% -p /dev/sda	Chequea el uso de disco, muestra un mensaje de advertencia si el espacio libre es menor 10% y un crítico si es menor a 5%.
check_procs -w 5 -c 10 -s Z	Chequea el número de procesos zombis, muestra un mensaje de advertencia si el número es mayor a 5 y un crítico si es mayor a 10.
check_procs -w 250 -c 400	Chequea el número de procesos ejecutándose, muestra un mensaje de advertencia si el número es mayor a 350 y un crítico si es mayor a 450.
check_ssh 127.0.0.1	Chequea el estado del servicio SSH en el equipo local.
check_swap -w 95% -c 90%	Chequea el uso de memoria swap, muestra un mensaje de advertencia si el espacio libre es menor 95% y un crítico si es menor al 90%.
check_tcptraffice -i eth0 -s 100 -w 1310720 -c 1835008	Chequea el consumo de ancho de banda en la interfaz eth0, muestra un mensaje de advertencia si el tráfico es mayor a 10 Mb y un crítico si es mayor a 14 Mb.
check_lm_sensors --high 'Core 0'=50,60 --high 'Core 1'=50,60	Chequea la temperatura de cada core del procesador, muestra un mensaje de advertencia si la temperatura es mayor a los 50 °C y un crítico si es mayor al 60°C.
check_linux_stats.pl -C -w 60 -c 80	Chequea el uso del procesador, muestra un mensaje de advertencia si el uso es mayor al 60% y un crítico si es mayor al 80%.
check_mem -w 60 -c 80	Chequea el uso de memoria RAM, muestra un mensaje de advertencia si el uso es mayor al 60% y un crítico si es mayor al 80%.
check_http -H 172.20.1.240 -p 888 -u http://172.20.1.240:888/fica/moodle/	Chequea el acceso web al servidor Moodle, muestra un mensaje de crítico si se pierde el acceso.
libexec/check_http_internet -H youtube.com -u http://www.youtube.com	Chequea el acceso web al servidor YouTube, muestra un mensaje de crítico si se pierde la conexión a internet.



### 3.1.2 PLUGIN

Son archivos escritos en PHP que permiten recoger información específica en un equipo LINUX, los plugin utilizados para realizar los chequeos se encuentran ubicados en el directorio `/usr/local/nagios/libexec`, la tabla 73 describe cada uno de los plugin utilizados por el sistema NAGIOS para monitorear los servidores LINUX alojados en la FICA y deben ser utilizados para monitorear cualquier nuevo equipo LINUX que se agregue al sistema.

Tabla 73. Plugin utilizados en equipos LINUX  
Fuente: Plugin instalados en el servidor MOODLE

PLUGIN	DESCRIPCIÓN
check_nrpe	Recoge información del agente NRPE
check_ssh	Chequea el servicio SSH
check_http	Chequea el servicio web
check_tcptraffic	Chequea el tráfico que cursa por la interfaz
check_swap	Chequea la memoria swap
check_disk	Chequea la unidad de disco
check_users	Chequea el número de usuarios logueados en el sistema
check_load	Chequea la carga de la CPU
check_linux_stats.pl	Chequea la utilidad de la CPU
check_procs	Chequea el número de procesos ejecutándose
check_lm_sensors	Chequea la temperatura del procesador
check_mem	Chequea el uso de memoria RAM
check_ping	Chequea el estado del equipo a través de paquetes ICMP

### 3.1.3 CONFIGURACIÓN DE COMANDOS

Para conocer el funcionamiento de los servidores LINUX monitoreados el servidor NAGIOS utiliza comandos pre definidos para la ejecución de los plugin, el archivo que almacena los comandos está ubicado en `/usr/local/nagios/etc/import/commands.cfg`, los comandos utilizan macros que son variables definidas por el sistema, los macros utilizados son los siguientes.

- `$USER1$`: Define la ubicación del plugin que será ejecutado por el comando, inicia la línea de comando y por defecto apunta al directorio `/usr/local/nagios/libexec`, esta ubicación se puede cambiar en el archivo `/usr/local/nagios/etc/resource.cfg`.

- **\$HOSTADDRESS\$**: Define la dirección ip del equipo a monitorear, es precedido del indicador -H, el directorio que contiene la definición de todos los equipos se encuentra en /usr/local/nagios/etc/import/hosts.
- **\$ARG1\$**: Es una variable que representa valores establecidos en la definición del servicio para poder ejecutar un plugin, es precedido del indicador -c.

Para monitorear equipos LINUX se deben configurar comandos de ejecución como se indica en la tabla 74 para cada servicio monitoreado, solo se debe cambiar el parámetro `command_name` y `command_line` para la configuración de cada comando que se agregue al sistema.

Tabla 74. Ejemplo de configuración de comando en servicios LINUX  
Fuente: Comandos configurados en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define command{		Inicia la definición
command_name	check_local_disk	Especifica el nombre del comando
command_line	\$USER1\$/check_disk -w \$ARG1\$ -c \$ARG2\$ -p \$ARG3\$	Especifica cómo se ejecutará el comando
}		

La tabla 54 muestra la configuración del parámetro `command_line`, véase la tabla 75, para cada comando configurado en el sistema NAGIOS, estos comandos permiten el chequeo de los servicios ejecutados en los servidores LINUX monitoreados en la UTN y se deben utilizar para monitorear cualquier nuevo equipo LINUX que se agregue al sistema.

Tabla 75. Ejecución de comandos para equipos LINUX  
Fuente: Comandos configurados en el servidor NAGIOS

PLUGIN	LÍNEA DE COMANDO
check_ssh	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_http	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_tcptraffic	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_swap	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_disk	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_users	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_load	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_linux_stats.pl	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_procs	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_lm_sensors	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_mem	\$USER1\$/check_nrpe -H \$HOSTADDRESS\$ -c \$ARG1\$
check_ping	check_ping!100.0,20%!500.0,60%

### 3.1.4 CONFIGURACIÓN DE PLANTILLAS PARA EQUIPOS

NAGIOS maneja la configuración de equipos en base a plantillas, las plantillas son pre configuraciones que se heredan a las nuevas configuraciones y definiciones de equipos con solo utilizar el nombre que se le ha asignado. Las plantillas para equipos se encuentran en el archivo `/usr/local/nagios/etc/import/hosttemplates.cfg`. La tabla 76 describe la plantilla base utilizada para configurar el monitoreo de los servidores LINUX alojados en la FICA y se debe utilizar para configurar los nuevos equipos LINUX que se agreguen al sistema, no se debe cambiar ningún parámetro de esta plantilla ya que cambiaría el correcto funcionamiento del sistema.

Tabla 76. Plantilla base para la configuración de equipos LINUX (generic-host-server)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define host{		Inicia la definición
name	generic-host-server	Especifica el nombre de la plantilla
notifications_enabled	1	Activa las notificaciones para el equipo. 1: activa, 0: desactiva
event_handler_enabled	1	Activa el controlador de eventos del sistema. 1: activa, 0: desactiva
flap_detection_enabled	1	Activa la detección de flapeo en el estado del equipo. 1: activa, 0: desactiva
process_perf_data	1	Activa el procesamiento de los datos de rendimiento. 1: activa, 0: desactiva
retain_status_information	1	Activa el almacenamiento de información con el estado del equipo antes de un reinicio. 1: activa, 0: desactiva
retain_nonstatus_information	1	Activa el almacenamiento del resto de información del equipo antes de un reinicio. 1: activa, 0: desactiva
notification_period	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones.
register	0	Desactiva el registro de la información. 1: activa, 0: desactiva
}		Finaliza la definición

La plantilla de configuración de equipos linux-server, véase la tabla 77, hereda la pre configuración de la plantilla base generic-host-server, véase la tabla 76, por medio del parámetro use, la tabla 77 muestra la configuración realizada para el monitoreo de los servidores LINUX alojados en la FICA, esta configuración se realizó en base a los requerimientos de monitoreo establecidos por el administrador de la red y en caso de querer modificar esta configuración se debe cambiar solo los parámetros en negrita.

Tanto la plantilla linux-server como generic-host-server se debe utilizar para configurar el monitoreo de los nuevos equipos Linux que se agreguen al sistema NAGIOS.

Tabla 77. Plantilla de configuración de equipos LINUX (linux-server)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define host{		Inicia la definición
name	linux-server	Especifica el nombre de la plantilla
use	generic-host-server	Especifica el nombre de la plantilla que se hereda
check_period	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para chequear el estado del equipo.
<b>check_interval</b>	5	Especifica el intervalo de tiempo (min) entre cada chequeo mientras el equipo devuelva un estado up
<b>retry_interval</b>	1	Especifica el intervalo de tiempo (min) entre cada chequeo si el equipo devuelve un estado no up
<b>max_check_attempts</b>	10	Especifica el número de veces que se ejecutara el comando de verificación si el equipo cambia a un estado no up
check_command	check-host-alive	Especifica el nombre del comando que comprobará el estado del equipo
<b>notification_period</b>	Workhours	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones.
<b>notification_interval</b>	60	Especifica el periodo de tiempo para volver a notificar al contacto
notification_options	d,u,r	Especifica el tipo de notificación a enviar d:dawn, u:unreachable, r: up
<b>contact_groups</b>	admins	Especifica el nombre del grupo de contacto al que se enviarán las notificaciones
register	0	Desactiva el registro de la información.
}		Finaliza la definición

### 3.1.5 CONFIGURACIÓN DE PLANTILLAS PARA SERVICIOS

La configuración de los servicios monitoreados en el sistema NAGIOS se realiza en base a plantillas, que son pre configuraciones que se heredan a las nuevas configuraciones y definiciones de servicios con solo utilizar el nombre que se le ha asignado. Las plantillas de configuración para el chequeo de servicios ejecutados en equipos LINUX como por ejemplo el consumo de recursos de hardware o consumo de ancho de banda se encuentran en el archivo /usr/local/nagios/etc/import/servicetemplates.cfg. La tabla 78 describe la plantilla de configuración base utilizada para monitorear los servicios ejecutados en los servidores LINUX de la FICA y se debe utilizar en la configuración de los servicios en los nuevos equipos que se agreguen al sistema, no se debe cambiar ningún parámetro de esta plantilla ya que cambiaría el correcto funcionamiento del sistema.

Tabla 78. Plantilla base para la configuración de servicios LINUX (generic-service)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define service{		Inicia la definición
name	generic-service	Especifica el nombre de la plantilla
active_checks_enabled	1	Activa los controles activos. 1: activa, 0: desactiva
passive_checks_enabled	1	Activa los controles pasivos. 1: activa, 0: inactiva
parallelize_check	1	Activa la comprobación de servicios paralelamente
obsess_over_service	0	Desactiva la ejecución de comandos después de cada chequeo
check_freshness	0	Desactiva los controles de frescura para los chequeos pasivos.
notifications_enabled	1	Activa las notificaciones para el servicio. 1: activa, 0: desactiva
event_handler_enabled	1	Activa el controlador de eventos del sistema. 1: activa, 0: desactiva
flap_detection_enabled	1	Activa la detección de flapeo en el estado del servicio. 1: activa, 0: desactiva
process_perf_data	1	Activa el procesamiento de los datos de rendimiento. 1: activa, 0: desactiva
retain_status_information	1	Activa el almacenamiento de información con el estado del servicio antes de un reinicio. 1: activa, 0: desactiva
retain_nonstatus_information	1	Activa el almacenamiento del resto de información del servicio antes de un reinicio. 1: activa, 0: desactiva
is_volatile	0	Desactiva el servicio como volátil
check_period	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para chequear el estado del servicio.
max_check_attempts	3	Especifica el número de veces que se ejecutará el comando de verificación si el servicio devuelve un estado no aceptable.
normal_check_interval	1	Especifica el intervalo de tiempo (min) entre cada chequeo mientras el servicio devuelva un estado aceptable
retry_check_interval	2	Especifica el intervalo de tiempo (min) entre cada chequeo si el servicio cambia a un estado no aceptable
contact_groups	admins	Especifica el nombre del grupo de contacto al que se enviarán las notificaciones
notification_options	w,u,c,r	Especifica el tipo de notificación a enviar w:warning, u:unknown, c:critical, r: ok
notification_interval	60	Especifica el periodo de tiempo para volver a notificar al contacto
notification_period	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones.
register	0	Desactiva el registro de la información.
}		Finaliza la definición

La plantilla de configuración de servicios local-service, véase la tabla 79, hereda la pre configuración de la plantilla base generic-service, véase la tabla 78, por medio del parámetro use, la tabla 79 muestra la configuración realizada para el monitoreo de los servicios ejecutados en los servidores LINUX alojados en la FICA como por ejemplo el consumo de recursos de hardware o consumo de ancho de banda, esta configuración se realizó en base a los requerimientos de monitoreo establecidos por el administrador de la red y en caso de querer modificar esta configuración se deben cambiar solo los parámetros en negrita.

Tanto la plantilla local-service como generic-service se debe utilizar para la configuración de los servicios ejecutados en los nuevos equipos LINUX que se agreguen al sistema.

Tabla 79. Plantilla de configuración de servicios (local-service)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define service{		Inicia la definición
name	local-service	Especifica el nombre de la plantilla
use	generic-service	Especifica el nombre de la plantilla con la configuración a heredar
<b>max_check_attempts</b>	4	Especifica el número de veces que se ejecutará el comando de verificación si el servicio devuelve un estado no aceptable.
<b>normal_check_interval</b>	1	Especifica el intervalo de tiempo (min) entre cada chequeo mientras el servicio devuelve un estado aceptable
<b>retry_check_interval</b>	1	Especifica el intervalo de tiempo (min) entre cada chequeo si el servicio cambia a un estado no aceptable
register	0	Desactiva el registro de la información
}		Finaliza la definición

### 3.1.6 DEFINICIÓN DE EQUIPOS

Para agregar un nuevo equipo LINUX al sistema de monitoreo es necesario definir los parámetros que se indican en la tabla 80, solo se deberá cambiar la definición de los parámetros en negrita para cada nuevo equipo, el parámetro use permite heredar la pre configuración establecida en la plantilla linux-server, véase la tabla 77. La definición de cada equipos se realiza en el directorio /usr/local/nagios/etc/import/hosts.

Tabla 80. Ejemplo de definición de equipo (servidor-moodle)  
Fuente: Archivo de definición de quipos en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN	DESCRIPCIÓN
define host{		Inicia la definición
use	linux-server	Especifica el nombre de la plantilla que se hereda
<b>host_name</b>	Serv-Moodle	Especifica el nombre del equipo
<b>alias</b>	Servidor-Moodle	Especifica el alias del equipo
<b>address</b>	x.x.x.x	Especifica la dirección ip del equipo
hostgroups	Servidores-FICA	Especifica el nombre del grupo al que pertenece el equipo
parents	sw-Fica	Especifica el equipo del padre
<b>icon_image</b>	./vendors/centos.gif	Especifica la imagen utilizada como icono en la interfaz web
<b>icon_image_alt</b>	Servidor-Moodle	Especifica el nombre para el icono utilizado en la interfaz web
<b>statusmap_image</b>	./vendors/centos.gd2	Especifica la imagen mostrada en el mapa de red
}		Finaliza la definición

### 3.1.7 DEFINICIÓN DE SERVICIOS

Para agregar el monitoreo de los servicios ejecutados en un equipo LINUX como el consumo de recursos de hardware o ancho de banda al sistema NAGIOS es necesario definir los parámetros que se indican en la tabla 81, el parámetro host\_name debe cambiar para cada equipo mientras que el parámetro use permite heredar la pre configuración establecida en la

plantilla local-service, véase la tabla 79. La definición de servicios se realiza en el directorio /usr/local/nagios/etc/import/services.

El parámetro check\_command define la ejecución del plugin check\_nrpe, véase la tabla 81, el valor seguido del signo de exclamación es el nombre del plugin que reemplazará el argumento establecido en la configuración de comandos (\$ARG1\$) como se muestra en la tabla 54.

Tabla 81. Ejemplo de definición de servicio (servidor-Moodle)  
Fuente: Archivo de definición de servicios en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN	DESCRIPCIÓN
define service{		Inicia la definición
use	local-service	Especifica el nombre de la plantilla que se hereda
host_name	Serv-Moodle	Especifica el nombre del equipo
service_description	09.Usuarios	Especifica la descripción del servicio a chequear
check_command	check_nrpe!check_users	Especifica el comando que ejecutará el servicio
}		Finaliza la definición

Cada vez que se requiera chequear un nuevo servicio en el mismo equipo bastará definir el servicio como se indica en la tabla 81, cambiando solo la definición del parámetro check\_command con cada una de las definiciones establecidas en la tabla 82, cada definición permite el chequeo de un servicio específico, la descripción de cada plugin utilizado por el sistema NAGIOS para monitorear los servicios ejecutados en los servidores LINUX de la FICA se muestra en la tabla 73 y se deben utilizar para monitorear los nuevos equipos LINUX que se agreguen al sistema.

Tabla 82. Definición del parámetro check\_command para servicios LINUX  
Fuente: Definición de servicios en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN
check_command	check_ping!100.0,20%!500.0,60%
check_command	check_nrpe!check_disk
check_command	check_nrpe!check_users
check_command	check_nrpe!check_procs
check_command	check_nrpe!check_load
check_command	check_nrpe!check_swap
check_command	check_nrpe!check_ssh
check_command	check_nrpe!check_http
check_command	check_nrpe!check_tcptraffic
check_command	check_nrpe!check_lm_sensors
check_command	check_nrpe!check_mem
check_command	check_nrpe!check_linux_stats.pl

## 3.2 POLÍTICAS PARA MONITOREAR SWITCHES

- Habilitar el protocolo SNMPv1 o SNMPv2 en el equipo indicando la comunidad de administración y los permisos que pueden ser de lectura o escritura.
- Configurar los comandos que ejecutarán los plugins en el archivo de configuración `/usr/local/nagios/etc/objects/commands.cfg` en el servidor NAGIOS.
- Definir los equipos y los servicios a monitorear desde el sistema NAGIOS en el directorio `/usr/local/nagios/etc/objects/hosts`.
- Seleccionar los grupos a los que pertenecerán cada equipo en la red y configurar las condiciones en las que se recibirán notificaciones del dispositivo en el directorio `/usr/local/nagios/etc/objects/`
- Configurar las cuentas de correo que recibirán las notificaciones emitidas por NAGIOS en el archivo `/usr/local/nagios/etc/objects/contacts`.
- Ejecutar el comando de comprobación de configuración `/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg` en el sistema NAGIOS, si los resultados son positivos reiniciar el servidor de monitoreo `/etc/init.d/nagios start`.

### 3.2.1 CONFIGURACIÓN DE AGENTES DE MONITOREO

Los switches y routers pueden ser monitoreados utilizando SNMP para solicitar información sobre su estado, véase la figura 30, para esto es necesario habilitar el protocolo SNMP en el equipo y establecer el nombre de la comunidad con privilegios de lectura o escritura, la configuración que se utilizó en los equipos monitoreados dentro de la UTN fue de solo lectura con la finalidad de impedirle al sistema de monitoreo o a cualquier otro usuario realizar modificaciones en la configuración de los equipos monitoreados ya que así lo dispuso el administrador de la red por motivos de seguridad.



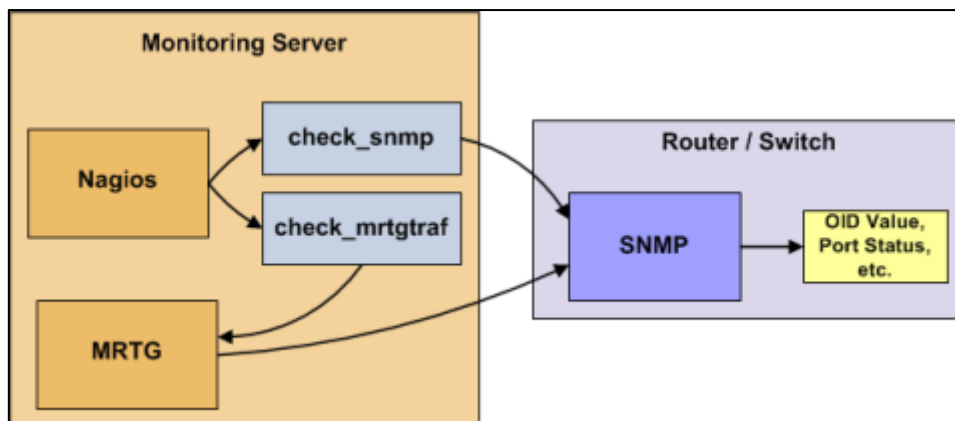


Figura 30. Monitoreo de routers y switches utilizando SNMP

Fuente: <http://nagios.sourceforge.net/docs/nagioscore/4/en/monitoring-routers.html>

Para habilitar el protocolo SNMP en equipos CISCO y LINKSYS se debe escribir el siguiente comando:

- SW(config)#snmp-server community XXX RO

En equipos 3COM se debe acceder a system-management-snmp-community y escribir el nombre de la comunidad en el usuario monitor, este usuario por defecto tiene privilegios de lectura, la figura 31 y 32 muestra el procedimiento.

```

-----Sw 6 Rack Derecho Planta C., SW 6 Rack Derecho Planta C. (1)
enu options: -----3Com SuperStack 3 Switch 4200-----
bridge          - Administer bridge-wide parameters
gettingStarted  - Basic device configuration
logout          - Logout of the Command Line Interface
physicalInterface - Administer physical interfaces
protocol        - Administer protocols
security        - Administer security
system         - Administer system-level functions
trafficManagement - Administer traffic management

Type ? for help
-----Sw 6 Rack Derecho Planta C., SW 6 Rack Derecho Planta C. (1)
                                                    elect menu option: system

Menu options: -----3Com SuperStack 3 Switch 4200-----
control         - Administer system control
inventory       - Stack information
management     - Administer system management
summary        - Display summary information
unit           - Administer unit

Type "quit" to return to the previous menu or ? for help
-----Sw 6 Rack Derecho Planta C., SW 6 Rack Derecho Planta C. (1)
                                                    elect menu option (system): management

```

Figura 31. Habilitando SNMP en switch 3com, paso 1

Fuente: Configuración de switch 3com

```

Menu options: -----3Com SuperStack 3 Switch 4200-----
alert          - Administer email/pager alerts
contact        - Set the system contact
location       - Set the system location
monitor        - Administer monitored items
name           - Set the system name
password       - Set the system password
remoteAccess   - Change remote access permissions
snmp           - Administer SNMP

Type "quit" to return to the previous menu or ? for help
-----Sw 6 Rack Derecho Planta C., SW 6 Rack Derecho Planta C. (1)
                                                                    elect menu option (system/management): snmp

Menu options: -----3Com SuperStack 3 Switch 4200-----
community      - Set the SNMP community string
get            - Get SNMP objects
next           - Getnext SNMP objects
set            - Set SNMP objects
trap           - Administer SNMP trap destinations

Type "quit" to return to the previous menu or ? for help
-----Sw 6 Rack Derecho Planta C., SW 6 Rack Derecho Planta C. (1)
                                                                    elect menu option (system/management/snmp): community

Enter new community for user 'admin' [1]:
Enter new community for user 'manager' [2]:
Enter new community for user 'monitor' [utn]: utn
    
```

Figura 32. Habilitando SNMP en switch 3COM, paso 2  
 Fuente: Configuración de switch 3COM

### 3.2.2 PLUGIN

Son archivos escritos en PHP que permiten recoger información específica del switch, los plugin utilizados para realizar los chequeos se encuentran ubicados en el directorio /usr/local/nagios/libexec, la tabla 83 describe cada uno de los plugin utilizados para el monitoreo de los servicios ejecutados en los switches que conforman la capa de acceso y distribución en la red de datos de la UTN y deben ser utilizados para monitorear los nuevos equipos que se agreguen al sistema NAGIOS.

Tabla 83. Plugin utilizados en switches  
 Fuente: Plugin instalados en el servidor NAGIOS

PLUGIN	DESCRIPCIÓN
check_iftraffic43a	Chequea el tráfico que cursa por una interfaz física o virtual
check_ping	Chequea el estado del equipo a través de paquetes ICMP
check_snmp_mem.pl	Chequea el uso de memoria RAM
check-cisco.pl	Chequea el uso de la CPU
check-cisco.pl	Chequea el estado de los ventiladores
check-cisco.pl	chequea el estado de la fuente
check_snmp	Chequea el tiempo que permanece encendido el equipo
check_snmp	Chequea el estado de una interfaz

### 3.2.3 CONFIGURACIÓN DE COMANDOS

Los comandos son utilizados por el sistema de monitoreo para la ejecución de los plugin que permiten conocer el funcionamiento de un switch en la red, el archivo que almacena los

comandos está ubicado en `/usr/local/nagios/etc/import/commands.cfg`, los comandos utilizan macros que son variables definidas por el sistema, los macros utilizados son los siguientes.

- `$USER1$`: Define la ubicación del plugin que será ejecutado por el comando, inicia la línea de comando y por defecto apunta al directorio `/usr/local/nagios/libexec`, esta ubicación se puede cambiar en el archivo `/usr/local/nagios/etc/resource.cfg`.
- `$HOSTADDRESS$`: Define la dirección IP del equipo a monitorear, es precedido del indicador `-H`, el archivo que contiene la definición de todos los equipos se encuentra en `/usr/local/nagios/etc/import/hosts`.
- `$ARG1$`: Es una variable que representa valores establecidos en la definición del servicio para poder ejecutar un plugin, puede haber más de uno y en la secuencia `$ARG1$`, `$ARG2$`, etc.

Para monitorear equipos de conmutación se deben configurar comandos de ejecución como se indica en la tabla 84 para cada nuevo servicio monitoreado, solo se debe cambiar el parámetro `command_name` y `command_line` para la configuración de cada comando que se agregue al sistema.

Tabla 84. Ejemplo de configuración de comandos para switches  
Fuente: Comandos configurados en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
<code>define command{</code>		Inicia la definición
<code>command_name</code>	<code>check_snmp_memcorecent</code>	Especifica el nombre del comando
<code>command_line</code>	<code>\$USER1\$/check_snmp_mem.pl -H \$HOSTADDRESS\$ \$ARG1\$</code>	Especifica cómo se ejecutará el comando
<code>}</code>		

La tabla 64 muestra la configuración del parámetro `command_line`, véase la tabla 85, para cada comando configurado en el sistema NAGIOS, estos comandos permiten el chequeo de los servicios ejecutados en los switches de la capa de acceso y distribución en la UTN y se deben utilizar para monitorear cualquier nuevo switch que se agregue al sistema.

Tabla 85. Ejecución de comandos para switches

Fuente: Comandos configurados en el servidor NAGIOS

PLUGIN	LÍNEA DE COMANDO
check_iftraffic43a	\$USER1\$/ check_iftraffic43a -H \$HOSTADDRESS\$ \$ARG1\$ \$ARG2\$ \$ARG3\$
check_ping	\$USER1\$/check_ping -H \$HOSTADDRESS\$ -w \$ARG1\$ -c \$ARG2\$ -p 5
check_snmp_mem.pl	\$USER1\$/check_snmp_mem.pl -H \$HOSTADDRESS\$ \$ARG1\$
check-cisco.pl	\$USER1\$/check-cisco.pl -H \$HOSTADDRESS\$ \$ARG1\$
check-cisco.pl	\$USER1\$/check-cisco.pl -H \$HOSTADDRESS\$ \$ARG1\$
check-cisco.pl	\$USER1\$/check-cisco.pl -H \$HOSTADDRESS\$ \$ARG1\$
check_snmp	\$USER1\$/ check_snmp -H \$HOSTADDRESS\$ \$ARG1\$
check_snmp	\$USER1\$/ check_snmp -H \$HOSTADDRESS\$ \$ARG1\$

### 3.2.4 CONFIGURACIÓN DE PLANTILLAS PARA EQUIPOS

La configuración de equipos se realiza en base a plantillas, las plantillas son pre configuraciones que se heredan a las nuevas configuraciones y definiciones de un switch, con solo utilizar el nombre que se le ha asignado. Las plantillas se encuentran en el archivo `/usr/local/nagios/etc/import/hosttemplates.cfg`.

La tabla 86 describe la plantilla base utilizada para configurar el monitoreo de los switches dentro de la red de datos de la UTN y se debe utilizar para configurar los nuevos equipos de conmutación que se agreguen al sistema, no se debe cambiar ningún parámetro de esta plantilla ya que cambiaría el correcto funcionamiento del sistema.

Tabla 86. Plantilla base para la configuración de switches (generic-host-switch)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define host{		Inicia la definición
name	generic-host-switch	Especifica el nombre de la plantilla
notifications_enabled	1	Activa las notificaciones para el equipo. 1: activa, 0: desactiva
event_handler_enabled	1	Activa el controlador de eventos del sistema. 1: activa, 0: desactiva
flap_detection_enabled	1	Activa la detección de flapeo en el estado del equipo. 1: activa, 0: desactiva
failure_prediction_enabled	1	Se elimino
process_perf_data	1	Activa el procesamiento de los datos de rendimiento. 1: activa, 0: desactiva
retain_status_information	1	Activa el almacenamiento de información con el estado del equipo antes de un reinicio. 1: activa, 0: desactiva
retain_nonstatus_information	1	Activa el almacenamiento del resto de información del equipo antes de un reinicio. 1: activa, 0: desactiva
notification_period	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones.
register	0	Desactiva el registro de la información. 1: activa, 0: desactiva
}		Finaliza la definición

La plantilla de configuración de switches, generic-switch, véase la tabla 87, hereda la pre configuración de la plantilla base, generic-host-switch, véase la tabla 86, por medio del parámetro use, la tabla 87 muestra la configuración realizada para el monitoreo de los

equipos de conmutación alojados en la UTN, esta configuración se realizó en base a los requerimientos de monitoreo establecidos por el administrador de la red y en caso de querer modificar esta configuración se debe cambiar solo los parámetros en negrita.

Tanto la plantilla generic-switch como generic-host-switch se debe utilizar para configurar el monitoreo de los nuevos equipos de conmutación que se agreguen al sistema NAGIOS.

Tabla 87. Plantilla de configuración de switches  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define host{		Inicia la definición
name	generic-switch	Especifica el nombre de la plantilla
use	generic-host-switch	Especifica el nombre de la plantilla con la configuración a heredar
<b>check_period</b>	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para chequear el estado del equipo.
<b>check_interval</b>	5	Especifica el intervalo de tiempo (min) entre cada chequeo mientras el equipo devuelva un estado up
<b>retry_interval</b>	1	Especifica el intervalo de tiempo (min) entre cada chequeo si el equipo devuelve un estado no up
<b>max_check_attempts</b>	10	Especifica el número de veces que se ejecutara el comando de verificación si el equipo cambia a un estado no up
check_command	check-host-alive	Especifica el nombre del comando que comprobará el estado del equipo
<b>notification_period</b>	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones.
<b>notification_interval</b>	60	Especifica el periodo de tiempo para volver a notificar al contacto
notification_options	d,r	Especifica el tipo de notificación a enviar d:dawn, u:unreachable, r: up
<b>contact_groups</b>	admins	Especifica el nombre del grupo de contacto al que se enviarán las notificaciones
register	0	Desactiva el registro de la información.
}		Finaliza la definición

### 3.2.5 CONFIGURACIÓN DE PLANTILLAS PARA SERVICIOS

Dentro del sistema NAGIOS la configuración de los servicios monitoreados en los equipos de conmutación se realiza en base a plantillas, las plantillas contienen configuraciones que se heredan a las nuevas definiciones de servicios con solo utilizar el nombre que se le ha asignado, estas plantillas se encuentran ubicadas en el archivo /usr/local/nagios/etc/import/servicetemplates.cfg. La tabla 88 describe la plantilla de configuración utilizada para monitorear los servicios ejecutados en los equipos de conmutación en la red de datos de la UTN tales como el consumo de recursos de hardware o consumo de ancho de banda y se debe utilizar en la configuración de los servicios en los nuevos equipos que se agreguen al sistema, la configuración de esta plantilla se realizó en

base a los requerimientos de monitoreo establecidos por el administrador de la red y en caso de querer modificar esta configuración se debe cambiar solo los parámetros en negrita.

Tabla 88. Plantilla de configuración de servicios en switches (generic-service)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define service{		Inicia la definición
name	generic-service	Especifica el nombre de la plantilla
active_checks_enabled	1	Activa los controles activos. 1: activa, 0: desactiva
passive_checks_enabled	1	Activa los controles pasivos. 1: activa, 0: inactiva
parallelize_check	1	Activa la comprobación de servicios paralelamente
obsess_over_service	0	Desactiva la ejecución de comandos después de cada chequeo
check_freshness	0	Desactiva los controles de frescura para los chequeos pasivos.
notifications_enabled	1	Activa las notificaciones para el servicio. 1: activa, 0: desactiva
event_handler_enabled	1	Activa el controlador de eventos del sistema. 1: activa, 0: desactiva
flap_detection_enabled	1	Activa la detección de flapeo en el estado del servicio. 1: activa, 0: desactiva
process_perf_data	1	Activa el procesamiento de los datos de rendimiento. 1: activa, 0: desactiva
retain_status_information	1	Activa el almacenamiento de información con el estado del servicio antes de un reinicio. 1: activa, 0: desactiva
retain_nonstatus_information	1	Activa el almacenamiento del resto de información del servicio antes de un reinicio. 1: activa, 0: desactiva
is_volatile	0	Desactiva el servicio como volátiles
check_period	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para chequear el estado del servicio.
<b>max_check_attempts</b>	3	Especifica el número de veces que se ejecutará el comando de verificación si el servicio devuelve un estado no aceptable.
<b>normal_check_interval</b>	1	Especifica el intervalo de tiempo (min) entre cada chequeo mientras el servicio devuelva un estado aceptable
<b>retry_check_interval</b>	2	Especifica el intervalo de tiempo (min) entre cada chequeo si el servicio cambia a un estado no aceptable
<b>contact_groups</b>	admins	Especifica el nombre del grupo de contacto al que se enviarán las notificaciones
notification_options	w,u,c,r	Especifica el tipo de notificación a enviar w:warning, u:unknown, c: critical, r: ok
<b>notification_interval</b>	60	Especifica el periodo de tiempo para volver a notificar al contacto
notification_period	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones.
register	0	Desactiva el registro de la información.
}		Finaliza la definición

### 3.2.6 DEFINICIÓN DE EQUIPOS

Para agregar un nuevo equipo de conmutación al sistema de monitoreo es necesario definir los parámetros que se indican en la tabla 89, solo se debe cambiar la definición de los parámetros en negrita para cada nuevo equipo, el parámetro use permitirá heredar la pre configuración establecida en la plantilla generic-switch, véase la tabla 87. La definición de equipos se realiza en el directorio /usr/local/nagios/etc/import/hosts.

Tabla 89. Ejemplo de definición de equipo (sw-Fica)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN	DESCRIPCIÓN
define host{		Inicia la definición
use	generic-switch	Especifica el nombre de la plantilla que se hereda
<b>host_name</b>	sw-Fica	Especifica el nombre del equipo
<b>alias</b>	sw-Fica	Especifica el alias del equipo
<b>address</b>	x.x.x.x	Especifica la dirección ip del equipo

hostgroups	Switches-FICA	Especifica el nombre del grupo al que pertenece el equipo
parents	Serv-Nagios	Especifica el equipo del padre
icon_image	./ng-switch40.gif	Especifica la imagen utilizada como icono en la interfaz web
icon_image_alt	Switch	Especifica el nombre para el icono utilizado en la interfaz web
statusmap_image	./ng-switch40.png	Especifica la imagen mostrada en el mapa de red
}		Finaliza la definición

### 3.2.7 DEFINICIÓN DE SERVICIOS

Para agregar el monitoreo de los servicios ejecutados en los equipos de conmutación al sistema NAGIOS es necesario definir los parámetros que se indican en la tabla 90, el parámetro `host_name` debe cambiar para cada equipo mientras que el parámetro `use` permitirá heredar la pre configuración establecida en la plantilla `generic-service`, véase la tabla 88. La definición de servicios se realiza en el directorio `/usr/local/nagios/etc/import/services`.

El parámetro `check_command`, véase la tabla 90, define la ejecución del plugin `check_ping`, los valores seguidos de los signos de exclamación son valores de ejecución que reemplazan los argumentos establecidos en la configuración de comandos (`$ARG1$, $ARG2$, etc.`), como se muestra en la tabla 85.

Tabla 90. Ejemplo de definición de servicio (sw-Fica)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN	DESCRIPCIÓN
define service{		Inicia la definición
use	generic-service	Especifica el nombre de la plantilla que se hereda
host_name	sw-Fica	Especifica el nombre del equipo
service_description	01.PING	Especifica la descripción del servicio a chequear
check_command	check_ping!200.0,20%!600.0,60%	Especifica el comando que ejecutará el servicio
}		Finaliza la definición

Cada vez que se requiera chequear un nuevo servicio en el mismo switch bastará definir el servicio como se indica en la tabla 90, cambiando solo la definición del parámetro `check_command` con cada una de las definiciones establecidas en la tabla 91, cada definición permite el chequeo de un servicio específico, la descripción de cada plugin utilizado por el sistema NAGIOS para monitorear los servicios ejecutados en los equipos de conmutación de la capa de acceso y distribución en la red de datos de la UTN se muestra en la tabla 92 así como las condiciones en las que se mostrarán mensajes de advertencia o peligro desde la web

que posteriormente serán enviadas al correo electrónico del administrador de la red, esta configuración se debe utilizar en los nuevos equipos que se agreguen al sistema o modificarla según los nuevos requerimientos impuestos por el administrador.

Tabla 91. Definición del parámetro check\_command para servicios en un switch  
Fuente: Definición de servicios en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN
check_command	check_ping!200.0,20%!600.0,60%
check_command	check_snmp!-C utn -o 1.3.6.1.2.1.1.3.0
check_command	check_snmp_mem.pl!-C utn -I -w 80% -c 90%
check_command	check-cisco.pl!-C utn -t cpu -w 80 -c 90
check_command	check-cisco.pl!-C utn -t fan
check_command	check-cisco.pl!-C utn -t ps
check_command	check_snmp!-C utn -o 1.3.6.1.2.1.2.2.1.8.10001 -r 1 -m RFC1213-MIB
check_command	check_traffic43a!-C utn -w 30 -c 40 -i 10101

Tabla 92. Descripción de la ejecución de plugin para el chequeo de switches  
Fuente: Plugin instalados en el servidor NAGIOS

DEFINICIÓN	DESCRIPCIÓN
check_traffic43a!-C utn -w 30 -c 40 -i 10101	Chequea el tráfico que cursa por la interfaz GigabitEthernet 01, muestra un mensaje de advertencia si el tráfico es superior al 30 % y un crítico si es superior al 40%
check_ping!200.0,20%!600.0,60%	Chequea el estado del equipo en base a paquetes ICMP, muestra un mensaje de advertencia si el tiempo promedio de ida y vuelta es mayor a 200 ms o la pérdida de paquetes es mayor al 20 % y un crítico si el tiempo promedio de ida y vuelta es mayor a 600 ms o la pérdida de paquetes es mayor al 60 %
check_snmp_mem.pl!-C utn -I -w 80% -c 90%	Chequea el uso de memoria RAM, muestra un mensaje de advertencia si el uso es mayor al 80% y un crítico si es mayor al 90%
check-cisco.pl!-C utn -t cpu -w 80 -c 90	Chequea el uso de la CPU, muestra un mensaje de advertencia si el uso es superior al 80% y un crítico si supera el 90%
check-cisco.pl!-C utn -t fan	Chequea el estado de funcionamiento de los ventiladores.
check-cisco.pl!-C utn -t ps	Chequea el estado de funcionamiento de la fuente.
check_snmp!-C utn -o 1.3.6.1.2.1.1.3.0	Chequea el tiempo que el equipo permanece encendido
check_snmp!-C utn -o 1.3.6.1.2.1.2.2.1.8.10001 -r 1 -m RFC1213-MIB	Chequea el estado de la interfaz GigabitEthernet 02

### 3.2.8 WIRELESS CONTROLLER Y PUNTOS DE ACCESO INALÁMBRICO

### 3.2.9 CONFIGURACIÓN DE AGENTES DE MONITOREO

Para monitorear el Wireless Controller y puntos de acceso inalámbricos, es necesario habilitar el protocolo SNMP en cada equipo y establecer el nombre de la comunidad con privilegios de lectura o escritura, la configuración que se utilizó en los equipos monitoreados dentro de la UTN fue de solo lectura con la finalidad de impedirle al sistema de monitoreo o a cualquier otro usuario realizar modificaciones en la configuración de los equipos



monitoreados ya que así lo dispuso el administrador de la red por motivos de seguridad. Para habilitar el protocolo SNMP en el equipo se debe ingresar el siguiente comando:

- SW(config)#snmp-server community XXX RO

### 3.2.10 PLUGIN

Son archivos escritos en PHP que permiten recoger información acerca del funcionamiento de los equipos que conforman la red inalámbrica en la UTN, los plugin utilizados para realizar los chequeos se encuentran ubicados en el directorio /usr/local/nagios/libexec, la tabla 93 describe cada uno.

Tabla 93. Plugin utilizados en puntos de acceso y en el Wireless Controller  
Fuente: Plugin instalados en el servidor NAGIOS

PLUGIN	DESCRIPCIÓN
check_iftraffic43a	Chequea el tráfico que cursa por una interfaz física o virtual
check_ping	Chequea el estado del equipo a través de paquetes ICMP
check_Cisco_WLC.sh	Chequea el número de clientes conectados y el Firmware instalado

### 3.2.11 CONFIGURACIÓN DE COMANDOS

El sistema NAGIOS utiliza comandos pre definidos para la ejecución de los plugin que permiten recoger información acerca del funcionamiento de los equipos en la red, el archivo que almacena los comandos está ubicado en /usr/local/nagios/etc/import/commands.cfg, los comandos utilizan macros que son variables definidas por el sistema, los macros utilizados son los siguientes.

- \$USER1\$: Define la ubicación del plugin que será ejecutado por el comando, inicia la línea de comando y por defecto apunta al directorio /usr/local/nagios/libexec, esta ubicación se puede cambiar en el archivo /usr/local/nagios/etc/resource.cfg.
- \$HOSTADDRESS\$: Define la dirección ip del equipo a monitorear, es precedido del indicador -H, el archivo que contiene la definición de todos los equipos se encuentra en /usr/local/nagios/etc/import/hosts.

- **\$ARG1\$:** Es una variable que representa valores establecidos en la definición del servicio para poder ejecutar un plugin, puede haber más de uno, en la secuencia **\$ARG1\$, \$ARG2\$, etc.**

Para monitorear puntos de acceso inalámbricos o el Wireless Controller, se deben configurar comandos de ejecución como se indica en la tabla 94 para cada nuevo servicio monitoreado, solo se debe cambiar el parámetro **command\_name** y **command\_line** para la configuración de cada comando que se agregue al sistema.

*Tabla 94.* Ejemplo de configuración de comandos para el Wireless Controller y puntos de acceso  
Fuente: Comandos configurados en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define command{		Inicia la definición
command_name	check_Cisco_WLC.sh	Especifica el nombre del comando
command_line	\$USER1\$/check_Cisco_WLC.sh -H \$ARG1\$ -C \$ARG2\$ -v \$ARG3\$ -A \$ARG4\$ -w \$ARG5\$ -c \$ARG6\$	Especifica cómo se ejecutará el comando
}		

La tabla 95 muestra la configuración del parámetro **command\_line**, véase la tabla 94, para cada comando configurado en el sistema NAGIOS, estos comandos permiten el chequeo de los servicios ejecutados en los puntos de acceso inalámbricos o en el Wireless Controller y se deben utilizar para monitorear los nuevos equipos que se agreguen al sistema.

*Tabla 95.* Ejecución de comandos para el Wireless Controller y puntos de acceso  
Fuente: Comandos configurados en el servidor NAGIOS

PLUGIN	LÍNEA DE COMANDO
check_iftraffic43a	\$USER1\$/ check_iftraffic43a -H \$HOSTADDRESS\$ \$ARG1\$ \$ARG2\$ \$ARG3\$
check_ping	\$USER1\$/check_ping -H \$HOSTADDRESS\$ -w \$ARG1\$ -c \$ARG2\$ -p 5
check_Cisco_WLC.sh	\$USER1\$/check_Cisco_WLC.sh -H \$ARG1\$ -C \$ARG2\$ -v \$ARG3\$ -A \$ARG4\$ -w \$ARG5\$ -c \$ARG6\$

### 3.2.12 CONFIGURACIÓN DE PLANTILLAS PARA EQUIPOS

La configuración de equipos se realiza en base a plantillas, las plantillas son pre configuraciones que se heredan a las nuevas configuraciones y definiciones de puntos de acceso o Wireless Controller, las plantillas se encuentran en el archivo `/usr/local/nagios/etc/import/hosttemplates.cfg`. La tabla 96 describe la plantilla base utilizada

para configurar el monitoreo de los equipos que conforman la red inalámbrica en la UTN y se debe utilizar para configurar los nuevos equipos que se agreguen al sistema, no se debe cambiar ningún parámetro de esta plantilla de lo contrario se alteraría el correcto funcionamiento del sistema.

Tabla 96. Plantilla base para la configuración del Wireless Controller y puntos de acceso (*generic-host- wireless*)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define host{		Inicia la definición
name	generic-host-wireless	Especifica el nombre de la plantilla
notifications_enabled	1	Activa las notificaciones para el equipo. 1: activa, 0: desactiva
event_handler_enabled	1	Activa el controlador de eventos del sistema. 1: activa, 0: desactiva
flap_detection_enabled	1	Activa la detección de flapeo en el estado del equipo. 1: activa, 0: desactiva
failure_prediction_enabled	1	C elimino
process_perf_data	1	Activa el procesamiento de los datos de rendimiento. 1: activa, 0: desactiva
retain_status_information	1	Activa el almacenamiento de información con el estado del equipo antes de un reinicio. 1: activa, 0: desactiva
retain_nonstatus_information	1	Activa el almacenamiento del resto de información del equipo antes de un reinicio. 1: activa, 0: desactiva
notification_period	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones.
register	0	Desactiva el registro de la información. 1: activa, 0: desactiva
}		Finaliza la definición

La plantilla de configuración de equipos inalámbricos, Wireless, véase la tabla 97, hereda la pre configuración de la plantilla base, generic-host-wireless, véase la tabla 96, por medio del parámetro use, la tabla 97 muestra la configuración realizada para el monitoreo de los equipos inalámbricos alojados en la UTN, esta configuración se realizó en base a los requerimientos de monitoreo establecidos por el administrador de la red y en caso de querer modificar esta configuración se debe cambiar solo los parámetros en negrita. La plantilla Wireless como generic-host-wireless se debe utilizar para configurar el monitoreo de los nuevos equipos inalámbricos que se agreguen al sistema NAGIOS.

Tabla 97. Plantilla de configuración del Wireless Controller y puntos de acceso (Wireless)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define host{		Inicia la definición
name	Wireless	Especifica el nombre de la plantilla
use	generic-host-wireless	Especifica el nombre de la plantilla que se hereda
<b>check_period</b>	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para chequear el estado del equipo.
<b>check_interval</b>	5	Especifica el intervalo de tiempo (min) entre cada chequeo mientras el equipo devuelva un estado up
<b>retry_interval</b>	1	Especifica el intervalo de tiempo (min) entre cada chequeo si el equipo

<b>max_check_attempts</b>	10	devuelve un estado no up
check_command	check-host-alive	Especifica el número de veces que se ejecutara el comando de verificación si el equipo cambia a un estado no up
<b>notification_period</b>	Workhours	Especifica el nombre del comando que comprobará el estado del equipo
<b>notification_interval</b>	60	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones.
notification_options	d,u,r	Especifica el periodo de tiempo para volver a notificar al contacto
<b>contact_groups</b>	admins	Especifica el tipo de notificación a enviar d:dawn, u:unreachable, r: up
register	0	Especifica el nombre del grupo de contacto al que se enviarán las notificaciones
}		Desactiva el registro de la información.
		Finaliza la definición

### 3.2.13 CONFIGURACIÓN DE PLANTILLAS PARA SERVICIOS

La configuración de servicios monitoreados se realiza en base a plantillas, las plantillas son pre configuraciones que se heredan a las nuevas definiciones de servicios con solo utilizar el nombre que se le ha asignado. Las plantillas se encuentran en el archivo `/usr/local/nagios/etc/import/servicetemplates.cfg`.

La tabla 98 describe la plantilla de configuración para monitorear los servicios ejecutados en los equipos que conforman la red inalámbrica en la UTN y se debe utilizar en la configuración de los servicios en los nuevos equipos que se agreguen al sistema, la configuración de esta plantilla se realizó en base a los requerimientos de monitoreo establecidos por el administrador de la red y en caso de querer modificar esta configuración se debe cambiar solo los parámetros en negrita.

Tabla 98. Plantilla de configuración de servicios para el Wireless Controller y puntos de acceso (Wireless-Service)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define service{		Inicia la definición
name	Wireless-Service	Especifica el nombre de la plantilla
active_checks_enabled	1	Activa los controles activos. 1: activa, 0: desactiva
passive_checks_enabled	1	Activa los controles pasivos. 1: activa, 0: desactiva
parallelize_check	1	Activa la comprobación de servicios paralelamente
obsess_over_service	0	Desactiva la ejecución de comandos después de cada chequeo
check_freshness	0	Desactiva los controles de frescura para los chequeos pasivos.
notifications_enabled	1	Activa las notificaciones para el servicio. 1: activa, 0: desactiva
event_handler_enabled	1	Activa el controlador de eventos del sistema. 1: activa, 0: desactiva
flap_detection_enabled	1	Activa la detección de flapeo en el estado del servicio. 1: activa, 0: desactiva
process_perf_data	1	Activa el procesamiento de los datos de rendimiento. 1: activa, 0: desactiva
retain_status_information	1	Activa el almacenamiento de información con el estado del servicio antes de un reinicio. 1: activa, 0: desactiva
retain_nonstatus_information	1	Activa el almacenamiento del resto de información del servicio antes de un reinicio. 1: activa, 0: desactiva
is_volatile	0	Desactiva el servicio como volátiles
check_period	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para chequear el estado del servicio.
<b>max_check_attempts</b>	3	Especifica el número de veces que se ejecutará el comando de verificación si el

<b>normal_check_interval</b>	1	servicio devuelve un estado no aceptable. Especifica el intervalo de tiempo (min) entre cada chequeo mientras el servicio devuelva un estado aceptable
<b>retry_check_interval</b>	2	Especifica el intervalo de tiempo (min) entre cada chequeo si el servicio cambia a un estado no aceptable
<b>contact_groups</b>	admins	Especifica el nombre del grupo de contacto al que se enviarán las notificaciones
<b>notification_options</b>	w,u,c,r	Especifica el tipo de notificación a enviar w:warning, u:unknown, c: critical, r: ok
<b>notification_interval</b>	60	Especifica el periodo de tiempo para volver a notificar al contacto
<b>notification_period</b>	24x7	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones.
Register	0	Desactiva el registro de la información.
}		Finaliza la definición

### 3.2.14 DEFINICIÓN DE EQUIPOS

Para agregar un nuevo punto de acceso inalámbrico o Wireless Controller al sistema de monitoreo es necesario definir los parámetros que se indican en la tabla 99, solo se debe cambiar la definición de los parámetros en negrita para cada equipo, el parámetro use permite heredar la pre configuración establecida en la plantilla Wireless, véase la tabla 97. La definición de equipos se realiza en el directorio `/usr/local/nagios/etc/import/hosts`.

Tabla 99. Ejemplo de definición de equipo (ap-fica-pa2d)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN	DESCRIPCIÓN
define host{		Inicia la definición
use	Wireless	Especifica el nombre de la plantilla que se hereda
<b>host_name</b>	ap-fica-pa2d	Especifica el nombre del equipo
<b>alias</b>	ap-fica-pa2d	Especifica el alias del equipo
<b>address</b>	x.x.x.x	Especifica la dirección ip del equipo
hostgroups	Wireless-FICA	Especifica el nombre del grupo al que pertenece el equipo
parents	sw-Fica	Especifica el equipo del padre
<b>icon_image</b>	./equipment/wifi3.gif	Especifica la imagen utilizada como icono en la interfaz web
<b>icon_image_alt</b>	Access Point	Especifica el nombre para el icono utilizado en la interfaz web
<b>statusmap_image</b>	./equipment/wifi3.gd2	Especifica la imagen mostrada en el mapa de red
}		Finaliza la definición

### 3.2.15 DEFINICIÓN DE SERVICIOS

Para agregar el monitoreo de los servicios ejecutados en los equipos que conforman la red inalámbrica es necesario definir los parámetros que se indican en la tabla 100, el parámetro `host_name` deberá cambiar para cada equipo mientras que el parámetro `use` permitirá heredar la pre configuración establecida en la plantilla Wireless-Service, véase la tabla 98. La definición de servicios se realiza en el directorio `/usr/local/nagios/etc/import/services`. El parámetro `check_command`, véase la tabla 100, define la ejecución del plugin `check_ping`, los

valores seguidos de los signos de exclamación son valores de ejecución que remplazan los argumentos establecidos en la configuración de comandos (\$ARG1\$, \$ARG2\$, etc.), como se muestra en la tabla 95.

Tabla 100. Ejemplo de definición de servicios (ap-fica-pa2d)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN	DESCRIPCIÓN
define service{		Inicia la definición
use	Wireless-Service	Especifica el nombre de la plantilla que se hereda
host_name	ap-fica-pa2d	Especifica el nombre del equipo
service_description	01.PING	Especifica la descripción del servicio a chequear
check_command	check_ping!200.0,20%!600.0,60%	Especifica el comando que ejecutará el servicio
}		Finaliza la definición

Si se desea chequear un nuevo servicio en el mismo equipo bastará definir el servicio como se indica en la tabla 100, cambiando solo la definición del parámetro check\_command con cada una de las definiciones establecidas en la tabla 101, cada definición permite el chequeo de un servicio específico, la descripción de cada plugin utilizado por el sistema NAGIOS para monitorear los servicios ejecutados en los equipos que conforman la red inalámbrica de la UTN se muestra en la tabla 102 así como las condiciones en las que se mostrarán mensajes de advertencia o peligro desde la web que posteriormente serán enviadas al correo electrónico del administrador de la red, esta configuración se debe utilizar en los nuevos equipos que se agreguen al sistema o modificarla según los nuevos requerimientos impuestos por el administrador.

Tabla 101. Definición del parámetro check\_command para servicios en el Wireless Controller y puntos de acceso  
Fuente: Definición de servicios en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN
check_command	check_ping!200.0,20%!600.0,60%
check_command	check_traffic43a!-C utn -w 30 -c 40 -i 1
check_command	check_Cisco_WLC.sh!172.20.2.10!utn!2c!2!50!80

Tabla 102. Descripción de la ejecución de plugin para el chequeo del Wireless Controller y puntos de acceso  
Fuente: Plugin instalados en el servidor NAGIOS

DEFINICIÓN	DESCRIPCIÓN
check_ping!200.0,20%!600.0,60%	Chequea el estado del equipo en base a paquetes ICMP, muestra un mensaje de advertencia si el tiempo promedio de ida y vuelta es mayor a 200 ms o la pérdida de paquetes es mayor al 20 % y un crítico si el tiempo promedio de ida y vuelta es mayor a 600 ms o la pérdida de paquetes es mayor al 60 %
check_Cisco_WLC.sh!172.20.2.10!utn!2c!2!50!80	Chequea el número de usuarios conectados en el ap, su ubicación y el firmware instalado
check_traffic43a!-C utn -w 30 -c 40 -i 10101	Chequea el tráfico que cursa por la interfaz GigabitEthernet 01, muestra un mensaje de advertencia si el tráfico es superior al 30 % y un crítico si es superior al 40%

### 3.3 CONFIGURAR UN NUEVO GRUPO DE QUIPOS

Con la finalidad de observar los equipos que conforman la red de datos de la UTN de manera distribuida se crearon grupos pertenecientes a cada facultad o edificación dentro de la universidad, se configuraron grupos de switches, puntos de acceso inalámbricos y servidores según su ubicación. Los grupos creados en el sistema se muestran en la tabla 103.

*Tabla 103.* Grupos de equipos creados en el sistema NAGIOS  
Fuente: Sistema de monitoreo NAGIOS

GRUPOS DE EQUIPOS
SWITCHES-FICA
SWITCHES-FACAE
SWITCHES-FECYT
SWITCHES-FICAYA
SWITCHES-POSTGRADO
SWITCHES-CAI
SWITCHES-ED. CENTRAL
SWITCHES-BIEN. ESTUDIANTIL
SWITCHES-BIBLIOTECA
SWITCHES-SALUD
WIRELESS LAN(MODIFICAR)
SERVIDORES FICA
SWITCHES-ED. FÍSICA

Para agregar un nuevo grupo de equipos al sistema de monitoreo, es necesario especificar los parámetros que se indican en la tabla 104, solo se debe cambiar la configuración de los parámetros `hostgroup_name` y `alias` para cada nuevo grupo, la configuración de grupos de equipos se realiza en el archivo `/usr/local/nagios/etc/import/hostgroups.cfg`.

*Tabla 104.* Ejemplo de configuración de grupo de equipos  
Fuente: Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
<code>define hostgroup{</code>		Inicia la definición
<code>hostgroup_name</code>	Servidores-FICA	Especifica el nombre de la plantilla o grupo
<code>alias</code>	Servidores FICA	Especifica el alias del grupo
<code>}</code>		Finaliza la definición

### 3.4 CONFIGURAR UN NUEVO PERIODO DE TIEMPO DE MONITOREO

Nagios permite el monitoreo de los equipos en la red y el envío de notificaciones al correo electrónico en base a periodos de tiempo programados, debido a que se monitorean equipos prioritarios como equipos de conmutación tanto de la capa de acceso y distribución,

servidores LINUX y puntos de acceso inalámbricos en la UTN los periodos de tiempo configurados son de lunes a domingo las 24 horas del día tanto para el envío de notificaciones al correo como para el monitoreo de equipos, véase la tabla 105, si bien es cierto el trabajo del servidor de monitoreo es constante el periodo de tiempo programado es necesario ya que el funcionamiento de los equipos monitoreados se refleja en la disponibilidad y rendimiento de la red de datos en la UTN que requiere supervisión continua.

Para agregar un nuevo periodo de tiempo programado es necesario especificar los parámetros que se indican en la tabla 105, se debe cambiar la configuración de los parámetros `timeperiod_name` y `alias` así como los periodos de inicio y fin del monitoreo, posteriormente esta nueva plantilla de configuración se debe agregar a las plantillas de configuración de los servicios monitoreados en el sistema NAGIOS, la configuración de los periodos de monitoreo se realiza en el archivo `/usr/local/nagios/etc/import/timeperiods.cfg`.

Tabla 105. Ejemplo de configuración de grupo de equipos  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
<code>define timeperiod{</code>		Inicia la definición
<code>timeperiod_name</code>	<code>24x7</code>	Especifica el nombre de la plantilla o periodo de tiempo
<code>alias</code>	<code>24 Hours A Day, 7 Days A Week</code>	Especifica el alias para el periodo de tiempo
<code>sunday</code>	<code>00:00-24:00</code>	Inicio-Fin
<code>monday</code>	<code>00:00-24:00</code>	Inicio-Fin
<code>tuesday</code>	<code>00:00-24:00</code>	Inicio-Fin
<code>wednesday</code>	<code>00:00-24:00</code>	Inicio-Fin
<code>thursday</code>	<code>00:00-24:00</code>	Inicio-Fin
<code>friday</code>	<code>00:00-24:00</code>	Inicio-Fin
<code>saturday</code>	<code>00:00-24:00</code>	Inicio-Fin
<code>}</code>		Finaliza la definición

## 3.5 ENVÍO DE NOTIFICACIONES

### 3.5.1 CONFIGURACIÓN DE PLANTILLA PARA CONTACTOS

La configuración de contactos para el envío de notificaciones al correo electrónico se realiza en base a plantillas, las plantillas son pre configuraciones que se heredan a las nuevas definiciones de contactos con solo utilizar el nombre que se le ha asignado. La tabla 106



describe la plantilla de configuración de contactos creada en el sistema NAGIOS en base a los requerimientos del administrador de la red, esta plantilla se encuentran en el archivo `/usr/local/nagios/etc/import/contacttemplates.cfg`.

Tabla 106. Plantilla de configuración de contactos (generic-contact)  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
<code>define contact{</code>		Inicia la definición.
<code>name</code>	<code>generic-contact</code>	Especifica el nombre de la plantilla.
<code>service_notification_period</code>	<code>24x7</code>	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones de servicios.
<code>host_notification_period</code>	<code>24x7</code>	Especifica el nombre de la plantilla con el periodo de tiempo escogido para el envío de notificaciones de equipos.
<code>service_notification_options</code>	<code>w,u,c,r,f</code>	Especifica el tipo de notificación a enviar w: warning, u: unknown, c: critical, r: ok, f: flapping para los servicios.
<code>host_notification_options</code>	<code>d,u,r,f</code>	Especifica el tipo de notificación a enviar d:dawn, u:unreachable, r: up, f:flapping para los equipos.
<code>service_notification_commands</code>	<code>notify-service-by-email</code>	Especifica el nombre del comando que se ejecutará para notificar a un contacto acerca del problema de algún servicio.
<code>host_notification_commands</code>	<code>notify-host-by-email</code>	Especifica el nombre del comando que se ejecutará para notificar a un contacto acerca del problema de algún equipo.
<code>register</code>	<code>0</code>	Deshabilita el registro de la información.
<code>host_notifications_enabled</code>	<code>1</code>	Activa el envío de notificaciones de equipos
<code>service_notifications_enabled</code>	<code>1</code>	Activa el envío de notificaciones de servicios.
<code>}</code>		Finaliza la definición.

### 3.5.2 DEFINICIÓN DEL GRUPO DE CONTACTOS

Para que el sistema de monitoreo pueda enviar notificaciones acerca del estado de los equipos en la red de la UTN es necesario definir el o los grupos de contactos a los que se asociarán los miembros con los correos electrónicos que recibirán las notificaciones, el sistema NAGIOS se configuró con un grupo de contactos llamado `admins` como se puede ver en la tabla 107, el cual tiene asociado el miembro `nagiosadmin` al cual se envían las notificaciones emitidas por el sistema de monitoreo. Si se desea crear nuevos grupos de contactos se deben definir los parámetros que se muestran en la tabla 107 directamente en el archivo `/usr/local/nagios/etc/import/contactgroups.cfg`. Para agregar nuevos miembros al mismo grupo de contactos es necesario indicar el nombre del miembro seguido de una coma en el parámetro `members`, véase la tabla 108, después de definir el nuevo contacto, véase la tabla 86.

Tabla 107. Ejemplo de definición del grupo de contactos  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN	DESCRIPCIÓN
define contactgroup{		Inicia la definición.
contactgroup_name	admins	Especifica el nombre del grupo de contactos
alias	Nagios Administrators	Especifica el alias para el grupo de contactos
members	nagiosadmin, nuevo contacto	Especifica los miembros del grupo a los que se enviarán las notificaciones
}		Finaliza la definición

### 3.5.3 DEFINICIÓN DE CONTACTO

El sistema NAGIOS se complementó con un servidor de correo electrónico para el envío de notificaciones en el cual se tiene creada la cuenta usuario2@sewebmaster.com, véase la tabla 108, esta cuenta de correo pertenece al miembro nagiosadmin que a su vez forma parte del grupo admins, véase la tabla 107. Si se desea agregar nuevas cuentas de correo al sistema NAGIOS se deben crear previamente en el servidor de correo para asociarlas posteriormente a la definición del contacto como se muestra en la tabla 108. Para agregar nuevos contactos y así realizar el envío de notificaciones es necesario definir los parámetros mostrados en la tabla 108, el parámetro use permite heredar la configuración de la plantilla generic-contact, véase la tabla 106. Después de definir un nuevo contacto, se lo debe agregar como miembro del grupo de contactos previamente configurado, véase la tabla 107.

Tabla 108. Ejemplo de definición de contacto  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	DEFINICIÓN	DESCRIPCIÓN
define contact{		Inicia la definición
contact_name	nagiosadmin	Especifica el nombre del contacto
use	generic-contact	Especifica el nombre de la plantilla con la configuración a heredar
alias	Nagios Admin	Especifica el alias para el contacto
email	usuario2@sewebmaster.com	Especifica el correo electrónico al que se enviarán las notificaciones.
}		Finaliza la definición.

## 3.6 MÓDULO DE GRÁFICAS PNP4NAGIOS

### 3.6.1 CONFIGURACIÓN DEL COMANDO DE EJECUCIÓN

Para mostrar gráficas de los servicios monitoreados, el sistema NAGIOS debe procesar los datos de rendimiento obtenidos después de la ejecución de cada plugin mediante un comando

pre definido como se indica en la tabla 109, el archivo que almacena los comandos está ubicado en `/usr/local/nagios/etc/import/commands.cfg`. La ejecución del comando utiliza un macro que es una variable definida por el sistema, el macro utilizado se describe a continuación.

- `$TIMET$`: Contiene la fecha y hora actual en formato UNIX para evitar la sobrescrita de archivos antiguos.

Tabla 109. Comando para procesar los datos de rendimiento  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
<code>define command{</code>		Inicia la definición
<code>command_name</code>	<code>process-service-perfdata-file</code>	Especifica el nombre del comando
<code>command_line</code>	<code>/bin/mv /usr/local/pnp4nagios/var/service-perfdata /usr/local/pnp4nagios/var/spool/service- perfdata.\$TIMET\$</code>	Mueve el archivo de encolamiento <code>service-perfdata</code> al directorio <code>spool</code> .
<code>}</code>		Finaliza la definición

### 3.6.2 CONFIGURACIÓN DE PLANTILLA PARA SERVICIOS

La plantilla de configuración `srv-pnp`, véase la tabla 110, permite apuntar al icono que mostrará la gráfica en base al nombre del equipo y a la descripción del servicio monitoreado, la configuración de esta plantilla utiliza macros que son variables definidas por el sistema, a continuación se describe cada macro utilizado.

- `$HOSTNAME$`: Especifica el parámetro `host_name` establecido al momento de definir el equipo.
- `$SERVICEDESC$`: Especifica el parámetro `service_description` establecido al momento de definir el servicio.

La plantilla para generar gráficas de los servicios monitoreados se encuentran en el archivo `/usr/local/nagios/etc/objects/templates.cfg` y se debe utilizar en los nuevos servicios que se agreguen al sistema.

Tabla 110. Plantilla para generar graficas de rendimiento de servicios  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define service {		Inicia la definición
name	srv-pnp	Especifica el nombre de la plantilla
action_url	/pnp4nagios/index.php/graph?host=\$HOSTN AME&srv=\$SERVICEDESC\$	Apunta al icono graph, y permite la gráfica en base al nombre del equipo y la descripción de servicio.
register	0	Desactiva el registro de la información.
}		Finaliza la definición

### 3.6.3 DEFINICIÓN DE GRÁFICAS PARA SERVICIOS

Para generar las gráficas de rendimiento de los servicios monitoreados se debe utilizar la plantilla `srv-pnp` descrita en la tabla 110 seguida de una coma en el parámetro `use`, véase la tabla 111, esta configuración se realiza al momento de definir el servicio monitoreado.

Tabla 111. Ejemplo de definición de servicio y uso de la plantilla de gráficas, para los datos de rendimiento  
Fuente: Archivo de configuración en el servidor NAGIOS

PARÁMETRO	CONFIGURACIÓN	DESCRIPCIÓN
define service{		Inicia la definición
use	generic-service,srv-pnp	Especifica el nombre de la plantilla <code>generic-service</code> de la cual heredara una pre configuración y el uso de la plantilla <code>srv-pnp</code> para mostrar las gráficas de rendimiento de esa definición de servicio.
host_name	sw-Fica	Especifica el nombre del equipo
service_description	41.FAST ETH SERV-NAGIOS	Especifica la descripción para el servicio
check_command	check_traffic-fica!-C utn -w 30 -c 40 -i 37	Especifica el comando ejecutado para realizar el chequeo del servicio
notes	--- FAST ETH 4/17 ---	Especifica una pequeña descripción que se mostrara en la interfaz web
}		Finaliza la definición

## CAPITULO IV

### RENDIMIENTO DE LA RED DE DATOS DE LA UTN

#### 4.1 INTRODUCCIÓN

La red de datos de la UTN, tiene acceso hacia la nube de internet a través de un equipo CISCO CATALYST 4506-E alojado en el edificio central, el mismo que soporta todo el tráfico de datos de la universidad y permite la propagación de VLAN hacia la capa de acceso ya que se encuentra configurado como servidor VTP.

La redundancia de la red se maneja con STP y el equipo CISCO CATALYST 4506-E alojado en el edificio central está configurado como puente raíz para la determinación de rutas redundantes que se deben bloquear, el equipo CISCO CATALYST 4506-E alojado en la FICA se encuentra configurado como puente raíz alternativo en caso de que se presente alguna falla con el puente raíz principal, cabe recalcar que únicamente el CISCO CATALYST 4506-E alojado en el edificio central tiene acceso hacia la nube de internet por lo que si se tiene algún problema con este equipo toda la red de la UTN perdería conectividad hacia la nube de internet.

El rendimiento de la red de datos de la UTN se verifico principalmente en la capa de distribución compuesta por los equipos CISCO CATALYST 4506-E alojados en el edificio central y en la FICA ya que estos equipos soportan directamente todo el tráfico de la UTN y proveen los mecanismos de redundancia y segmentación para la misma.

#### 4.2 MEDICIÓN DEL TRÁFICO DE LA RED

Para conocer el tráfico que cursa por la red de datos de la UTN se realizó una medición en tiempo real para identificar el patrón característico acerca del uso de los recursos de la red.

Para realizar la medición del tráfico de red se utilizó la aplicación gratuita de código abierto NTOP que es una sonda de tráfico de red diseñada para ejecutarse tanto en plataformas UNIX como en Windows y se basa en la librería de captura de paquetes libpcap.

La captura del tráfico se realiza mediante la configuración de un puerto espejo (SPAN, Switched Port Analyzer) en el switch de distribución Cisco Catalyst 4506-E alojado en el edificio central ya que este equipo presenta la configuración de todas las VLAN que se propagan por medio de VTP a la capa de acceso de la universidad y soporta todo el tráfico de la misma, por medio del puerto espejo se duplica el tráfico que circula por todas las VLAN y se replica hacia el host en el que se ha implementado NTOP para el análisis del tráfico. A continuación, se describen los resultados obtenidos tras el monitoreo del tráfico durante un período de tiempo de siete días consecutivos.

#### 4.2.1 ANÁLISIS GENERAL DE TRÁFICO

Las estadísticas generadas señalan que el 99.4% del total de datos capturados por NTOP corresponden al protocolo de internet IP, de los cuales 91.3% coinciden con el protocolo TCP, el 8.6% a UDP y el 0.1% restante se distribuye entre los protocolos ICMP, ICMPv6, IGMP19 y varios no identificados por el software, véase figura 33.

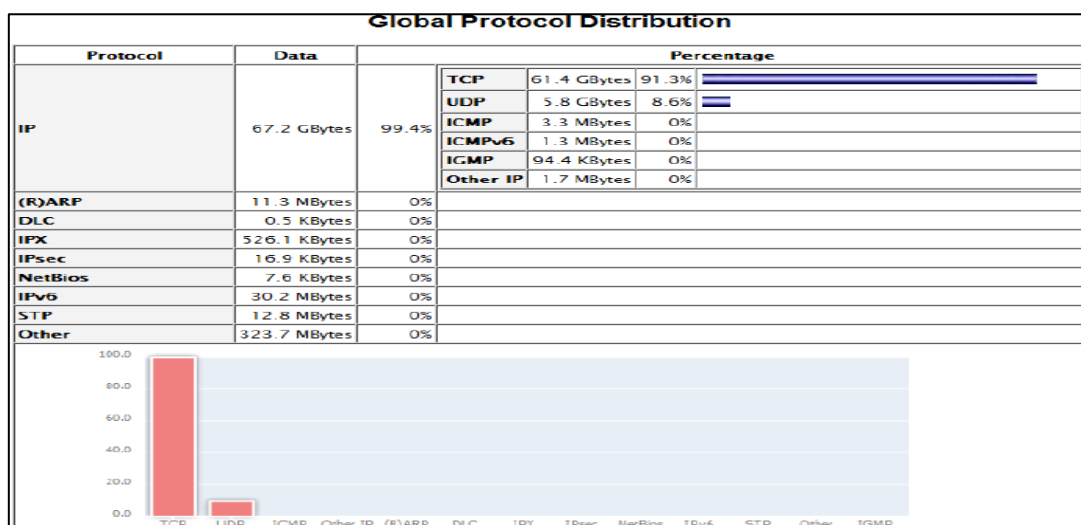


Figura 33. Distribución global de datos de acuerdo al tipo de protocolo utilizando NTOP

Fuente: Análisis general de tráfico en el Cisco Catalyst 4506-E

#### 4.2.1.1 Distribución del tráfico por protocolo/aplicación

A continuación describen los protocolos/aplicaciones mayormente empleados en la red de datos de la UTN.

El tráfico HTTP alcanza un volumen de datos máximo de 11.5 Mbytes/s y de 3.3 Mbytes/s en promedio, debido a que el monitoreo de la red se efectuó ininterrumpidamente se visualizan repentinos altos y bajos en las gráficas que se crean por los horarios de mayor y menor utilización de la red, véase la figura 34. Se concluye que la mayor cantidad de tráfico de la red se destina a la navegación web y que el puerto utilizado con mayor frecuencia es el 80.

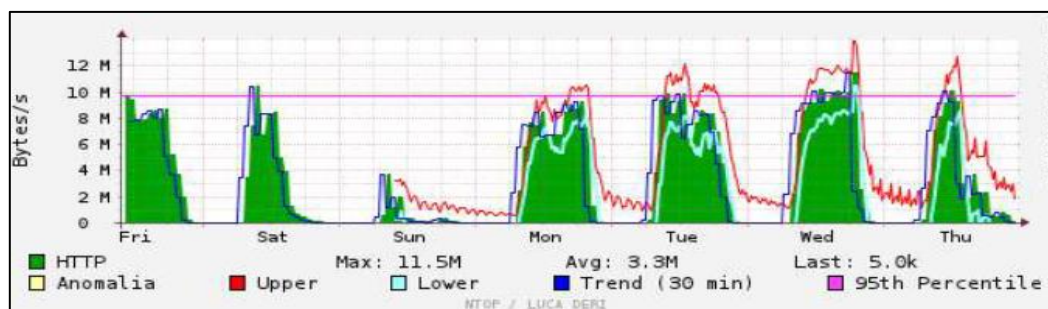


Figura 34. Vista histórica del protocolo HTTP en la red  
Fuente: Análisis general de tráfico en el Cisco Catalyst 4506-E

El tráfico generado por la mensajería instantánea Windows Live Messenger asciende a un máximo de 85.6 Kbytes/s y a un promedio de 3.3 Kbytes/s, véase la figura 35.

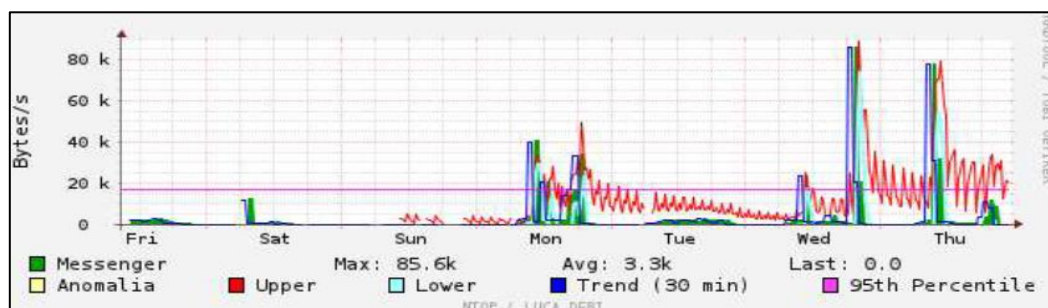


Figura 35. Vista histórica de la aplicación Windows Live Messenger en la red  
Fuente: Análisis general de tráfico en el Cisco Catalyst 4506-E

El protocolo NETBIOS<sup>57</sup> sobre TCP/IP genera un tráfico máximo de 28.1 Kbytes/s y un promedio de 2K bytes/s, véase figura 36.

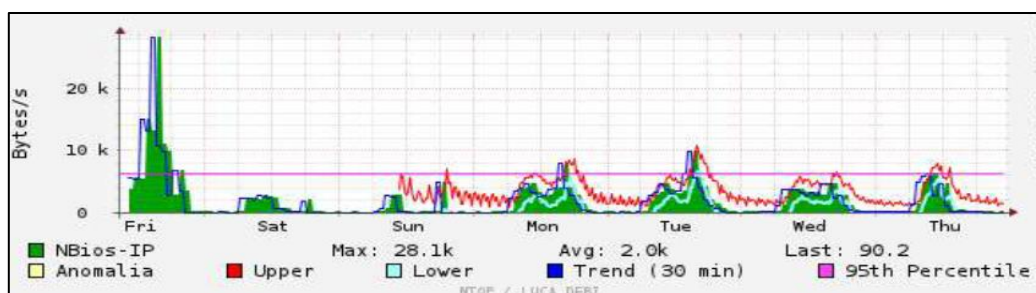


Figura 36. Vista histórica del protocolo NeBios-IP la red  
Fuente: Análisis general de tráfico en el Cisco Catalyst 4506-E

El tráfico DNS<sup>58</sup>, genera un volumen de datos máximo de 19.3 Kbytes/s y un promedio de 5.7 Kbytes/s, véase figura 37.

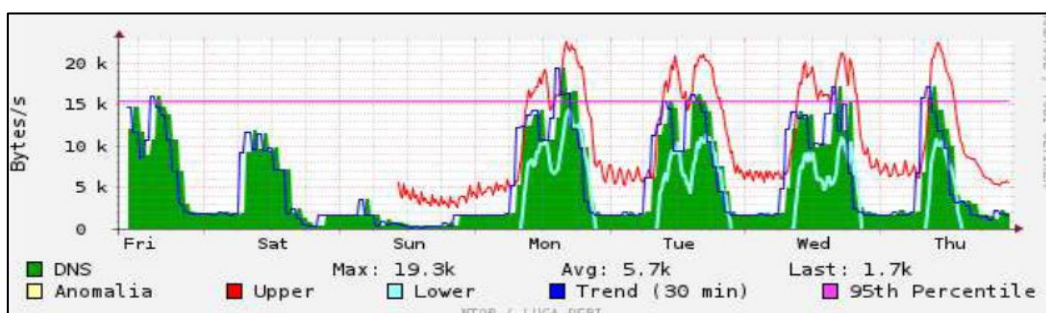


Figura 37. Vista histórica del protocolo DNS en la red  
Fuente: Análisis general de tráfico en el Cisco Catalyst 4506-E

El tráfico FTP genera un volumen de datos de 16.0 Kbytes/s y un promedio de 493.3 Bytes/s, véase figura 38.

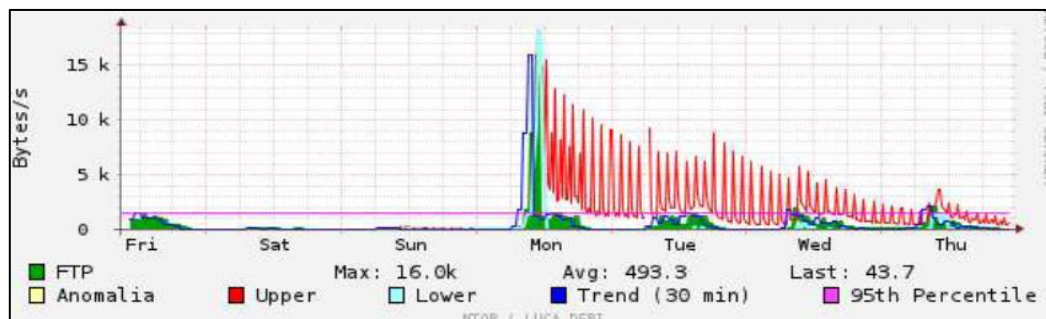


Figura 38. Vista histórica del protocolo FTP en la red  
Fuente: Análisis general de tráfico en el Cisco Catalyst 4506-E

<sup>57</sup> NETBIOS: Network Basic Input/Output System (sistema básico de entrada y salida)

<sup>58</sup> DNS: Domain Name Service (Servicio de Nombres de Dominio)





- Ultimo chequeo: Muestra la hora del último chequeo programado para el servicio.
- Duración: Muestra el tiempo que el servicio permanece sin cambiar de estado.
- Intentos: Muestra el número de intentos de verificación en los que el servicio devolvió un estado no Ok.
- Información de estado: Muestra información detallada del servicio.

Cada uno de estos parámetros entrega información acerca del estado del servicio ejecutado en el tiempo, toda esta información es almacenada y registrada por el sistema NAGIOS para el manejo de incidencias y reportes del rendimiento del equipo.

#### 4.3.1 CAPA DE DISTRIBUCIÓN DE LA UTN

El equipo CISCO CATALYST 4506-E alojado en el edificio central, nombrado SW-Zeus, véase la figura 41, muestra los siguientes servicios:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
sw-core- utn	01.PING	OK	12-30-2013 11:48:43	18d 23h 44m 0s	1/3	PING OK - Packet loss = 0%, RTA = 0.53 ms
	02.CPU_5s_1min_5min	OK	12-30-2013 11:53:12	63d 9h 10m 13s	1/3	Cpu: OK - Cpu Load 13% 13% 13%
	03.Mem_Ram	OK	12-30-2013 11:53:32	18d 23h 48m 47s	1/3	Processor:61% : 61% : : OK
	04.Ventilacion	OK	12-30-2013 11:52:59	63d 9h 10m 13s	1/3	Fans: OK - 3 Fans are running all good
	05.Fuente	OK	12-30-2013 11:53:12	63d 9h 10m 13s	1/3	PS: OK - 2 PS are running all good
	06.Uptime	OK	12-30-2013 11:53:22	18d 23h 48m 47s	1/3	SNMP OK - Timeticks: (153486115) 17 days, 18:21:01.15

Figura 41. Servicios ejecutados en el SW-Zeus  
Fuente: Sistema de monitoreo NAGIOS

- Ping: Muestra el porcentaje de paquetes ICMP perdidos y el tiempo de retardo de ida y vuelta.
- CPU\_5s\_1min\_5min: Muestra la carga de la CPU, en los últimos 5 segundos, 1 minuto y 5 minutos.
- Mem\_Ram: Muestra el porcentaje en el consumo de memoria del procesador.
- Ventilación: Muestra en número de ventiladores y estado de funcionamiento de cada uno.

- Fuente: Muestra en número de fuentes de poder y el estado de funcionamiento de cada uno.
- Uptime: Muestra el tiempo que el equipo permanece encendido desde el último reinicio o apagado inesperado.

La figura 42 muestra el estado de las interfaces Gigabitethernet, Tengigabitethernet y Portchannel configurados en el SW-Zeus, este equipo permite la salida hacia la nube de internet a toda la red de datos de la UTN, además se encuentra configurado como puente raíz para la determinación de las rutas redundantes que se deben bloquear, la figura 43 muestra los enlaces de fibra que brindan conectividad al resto de facultades. Actualmente la redundancia de la red se da a través del equipo CISCO CATALYST 4506-E alojado en la FICA, nombrado SW-Aristóteles el mismo que se encuentra configurado como puente raíz de respaldo. En la figura 43 se puede observar el porcentaje de utilización de cada interfaz así como el tráfico entrante y saliente, dando clic en el vínculo al lado del nombre de la interfaz, se muestra la gráfica del consumo de ancho de banda en el tiempo, véase la figura 44.

07.LIBRE PORT-CHANNEL		CRITICAL	11-14-2014 01:59:25	1d 16h 32m 25s	3/3	CRITICAL: Interface Port-channel1 is down!
08.PORT-CHANNEL A SW-CONCENTRADOR 2		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for Port-channel2 - Average IN: 4.20Mbps 0.53% Average OUT: 4.24Mbps 0.53%
09.TENGIGABITETHERNET		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for TenGigabitEthernet1/1 - Average IN: 2.07Kbps 0.00% Average OUT: 34.04Kbps 0.00%
10.LIBRE TENGIGABITETHERNET		CRITICAL	11-14-2014 01:59:25	1d 16h 32m 26s	3/3	CRITICAL: Interface TenGigabitEthernet1/2 is down!
11.GIGABITETHERNET A ROUTER TELCONET		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet1/3 - Average IN: 91.97Kbps 0.01% Average OUT: 2.12Mbps 0.21%
12.GIGABITETHERNET A CHASIS BLADE		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet1/4 - Average IN: 1.12Mbps 0.11% Average OUT: 216.74Kbps 0.02%
13.GIGABITETHERNET A WLC-UTN		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet1/5 - Average IN: 72.45Kbps 0.01% Average OUT: 60.20Kbps 0.01%
14.GIGABITETHERNET A TERRAZA		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet1/6 - Average IN: 8.74Mbps 0.87% Average OUT: 37.45Kbps 0.00%
15.GIGABITETHERNET A FICA		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet2/1 - Average IN: 9.41Mbps 0.94% Average OUT: 116.09Kbps 0.01%
16.GIGABITETHERNET A BIBLIOTECA		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet2/2 - Average IN: 3.02Kbps 0.00% Average OUT: 30.48Kbps 0.00%
17.GIGABITETHERNET A FICAYA		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet2/3 - Average IN: 1.90Mbps 0.19% Average OUT: 32.92Kbps 0.00%
18.GIGABITETHERNET A FACAE		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet2/4 - Average IN: 2.54Mbps 0.25% Average OUT: 35.33Kbps 0.00%
19.GIGABITETHERNET A DERECHO		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet2/5 - Average IN: 1.24Kbps 0.00% Average OUT: 30.49Kbps 0.00%
20.GIGABITETHERNET A SALUD		CRITICAL	11-14-2014 01:59:25	1d 16h 32m 26s	3/3	CRITICAL: Interface GigabitEthernet2/6 is down!
21.GIGABITETHERNET A FECYT		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet3/1 - Average IN: 1.46Mbps 0.15% Average OUT: 36.21Kbps 0.00%
22.GIGABITETHERNET A EDIFICIO DE BIENESTAR-DOCENTES		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet3/2 - Average IN: 5.30Kbps 0.00% Average OUT: 33.14Kbps 0.00%
23.GIGABITETHERNET A AUDITORIO		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet3/3 - Average IN: 1.32Kbps 0.00% Average OUT: 32.34Kbps 0.00%
24.GIGABITETHERNET A EDUCACION FISICA		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet3/4 - Average IN: 1.45Kbps 0.00% Average OUT: 31.83Kbps 0.00%
25.GIGABITETHERNET A SEGUNDO PISO		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet3/5 - Average IN: 1.85Kbps 0.00% Average OUT: 30.40Kbps 0.00%
26.GIGABITETHERNET A JOSE MARTI		OK	11-14-2014 01:59:25	0d 1h 24m 19s	1/3	OK for GigabitEthernet3/6 - Average IN: 1.20Kbps 0.00% Average OUT: 30.35Kbps 0.00%

Figura 42. Servicios ejecutados en el SW-Zeus  
Fuente: Sistema de monitoreo NAGIOS

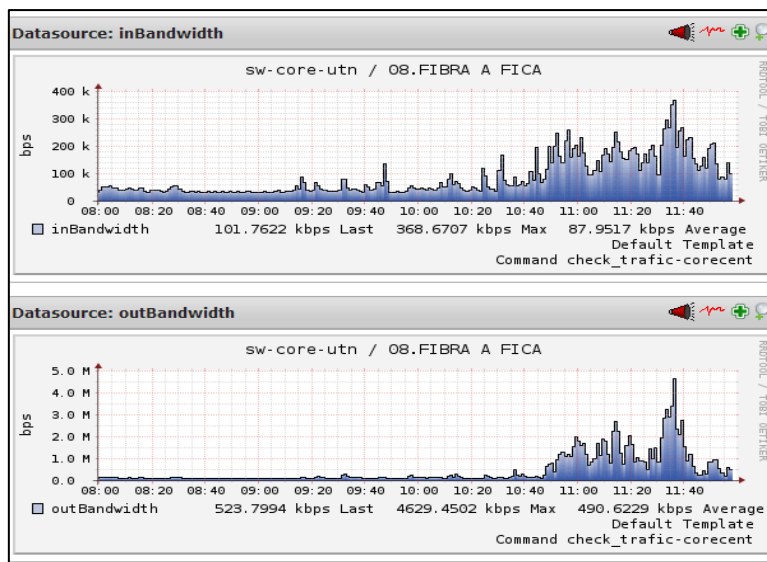


Figura 43. Tráfico de red en el SW-Zeus  
Fuente: Sistema de monitoreo NAGIOS

La figura 44, muestra la utilización de las VLAN configuradas en el SW-Zeus, este equipo de encuentra configurado como servidor VTP y se encarga de propagarlas hacia la capa de acceso de la UTN, se puede observar el estado de las interfaces virtuales, así como el tráfico entrante y saliente por cada interfaz.

27.VLAN 1 SERVIDORES		OK	11-14-2014 02:22:26	0d 1h 46m 58s	1/3	OK for Vlan1 - Average IN: 928.45Kbps 0.09% Average OUT: 1.01Mbps 0.10%
28.VLAN 2 EQUIPOS-ACTIVOS		OK	11-14-2014 02:22:26	0d 1h 46m 58s	1/3	OK for Vlan2 - Average IN: 25.68Kbps 0.00% Average OUT: 9.08Kbps 0.00%
29.VLAN 4 EDIFCENTRAL-FINANCIERO		OK	11-14-2014 02:22:15	0d 0h 0m 56s	1/3	OK for Vlan4 - Average IN: 23.13bps 0.00% Average OUT: 0.00bps 0.00%
30.VLAN 6 EDIFCENTRAL-DEPT.INFORMAT		OK	11-14-2014 02:22:26	0d 1h 46m 58s	1/3	OK for Vlan6 - Average IN: 5.32Kbps 0.00% Average OUT: 9.88Kbps 0.00%
31.VLAN 7 CECI		OK	11-14-2014 02:22:21	0d 1h 46m 58s	1/3	OK for Vlan7 - Average IN: 528.79bps 0.00% Average OUT: 0.00bps 0.00%
32.VLAN 8 EDIFCENTRAL-AUTORIDADES		OK	11-14-2014 02:22:26	0d 1h 46m 58s	1/3	OK for Vlan8 - Average IN: 1.68Kbps 0.00% Average OUT: 1.20Kbps 0.00%
33.VLAN 10 EDIFCENTRAL-ADMINISTRATIV		OK	11-14-2014 02:22:26	0d 1h 46m 58s	1/3	OK for Vlan10 - Average IN: 1.29Kbps 0.00% Average OUT: 502.40bps 0.00%
34.VLAN 12 EDIFCENTRAL-COMUN.ORGANIZ		OK	11-14-2014 02:22:26	0d 1h 46m 58s	1/3	OK for Vlan12 - Average IN: 1.70Kbps 0.00% Average OUT: 933.07bps 0.00%
35.VLAN 14 FICA-ADM		OK	11-14-2014 02:22:25	0d 0h 5m 46s	1/3	OK for Vlan14 - Average IN: 2.47Kbps 0.00% Average OUT: 1.91Kbps 0.00%
36.VLAN 16 FICA-LAB		OK	11-14-2014 02:22:26	0d 1h 46m 58s	1/3	OK for Vlan16 - Average IN: 225.87bps 0.00% Average OUT: 190.13bps 0.00%
37.VLAN 18 FICA-CISCO		CRITICAL	11-14-2014 02:22:26	0d 8h 14m 42s	3/3	CRITICAL Traffic IN for Vlan18 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: Vlan18
38.VLAN 20 FICAYA-ADM		CRITICAL	11-14-2014 02:22:26	0d 0h 31m 46s	3/3	CRITICAL Traffic IN for Vlan20 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: Vlan20
39.VLAN 22 FICAYA-LAB		CRITICAL	11-14-2014 02:22:26	0d 5h 50m 43s	3/3	CRITICAL Traffic IN for Vlan22 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: Vlan22
40.VLAN 24 CEC-UTN		OK	11-14-2014 02:22:26	0d 0h 2m 45s	1/3	OK for Vlan24 - Average IN: 1.10Kbps 0.00% Average OUT: 991.60bps 0.00%
41.VLAN 26 POSTGRADO		CRITICAL	11-14-2014 02:22:26	0d 6h 33m 43s	3/3	CRITICAL Traffic IN for Vlan26 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: Vlan26
42.VLAN 28 CAI-ADM		CRITICAL	11-14-2014 02:22:26	0d 5h 36m 42s	3/3	CRITICAL Traffic IN for Vlan28 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: Vlan28
43.VLAN 30 CAI-ADM		CRITICAL	11-14-2014 02:22:26	1d 16h 55m 5s	3/3	CRITICAL Traffic IN for Vlan30 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: Vlan30
44.VLAN 32 FFCSS-ADM		OK	11-14-2014 02:22:26	0d 1h 46m 58s	1/3	OK for Vlan32 - Average IN: 2.05Kbps 0.00% Average OUT: 4.82Kbps 0.00%
45.VLAN 36 BIBLIOTECA-ADM		OK	11-14-2014 02:22:15	0d 0h 1m 56s	1/3	OK for Vlan36 - Average IN: 511.05bps 0.00% Average OUT: 458.03bps 0.00%

Figura 44. Servicios ejecutados en el SW-Zeus  
Fuente: Sistema de monitoreo NAGIOS

El equipo CISCO CATALYST 4506-E alojado en la FICA, nombrado SW-Aristóteles, véase la figura 45, muestra los siguientes servicios:

Host	Service	Status	Last Check	Duration	Attempt	Status Information
sw-Fica	01.PING	OK	01-02-2014 11:09:01	21d 23h 0m 25s	1/3	PING OK - Packet loss = 0%, RTA = 0.56 ms
	02.CPU_5s_1min_5min	OK	01-02-2014 11:09:28	27d 1h 5m 52s	1/3	Cpu: OK - Cpu Load 11% 13% 13%
	03.Mem_Ram	OK	01-02-2014 11:10:03	21d 23h 6m 12s	1/3	Processor:70% : 70% : : OK
	04.Ventilacion	OK	01-02-2014 11:09:23	124d 18h 40m 32s	1/3	Fans: OK - 3 Fans are running all good
	05.Fuente	OK	01-02-2014 11:09:28	124d 18h 40m 0s	1/3	PS: OK - 2 PS are running all good
	06.Uptime	OK	01-02-2014 11:09:46	21d 23h 6m 12s	1/3	SNMP OK - Timeticks: (85372035) 9 days, 21:08:40.35

Figura 45. Servicios ejecutados en el SW-Aristóteles

Fuente: Sistema de monitoreo NAGIOS

- Ping: Muestra el porcentaje de paquetes ICMP perdidos y el tiempo de retardo de ida y vuelta.
- CPU\_5s\_1min\_5min: Muestra la carga de la CPU, en los últimos 5 segundos, 1 minuto y 5 minutos.
- Mem\_Ram: Muestra el porcentaje en el consumo de memoria del procesador.
- Ventilación: Muestra en número de ventiladores y estado de funcionamiento de cada uno.
- Fuente: Muestra en número de fuentes de poder y el estado de funcionamiento de cada uno.
- Uptime: Muestra el tiempo que el equipo permanece encendido desde el último reinicio o apagado inesperado.

La figura 46, muestra el estado de los enlaces redundantes desde el SW-Aristóteles hacia el resto de facultades de la universidad, este equipo se encuentra configurado como puente raíz alternativo en el caso de que presente algún problema el SW-Zeus que se encuentra como puente raíz principal, cabe recalcar que se tiene únicamente una salida hacia la nube de internet desde el SW-Zeus por lo que si este equipo se cae toda la red de la UTN perdería conectividad con el exterior. En la figura 46 se puede observar el porcentaje de utilización de

cada interfaz así como el tráfico entrante y saliente, dándole clic en el vínculo al lado del nombre de la interfaz desde la web, se muestra la gráfica del consumo de ancho de banda en el tiempo, véase la figura 47.

07.FIBRA FICA-ADM-CENT-IZD		OK	01-02-2014 11:17:30	9d 21h 10m 9s	1/3	OK for 9 - Average IN: 44.96Mbps 4.50% Average OUT: 14.68Mbps 1.47%
08.FIBRA FICA-BIBLIOTECA		OK	01-02-2014 11:17:30	0d 0h 0m 40s	1/3	OK for 10 - Average IN: 111.44bps 0.00% Average OUT: 257.34Kbps 0.03%
09.FIBRA FICA-FICAYA		OK	01-02-2014 11:17:07	9d 21h 9m 29s	1/3	OK for 11 - Average IN: 7.52Kbps 0.00% Average OUT: 190.95Kbps 0.02%
10.FIBRA FICA-FACAE		CRITICAL	01-02-2014 11:17:30	21d 23h 13m 36s	3/3	CRITICAL: Interface 12 is down!
11.FIBRA FICA-ADM-CENT-DER		CRITICAL	01-02-2014 11:17:30	21d 23h 13m 14s	3/3	CRITICAL: Interface 13 is down!
12.FIBRA FICA-SALUD		CRITICAL	01-02-2014 11:18:03	21d 23h 13m 56s	3/3	CRITICAL: Interface 14 is down!
13.FIBRA FICA-FECYT		CRITICAL	01-02-2014 11:17:30	21d 23h 13m 36s	3/3	CRITICAL: Interface 15 is down!
14.FIBRA FICA-POSTGRADO		OK	01-02-2014 11:17:30	9d 12h 30m 49s	1/3	OK for 16 - Average IN: 533.03Kbps 0.05% Average OUT: 4.28Mbps 0.43%
15.FICA-LABCISCO-01		OK	01-02-2014 11:17:30	9d 21h 14m 28s	1/3	OK for 17 - Average IN: 30.56Kbps 0.00% Average OUT: 302.60Kbps 0.03%

Figura 46. Servicios ejecutados en el SW-Aristóteles  
Fuente: Sistema de monitoreo NAGIOS

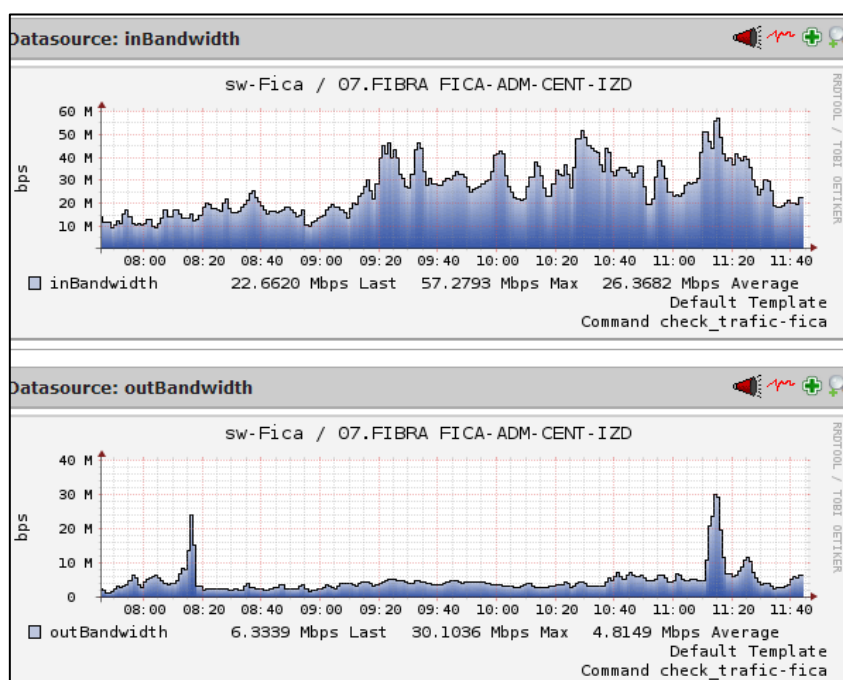


Figura 47. Tráfico de red en el SW-Aristóteles  
Fuente: Sistema de monitoreo NAGIOS

En la figura 48 se puede observar el estado de las VLAN, así como el tráfico entrante y saliente por cada interfaz configurada en el equipo. Las VLAN son propagadas por el equipo SW-Zeus al resto de equipos de la red de la UTN, ya que se encuentra configurado como servidor VTP.

16.VLAN 1 SERVIDORES		OK	01-02-2014 12:03:49	9d 22h 1m 11s	1/3	OK for 166 - Average IN: 2.29Kbps 0.00% Average OUT: 738.17Kbps 0.07%
17.VLAN 2 EQUIPOS-ACTIVOS		OK	01-02-2014 12:03:30	9d 21h 59m 54s	1/3	OK for 172 - Average IN: 975.33bps 0.00% Average OUT: 95.47bps 0.00%
18.VLAN 4 EDIFCENTRAL-FINANCIERO		OK	01-02-2014 12:03:31	0d 3h 41m 5s	1/3	OK for 173 - Average IN: 673.63bps 0.00% Average OUT: 103.32bps 0.00%
19.VLAN 14 FICA-ADM		OK	01-02-2014 12:03:35	9d 5h 47m 11s	1/3	OK for 179 - Average IN: 98.94Kbps 0.01% Average OUT: 3.80Kbps 0.00%
20.VLAN 16 FICA-LAB		OK	01-02-2014 12:04:07	0d 4h 54m 29s	1/3	OK for 180 - Average IN: 29.44Kbps 0.00% Average OUT: 2.49Kbps 0.00%
21.VLAN 18 FICA-CISCO		OK	01-02-2014 12:04:23	0d 4h 13m 13s	1/3	OK for 181 - Average IN: 1.60Kbps 0.00% Average OUT: 595.93bps 0.00%
22.VLAN 64 TELEFONIA IP		CRITICAL	01-02-2014 12:03:35	21d 0h 42m 12s	3/3	CRITICAL Traffic IN for 200 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: 200
23.VLAN 68 WIRELESS FICA		CRITICAL	01-02-2014 12:03:30	21d 1h 1m 53s	3/3	CRITICAL Traffic IN for 202 - 0.00bps, No Traffic Throughput! Please check GGSN Tunnel, for Interface: 202

Figura 48. Servicios en el SW-Aristóteles  
Fuente: Sistema de monitoreo NAGIOS

El estado de las interfaces Fastethernet hacia los switches de acceso ubicados en los laboratorios de la FICA, así como el tráfico entrante y saliente en la misma se puede observar en la figura 49.

24.FAST ETH LABORATORIO I		OK	01-02-2014 12:07:31	3d 13h 4m 32s	1/3	OK for 63 - Average IN: 596.31bps 0.00% Average OUT: 195.44Kbps 0.20%
25.FAST ETH LABORATORIO II		OK	01-02-2014 12:07:35	9d 6h 16m 20s	1/3	OK for 64 - Average IN: 14.62Kbps 0.01% Average OUT: 291.04Kbps 0.29%
26.FAST ETH LABORATORIO III		OK	01-02-2014 12:07:07	9d 22h 0m 1s	1/3	OK for 65 - Average IN: 34.19Kbps 0.03% Average OUT: 616.36Kbps 0.62%
27.FAST ETH LABORATORIO IV		OK	01-02-2014 12:07:23	9d 21h 59m 41s	1/3	OK for 66 - Average IN: 1.70Kbps 0.00% Average OUT: 215.92Kbps 0.22%
28.FAST ETH ASOCIACION DE PROFESORES		OK	01-02-2014 12:07:35	9d 9h 30m 20s	1/3	OK for 67 - Average IN: 171.60Kbps 0.17% Average OUT: 2.65Mbps 2.65%
29.FAST ETH SALA DE INVESTIGACION		OK	01-02-2014 12:07:30	9d 21h 59m 1s	1/3	OK for 68 - Average IN: 2.24Kbps 0.00% Average OUT: 215.57Kbps 0.22%

Figura 49. Servicios en el SW-Aristóteles  
Fuente: Sistema de monitoreo NAGIOS

El estado de las interfaces Fastethernet hacia los puntos de acceso inalámbrico ubicados en la FICA, así como su tráfico entrante y saliente se muestra en la figura 50.

30.FAST ETH AP-FICA-PB		OK	01-02-2014 12:11:23	9d 22h 3m 17s	1/3	OK for 91 - Average IN: 161.20Kbps 0.16% Average OUT: 1.14Mbps 1.14%
31.FAST ETH AP-FICA-PA2D		OK	01-02-2014 12:11:35	9d 5h 55m 54s	1/3	OK for 30 - Average IN: 4.02Mbps 4.02% Average OUT: 5.66Mbps 5.66%
32.FAST ETH AP-FICA-PA2I		OK	01-02-2014 12:11:31	9d 22h 2m 37s	1/3	OK for 34 - Average IN: 272.63Kbps 0.27% Average OUT: 2.15Mbps 2.15%
33.FAST ETH AP-FICA-PA3D		OK	01-02-2014 12:11:31	9d 22h 2m 18s	1/3	OK for 60 - Average IN: 237.61Kbps 0.24% Average OUT: 2.56Mbps 2.56%
37.FAST ETH AP-FICA-PA4		OK	01-02-2014 12:11:31	0d 12h 4m 54s	1/3	OK for 57 - Average IN: 2.43Kbps 0.00% Average OUT: 5.51Kbps 0.01%

Figura 50. Servicios en el SW-Aristóteles  
Fuente: Sistema de monitoreo NAGIOS

El tráfico entrante y saliente así como el estado de las interfaces Fastethernet hacia los servidores alojados en la FICA se muestra en la figura 51.

38.FAST ETH SERV-DHCP		OK	01-02-2014 12:11:07	9d 22h 8m 36s	1/3	OK for 63 - Average IN: 25.57Kbps 0.03% Average OUT: 197.65Kbps 0.20%
39.FAST ETH SERV-MOODLE		OK	01-02-2014 12:11:31	9d 22h 8m 16s	1/3	OK for 50 - Average IN: 3.29Kbps 0.00% Average OUT: 11.30Kbps 0.01%
41.FAST ETH SERV-NAGIOS		OK	01-02-2014 12:11:16	9d 22h 9m 56s	1/3	OK for 37 - Average IN: 81.12Kbps 0.08% Average OUT: 33.96Kbps 0.03%

Figura 51. Servicios en el SW-Aristóteles  
Fuente: Sistema de monitoreo NAGIOS

## CAPÍTULO V

### CONTROL DE FALLAS

#### 5.1 INTRODUCCIÓN

La red de datos de la UTN<sup>59</sup> dispone de dos switches CATALYST 4506-E como equipos de distribución, estos equipos están configurados como puente raíz y puente raíz de respaldo dentro del protocolo STP<sup>60</sup> para solventar los problemas de redundancia dentro de la red. El rendimiento en la red de datos de la UTN se monitorea directamente desde estos switches por el sistema NAGIOS ya que estos equipos reciben todo el tráfico que cursa hacia y desde la nube de internet y permiten la propagación de las VLAN hacia la capa de acceso por lo que el control de fallas se orientó al análisis de su configuración y estado actual dentro de la red así como a las recomendaciones específicas para los problemas de consumo de recursos físicos y lógico de los equipos.

#### 5.2 POLÍTICAS PARA EL CONTROL DE FALLAS

- Monitorear el estado de las alarmas generadas por el sistema así como los correos de notificación que se envían a la cuenta del administrador ya que permiten conocer cualquier cambio en el funcionamiento dentro de la red.
- Monitorear el consumo de recursos de hardware como el uso de la memoria RAM, CPU, temperatura o utilidad de disco de los equipos en la red con la finalidad de conocer su rendimiento y detectar que equipos se deberían actualizar con mejores características.
- Monitorear la disponibilidad de los equipos en la red para identificar cualquier desconexión o servicio caído para poder tratar el problema al momento de generarse y mejorar los tiempos de respuesta ante cualquier incidente.
- Monitorear el tráfico de la red para identificar cuellos de botella en interfaces específicas y así poder mejorar el dimensionamiento de la red.

---

<sup>59</sup> UTN: Universidad Técnica del Norte.

<sup>60</sup> STP: Spanning tree protocol (Protocolo de árbol de expansión).



Para conocer las condiciones de operación de los equipos de core dentro de la red se debe diferenciar los términos, estado de servicio y estado de equipo, en la parte superior de la figura 52 se pueden observar estos dos apartados.

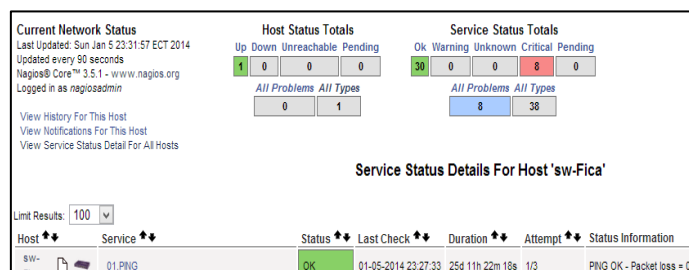


Figura 52. Estado de servicios y equipos en el sistema NAGIOS  
Fuente: Sistema de monitoreo NAGIOS-UTN

### 5.2.1 ESTADO DE HOST

El estado de los equipos de core en la red está definido por el sistema de monitoreo en base a cuatro parámetros, véase la figura 53.

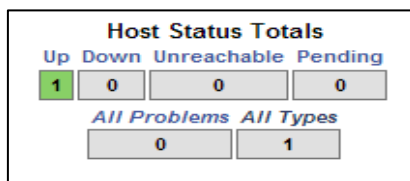


Figura 53. Estado de host  
Fuente: Sistema de monitoreo NAGIOS-UTN

- ✓ Up: Indica el estado activo y alcanzable del equipo en la red.
- ✓ Down: Indica el estado inactivo del equipo en la red.
- ✓ Unreachable: Indica el estado inalcanzable del equipo en la red debido a que otro equipo intermediario se encuentra down.
- ✓ Pending: Indica un problema en el servidor de monitoreo para determinar el estado del equipo debido a una sobrecarga o consumo excesivo de recursos.

### 5.2.2 ESTADO DE SERVICIOS

El estado de los servicios que se ejecutan en los equipos de core son definidos en base a cinco parámetros, por NAGIOS, véase la figura 54.

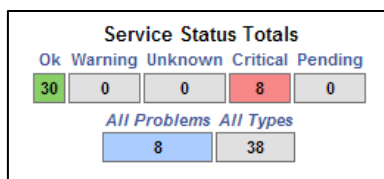


Figura 54. Estado se servicio  
Fuente: Sistema de monitoreo NAGIOS-UTN

- ✓ Ok: Indica el número de servicios que se ejecutan de manera funcional en el equipo.
- ✓ Warning: Indica el número de servicios en estado de advertencia según los parámetros configurados en el servidor.
- ✓ Unknown: Indica el número de servicios interpretados como desconocidos por el servidor de monitoreo, debido a una incorrecta configuración del comando que ejecuta el chequeo del servicio.
- ✓ Critical: Indica el número de servicios en estado crítico según los parámetros configurados en el servidor de monitoreo.
- ✓ Pending: Indica el número de servicios que no pueden ser chequeados por el servidor de monitoreo, debido a una sobrecarga o consumo excesivo de recursos.

El sistema de monitoreo advierte sobre los cambios en el funcionamiento de la CPU<sup>61</sup>, memoria RAM, temperatura, ventiladores, fuente y el tiempo que el equipo ha permanecido encendido. El chequeo de la CPU y memoria RAM permiten conocer el rendimiento del equipo en la red, véase la figura 55.

<sup>61</sup> CPU: Central Processing Unit (Unidad Central de Procesamiento)

Host	Service	Status	Last Check	Duration	Attempt	Status Information
sw-Fica	01.PING	OK	02-04-2014 14:44:56	0d 12h 19m 33s	1/3	ECO OK - Paquetes perdidos = 0%, RTA = 0.46 ms
	02.CPU_5s_1min_5min	OK	02-04-2014 14:48:13	0d 13h 13m 20s	1/3	Cpu: OK - Cpu Load 13% 13% 13%
	03.Mem_Ram	OK	02-04-2014 14:47:18	0d 1h 43m 9s	1/3	Processor:70% : 70% : : OK
	04.Ventilacion	CRITICAL	02-04-2014 14:48:13	0d 1h 43m 12s	3/3	Fans: Crit - 3 Fans are running , Power Supply 1 Fan -> notFunctioning have an error
	05.Fuente	CRITICAL	02-04-2014 14:48:13	0d 1h 43m 12s	3/3	PS: Crit - 2 PS are running , Power Supply 1 -> critical have an error
	06.Uptime	OK	02-04-2014 14:48:03	0d 1h 43m 22s	1/3	SNMP OK - Timeticks: (625874) 1:44:18.74

Figura 55. Servicios monitoreados en los switches de distribución de la UTN  
Fuente: Sistema de monitoreo NAGIOS-UTN

Las razones más comunes para el uso elevado de la CPU debido al procesamiento de paquetes conmutados son:

- Alto número de instancias de puertos STP.
- Bucles de reenvío de Capa 2.
- Reconocimiento del host.
- Recursos de hardware TCAM<sup>62</sup> no disponibles para ACL<sup>63</sup> de seguridad.

### 5.2.3 UN ALTO NÚMERO DE INSTANCIAS DE PUERTOS STP

La capa de distribución de la UTN compuesta por los switches CATALYST 4506-E de capa 3, disponen de los módulos de supervisión que se indican en la tabla 112.

Tabla 112. Módulos de supervisión en los switch de distribución de la UTN  
Fuente: Switches de core UTN

NOMBRE	UBICACIÓN	MÓDULO DE SUPERVISIÓN	MODELO
SW-ZEUS	EDIFICIO CENTRAL	SUP II+10GE 10GE	WS-X4013+10GE
SW-ARISTÓTELES	FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS	SUP II+10GE 10GE	WS-X4013+10GE

Los módulos de supervisión II+10GE soportan hasta 1500 instancias de puertos de árbol de expansión o puertos activos en el modo PVST<sup>64</sup>. Si se excede el número de instancias STP, el switch exhibirá un uso elevado de la CPU. Es posible calcular las instancias de puerto en modo STP con la siguiente fórmula (CISCO, 2010).

<sup>62</sup> TCAM: Ternary content addressable memory (Memoria direccionable por contenido ternario).

<sup>63</sup> ACL: Access control list (Lista de control de acceso).

<sup>64</sup> PVST: Per VLAN Spanning Tree (spanning tree por VLAN).

Tabla 113. Fórmula para calcular el número de instancias STP

Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

FÓRMULA PARA EL NÚMERO DE INSTANCIAS STP
NUMERO DE INSTANCIAS STP = NUMERO DE PUERTOS DE ACCESO + SUMA DE TODAS LAS VLANS ENVIADAS POR CADA UNO DE LOS ENLACES TRONCALES.

El switch SW-Zeus está configurado como puente raíz en el protocolo STP y como servidor VTP para la propagación de VLAN y presenta en su configuración 44 VLAN, 20 interfaces en modo troncal y 144 en modo de acceso mientras que el SW-Aristóteles está configurado como puente raíz de respaldo, considerando la formula en la tabla 113, se puede calcular el número de instancias STP en el switch Zeus, véase la tabla 114.

Tabla 114. Instancias STP en el SW-Zeus

Fuente: Switch Zeus

SW-ZEUS
NUMERO DE INSTANCIAS STP= 144 + (44X20)
NUMERO DE INSTANCIAS STP= 144+880
NUMERO DE INSTANCIAS STP= 1024

### 5.2.3.1 Conclusión y recomendación

El número de instancias STP que presenta el switch Zeus, véase la tabla 114 está por debajo del límite de 1500, que es el valor soportado por los módulos de supervisión. Para la solución del problema a un número de instancias STP por encima del límite, tener en cuenta los siguientes pasos:

Paso 1: Verifique los procesos del IOS65 de CISCO.

El comando show processes CPU muestra que existen dos procesos principales en ejecución, Cat4k Mgmt LoPri y Spanning, la figura 56 muestra que los procesos del árbol de expansión consumen una porción considerable de los ciclos de la CPU (Cisco Systems, 2010).

<sup>65</sup> IOS: Internetwork Operating System (Sistema operativo de red).

```

Switch#show processes cpu
CPU utilization for five seconds: 74%/1%; one minute: 73%; five minutes: 50%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min   TTY Process
  1         4         198        20  0.00%  0.00%  0.00%  0 Chunk Manager
  2         4         290        13  0.00%  0.00%  0.00%  0 Load Meter
!--- Resultado suprimido.
 25         488         33       14787  0.00%  0.02%  0.00%  0 Per-minute Jobs
 26       90656       223674       405  6.79%  6.90%  7.22%  0 Cat4k Mgmt HiPri
 27     158796     59219       2681 32.55% 33.80% 21.43%  0 Cat4k Mgmt LoPri
 28         20         1693        11  0.00%  0.00%  0.00%  0 Galios Reschedul
 29         0         1         0  0.00%  0.00%  0.00%  0 IOS ACL Helper
 30         0         2         0  0.00%  0.00%  0.00%  0 NAM Manager
!--- Resultado suprimido.
 41         0         1         0  0.00%  0.00%  0.00%  0 SFF8472
 42         0         2         0  0.00%  0.00%  0.00%  0 AAA Dictionary R
 43     78564     20723       3791 32.63% 30.03% 17.35%  0 Spanning Tree
 44         112         999        112  0.00%  0.00%  0.00%  0 DTP Protocol
 45         0         147         0  0.00%  0.00%  0.00%  0 Ethchnl

```

Figura 56. Comando show processes cpu

Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

La tabla 115 muestra los procesos de alta y baja prioridad manejados por la CPU, este mecanismo permite ejecutar procesos de alta prioridad cuando sea necesario y que los ciclos de la CPU inactivos restantes se utilicen para los procesos de baja prioridad.

Tabla 115. Procesos de alta y baja prioridad

Fuente: Cisco Systems, Alta utilización de la CPU en el Catalyst 4506-E, 2010, recuperado de: [http://www.cisco.com/cisco/web/support/LA/7/77/77440\\_cat4500\\_high\\_cpu.html](http://www.cisco.com/cisco/web/support/LA/7/77/77440_cat4500_high_cpu.html)

PROCESOS DE ALTA Y BAJA PRIORIDAD	
Cat4k Mgmt HiPri	Cuando un proceso está dentro de lo establecido, la CPU ejecuta el proceso dentro del contexto de alta prioridad.
Cat4k Mgmt LoPri	Si un proceso excede la utilización predeterminada de la CPU, el proceso se ejecuta bajo el contexto de baja prioridad. Cat4k Mgmt LoPri también se utiliza para ejecutar procesos en segundo plano

Paso 2: Verifique los procesos específicos del CATALYST 4506-E.

El comando *show platform health* permite conocer el nivel de utilización de la CPU, para esto se observa la columna %CPU actual, véase la figura 57. La salida del comando muestra el proceso K2CpuMan Review, véase la tabla 116, un proceso que maneja los paquetes vinculados a la CPU (Cisco Systems, 2010).

```

Switch#show platform health
%CPU %CPU RunTimeMax Priority Average %CPU Total
      Target Actual Target Actual  Fg Bg 5Sec Min Hour CPU
!--- Resultado suprimido.
TagMan-RecreateMtegR  1.00  0.00    10     0  100  500  0  0  0  0:00
K2CpuMan Review      30.00 37.62    30    53  100  500 41 33  1 2:12
K2AccelPacketMan: Tx  10.00  4.95    20     0  100  500  5  4  0 0:36
K2AccelPacketMan: Au   0.10  0.00     0     0  100  500  0  0  0 0:00
K2AclMan-taggedFlatA  1.00  0.00    10     0  100  500  0  0  0 0:00

```

Figura 57. Comando show platform health

Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

La tabla 116, ofrece información básica sobre los procesos de plataforma más comunes que se obtienen como resultado del comando `show platform health`.

Tabla 116. Procesos de plataforma

Fuente: CISCO, High CPU utilization on Cisco IOS software based Catalyst 4500 switches, 2010, recuperado de: <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

PROCESO DE PLATAFORMA	DESCRIPCIÓN
Pim-review	Administración del estado de la tarjeta de línea/chasis.
Ebm	Módulo Ethernet Bridge, como vencimiento y control.
Acl-Flattener /K2AclMan	Proceso de fusión de ACL.
KxAclPathMan - PathTagMan-Review	Mantenimiento y administración de ACL.
K2CpuMan Review	Proceso que realiza el reenvío de paquetes por software. Si existe una alta utilización de la CPU debido a este proceso, estudie el tipo de paquete con el comando <code>show platform CPU packet statistics</code> .
K2AccelPacketMan	Controlador que interactúa con el envío de los paquetes que están destinados desde la CPU.
K2AclCamMan	Administra el hardware TCAM de entrada y salida para las funciones QoS <sup>66</sup> y de seguridad.
K2AclPolicerTableMan	Administra los reguladores de entrada y salida.
K2L2	Representa el sistema de reenvío de L2 del switch Catalyst de la serie 4500 con software Cisco IOS. Estos procesos son responsables del mantenimiento de las distintas tablas L2.
K2PortMan Review	Administra las diferentes funciones de programación relacionadas con los puertos.
K2Fib	Administración FIB <sup>67</sup> .
K2FibFlowCache	Administración de caché PBR <sup>68</sup> .
K2FibAdjMan	Administra la tabla de adyacencia FIB.
K2FibMulticast	Administra entradas FIB de multidifusión.
K2MetStatsMan Review	Administra estadísticas MET <sup>69</sup> .
K2QosDblMan Review	Administra QoS DBL <sup>70</sup> .
IrmFibThrottler Thro	Módulo de IP Routing.
K2 L2 Aging Table Re	Administra la función de vencimiento L2.
GalChassisVp-review	Supervisión del estado del chasis.
S2w-JobEventSchedule	Administra los protocolos S2W <sup>71</sup> para controlar el estado de las tarjetas de línea.
Stub-JobEventSchedul	Control y mantenimiento de la tarjeta de línea basada en ASIC <sup>72</sup> Stub.
RkiosPortMan Port Re	Mantenimiento y control del estado del puerto.
Rkios Module State R	Mantenimiento y control de la tarjeta de línea.
EthHoleLinecardMan	Administra los GBIC <sup>73</sup> en cada una de las tarjetas de línea.

Paso 3: Verifique la cola de la CPU que recibe el tráfico para poder identificarlo.

El comando `show platform cpu packet statistics` permite verificar qué cola de la CPU recibe los paquetes, la figura 58 muestra que la cola de control recibe un alto número de paquetes. La tabla 117, describe el tipo de cola y el tráfico asociado a la misma (CISCO, 2010).

<sup>66</sup> QOS: Quality of service (Calidad de Servicio).

<sup>67</sup> FIB: Forwarding information base (Base de información de reenvío).

<sup>68</sup> PBR: Policy based routing (Enrutamiento basado en políticas).

<sup>69</sup> MET: Multicast expansion table (Tabla de expansión multicast).

<sup>70</sup> DBL: Dynamic buffer limiting (Buffer dinámico limitado).

<sup>71</sup> S2W: Serial to wire (Cable serial 2).

<sup>72</sup> ASIC: Application specific integrated circuit (Circuito integrado de aplicación específica).

<sup>73</sup> GBIC: Gigabit interface converter (Convertidor de interfaz gigabit).

```

Switch#show platform cpu packet statistics
/--- Resultado suprimido.
Total packet queues 16
Packets Received by Packet Queue
-----
Queue                Total          5 sec avg 1 min avg 5 min avg 1 hour avg
-----
EsmP                  202760         196         173         128         28
Control               388623         2121        1740         598         16

Packets Dropped by Packet Queue
-----
Queue                Total          5 sec avg 1 min avg 5 min avg 1 hour avg
-----
Control               17918          0           19           24           3

```

Figura 58. Comando show platform cpu packet statistics

Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

Tabla 117. Colas de la CPU

Fuente: CISCO, High CPU utilization on Cisco IOS software based Catalyst 4500 switches, 2010, recuperado de: <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

NÚMERO DE COLA	NOMBRE DE COLA	PAQUETES EN COLA
0	EsmP <sup>74</sup>	Paquetes de administración interna para las tarjetas de línea ASIC u otros componentes de administración.
1	Control	Paquetes del plano de control L2, como STP, CDP <sup>75</sup> , PAgP <sup>76</sup> , LACP <sup>77</sup> o UDLD <sup>78</sup>
2	Host Learning	Tramas con direcciones MAC de origen desconocidas que se copian a la CPU para poder construir la tabla de reenvío L2
3, 4, 5	L3 Fwd Highest, L3 Fwd High/Medium, L3 Fwd Low	Los paquetes se deben reenviar por software como Túneles GRE <sup>79</sup> . Si no se resuelve el ARP <sup>80</sup> para la dirección IP <sup>81</sup> de destino, los paquetes se envían a esta cola
6, 7, 8	L2 Fwd Highest, L2 Fwd High/Medium, L2 Fwd Low	Los paquetes que se reenvían como resultado de un bridge: <ul style="list-style-type: none"> <li>• Los protocolos que no se soportan en el hardware, como IPX<sup>82</sup> y los paquetes enrutados Apple Talk, se conectan a través de un bridge a la CPU.</li> <li>• Solicitud y respuesta ARP</li> <li>• Los paquetes con una dirección de destino MAC en interfaz SVI<sup>83</sup>/L3 del switch se conectan por bridges si los paquetes no se pueden enrutar por el hardware debido a alguna de las siguientes razones: <ul style="list-style-type: none"> <li>• Las opciones de encabezado IP</li> <li>• TTL<sup>84</sup> expirado</li> <li>• No existe una encapsulación Ethernet II.</li> </ul> </li> </ul>
9, 10	L3 Rx High, L3 Rx Low	El tráfico del plano de control L3, protocolos de ruteo, que están destinados a otras direcciones IP. Algunos ejemplos incluyen: Telnet, SNMP <sup>85</sup> y SSH <sup>86</sup> .
11	RPF Failure	Verificar los paquetes de multidifusión que fallaron en el RPF <sup>87</sup> .
12	ACL fwd(snooping)	Paquetes que están procesados por el DHCP <sup>88</sup> snooping, por una inspección ARP dinámica o por las funciones de indagación IGMP <sup>89</sup>
13	ACL log, unreachable	Paquetes que llegan a un ACE <sup>90</sup> con la palabra clave log o paquetes que fueron rechazados debido a una negación en una ACL de salida o a la falta de una ruta al destino.
14	ACL sw processing	Estos paquetes requieren la generación de mensajes de ICMP <sup>91</sup> fuera de alcance. Paquetes que son impulsados a la CPU debido a la falta de recursos de hardware ACL adicionales, como TCAM, por razones de seguridad ACL.
	MTU Fail/Invalid	Los paquetes que necesitan ser fragmentados debido a que el tamaño de la interfaz de salida MTU <sup>92</sup> es más pequeño que el tamaño del paquete

<sup>74</sup> ESMP = Even simpler management protocol (Protocolo de administración simple).

<sup>75</sup> CDP: Cisco Discovery Protocol (Protocolo de descubrimiento de Cisco).

<sup>76</sup> PAgP: Port aggregation protocol (Protocolo de agregación de puertos).

<sup>77</sup> LACP: Link aggregation control protocol (Protocolo de control de agregación de enlaces).

<sup>78</sup> UDLD: Unidirectional link detection (Detección de enlace unidireccional).

<sup>79</sup> GRE: Generic routing encapsulation (Encapsulación de ruteo genérica).

<sup>80</sup> ARP: Address resolution protocol (Protocolo de resolución de direcciones).

<sup>81</sup> IP: Internet protocol (Protocolo de internet).

<sup>82</sup> IPX: Internetwork packet exchange (Intercambio de paquetes inter red)

<sup>83</sup> SVI: Switch virtual interface (Interfaz virtual conmutada).

<sup>84</sup> TTL: Time to live (Tiempo de vida).

<sup>85</sup> SNMP: Simple network management protocol (Protocolo simple de administración de red).

<sup>86</sup> SSH: Secure shell (Intérprete de órdenes segura).

<sup>87</sup> RPF: Reverse Path Forwarding (Trayecto inverso Unicast).

<sup>88</sup> DHCP: Dynamic Host Configuration Protocol (Protocolo de configuración dinámica de hosts).

<sup>89</sup> IGMP: Internet group management protocol (Protocolo de administración de grupos de Internet).

<sup>90</sup> ACE: Access control entry (Entrada de control de acceso).

<sup>91</sup> ICMP: Internet Control Message Protocol (Protocolo de control de mensajes de internet).

La conclusión del paso 1 y la información obtenida en la tabla 117, determina que la alta utilización de la CPU se debe al procesamiento excesivo de la BPDU.

Paso 4: Identifique la causa del problema.

El comando `show spanning-tree summary`, permite verificar si el procesamiento excesivo de la BPDU se debe a un alto número de instancias STP, la figura 59 identifica claramente la raíz del problema (Cisco Systems, 2010).

```
Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID          is enabled
Portfast Default            is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default          is disabled
EtherChannel misconfig guard is enabled
UplinkFast                  is disabled
BackboneFast                is disabled
Configured Pathcost method used is short
!--- Resultado suprimido.
Name                        Blocking Listening Learning Forwarding STP Active
-----
2994 vlans                  0          0          0          5999      5999
```

Figura 59. Comando `show spanning-tree summary`

Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

Paso 5: Conclusión y recomendación.

Los switches de core Catalyst 4506 E que brindan el acceso hacia la nube de internet a la UTN, presentan una configuración PVST+ como mecanismo de redundancia en caso de haber algún enlace caído, ambos equipos cuentan con los módulos de supervisión II+10GE que soportan hasta 1500 instancias de puertos activos en modo STP por VLAN (PVST).

Si se excede el número de instancias STP, el switch exhibirá un uso elevado de la CPU. Ya que en el modo de redundancia PVST+ cada VLAN representa una instancia STP y el número de puertos troncales y de acceso será mayor mientras crece la infraestructura de red, sería necesario cambiar el modo PVST a MST (Multiple Spanning Tree, árbol de expansión múltiple) el cual permite asignar varias VLAN a una misma instancia STP, separando las

---

<sup>92</sup> MTU: Maximum transfer unit (Unidad máxima de transferencia).



VLAN que no son necesarias del enlace troncal para disminuir la cantidad de puertos activos STP (CISCO, 2010).

#### **5.2.4 BUCLES DE REENVÍO DE CAPA 2**

STP hace suposiciones acerca de su entorno operativo, como que cada enlace entre dos switches es bidireccional, esto significa que, si A se conecta directamente a B, entonces A recibe lo que B envía y B recibe lo que A envía.

Cada switch que ejecuta STP es capaz de recibir con regularidad, procesar y transmitir BPDU. Aunque estos supuestos parezcan obvios, hay situaciones en las que no se cumplen, situaciones que implican problemas de hardware o defectos en el software. Fallos de hardware, errores de configuración, problemas en el cableado o conexiones adicionales innecesarias entre switches causan problemas con STP, por ello uno o más switches podrían dejar de recibir o procesar las BPDU recibidas y no podrán descubrir la topología de red, sin el conocimiento de la topología correcta, el switch no podrá bloquear los enlaces redundantes y generar bucles de capa 2 o en consecuencia tormentas de broadcast, consumiendo todo el ancho de banda de la red., para poder evitar que se generen bucles de capa 2, es necesario asegurar la red con características avanzadas de STP:

- **BDPU Guard:** Evita la recepción de BPDU emitidas por switches no autorizados dentro de la red. Revisar el anexo 1 para más información.
- **Loop Guard:** Proporciona protección adicional contra bucles de capa 2 y bloquea los puertos del switch si no se reciben BPDU. Revisar anexo 2 para más información.
- **Root Guard:** Controla donde puede encontrarse y conectarse el puente raíz dentro de la red. Revisar anexo 3 para más información.
- **UDLD:** Monitoriza los puerto para conocer si el enlace es bidireccional. Revisar anexo 4 para más información.

### 5.2.5 RECONOCIMIENTO DEL HOST

El switch Catalyst 4500 reconoce las direcciones MAC de distintos hosts si no figuran en la tabla de direcciones. El motor de conmutación reenvía una copia del paquete con la nueva dirección MAC a la CPU. Si existe una cantidad excesiva de nuevas direcciones que el switch tendría que reconocer, se ocasionaría una alta utilización de la CPU, para identificar esta situación considerar los siguientes pasos:

Paso 1: Verifique los procesos del IOS con el comando *show processes cpu*.

El comando *show processes cpu* permite identificar los procesos que consumen la CPU. La figura 60 muestra que el proceso Cat4k Mgmt LoPri, véase la tabla 115, consume un alto porcentaje de la CPU. (Cisco Systems, 2010)

```
Switch#show processes cpu
CPU utilization for five seconds: 89%/1%; one minute: 74%; five minutes: 71%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TY Process
  1         4         53        75     0.00%  0.00%  0.00%  0 Chunk Manager
!--- Resultado suprimido.
 25         8008        1329154     6     0.00%  0.00%  0.00%  0 Per-Second Jobs
 26        413128        38493    10732   0.00%  0.02%  0.00%  0 Per-minute Jobs
 27    148288424    354390017     418   26.47% 10.28% 10.11%  0 Cat4k Mgmt HiPri
 28    285796820    720618753     396  52.71% 56.79% 55.70%  0 Cat4k Mgmt LoPri
```

Figura 60. Comando show processes cpu

Fuente: Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

Paso 2: Verifique los procesos específicos del Catalyst 4500 con el comando *show platform health*.

Para conocer el nivel de utilización de la CPU se debe ejecutar el comando *show platform health*, el cual muestra el consumo de cada proceso en ejecución, la columna %CPU actual, véase la figura 61, muestra el consumo real de la CPU. La tabla 116 muestra que el proceso K2CpuMan Review, el cual se encarga de vincular los paquetes a la CPU, presenta un alto consumo (CISCO, 2010).

```
Switch#show platform health
```

	%CPU Target	%CPU Actual	RunTimeMax Target	RunTimeMax Actual	Priority Fg	Priority Bg	Average 5Sec	%CPU Min	%CPU Hour	Total CPU
!--- Resultado suprimido.										
TagMan-RecreateMtegR	1.00	0.00	10	4	100	500	0	0	0	0:00
K2CpuMan Review	30.00	46.88	30	47	100	500	30	29	21	265:01
K2AccelPacketMan: Tx	10.00	8.03	20	0	100	500	21	29	26	270:4

Figura 61. Comando show platform health

Fuente: Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

Paso 3: Verifique la cola de la CPU que recibe el tráfico para identificar el tipo de tráfico entrante.

El comando *show platform cpu packet statistics* permite determinar el tráfico que llega a la CPU, la figura 62 muestra que la cola *host learning* recibe un alto número de paquetes, ver la tabla 117. De modo que la alta utilización de la CPU es el aprendizaje de un alto número de direcciones Mac (Cisco Systems, 2010).

```
Switch#show platform cpu packet statistics
```

!--- Resultado suprimido.

Packets Received by Packet Queue

Queue	Total	5 sec avg	1 min avg	5 min avg	1 hour avg
Eemp	48613268	38	39	38	39
Control	142166648	74	74	73	73
Host Learning	1845568	1328	1808	1393	1309
L3 Fwd High	17	0	0	0	0
L3 Fwd Medium	2626	0	0	0	0
L3 Fwd Low	1582414	1	1	1	1
L2 Fwd Medium	1	0	0	0	0
L2 Fwd Low	576905398	37	7	8	5
L3 Rx High	257147	0	0	0	0
L3 Rx Low	5325772	10	19	13	7
RPF Failure	155	0	0	0	0
ACL fwd(enooping)	65604591	53	54	54	53
ACL log, unreach	11013420	9	8	8	8

Figura 62. Comando show platform cpu packet statistics

Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

Paso 4: Conclusión y recomendación.

El resultado obtenido en el paso 1 y 2 muestra que la CPU puede ver una gran cantidad de nuevas direcciones MAC. Esta situación es el resultado de una inestabilidad en la topología de red, cuando se originan cambios en la topología del árbol de expansión, el switch genera notificaciones de cambio en la topología (TCN), la emisión de TCN reduce el tiempo de vencimiento MAC a 15 segundos en el modo PVST+, las entradas de las direcciones MAC se purgan si no se reconocen dentro de este tiempo.

En el caso de STP rápido (RSTP) (IEEE 802.1w) o MST (IEEE 802.1s), las entradas se vencen automáticamente. Este vencimiento hace que las direcciones MAC se tengan que aprender o reconocer nuevamente. Esto no representa un aspecto importante cuando los cambios en la topología están dentro de lo normal, pero es posible que exista una cantidad excesiva de cambios topológicos a causa de un enlace alternado, un switch defectuoso o puertos de host que no están activos en modo PortFast, lo que podría resultar en una gran cantidad de depuraciones en la tabla MAC y su posterior reaprendizaje, en este caso también se podría aumentar el tiempo de vencimiento de las direcciones MAC para que el switch disponga de más tiempo y le permita retener las direcciones MAC de los dispositivos durante un mayor periodo de tiempo antes de que venzan (Cisco Systems, 2010).

### 5.2.6 RECURSOS DE HARDWARE (TCAM) NO DISPONIBLES PARA LAS ACL DE SEGURIDAD

El Catalyst 4500 programa las ACL configuradas con el uso de la TCAM. La tabla TCAM permite evaluar un paquete contra una lista de acceso entera con una simple búsqueda en la tabla TCAM, esta tabla permite las aplicaciones de ACL en trayecto de reenvío por hardware, este trayecto no tiene ningún impacto en el desempeño del switch, el desempeño es constante a pesar del tamaño de la ACL, sin embargo, la TCAM es un recurso limitado. Entonces, si se configura una cantidad excesiva de entradas ACL se puede exceder la capacidad de la TCAM, la tabla 118 muestra el número de recursos TCAM disponible en los motores de supervisión (Supervisor Engine) instalados en los equipos de core.

*Tabla 118.* Disponibilidad de la TCAM en los switches de core UTN  
Fuente: Cisco Systems, Alta utilización de la CPU en el Catalyst 4506-E, 2010, recuperado de:  
[http://www.cisco.com/cisco/web/support/LA/7/77/77440\\_cat4500\\_high\\_cpu.html](http://www.cisco.com/cisco/web/support/LA/7/77/77440_cat4500_high_cpu.html)

PRODUCTO	FUNCIÓN TCAM (POR DIRECCIÓN)	TCAM DE CALIDAD DE SERVICIO (QOS) (POR DIRECCIÓN)
Supervisor Engine II+/II+TS	8192 entradas con 1024 máscaras	8192 entradas con 1024 máscaras
Supervisor Engine III/IV/V y Catalyst 4948	16.384 entradas con 2048 máscaras	16.384 entradas con 2048 máscaras
Supervisor Engine V-10GE y Catalyst 4948-10GE	16.384 entradas con 16.384 máscaras	16.384 entradas con 16.384 máscaras

Si el Catalyst 4500 se queda sin recursos TCAM durante la programación de una ACL de seguridad, una parte de la aplicación de la ACL se lleva a cabo a través del trayecto por software, lo que causa una alta utilización de la CPU.

La figura 63 muestra el mensaje de error que se presenta en la salida del comando show logging. El mensaje indica que se llevará a cabo el procesamiento por software y que esto podría generar una alta utilización de la CPU.

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
Security: 140 - insufficient hardware TCAM masks.
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing will be software switched.
```

Figura 63. Comando show logging

Fuente: Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

Paso 1: Verifique los procesos del IOS de Cisco.

El comando show processes cpu permite identificar los procesos que consumen la CPU. La figura 64 muestra que el proceso Cat4k Mgmt LoPri, véase la tabla 115, consume un alto porcentaje de la CPU (Cisco Systems, 2010).

```
Switch#show processes cpu
CPU utilization for five seconds: 99%/0%; one minute: 99%; five minutes: 99%
PID Runtime(ms)   Invoked    uSecs   5Sec   1Min   5Min  TTY Process
  1         0         11         0  0.00%  0.00%  0.00%  0 Chunk Manager
  2      9716     632814     15  0.00%  0.00%  0.00%  0 Load Meter
  3       780       302     2582  0.00%  0.00%  0.00%  0 SpanTree Helper
!--- Resultado suprimido.
 23     18208   3154201      5  0.00%  0.00%  0.00%  0 TTY Background
 24     37208   3942818      9  0.00%  0.00%  0.00%  0 Per-Second Jobs
 25    1046448   110711    9452  0.00%  0.03%  0.00%  0 Per-minute Jobs
 26   175803612 339500656    517  4.12%  4.31%  4.48%  0 Cat4k Mgmt HiPri
 27   835809548 339138782   2464 86.81% 89.20% 89.76%  0 Cat4k Mgmt LoPri
 28     28668   2058810     13  0.00%  0.00%  0.00%  0 Galios Reschedul
```

Figura 64. Comando show processes cpu

Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

Paso 2: Verifique los procesos específicos al Catalyst 4500.

El comando *show platform health* muestra el nivel de utilización de la CPU que consume cada proceso en ejecución, la columna %CPU actual, muestra el consumo real de la CPU, véase la figura 65.

Se puede observar que el proceso K2CpuMan Review, véase la tabla 116, el cual se encarga de vincular los paquetes a la CPU, presenta un alto consumo (Cisco Systems, 2010).

```
Switch#show platform health
%CPU %CPU RunTimeMax Priority Average %CPU Total
Target Actual Target Actual Fg Bg 5Sec Min Hour CPU
Lj-poll 1.00 0.01 2 0 100 500 0 0 0 13:45
GalChassisVp-review 3.00 0.20 10 16 100 500 0 0 0 88:44
S2w-JobEventSchedule 10.00 0.57 10 7 100 500 1 0 0 404:22
Stub-JobEventSchedule 10.00 0.00 10 0 100 500 0 0 0 0:00
StatValueMan Update 1.00 0.09 1 0 100 500 0 0 0 91:33
Pim-review 0.10 0.00 1 0 100 500 0 0 0 4:46
Ebm-host-review 1.00 0.00 8 4 100 500 0 0 0 14:01
Ebm-port-review 0.10 0.00 1 0 100 500 0 0 0 0:20
Protocol-aging-revie 0.20 0.00 2 0 100 500 0 0 0 0:01
Acl-Flattener 1.00 0.00 10 5 100 500 0 0 0 0:04
KxAclPathMan create/ 1.00 0.00 10 5 100 500 0 0 0 0:21
KxAclPathMan update 2.00 0.00 10 6 100 500 0 0 0 0:05
KxAclPathMan reprogr 1.00 0.00 2 1 100 500 0 0 0 0:00
TagMan-InformMtegRev 1.00 0.00 5 0 100 500 0 0 0 0:00
TagMan-RecreateMtegR 1.00 0.00 10 14 100 500 0 0 0 0:18
K2CpuMan Review 30.00 91.31 30 92 100 500 128 119 84 13039:02
K2AccelPacketMan: Tx 10.00 2.30 20 0 100 500 2 2 2 1345:30
K2AccelPacketMan: Au 0.10 0.00 0 0 100 500 0 0 0 0:00
```

Figura 65. Comando show platform health

Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

Paso 3: Verifique la cola de la CPU que recibe el tráfico para identificar el tipo de tráfico.

El comando *show platform cpu packet statistics* permite conocer el tráfico que llega a la CPU, la figura 66 muestra que la cola ACL sw processing recibe un alto número de paquetes, ver la tabla 117. De modo que la alta utilización de la CPU es el desbordamiento de TCAM (CISCO, 2010).

```
Switch#show platform cpu packet statistics
!--- Resultado suprimido.
Packets Received by Packet Queue
Queue ----- Total ----- 5 sec avg 1 min avg 5 min avg 1 hour avg -----
Control 57902635 22 16 12 3
Host Learning 464678 0 0 0 0
L3 Fwd Low 623229 0 0 0 0
L2 Fwd Low 11267182 7 4 6 1
L3 Rx High 508 0 0 0 0
L3 Rx Low 1275695 10 1 0 0
ACL fwd(snooping) 2645752 0 0 0 0
ACL log, unreach 51443268 9 4 5 5
ACL sw processing 842889240 1453 1532 1267 1179

Packets Dropped by Packet Queue
Queue ----- Total ----- 5 sec avg 1 min avg 5 min avg 1 hour avg -----
L2 Fwd Low 3270 0 0 0 0
ACL sw processing 12636 0 0 0 0
```

Figura 66. Comando show platform cpu packet statistics

Fuente: Fuente: CISCO Catalyst serie 4500, (2010), recuperado de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>

Paso 4: Conclusión y recomendación

Después de determinar que la causa del alto consumo de la CPU es el desbordamiento de la TCAM debido a un ingreso elevado de listas de control de acceso, se podría optar por eliminar la ACL que causó el desbordamiento o minimizar el número de listas de acceso con métodos para optimizar la configuración y la programación de la ACL. Si se desea tener mayor capacidad en la TCAM para que se pueda soportar un mayor número de listas de acceso se puede mejorar las características del motor de supervisión. La tabla 119 muestra los motores de supervisión compatibles con el catalyst 4506-E, la tabla 118 muestra la capacidad de la TCAM para cada motor de supervisión (CISCO, 2010).

*Tabla 119.* Motores de supervisión compatibles con los switches de core UTN  
Fuente: CISCO, Features of the Catalyst 4506-E, 2013, recuperado de:  
<http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/hardware/catalyst4500e/installation/guide/Eseries/01intro.html#wp1028437>

SWITCH	MÓDULO DE SUPERVISIÓN
CATALYST 4506-E	SUPERVISOR ENGINE 7L-E
	SUPERVISOR ENGINE 7-E
	SUPERVISOR ENGINE 6L-E
	SUPERVISOR ENGINE 6-E
	SUPERVISOR ENGINE V-10GE
	SUPERVISOR ENGINE V
	SUPERVISOR ENGINE IV
	SUPERVISOR ENGINE II-PLUS-10GE
	SUPERVISOR ENGINE II-PLUS

### 5.2.7 PROTOCOLO HSRP<sup>93</sup> Y PORTCHANNEL

El sistema de monitoreo Nagios permitió conocer de forma gráfica configuraciones presentes en los equipos de distribución de la UTN que posteriormente fueron cambiadas debido a su poca utilidad o al impacto en el rendimiento de la red.

Se observó cómo protocolo de redundancia la configuración de HSRP que permite el despliegue de routers redundantes en la red, el switch Zeus se configuró como maestro y Aristóteles como equipo de respaldo además el único equipo que tiene salida hacia la nube de internet es Zeus, por lo que si este dispositivo fallara toda la red de la UTN perdería conectividad hacia el exterior, pensando en instalar enlaces redundantes hacia la nube de

<sup>93</sup> HSRP: Hot Standby Router Protocol (Protocolo de Enrutamiento de Reserva Directa)

internet se cambió la configuración HSRP por STP ya que permite el manejo de tráfico de datos en base a vlan y a enlaces redundantes. También se observó la configuración de un portchannel en el switch Zeus que agrupa 8 interfaces FastEthernet que se conectan al concentrador 2 o switch Ares en el mismo se agruparon 8 interfaces GigabitEthernet, esta interconexión genera un cuello de botella del lado del equipo Zeus pero la falta de disponibilidad de interfaces no permite cambiar esta conexión por ello se actualizará el equipo Zeus por un Cisco Catalyst 4500R+E que soportará el continuo crecimiento en la infraestructura de red de la UTN



## CAPITULO VI

### ANÁLISIS COSTO BENEFICIO

#### 6.1 INTRODUCCIÓN

El análisis costo beneficio comprende el presupuesto de hardware, software y herramientas necesarias para la implementación y funcionamiento del sistema de monitoreo de equipos y servicios en la red de datos de la UTN.

#### 5.2 PRESUPUESTO DE INVERSIÓN

La inversión propuesta se fundamenta en el análisis de todos los requerimientos necesarios para poner en marcha el sistema de monitoreo, el cual comprende de hardware y software que a continuación se detalla:

##### 5.2.1 PRESUPUESTO DE HARDWARE

Para realizar el monitoreo de la red de datos de la UTN se realizó una lista de las características de hardware instaladas en el servidor Nagios, véase la tabla 120, este equipo fue prestado por el área de sistemas con la finalidad de probar el sistema NAGIOS y conocer su utilidad dentro de la red de datos en la UTN.

Tabla 120. Presupuesto de inversión para el servidor de monitoreo  
Fuente: <http://www.ibm.com/>

HARDWARE	DESCRIPCIÓN	COSTO (\$)
SERVIDOR	IBM SYSTEM X3200 M2	1000
S.O	UBUNTU-SERVER 12.04	
CPU	INTEL(R) XEON(R) CPU / E3110 @ 3.00GHZ	
RAM	2GIB / 2 DIMM DDR2 DE 1GIB	
DISCO DURO	ATA DISK/HITACHI HDT72502/CAPACIDAD: 232GIB (250GB)	
ETHERNET	ETH1/GIGABIT ETHERNET PCI EXPRESS/ BROADCOM CORPORATION/ CAPACIDAD: 1GBIT/S ETH0/VT6105/VT6106S/ VIA TECHNOLOGIES/ CAPACIDAD: 100MBIT/S	
COSTO TOTAL		1000

### 5.2.2 PRESUPUESTO DE SOFTWARE

Además de los recursos de hardware, el sistema de monitoreo necesita distintos complementos de software para poder cumplir con los requerimientos de monitoreo, el software implementado es libre, por lo que no se requiere la compra de ninguna licencia para el funcionamiento del sistema, véase la tabla 121.

*Tabla 121.* Presupuestos de inversión para el software implementado en el sistema de monitoreo  
Fuente: <http://oss.oetiker.ch/rrdtool/license.en.html>, <http://doc.ubuntu-es.org/Postfix>,  
<http://www.nagiosql.org/nagiosql-license-guidelines.html>, <https://docs.pnp4nagios.org/es/pnp-0.6/about#licencia>,  
<http://nagios.sourceforge.net/docs/nagioscore/3/en/about.html#licensing>, <http://www.apache.org/licenses/>

APLICACIÓN	DESCRIPCIÓN	LICENCIA	COSTO (\$)
NAGIOS	SISTEMA DE MONITOREO	GNU GPL	0
APACHE 2	SERVIDOR WEB	SOFTWARE LIBRE/ LICENCIA APACHE	0
NAGIOSQL	HERRAMIENTA VISUAL DE CONFIGURACIÓN DE NAGIOS VÍA WEB	BSD	0
RRDTOOL	HERRAMIENTA DE BASE DE DATOS PARA EL ALMACENAMIENTO DE INFORMACIÓN DE RENDIMIENTO GENERADA POR NAGIOS.	GNU GPL	0
PNP4NAGIOS	ADITIVO PARA LA GENERACIÓN DE GRÁFICOS ESTADÍSTICOS Y REPORTES VISUALES	GNU GPL	0
POSTFIX	AGENTE DE TRANSPORTE DE CORREO	SOFTWARE LIBRE/ LICENCIA PÚBLICA IBM	0
COSTO TOTAL			0

### 5.2.3 ANÁLISIS DE GASTOS EN SOFTWARE PROPIETARIO

La inversión en la compra de un software de monitoreo propietario varía dependiendo de las características del mismo así como del número de equipos y servicios que se desean monitorear, para el análisis se seleccionó *whatsupgold*, que es un potente y complejo software de monitoreo utilizado ampliamente en grandes infraestructuras de red, el costo de este software en particular depende del número de equipos a monitorear y las licencias se deben actualizar cada año, la tabla 122 detalla información de este aplicativo.

*Tabla 122.* Presupuestos de inversión para el software propietario *whatsupgold*  
Fuente: <http://www.whatsupgold.com/online-shop/global/index.aspx>

NUMERO DE DISPOSITIVOS	COSTO (\$)
HASTA 25 DISPOSITIVOS	2195
HASTA 100 DISPOSITIVOS	3195
HASTA 300 DISPOSITIVOS	5995
HASTA 500 DISPOSITIVOS	8495

## 5.2.4 PRESUPUESTO TOTAL

El presupuesto total es el resultado del presupuesto de hardware y software implementados en el sistema de monitoreo: 1000 (\$) + 0 (\$) = 1000 (\$). Para el análisis costo beneficio se tendrá en cuenta este valor.

## 5.2.5 ANÁLISIS COSTO BENEFICIO

Tiene como objetivo fundamental proporcionar una medida de la rentabilidad de un proyecto, mediante la comparación de los costos previstos con los beneficios esperados en la realización del mismo. Además es una técnica importante que pretende determinar la conveniencia de un proyecto mediante la valoración posterior en términos monetarios de todos los costos y beneficios derivados de dicho proyecto.

### 5.2.5.1 Cálculo Beneficio/Costo

La fórmula de relación de beneficio/costo genera los siguientes criterios que guían las decisiones de aceptación o rechazo del proyecto:

- a) Si el B/C es mayor o igual a 1.0, el proyecto debe aceptarse.
- b) Caso contrario, el proyecto debe rechazarse.

Para conocer el beneficio/costo se cuenta con los siguientes datos obtenidos de las tablas de presupuesto de software, hardware y software propietario.

$$B/C = \frac{\text{Beneficio-Contrabeneficios}}{\text{Costo}}$$

*Ecuación 1. Fórmula Beneficio/Costo*  
Fuente: Leland Blank, Anthony T. (2006). Ingeniería Económica.  
McGrawHill. México

- Presupuesto del software propietario = presupuesto de hardware + presupuesto Whatsupgold.
- Presupuesto del software propietario = 1000 + 8495 = 9495 dólares.

- Presupuesto del software libre = presupuesto de hardware + presupuesto Nagios.
- Presupuesto del software libre = 1000 + 0 = 1000 dólares.
- Contra beneficios: 0 dólares.
- Beneficios: 9495 – 1000 = 8495 dólares

$$B/C = \frac{8495}{1000}$$

$$B/ C= 8,495$$

## CONCLUSIÓN

Como resultado se obtuvo un costo beneficio de 8,495 positivo, es decir que el proyecto se considera aceptable ya que los beneficios que se obtendrán con la propuesta son los requeridos en comparación a los costos de adquisición de un software propietario.

Se debe considerar que el presente proyecto es un tema de investigación desarrollado para la UTN por el que no habrá ninguna remuneración económica pero si el beneficio de contar con un sistema que permitirá conocer la ubicación e interconexión de los equipos de comunicación o servidores en la red, permitirá conocer el nivel de utilización del hardware, consumo de ancho de banda y estado de servicios ejecutados, el sistema se basa en software libre de modo que no se tendrá que comprar ninguna licencia para el funcionamiento de la aplicación, NAGIOS es una herramienta útil de monitoreo que ayudará al administrador a conocer el funcionamiento y rendimiento de la red.

## CAPITULO VII

### CONCLUSIONES Y RECOMENDACIONES

#### 7.1 CONCLUSIONES

- La redundancia en la red de la UTN se maneja con STP y el equipo CISCO CATALYST 4506-E alojado en el edificio central, nombrado SW-Zeus, está configurado como puente raíz para la determinación de rutas que se deben bloquear, el equipo CISCO CATALYST 4506-E alojado en la FICA nombrado SW-Aristóteles, se encuentra configurado como puente raíz alternativo en caso de que se presente alguna falla con el puente raíz principal, cabe recalcar que únicamente el SW-Zeus tiene acceso hacia la nube de internet por lo que si se tiene algún problema con este equipo toda la red de la UTN perdería conectividad hacia el exterior.
- Se optó como herramienta de monitoreo NAGIOS, por cumplir con los requerimientos propuestos como permitir el manejo de reportes, generación de gráficas y envío de notificaciones y por ser el primer sistema libre de monitoreo en aparecer en el mercado ya que su núcleo constituye la base del funcionamiento de nuevos software de monitoreo, por lo que NAGIOS se puede migrar o complementarse con otros sistemas con la finalidad de mejorar características propias, como frontales web más completos y vistosos o maneras de almacenar y procesar la información.
- Se instaló NagiosQL como sistema de administración para configurar el sistema de monitoreo Nagios por medio de una interfaz gráfica ya que normalmente la configuración se realiza en archivos.

- Para la visualización de gráficas se optó por el módulo PNP4NAGIOS que procesa los datos de rendimiento de cada servicio ejecutado por Nagios y almacena la información en la base de datos RRD (bases de datos Round Robin) para su visualización desde la web, por cada origen de datos se necesitará aproximadamente 400 KB de espacio en disco y es necesario que los plugin utilizados por Nagios permitan la recolección de datos de rendimiento de lo contrario no se podrían generar gráficas.
- Para poder monitorear equipo de conmutación desde el sistema Nagios, es necesario que el dispositivo tenga habilitado SNMP y pertenezca a la misma comunidad de administración, de modo que se pueda tener acceso a la información entregada por los OID desde la MIB, Nagios es compatible con SNMPv1 y SNMPv2, por otro lado para monitorear equipos LINUX es necesario instalar un agente de monitoreo que devolverá información del dispositivo al servidor NAGIOS.
- El sistema Nagios recoge información de los equipos monitoreados en base a consultas programadas en el sistema, el envío de traps desde los equipos monitoreados no fue la mejor opción ya que generaba un impacto en el consumo de recursos en los equipos de conmutación de la capa de acceso y distribución de la red en la UTN por lo que el administrador de la red recomendó que el consumo de recursos lo soporte directamente el servidor Nagios ya que se podrían mejorar sus características de hardware para poder cumplir esa función.
- Para que el sistema de monitoreo pueda realizar el envío de notificaciones sin errores es necesario configurarlo en base a un mapeo de red detallado, actualmente hay registros de los equipos y su ubicación dentro de la UTN mas no de su interconexión,

por ello se realizó el mapeo de red completo en la FICA para poder probar la utilidad del sistema.

## 7.2 RECOMENDACIONES

- Las características de hardware en el servidor de monitoreo se deben mejorar según el número de equipos y servicios monitoreados en la red ya que mientras más grande la infraestructura de red, mayor será el consumo de recursos en el servidor lo que se verá reflejado en el encolamiento de procesos y lentitud en el procesamiento de información por parte de NAGIOS.
- El monitoreo de la red de datos de la UTN la realiza un único equipo NAGIOS, no hay un monitoreo distribuido debido a la falta de servidores, aunque después de probar la utilidad del servidor NAGIOS y conocer el rendimiento de la red en la UTN se podría considerar la inversión en la adquisición de nuevos servidores para su posterior instalación en ciertas partes de la universidad para balancear la carga operativa en el actual servidor NAGIOS ya que este sistema permite el balanceo de carga.
- Es necesario establecer políticas de seguridad con normas bien definidas sobre las responsabilidades de los usuarios dentro de la UTN, de modo que se los encamine hacia el uso responsable de los recursos de la red y en conjunto con los sistemas implementados orientados al monitoreo, seguridad y calidad de servicio mejorar el rendimiento y disponibilidad en la misma.
- La actual distribución de Nagios instalada es la versión 3.5.2, este sistema presenta continuas actualizaciones y mejoras por la comunidad al estar disponible bajo

términos de la Licencia Publica General (GNU), por lo que la actualización del sistema debe ser previamente estudiado y probado ya que las nuevas versiones podrían no ser compatibles con los módulos instalados actualmente en el sistema Nagios.

- Actualmente hay registros de los equipos de comunicaciones y su ubicación dentro de la UTN mas no de su interconexión, por lo que la elaboración de un registro actualizado del mapeo de la red de la UTN es necesario si se desea cumplir con los requerimientos de monitoreo y administración de la misma.



## ANEXO A

### MANUAL DE ADMINISTRADOR

#### CONFIGURACIÓN DE EQUIPOS LINUX

##### 1. Definición de equipo

Para agregar un equipo LINUX al sistema de monitoreo se deben seguir los siguientes pasos:

- Acceder al apartado Supervisión-Host-Agregar, véase la figura A.1 y A.2

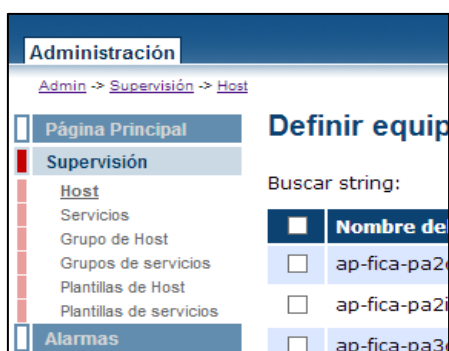


Figura A.1. Definición de equipo LINUX desde NAGIOSQL

Fuente: Sistema de administración NAGIOSQL

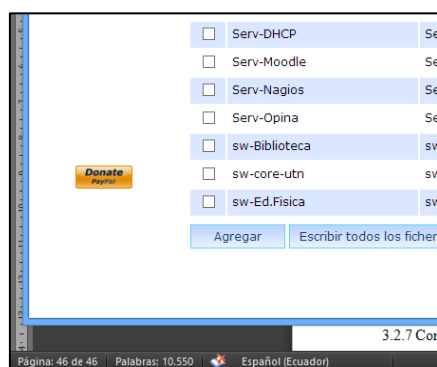


Figura A.2. Definición de equipo LINUX desde NAGIOSQL

Fuente: Sistema de administración NagiosQL

- En la pestaña configuración común, véase las figuras A.3 y A.4, se debe agregar:

- ✓ Nombre del equipo.

- ✓ Dirección IP.
- ✓ Equipo padre o al que se conecta.
- ✓ Descripción.
- ✓ Grupo de equipos al que pertenece.
- ✓ Plantilla de configuración de quipos.

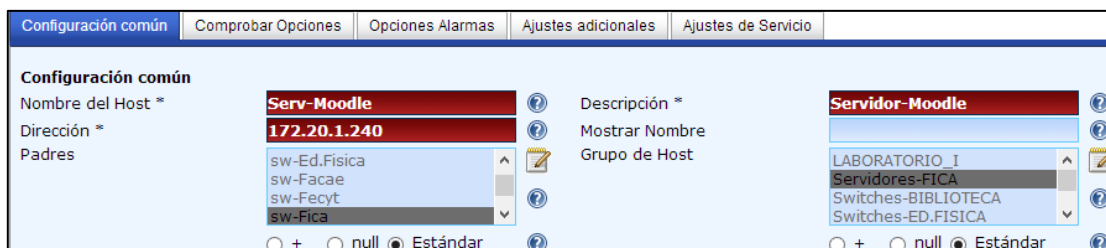


Figura A.3. Configuración general de equipo LINUX desde NagiosQL  
Fuente: Sistema de administración NagiosQL

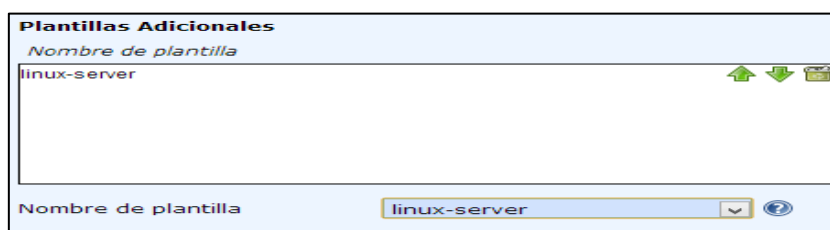


Figura A.4. Selección de plantilla de configuración de equipo LINUX desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- En la pestaña opciones de alarma se agrega el grupo y usuario de contacto para el envío de notificaciones, véase figura A.5.



Figura A.5. Selección de contacto para notificaciones de equipo LINUX desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- En la pestaña ajustes adicionales se agrega la ubicación de las imágenes y texto para el equipo, que se mostraran en la interfaz web, véase figura 38.

Figura A.6. Selección de iconos para equipos LINUX desde NagiosQL  
Fuente: Sistema de administración NagiosQL

## 2. Definición de servicio

Para agregar servicios que se ejecutan en equipos LINUX al sistema de monitoreo se deben seguir los siguientes pasos:

- Acceder al apartado Supervisión-Servicios-Agregar, véase la figura A.7 y A.8.

Figura A.7. Definición de servicios LINUX desde NagiosQL  
Fuente: Sistema de administración NagiosQL

Figura A.8. Definición de servicios LINUX desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- En la pestaña configuración común, véase la figura A.9, se debe agregar:
  - ✓ Equipo al que se desea monitorear los servicios ejecutados.
  - ✓ Descripción del servicio
  - ✓ Activar las casillas de registrado y activo

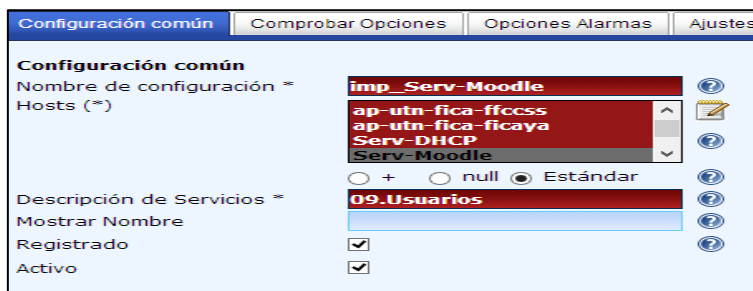


Figura A.9. Selección de equipo para el chequeo de servicios LINUX desde NagiosQL

Fuente: Sistema de administración NagiosQL

- Se selecciona el nombre del comando a utilizar y se especifican los argumentos para la ejecución del servicio, véase la figura A.10. Revisar el apartado, políticas para monitorear equipos LINUX, sección comandos y definición de servicios, donde se describen los comandos y argumentos que se pueden utilizar.



Figura A.10. Configuración general de servicios LINUX desde NagiosQL

Fuente: Sistema de administración NagiosQL

- Se agrega la plantilla de configuración para el servicio, si se desea visualizar la gráfica de rendimiento, también se debe agregar la plantilla srv-pnp, véase la figura A.11.



Figura A.11. Selección de plantilla de configuración de servicios LINUX desde NagiosQL

Fuente: Sistema de administración NagiosQL

- En la pestaña opciones de alarma se agrega el grupo y usuario de contacto para el envío de notificaciones, véase figura A.12.



Figura A.12. Selección de contacto para notificaciones de servicios LINUX desde NagiosQL  
Fuente: Sistema de administración NagiosQL

## CONFIGURACIÓN DE SWITCHES

### 1. Definición de equipo

Para agregar switches al sistema de monitoreo se deben seguir los siguientes pasos:

- Acceder al apartado Supervisión-Host-Agregar, véase la figura A.13 y A.14

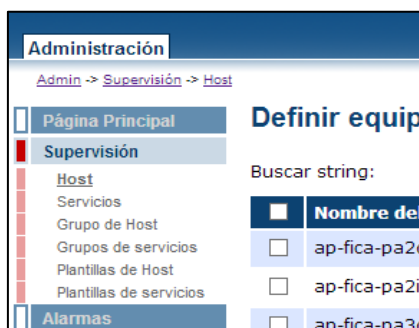


Figura A.13. Definición de switch desde NagiosQL  
Fuente: Sistema de administración NagiosQL

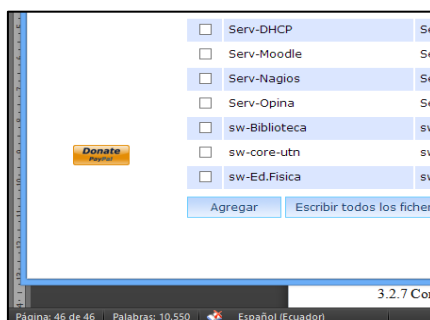


Figura A.14. Definición de switch desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- En la pestaña configuración común, véase las figuras A.15 y A.16, se debe agregar:
  - ✓ Nombre del equipo.
  - ✓ Dirección IP.
  - ✓ Equipo padre o al que se conecta.
  - ✓ Descripción.
  - ✓ Grupo de equipos al que pertenece.
  - ✓ Plantilla de configuración de equipos.

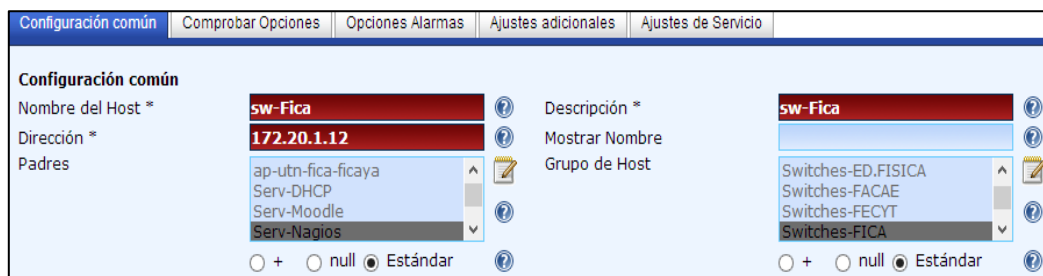


Figura A.15. Configuración general de switch desde NagiosQL

Fuente: Sistema de administración NagiosQL

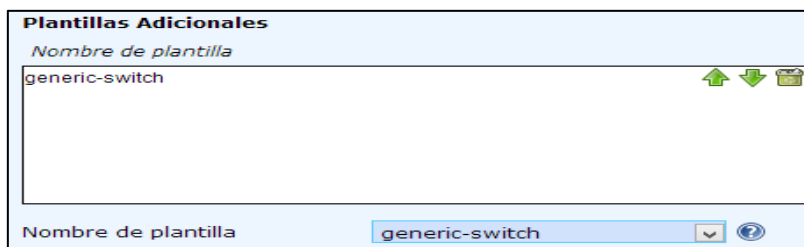


Figura A.16. Selección de plantilla de configuración de switch desde NagiosQL

Fuente: Sistema de administración NagiosQL

- En la pestaña opciones de alarma se agrega el grupo y usuario de contacto para el envío de notificaciones, véase la figura A.17.



Figura A.17. Selección de contacto para notificaciones en switches desde NagiosQL

Fuente: Sistema de administración NagiosQL

- En la pestaña ajustes adicionales se agrega la ubicación de las imágenes y texto para el equipo, que se mostrarán en la interfaz web, véase la figura A.18.

Ajustes adicionales	
Notas	
Notas URL	notes_url
URL de acción	
Imagen para el icono	./ng-switch40.gif
Imagen icono texto ALT	Switch
Imagen VRML	./ng-switch40.png
Estado Imagen	./ng-switch40.png
Coordenadas 2D	(x,y)
Coordenadas 3D	(x,y,z)

Figura A.18. Selección de iconos para switches desde NagiosQL

Fuente: Sistema de administración NagiosQL

## 2. Definición de servicio

Para agregar servicios que se ejecutan en un switches al sistema de monitoreo, se deben seguir los siguientes pasos:

- Acceder al apartado Supervisión-Servicios-Agregar, véase la figura A.19 y A.20.

Figura A.19. Definición de servicios ejecutados en switches desde NagiosQL

Fuente: Sistema de administración NagiosQL

Figura A.20. Definición de servicios ejecutados en switches desde NagiosQL

Fuente: Sistema de administración NagiosQL

- En la pestaña configuración común, véase la figura A.21, se debe agregar:

- ✓ Equipo al que se desea monitorear los servicios ejecutados.
- ✓ Descripción del servicio.
- ✓ Activar las casillas de registrado y activo.



Figura A.21. Selección de equipo para el chequeo de servicios en switches desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- Se selecciona el nombre del comando a utilizar y se especifican los argumentos para la ejecución del servicio, véase la figura A.22. Revisar el apartado, políticas para monitorear switches, sección comandos y definición de servicios, donde se describen los comandos y argumentos que se pueden utilizar.

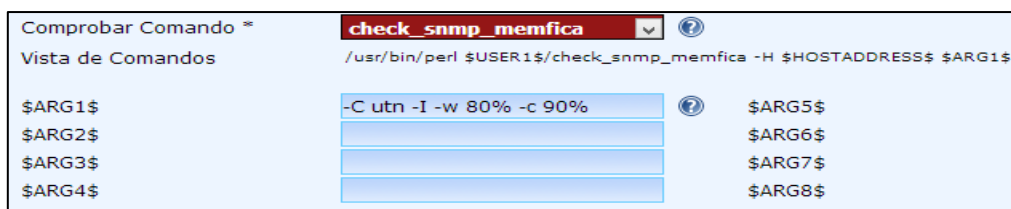


Figura A.22. Configuración general de servicios en switches desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- Se agrega la plantilla de configuración para el servicio, si se desea visualizar la gráfica de rendimiento, también se debe agregar la plantilla srv-pnp, véase la figura A.23.

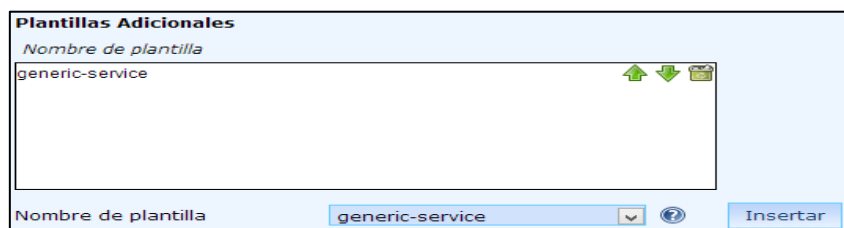


Figura A.23. Selección de plantilla de configuración de servicios en switches desde NagiosQL  
Fuente: Sistema de administración NagiosQL



- En la pestaña opciones de alarma, se agrega el grupo y usuario de contacto para el envío de notificaciones, véase figura A.24.



Figura A.24. Selección de contacto para notificaciones de servicios en switches desde NagiosQL  
Fuente: Sistema de administración NagiosQL

## CONFIGURACIÓN DEL WIRELESS CONTROLLER Y PUNTOS DE ACCESO INALÁMBRICOS

### 1. Definición de equipo

Para agregar un punto de acceso se deben seguir los siguientes pasos:

- Acceder al apartado Supervisión-Host-Agregar, véase la figura A.25 y A.26.

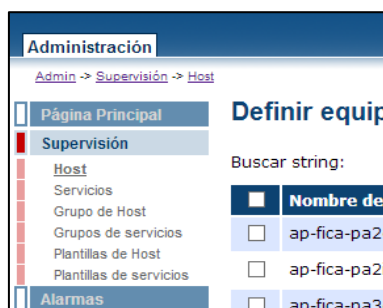


Figura A.25. Definición de Punto de Acceso desde NagiosQL  
Fuente: Sistema de administración NagiosQL

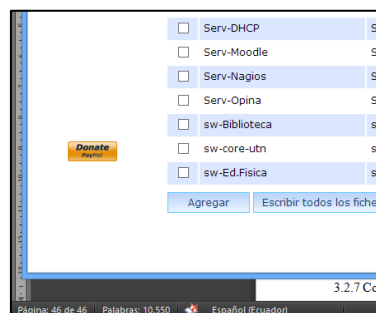


Figura A.26. Definición de Punto de Acceso desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- En la pestaña configuración común, véase la figura A.27 y A.28, se debe agregar:
  - ✓ Nombre del equipo.
  - ✓ Dirección IP.
  - ✓ Equipo padre o al que se conecta.
  - ✓ Descripción.
  - ✓ Grupo de equipos al que pertenece.
  - ✓ Plantilla de configuración de equipos.

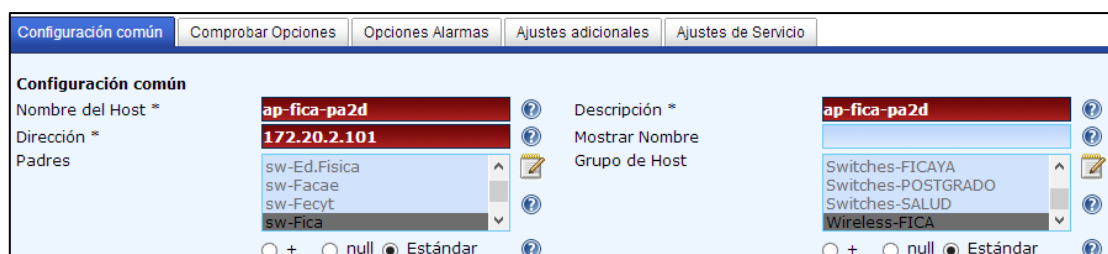


Figura A.27. Configuración general de Puntos de Acceso desde NagiosQL  
Fuente: Sistema de administración NagiosQL

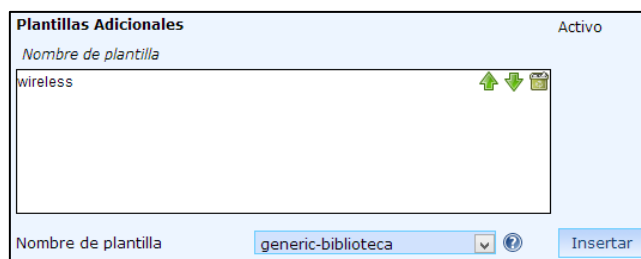


Figura A.28. Selección de plantilla de configuración de Puntos de Acceso desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- En la pestaña opciones de alarma se agrega el grupo y usuario de contacto para el envío de notificaciones, véase figura A.29.

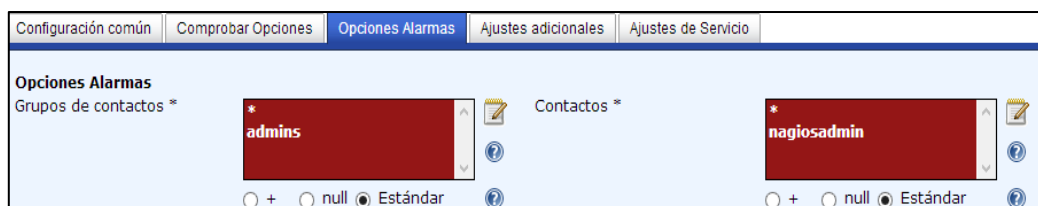


Figura A.29. Selección de contacto para notificaciones en Puntos de Acceso desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- En la pestaña ajustes adicionales se agrega la ubicación de las imágenes y texto para el equipo, que se mostraran en la interfaz web, véase figura A.30.

Figura A.30. Selección de iconos para Puntos de Acceso desde NagiosQL  
Fuente: Sistema de administración NagiosQL

## 2. Definición de servicio

Para agregar servicios en puntos de acceso, se deben seguir los siguientes pasos:

- Acceder al apartado Supervisión-Servicios-Agregar, véase la figura A.31 y A.32.

Figura A.31. Definición de servicios en Puntos de Acceso desde NagiosQL  
Fuente: Sistema de administración NagiosQL

Figura A.32. Definición de servicios en Puntos de Acceso desde NagiosQL  
Fuente: Sistema de administración NagiosQL

- En la pestaña configuración común, véase la figura A.33, se debe agregar:
  - ✓ Equipo al que se desea monitorear los servicios ejecutados.
  - ✓ Descripción del servicio.
  - ✓ Activar las casillas de registrado y activo.

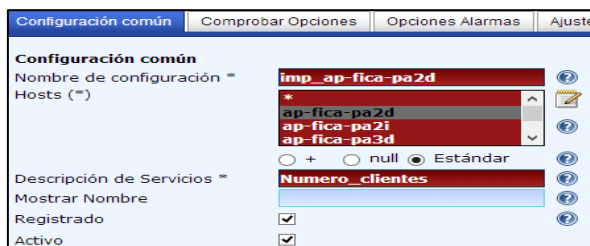


Figura A.33. Configuración general de servicios en Puntos de Acceso desde NagiosQL

Fuente: Sistema de administración NagiosQL

- Se agrega el nombre del comando y se especifica el argumento para el servicio, véase la figura A.34. Revisar el apartado, políticas para monitorear puntos de acceso, sección comandos y definición de servicios, donde se describen los comandos y argumentos que se pueden utilizar.

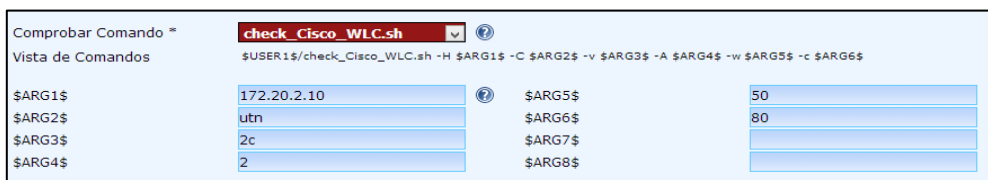


Figura A.34. Configuración general de servicios en Puntos de Acceso desde NagiosQL

Fuente: Sistema de administración NagiosQL

- Se agrega la plantilla de configuración para el servicio, si se desea visualizar la gráfica de rendimiento, también se debe agregar la plantilla srv-pnp, véase la figura A.35.

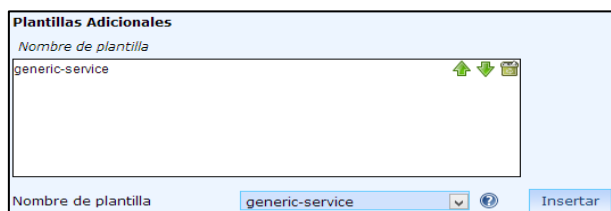


Figura A.35. Selección de plantilla de configuración de Puntos de Acceso desde NagiosQL

Fuente: Sistema de administración NagiosQL

- En la pestaña opciones de alarma se agrega el grupo y usuario de contacto para el envío de notificaciones, véase la figura A.36.



Figura A.36. Selección de contacto para notificaciones de Puntos de Acceso desde NagiosQL  
Fuente: Sistema de administración NagiosQL

## CONFIGURACIÓN DE UN NUEVO GRUPO DE EQUIPOS

Para agregar un grupo de equipos se deben seguir los siguientes pasos:

- Acceder al apartado Supervisión-Grupo de host-Agregar, véase la figura A.37 y A.38.

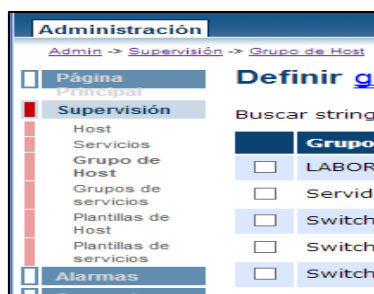


Figura A.37. Configuración de un nuevo grupo de equipos

Fuente: Sistema de administración NagiosQL

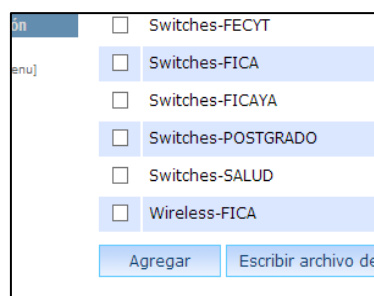


Figura A.38. Configuración de un nuevo grupo de equipos

Fuente: Sistema de administración NagiosQL

- Se agrega el nombre del grupo, descripción y se activan las casillas de registro y activo, véase la figura A.39.

Figura A.39. Configuración general de un nuevo grupo de equipos  
Fuente: Sistema de administración NagiosQL

## CONFIGURACIÓN DE PERIODOS DE MONITOREO

Para agregar un nuevo periodo de tiempo en el cual se dará el monitoreo se deben seguir los siguientes pasos.

- Acceder al apartado Alarmas-Periodo de tiempo-Agregar, véase la figura A.40 y A.41.

Figura A.40. Configuración de tiempos de monitoreo

Fuente: Sistema de administración NagiosQL

Figura A.41. Configuración de tiempos de monitoreo

Fuente: Sistema de administración NagiosQL

- Se agrega el periodo de tiempo de acuerdo a las necesidades de monitoreo, descripción y se habilita las casillas de registrado y activo, véase figura A.42.

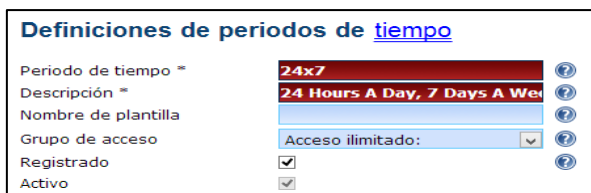


Figura A.42. Configuración general de periodos de monitoreo  
Fuente: Sistema de administración NagiosQL

- Se definen los días y las horas para el periodo de tiempo, véase la figura A.43.



Figura A.43. Definición de días y horas en el periodo de tiempo de monitoreo  
Fuente: Sistema de administración NagiosQL

## CONFIGURACIÓN DE CONTACTOS PARA ENVÍO DE NOTIFICACIONES

Para agregar un nuevo contacto para el envío de notificaciones se deben seguir los siguientes pasos:

- Acceder al apartado Alarmas-Datos de contacto-Agregar, véase la figura A.44 y A.45.

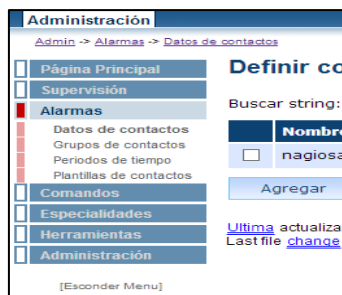


Figura A.44. Configuración de contactos para el envío de notificaciones  
Fuente: Sistema de administración NagiosQL

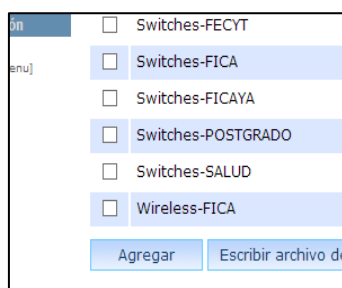


Figura A.45. Configuración de contactos para el envío de notificaciones  
Fuente: Sistema de administración NagiosQL

- Se agrega el nombre del contacto, descripción, correo electrónico y el grupo al que pertenece, véase las figuras A.46 y A.47.

The screenshot shows the 'Configuración común' tab with 'Ajustes adicionales' selected. The 'Nombre de Contacto \*' field contains 'nagiosadmin'. The 'Descripción' field contains 'Nagios Admin'. The 'Grupo de contactos' dropdown menu is open, showing 'admins' selected. At the bottom, there are radio buttons for 'null' and 'Estándar', with 'Estándar' selected.

Figura A.46. Configuración general de contactos para el envío de notificaciones  
Fuente: Sistema de administración NagiosQL

The screenshot shows the email configuration section with the following fields: 'Dirección Email' (usuario2@sewebmaster.com), 'Dirección extra 1', 'Dirección extra 3', and 'Dirección extra 5'. Each field has a help icon to its right.

Figura A.47. Configuración de correo electrónico para el envío de notificaciones  
Fuente: Sistema de administración NagiosQL

- Se habilita el envío de notificaciones para equipos como para servicios, véase la figura A.48.

The screenshot shows two notification activation settings. The first is 'Notif.Servicios Activos \*' with radio buttons for 'on' (selected), 'off', and 'saltar'. The second is '\* Notificación de servicio activada' with radio buttons for 'on' (selected), 'off', and 'saltar'. Both fields have help icons.

Figura A.48. Activación de notificaciones para equipos y servicios  
Fuente: Sistema de administración NagiosQL

- En la pestaña ajustes adicionales se agrega la plantilla de configuración del contacto, véase figura A.49.

The screenshot shows the 'Plantillas Adicionales' section. A list box contains 'generic-contact' with up, down, and delete icons. Below the list, the 'Nombre de plantilla' dropdown menu is set to 'generic-contact'.

Figura A.49. Asignación de plantilla de configuración de contactos  
Fuente: Sistema de administración NagiosQL

## CONFIGURACIÓN DE USUARIOS DE ADMINISTRACIÓN

Para agregar un nuevo contacto para el envío de notificaciones se deben seguir los



siguientes pasos.

- Acceder al apartado Administración-Usuario Administrador-Agregar, para agregar un nuevo usuario, véase la figura A.50.

Figura A.50. Configuración de un nuevo usuario de administración  
Fuente: Sistema de administración NagiosQL

- Se agrega los datos del nuevo usuario, nombre, descripción, clave, dominio y se activan las casillas de grupo de administración y activo, véase la figura A.51.

Figura A.51. Configuración general de un nuevo usuario de administración  
Fuente: Sistema de administración NagiosQL

- Ingresar al apartado Administración-Grupo admin-Agregar, véase la figura A.52, para la creación del nuevo grupo al que pertenecerá el usuario creado con anterioridad.

Se agrega el nombre del grupo, descripción, se selecciona el usuario otorgándole los derechos requeridos por el administrador y se habilita la casilla activo.

Figura A.52. Configuración de un nuevo grupo de administración  
Fuente: Sistema de administración NagiosQL

- En el apartado Administración-Menú de acceso, véase la figura 53, se seleccionan las páginas del menú que serán permitidas según los derechos otorgados para los usuarios pertenecientes al grupo creado con anterioridad.

Figura A.53. Configuración de derechos para el nuevo usuario de administración  
Fuente: Sistema de administración NagiosQL

## ANEXO B

### GUÍA DE INSTALACIÓN

#### NAGIOS CORE

#### INFORMACIÓN GENERAL

Estas instrucciones fueron escritas basadas en la distribución Linux Ubuntu Server 12.10 y se debe considerar la siguiente información:

- Nagios y los plugins serán instalados bajo `/usr/local/nagios`.
- Nagios será configurado para que empiece a monitorear algunos aspectos de su sistema local (carga de CPU, uso en disco, etc.)
- Se accederá a la interfaz WEB de Nagios a través de la dirección `http://localhost/nagios/`

#### PAQUETES REQUERIDOS

Se debe tener los siguientes paquetes en su instalación de Ubuntu antes de continuar, puede utilizar `apt-get` para instalar estos paquetes utilizando los siguientes comandos:

- Apache 2
- Compilador GCC y librerías de desarrollo
- Librerías de desarrollo GD
- `sudo apt-get install apache2`
- `sudo apt-get install build-essential`

Con Ubuntu-Server 12.10, el nombre de la librería `gd2` ha cambiado, por lo que se necesitará utilizar el siguiente comando:

- `sudo apt-get install libgd2-xpm-dev`

## **CREAR INFORMACIÓN DE LA CUENTA**

Cambiar a usuario root, crear nuevo usuario nagios y proporcionarle una contraseña, crear el grupo nagios y agregar el usuario nagios al grupo.

- `sudo -s`
- `/usr/sbin/useradd -m nagios`
- `passwd nagios`
- `/usr/sbin/groupadd nagios`
- `/usr/sbin/usermod -G nagios nagios`

Crear un grupo nuevo nagcmd para permitir que comandos externos sean ingresados por medio de la interfaz web. Agregar tanto el usuario nagios como el usuario apache al grupo.

- `/usr/sbin/groupadd nagcmd`
- `/usr/sbin/usermod -G nagcmd nagios`
- `/usr/sbin/usermod -G nagcmd www-data`

## **DESCARGAR NAGIOS Y PLUGIN**

Crear un directorio para guardar los archivos y descargar el código fuente comprimido de Nagios como de los plugin (visitar <http://www.nagios.org/download/> para enlaces de las últimas versiones). La versión de nagios que se utilizará en este caso es la 3.4.3 y las de los plugin es la versión 1.4.16.

- `mkdir ~/downloads`
- `cd ~/downloads`
- `wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.4.3.tar.gz`

- `wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplu/nagios-plugins-1.4.16.tar.gz`

## COMPILE E INSTALE NAGIOS

Extraiga el código fuente del archivo comprimido de Nagios, ejecute el script de configuración de Nagios indicando el nombre del grupo que se creó anteriormente y compile el código fuente de Nagios.

- `cd ~/downloads`
- `tar xzf nagios-3.0.3.tar.gz`
- `cd nagios-3.4.3`
- `./configure --with-command-group=nagcmd`
- `make all`

Instale los binarios, el script de inicio, archivos de configuración de ejemplo y otorgue permisos en el directorio de comandos externos.

- `make install`
- `make install-init`
- `make install-config`
- `make install-commandmode`

## PERSONALICE LA CONFIGURACIÓN

Archivos de configuración de ejemplo han sido instalados en el directorio `/usr/local/nagios/etc`. Estos archivos de ejemplo deben de trabajar adecuadamente para empezar a utilizar Nagios.

Edite el archivo de configuración `/usr/local/nagios/etc/objects/contacts.cfg` con su editor favorito y cambie la dirección de correo que está asociada con el contacto nagios admin con

la dirección de correo donde desea recibir las alertas.

- `vi /usr/local/nagios/etc/objects/contacts.cfg`

## **CONFIGURE LA INTERFAZ WEB**

Instale el archivo de configuración web en el directorio `conf.d` de Apache, se crea la cuenta `nagiosadmin` para entrar a la interfaz web de Nagios, recuerde la contraseña que asigno a esta cuenta, la necesitará después y reinicie Apache para que la nueva configuración tome efecto.

- `make install-webconf`
- `htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin`
- `/etc/init.d/apache2 reload`

## **COMPILE E INSTALE LOS PLUGIN DE NAGIOS**

Extraiga los plugin de Nagios del archivo comprimido, compile e instale los plugin, configure Nagios para que automáticamente se ejecute cuando el sistema inicie y revise los archivos de configuración de ejemplo, si no hay errores, inicie Nagios.

- `cd ~/downloads`
- `tar xzf nagios-plugins-1.4.16.tar.gz`
- `cd nagios-plugins-1.4.16`
- `./configure --with-nagios-user=nagios --with-nagios-group=nagios`
- `make`
- `make install`
- `ln -s /etc/init.d/nagios /etc/rcS.d/S99nagios`
- `/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg`
- `/etc/init.d/nagios start`

## **INGRESO A LA INTERFAZ WEB**

Ahora se podrá acceder a la interfaz web, le será solicitado el usuario (nagiosadmin) y la contraseña que especifico anteriormente.

- `http://localhost/nagios/`

## **OTRAS MODIFICACIONES**

Si se desea recibir notificaciones de alertas de Nagios por correo electrónico, se necesita instalar el paquete mailx (Postfix).

- `sudo apt-get install mailx`
- `sudo apt-get install postfix`

Necesitará editar los comandos de Nagios para la notificación por correo electrónico localizados en `/usr/local/nagios/etc/objects/commands.cfg` y cambiar cualquier `/bin/mail` a `/usr/bin/mail`. Una vez hecho esto se necesita reiniciar Nagios para que los cambios en la configuración tomen efecto.

## **NAGIOSQL**

NagiosQL es una interfaz web de administración que complementa al sistema de monitoreo Nagios, permite agregar o eliminar equipos, servicios, plantillas o comandos sin tener que modificar los archivos de configuración de Nagios y tener así un mejor control de la configuración del sistema.

## **REQUISITOS PREVIOS**

Antes de instalar NagiosQL se necesitan los siguientes requisitos y módulos PHP.

- APACHE WEB SERVER
- MYSQL SERVER VERSIÓN 4.1 EN ADELANTE

- PHP VERSIÓN 5.2 EN ADELANTE
- NAGIOS 2.X OR 3.X
- SESSION
- MYSQL (PHP5-MYSQL)
- GETTEXT
- FILTER
- FTP (OPCIONAL )
- SSH (OPCIONAL)

## **ESTRUCTURA DE DIRECTORIOS**

NagiosQL almacena los archivos de configuración de Nagios en una estructura de directorios independiente. La estructura se debe crear como se muestra a continuación.

- mkdir/etc/nagiosql
- mkdir/etc/nagiosql/hosts
- mkdir/etc/nagiosql/services
- mkdir/etc/nagiosql/backup
- mkdir/etc/nagiosql/backup/hosts
- mkdir/etc/nagiosql/backup/services

## **ARCHIVOS DE CONFIGURACIÓN DE NAGIOS**

NagiosQL necesita permisos de lectura y escritura en algunos archivos de configuración de Nagios, además deberán ser asociados al usuario del servidor web www-data y al grupo nagios, los siguientes archivos se ven afectados.

- chown -R wwwrun.nagios /etc/nagios/nagios.cfg
- chown -R wwwrun.nagios /etc/nagios/cgi.cfg



- `chown -R wwwrun.nagios /var/spool/nagios/nagios.cmd`
- `chmod 770 /etc/nagios/nagios.cfg`
- `chmod 770 /etc/nagios/cgi.cfg`
- `chmod 770 /var/spool/nagios/nagios.cmd`

## CONFIGURACIÓN DE APACHE

Se debe agregar en al archivo `/etc/php5/apache2/php.ini` las siguientes líneas.

- `file_uploads = on`
- `session.auto_start = 0`
- `date.timezone = America/Quito`

Adicionalmente se crea un archivo de configuración para el servidor web, el archivo debe tener el siguiente contenido y reiniciar el servidor apache.

- `touch /etc/apache2/conf.d/nagiosql.conf`
- ```
Alias /nagiosql "/opt/nagiosql"
<Directory "/opt/nagiosql">
Options None
AllowOverride None
Order allow,deny
Allow from all
# Order deny,allow
# Deny from all
# Allow from 127.0.0.1
# AuthName "NagiosQL Access"
# AuthType Basic
# AuthUserFile /etc/nagiosql/auth/nagiosql.users
```

```
# Require valid-user
```

```
</Directory>
```

- /etc/init.d/apache2 restart

## INSTALACIÓN DE NAGIOSQL

Se instaló NagiosQL 3.2 que es la última versión estable, se descomprimió el directorio.tar.gz, se agregó el directorio al usuario www-data de Apache y otorgaron permisos de lectura, escritura y ejecución al usuario. Ahora NagiosQL debe ser accesible a través del navegador web. La figura B.1 muestra una lista de requisitos para la instalación.

- cd /opt
- wget sourceforge.net/projects/nagiosql/files/latest/download
- tar xzf nagiosql\_320.tar.gz
- mv nagiosql32 nagiosql
- chown -R www-data /opt/nagiosql
- chmod 750 /opt/nagiosql/config
- http://localhost/nagiosql/install/index.php



Figura B.1. Requisitos previos para NagiosQL.

Fuente: <http://www.nagiosql.org/>

En la figura B.2 se muestran las pruebas ambientales divididas en siete secciones, se debe asegurar de tener todas estas pruebas ok antes de seguir con la instalación.

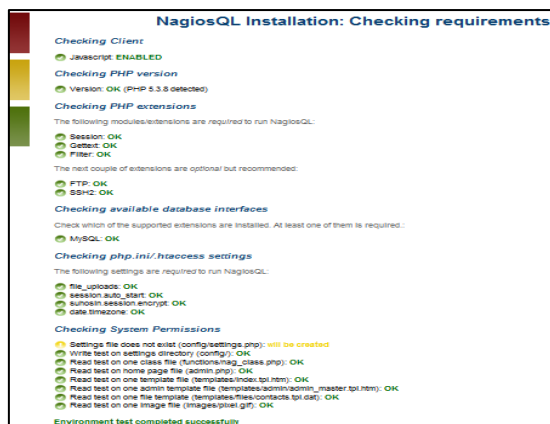


Figura B.2. Comprobación de requisitos para NagiosQL.  
Fuente: <http://www.nagiosql.org/>

La figura B.3 muestra la información que se debe especificar para poder crear la base de datos, a continuación se explican los campos a llenar.

- Database Type: Se debe escoger el tipo de base de datos instalado.
- Database Server: Nombre de host o dirección ip del servidor de base de datos
- Local hostname or IP address: Nombre de host o dirección IP del servidor Web.
- Database Server Port: Puerto TCP utilizado por el servidor de base de datos.
- Database name: Nombre de la base de datos creada para NagiosQL
- NagiosQL Database User: Nombre de usuario para la base de datos NagiosQL
- NagiosQL Database Password: Contraseña de usuario de la base de datos NagiosQL
- Drop database if already exists: Permite eliminar la base de datos creada con anterioridad para poder crear una nueva.
- Initial NagiosQL User: Nombre de usuario para el acceso web a NagiosQL.
- Initial NagiosQL Password: Contraseña de usuario para el acceso web a NagiosQL
- NagiosQL config path: Ubicación del directorio con los archivos de configuración de NagiosQL.
- Nagios config path: Ubicación del directorio con los archivos de configuración de Nagios.



**NagiosQL Installation: Setup**

Please complete the form below. Mandatory fields marked \*

**Database Configuration**

Database Type: mysql

Database Server \*: localhost

Local hostname or IP address \*: localhost

Database Server Port \*: 3306

Database name \*: db\_nagiosql\_v32

NagiosQL DB User \*: nagiosql\_user

NagiosQL DB Password \*: \*\*\*\*\*

Administrative Database User \*: root

Administrative Database Password \*: root

Drop database if already exists?

**NagiosQL User Setup**

Initial NagiosQL User \*: admin

Initial NagiosQL Password \*: [redacted]

Please repeat the password \*: [redacted]

**Nagios Configuration**

Import Nagios sample config?

**NagiosQL path values**

Create NagiosQL config paths?

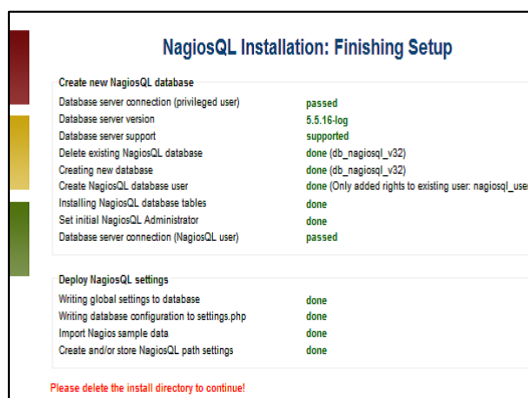
NagiosQL config path: /etc/nagiosql

Nagios config path: /etc/nagios

Figura B.3. Configuración de NagiosQL

Fuente: <http://www.nagiosql.org/>

Si toda la información se ha ingresado correctamente y la base de datos se puede crear, la figura B.4 muestra el resultado.



**NagiosQL Installation: Finishing Setup**

**Create new NagiosQL database**

Database server connection (privileged user) passed

Database server version 5.5.16-log

Database server support supported

Delete existing NagiosQL database done (db\_nagiosql\_v32)

Creating new database done (db\_nagiosql\_v32)

Create NagiosQL database user done (Only added rights to existing user: nagiosql\_user)

Installing NagiosQL database tables done

Set initial NagiosQL Administrator done

Database server connection (NagiosQL user) passed

**Deploy NagiosQL settings**

Writing global settings to database done

Writing database configuration to settings.php done

Import Nagios sample data done

Create and/or store NagiosQL path settings done

Please delete the install directory to continue!

Figura B.4. Resultados de la instalación de NagiosQL

Fuente: Fuente: <http://www.nagiosql.org/>

Si no se muestran errores se puede finalizar la instalación, después será necesario eliminar el archivo `/opt/NagiosQL/install` para tener acceso a la interfaz web NagiosQL.

- `rm -rf /opt/nagiosql/install`

Ahora NagiosQL debe ser accesible a través del navegador web y se podrá ver una página como se muestra en la figura B.5.

- `http://localhost/nagiosql`

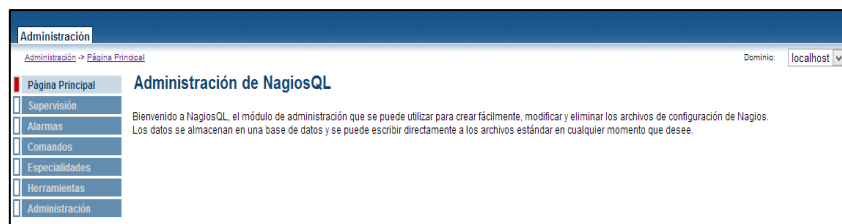


Figura B.5. Interfaz NagiosQL

Fuente: Fuente: <http://www.nagiosql.org/>

En la parte izquierda de la página web se pueden visualizar seis campos que se describirán a continuación.

- **Supervisión:** Este campo permite agregar nuevos equipos, servicios, grupo de equipos y grupo de servicios así como las plantillas utilizadas por los mismos de manera gráfica sin tener que hacer modificaciones en los archivos de definición de objetos de Nagios.
- **Alarmas:** Este campo permite definir nuevos contactos y grupos de contactos a quienes llegarán las notificaciones así como los periodos de tiempo que se utilizarán para chequear servicios.
- **Comandos:** Este campo permite definir los comandos utilizados por Nagios para ejecutar cada servicio.
- **Especialidades:** Este campo permite definir las dependencias de equipos o servicios con la finalidad de no enviar notificaciones innecesarias a los contactos.
- **Herramientas:** Este campo permite modificar los ficheros de configuración de Nagios, reiniciar el sistema e importar archivos con definiciones de objetos al servidor Nagios sin tener que utilizar la interfaz de administración.
- **Administración:** Este campo permite cambiar la clave y el usuario para NagiosQL y modificar las rutas hacia sus archivos de configuración.

## DOMINIO DE DATOS LOCAL

Dentro del campo administración se encuentra la opción dominio de datos local como se muestra en la figura B.6, el control de Nagios se determina mediante este dominio de administración que se utiliza para el almacenamiento de datos, es decir, contiene las rutas de los objetos y archivos de configuración de Nagios y no puede ser eliminado ni cambiado de nombre.



Figura B.6. Dominio de datos local.

Fuente: <http://www.nagiosql.org/>

Se puede modificar el dominio de datos local desde el apartado función y visualizar el contenido que se muestra en la figura B.7, los campos de describen a continuación.



Figura B.7. Configuración del dominio de datos.

Fuente: <http://www.nagiosql.org/>

- Objetivo de configuración: Nombre del dominio de configuración.
- Descripción: Nombre descriptivo del dominio.

- Nombre del servidor: Nombre o dirección ip del equipo que ejecuta la instalación de Nagios.
- Método: Define el tipo de conexión con el que NagiosQL tendrá acceso a los archivos de configuración.
- Directorio base: Directorio donde se almacenan los archivos de configuración de Nagios, estos archivos contendrán las configuraciones realizadas desde la interfaz de administración NagiosQL.
- Directorio de equipos: Directorio donde se almacenan los archivos con definiciones para todos los equipos.
- Directorio de servicios: Directorio donde se almacenan los archivos con definiciones para todos los servicios.
- Directorio de backup: Directorio donde NagiosQL almacena copias de seguridad de los archivos de configuración de Nagios excepto de equipos y servicios.
- Directorio de respaldo de equipos: Directorio donde NagiosQL almacena copias de seguridad de los archivos con la definición de equipos.
- Directorio de respaldo de servicios: Directorio donde NagiosQL almacena copias de seguridad de los archivos con la definición de servicios.
- Directorio base de Nagios: Directorio con los archivos de configuración principales de Nagios. Los archivos nagios.cfg y cgi.cfg se almacenan en este directorio.
- Directorio de importación: Directorio con los archivos de importación para Nagios, contiene archivos para la definición de servicios, equipos, plantillas, contactos, etc. La importación de datos es útil cuando se desea definir objetos directamente en los archivos de configuración de Nagios sin necesidad de utilizar la interfaz de administración.

- Directorio base de fotos imágenes: Directorio de imágenes alternativo al directorio utilizado por Nagios ubicado en /usr/local/nagios/share/images/logos.
- Fichero de comandos de Nagios: Ruta de acceso al archivo de comandos nagios.cmd, este archivo es necesario para enviar comandos externos a Nagios y se crea cuando la directiva check\_external\_commands esta activada o es igual a 1 en el archivo de configuración nagios.cfg.
- Fichero binario de Nagios: Ruta de acceso al archivo binario de Nagios.
- Fichero de proceso de Nagios: Ruta del archivo de proceso nagios.lock, este archivo permite reiniciar Nagios desde la interfaz de administración.
- Fichero de configuración de Nagios: Ruta del archivo de configuración principal de Nagios.
- Versión de Nagios: Versión de la instalación de Nagios (Versión 2.x o 3.x son compatibles).
- Grupo Acceso: Permite seleccionar que grupo de usuarios tiene acceso al dominio de datos
- Activo: Permite definir si el dominio de datos está activa o no

## CONFIGURACIÓN DE NAGIOS

El archivo de configuración de Nagios (nagios.cfg) tiene que ser adaptado para que pueda encontrar y utilizar los archivos de configuración escritos por NagiosQL. Esto se puede hacer usando el editor integrado de NagiosQL desde el campo herramientas en la interfaz de administración. Las nuevas rutas hacia los directorios y archivos que se deben especificar en nagios.cfg son las siguientes.

- cfg\_file = / etc / NagiosQL / contacttemplates.cfg
- cfg\_file = / etc / NagiosQL / contactgroups.cfg



- `cfg_file = / etc / NagiosQL / contacts.cfg`
- `cfg_file = / etc / NagiosQL / timeperiods.cfg`
- `cfg_file = / etc / NagiosQL / commands.cfg`
- `cfg_file = / etc / NagiosQL / hostgroups.cfg`
- `cfg_file = / etc / NagiosQL / servicegroups.cfg`
- `cfg_dir = / etc / NagiosQL / hosts`
- `cfg_dir = / etc / NagiosQL / servicios`
- `cfg_file = / etc / NagiosQL / hosttemplates.cfg`
- `cfg_file = / etc / NagiosQL / servicetemplates.cfg`
- `cfg_file = / etc / NagiosQL / servicedependencies.cfg`
- `cfg_file = / etc / NagiosQL / serviceescalations.cfg`
- `cfg_file = / etc / NagiosQL / hostdependencies.cfg`
- `cfg_file = / etc / NagiosQL / hostescalations.cfg`
- `cfg_file = / etc / NagiosQL / hostextinfo.cfg`
- `cfg_file = / etc / NagiosQL / serviceextinfo.cfg`

Todas las líneas existentes que comienzan con `cfg_file` o `cfg_dir` son las rutas utilizadas anteriormente por Nagios y deben ser eliminadas o desactivadas.

## **PNP4NAGIOS**

Es un módulo para Nagios que muestra gráficos de los servicios de cada host en diferentes periodos de tiempo, permite hacer comparativas de calidad entre los diferentes servicios configurados. PNP4Nagios analiza los datos de rendimiento de cada servicio, almacena automáticamente la información en la base de datos RRD (bases de datos Round Robin), requiere plugin Nagios que obtengan datos de rendimiento para poder mostrar

resultados en las gráficas. Cuando el plugin genera datos de rendimiento, se divide en dos partes. El símbolo de canalización (|) se utiliza como un delimitador.

### **Ejemplo check\_icmp:**

- OK - 127.0.0.1: rta 2.687ms, lost 0% | rta=2.687ms;3000.000;5000.000;0; pl=0%;80;100;;

Lo que resulta en el texto, en la parte izquierda de la barra vertical son los datos actuales obtenidos por check\_icmp

- OK - 127.0.0.1: rta 2.687ms, lost 0%

La información en la parte derecha de la barra vertical son los datos de rendimiento

- rta=2.687ms;3000.000;5000.000;0; pl=0%;80;100;;

## **REQUERIMIENTOS DE INSTALACIÓN**

Antes de instalar PNP4NAGIOS son necesarios los siguientes paquetes.

- Perl, a partir de la versión 5.x sin módulos adicionales.
- RRDtool<sup>94</sup>, a partir de la versión 1.2, instalar RRDtool sin un gestor de paquetes ya que si se muestran los gráficos sin texto, esto sería la causa.
- PHP, a partir de la versión 5.1.6 para el frontal web basado en Kohana.
- Nagios, a partir de la versión 2.x.
- KOHANA, REQUIERE EL MÓDULO MOD\_REWRITE HABILITADO.

## **INSTALACIÓN DE PNP4NAGIOS**

Se escogió la última versión PNP 0.6.21 disponible, se ubican los directorios PNP indicando el usuario nagios y el grupo nagcmd, se compilan los archivos binarios y se instalan en el sistema.

---

<sup>94</sup> RRDtool: *Round Robin Database Tool (Herramienta de Base de Datos Round Robin)*

- `wget http://sourceforge.net/projects/pnp4nagios/files/latest/download`
- `tar -xvzf pnp4nagios-HEAD.tar.gz`
- `cd pnp4nagios`
- `./configure --with-nagios-user=nagios --with-nagios-group=nagcmd`
- `make all`
- `make install`
- `make install-webconf`
- `make install-config`
- `make install-init`

La figura B.8 muestra las rutas donde se instalarán los componentes PNP, la ubicación de los directorios se debe revisar y comprobar que coincidan con la instalación.

```

General Options:
-----
Nagios user/group:      nagios nagios
Install directory:     /usr/local/pnp4nagios
HTML Dir:              /usr/local/pnp4nagios/share
Config Dir:            /usr/local/pnp4nagios/etc
Location of rrdtool binary: /usr/bin/rrdtool Version 1.2.12
RRDs Perl Modules:    FOUND (Version 1.2012)
RRD Files stored in:   /usr/local/pnp4nagios/var/perfdata
process_perfdata.pl Logfile: /usr/local/pnp4nagios/var/perfdata.log
Perfdata files (NPCD) stored in: /usr/local/pnp4nagios/var/spool

Web Interface Options: -----
HTML URL:              http://localhost/pnp4nagios/
Apache Config File:    /etc/apache2/conf.d/pnp4nagios.conf

Review the options above for accuracy.  If they look okay,
type 'make all' to compile.

```

*Figura B.8.* Rutas para la instalación de NagiosQL.  
Fuente: <http://docs.pnp4nagios.org>

Después de la instalación, los componentes PNP4NAGIOS se ubican en el sistema de la siguiente manera.

- Los archivos PHP para el frontal web: `/usr/local/pnp4nagios/share`
- El colector de datos `process_perfdata.pl`: `/usr/local/pnp4nagios/libexec`
- Los archivos de configuración de ejemplo: `/usr/local/pnp4nagios/etc`
- El archivo de configuración para la interfaz web: `/usr/local/pnp4nagios/etc`

## RECOLECCIÓN DE DATOS

Los datos de rendimiento se almacenan en la base de datos Round Robin con RRDtool, esto significa que después de algún tiempo, los datos más antiguos serán dados de baja en el extremo y serán reemplazados por nuevos valores al principio. Por cada origen de datos se necesitará aproximadamente 400 KB. PNP soporta varios modos para procesar los datos de rendimiento, los modos difieren en complejidad y en el rendimiento del servidor Nagios. Nagios invoca uno o más comandos para cada equipo o servicio y así poder procesar la información de rendimiento, los datos se pasan al script `process_perfdata.pl` y se procesan en un momento posterior, `process_perfdata.pl` escribe los datos XML de los archivos y los almacena en los ficheros RRD que utiliza RRDtool.

### Modos para el procesamiento de datos

#### Modo Síncrono

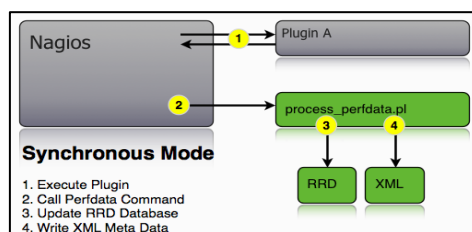


Figura B.9. Estructura del Modo Síncrono.

Fuente: <http://docs.pnp4nagios.org>

El modo de sincronización es la más simple y fácil de configurar ya que Nagios llama al script de perl `process_perfdata.pl` al ejecutar cada servicio para procesar los datos como se muestra en la figura B.9, de modo que cada evento dispara la ejecución de `process-service-perfdata`. El modo síncrono funciona muy bien hasta unos 1.000 servicios en un intervalo de 5 minutos.

#### Configuración

Inicialmente hay que habilitar el procesamiento de los datos de rendimiento en `nagios.cfg`,

se debe tener en cuenta que esta directiva ya exista en el archivo de configuración. El valor predeterminado es 0.

- `process_performance_data = 1`

El tratamiento de la información debe estar deshabilitado en la definición de cada host o servicio para que el rendimiento de los datos no sea procesado.

```
define service {
    .
    .
    process_perf_data 0
    .
}
```

Se deben especificar los comandos para procesar los datos de rendimiento de los servicios como de los equipos en el archivo

- `/usr/local/nagios/etc/nagios.cfg`.
- `service_perfdata_command=process-service-perfdata`
- `host_perfdata_command=process-host-perfdata`

Nagios debe saber sobre los comandos de referencia utilizados por PNP, por ello se tienen que definir en el archivo `/usr/local/nagios/etc/commands.cfg` como se muestra a continuación.

```
define command {
    command_name process-service-perfdata
    command_line /usr/bin/perl/usr/local/pnp4nagios/libexec/
                process_perfdata.pl
                }

define command {
    command_name process-host-perfdata
    command_line /usr/bin/perl /usr/local/pnp4nagios/libexec/
                process_perfdata.pl -d HOSTPERFDATA
                }
```

## Modo Masivo

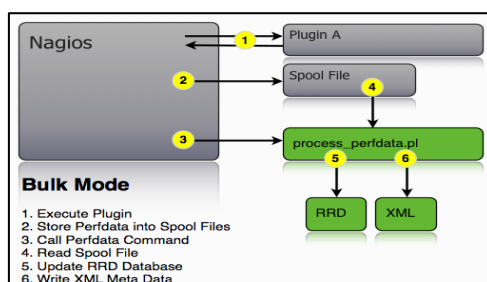


Figura B.10. Estructura del Modo Masivo

Fuente: <http://docs.pnp4nagios.org>

Este modo es más complicado que el modo síncrono, pero reduce la carga en el servidor Nagios significativamente debido a que el colector de datos `process_perfdata.pl` no se invoca para cada chequeo de servicio o equipo, en este modo, Nagios escribe los datos necesarios en un archivo temporal, una vez transcurrido un tiempo determinado, el archivo es procesado por `process_perfdata.pl` y eliminado como se muestra en la figura B.10.

El número de llamadas de `process_perfdata.pl` se reducirá considerablemente. Al utilizar este modo se debe considerar el tiempo de ejecución de `process_perfdata.pl`, ya que durante este tiempo Nagios no ejecutará ningún control.

## Configuración

El tratamiento de los datos de rendimiento se debe habilitar en el archivo de configuración de Nagios ubicado en `/usr/local/nagios/etc/nagios.cfg`.

- `process_performance_data = 1`
- `# service performance data`
- `service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata`
- `service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET$\tHOSTNAME::$HOSTNAME$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPERFDATA::$SERVICEPERFDATA$\tSERVICECHECKCOMMAND::$SERVI`

```

CECHECKCOMMAND$\tHOSTSTATE::$HOSTSTATES$\tHOSTSTATETYPE::$H
OSTSTATETYPE$\tSERVICESTATE::$SERVICESTATES$\tSERVICESTATETYP
E::$SERVICESTATETYPE$

```

- service\_perfdata\_file\_mode=a
- service\_perfdata\_file\_processing\_interval=15
- service\_perfdata\_file\_processing\_command=process-service-perfdata-file
- # host performance data starting with Nagios 3.0
- host\_perfdata\_file=/usr/local/pnp4nagios/var/host-perfdata
- host\_perfdata\_file\_template=DATATYPE::\$HOSTPERFDATA\tTIMET::\$TIMET\$\H
OSTNAME::\$HOSTNAME\$\tHOSTPERFDATA::\$HOSTPERFDATA\$\tHOSTCH
ECKCOMMAND::\$HOSTCHECKCOMMAND\$\tHOSTSTATE::\$HOSTSTATES\$\t
HOSTSTATETYPE::\$HOSTSTATETYPE\$
- host\_perfdata\_file\_mode=a
- host\_perfdata\_file\_processing\_interval=15
- host\_perfdata\_file\_processing\_command=process-host-perfdata-file

### Descripción de parámetros

- service\_perfdata\_file: Es la ruta de acceso al archivo donde serán escritos los datos de rendimiento después de cada chequeo de host o servicio.
- service\_perfdata\_file\_template: Indica el formato del archivo donde se escribirán los datos de rendimiento. Los datos se definen mediante macros de Nagios.
- service\_perfdata\_file\_mode: La opción a indica que los datos se van a añadir al archivo.
- service\_perfdata\_file\_processing\_interval: Especifica el intervalo de tiempo para procesar la información del archivo donde se escribirán los datos de rendimiento.

- `service_perfdata_file_processing_command`: Indica el comando que se debe ejecutar previamente establecido en `commands.cfg` para procesar el archivo que almacenará los datos de rendimiento, este comando se ejecuta cada intervalo de tiempo establecido en la línea de configuración anterior.

Nagios debe saber sobre los comandos de referencia utilizados por PNP, por ello se tienen que definir en el archivo `/usr/local/nagios/etc/commands.cfg` de la siguiente manera.

```
define command{
  command_name      process-service-perfdata-file
  command_line      /usr/local/pnp4nagios/libexec/
                    process_perfdata.pl --bulk=/usr/local
                    /pnp4nagios/var/service-perfdata
}

define command{
  command_name      process-host-perfdata-file
  command_line      /usr/local/pnp4nagios/libexec/
                    process_perfdata.pl --bulk=/usr/local/
                    pnp4nagios/var/host-perfdata
}
```

### Modo Masivo con NPCD<sup>95</sup>

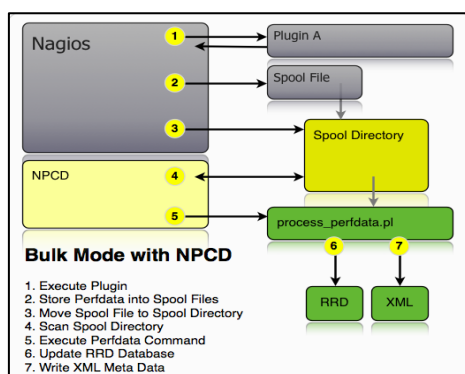


Figura B.11. Estructura del Modo Masivo con NPCD

Fuente: <http://docs.pnp4nagios.org>

<sup>95</sup> NPCD: Nagios Performance C Daemon (Demonio de Rendimiento de Nagios)



Este es el mejor modo de procesamiento ya que Nagios no se bloquea. Nagios utiliza un archivo temporal para almacenar los datos. En lugar de un procesamiento inmediato por `process_perfdata.pl` el archivo se mueve a un directorio de cola.

El demonio NPCD (Nagios Performance C Daemon) supervisará el directorio para los nuevos archivos y devolverá esta información a `process_perfdata.pl`, de modo que el tratamiento de los datos de rendimiento se desacopla de Nagios como se muestra en la figura B.11.

### Configuración

La configuración de este modo es idéntica al modo masivo excepto por el comando utilizado como se muestra a continuación:

- `process_performance_data = 1`
- `# service performance data`
- `service_perfdata_file=/usr/local/pnp4nagios/var/service-perfdata`
- `service_perfdata_file_template=DATATYPE::SERVICEPERFDATA\tTIMET::$TIMET$\tHOSTNAME::$HOSTNAMES$\tSERVICEDESC::$SERVICEDESC$\tSERVICEPERFDATA::$SERVICEPERFDATA$\tSERVICECHECKCOMMAND::$SERVICECHECKCOMMAND$\tHOSTSTATE::$HOSTSTATES$\tHOSTSTATETYPE::$HOSTSTATETYPE$\tSERVICESTATE::$SERVICESTATES$\tSERVICESTATETYPE::$SERVICESTATETYPE$`
- `service_perfdata_file_mode=a`
- `service_perfdata_file_processing_interval=15`
- `service_perfdata_file_processing_command=process-service-perfdata-file`
- `# host performance data starting with Nagios 3.0`
- `host_perfdata_file=/usr/local/pnp4nagios/var/host-perfdata`

- `host_perfdata_file_template=DATATYPE::HOSTPERFDATA\tTIMET::$TIMET$\tHOSTNAME::$HOSTNAMES$\tHOSTPERFDATA::$HOSTPERFDATA$\tHOSTCHECKCOMMAND::$HOSTCHECKCOMMAND$\tHOSTSTATE::$HOSTSTATES$\tHOSTSTATETYPE::$HOSTSTATETYPE$`
- `host_perfdata_file_mode=a`
- `host_perfdata_file_processing_interval=15`
- `host_perfdata_file_processing_command=process-host-perfdata-file`

### Descripción de parámetros

- `service_perfdata_file`: Es la ruta de acceso al archivo donde serán escritos los datos de rendimiento después de cada chequeo de host o servicio.
- `service_perfdata_file_template`: Indica el formato del archivo donde se escribirán los datos de rendimiento. Los datos se definen mediante macros de Nagios.
- `service_perfdata_file_mode`: La opción `a` indica que los datos se van a añadir al archivo.
- `service_perfdata_file_processing_interval`: Especifica el intervalo de tiempo para procesar la información del archivo donde se escribirán los datos de rendimiento.
- `service_perfdata_file_processing_command`: Indica el comando que se debe ejecutar previamente establecido en `commands.cfg` para procesar el archivo que almacenará los datos de rendimiento, este comando se ejecuta cada intervalo de tiempo establecido en la línea de configuración anterior.

Nagios debe saber sobre los comandos de referencia utilizados por PNP, por ello se tienen que definir en el archivo `/usr/local/nagios/etc/commands.cfg` de la siguiente manera.

```
define command{
    command_name    process-service-perfdata-file
    command_line    /bin/mv /usr/local/pnp4nagios/var/service-
```

```

        perfddata/usr/local/pnp4nagios/var/spool/
        service-perfddata.$TIMET$
    }

define command{
    command_name    process-host-perfddata-file
    command_line    /bin/mv /usr/local/pnp4nagios/var/host-
                    perfddata /usr/local/pnp4nagios/var/spool/host-
                    perfddata.$TIMET$
}

```

El uso de los comandos en el archivo del servicio y host perfddata se trasladó a var/ spool después de ser procesado. El macro Nagios \$TIMET\$ se añade al nombre del archivo para evitar la sobre escritura de archivos antiguos sin querer. La macro \$TIMET\$ contiene la fecha y hora actual en formato de time\_t (UNIX).

En el directorio /usr/local/pnp4nagios/var/spool/ se encuentra el archivo que será procesado por NPCD. NPCD monitoriza el directorio spool y devuelve la información al archivo process\_perfddata.pl. De esta manera el procesamiento de los datos de rendimiento está totalmente desacoplado de Nagios. Finalmente iniciamos NPCD.

- /usr/local/pnp4nagios/bin/npcd -d -f /usr/local/pnp4nagios/etc/npcd.cfg

## Modo Gearman

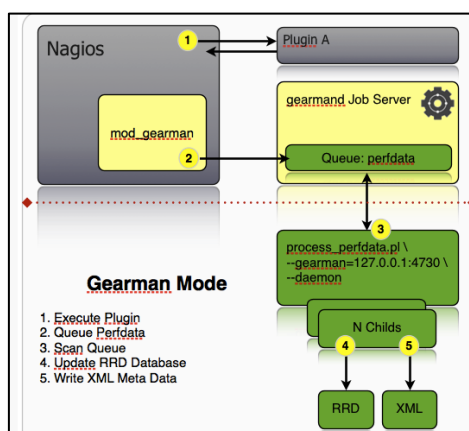


Figura B.12. Estructura del Modo Gearman  
Fuente: <http://docs.pnp4nagios.org>

Desde la versión 0.6.12 pnp4nagios se puede configurar como un trabajador gearman. De esta manera grandes instalaciones pueden ser monitoreadas por Nagios haciendo posible que Nagios y pnp4nagios puedan ejecutarse en diferentes máquinas reduciendo la carga en el servidor Nagios, la estructura del modo Gearman se muestra en la figura B.12.

### **Pre requisitos**

Para instalar Gearman y Mod-Gearman se necesitan los paquetes que se listan a continuación. Gearman se instalará en el directorio /opt para hacer más fácil su posterior eliminación, por ello agregamos la ruta /opt/lib a lib ld.

- apt-get update
- apt-get install autoconf automake make gcc g++ wget tar file netcat uuid-dev libltdl3-dev libncurses5-dev libevent-dev
- echo "/opt/lib" > /etc/ld.so.conf.d/opt\_lib.conf
- ldconfig

### **Instalación Gearman y Mod-Gearman**

Se instaló libgearman 0.32 que es la versión más reciente para las librerías utilizadas por Mod-Gearman, se especifica la ruta donde se realizará la instalación, se compilan los binarios y se instalan en el sistema.

- cd /tmp
- wget http://launchpad.net/gearmand/trunk/0.25/+download/gearmand-0.32.tar.gz
- tar zxf gearmand-0.32.tar.gz
- cd gearmand-0.32
- ./configure --prefix=/opt
- make

- make install

Después de instalar las librerías se instala el núcleo Mod-Gearman, para esto utilizaremos la última versión estable `mod_gearman-1.4.10.tar.gz`, se especifica la ruta donde se realizará la instalación y el usuario Nagios, se compilan los binarios y se instalan en el sistema.

- cd /tmp
- wget [http://labs.consol.de/wp-content/uploads/2013/09/mod\\_gearman-1.4.10.tar.gz](http://labs.consol.de/wp-content/uploads/2013/09/mod_gearman-1.4.10.tar.gz)
- tar xzf mod\_gearman-1.4.10.tar.gz
- cd mod\_gearman-1.4.10
- ./configure --prefix=/opt --with-gearman=/opt --with-user=nagios --with-init-dir=/etc/init.d
- make
- make install
- make install-config
- cp ./extras/gearmand-init /etc/init.d/gearmand

Mod-Gearman se ejecuta como usuario Nagios y necesita una shell válida. Ahora se puede iniciar el demonio Gearman y el trabajador Mod-Gearman.

- chsh Nagios

Changing the login shell for nagios

Enter the new value, or press ENTER for the default

Login Shell [/bin/false]: /bin/bash

- /etc/init.d/gearmand start

Starting gearmand done

- /etc/init.d/gearmand status

gearmand is running with pid 31869

- /etc/init.d/mod\_gearman\_worker start

Starting mod\_gm\_worker done

- /etc/init.d/mod\_gearman\_worker status

mod\_gm\_worker is running with pid 31939

### Configuración de Nagios

Para que Nagios pueda operar como un trabajador Geaman se debe abrir el archivo /usr/local/nagios/etc/nagios.cfg, habilitar la línea de eventos eventbroker y agregar las siguientes líneas de configuración.

- event\_broker\_options=-1
- broker\_module=/opt/lib/mod\_gearman/mod\_gearman.o  
config=/opt/etc/mod\_gearman.conf

Finalmente se reinicia Nagios.

- /etc/init.d/nagios restart

El archivo.log de Nagios debe contener las siguientes líneas.

- Grep mod\_gearman / var/log/nagios3/nagios.log

[1295003042] mod\_gearman: Versión 1.4.2

[1295003042] Event broker module '/opt/lib/mod\_gearman/mod\_gearman.o'

initialized successfully.

## ANEXO C

### SPANNING TREE PORTFAST BPDU GUARD ENHANCEMENT

#### INTRODUCTION

This document explains the PortFast Bridge Protocol Data Unit (BPDU) guard feature. This feature is one of the Spanning Tree Protocol (STP) enhancements that Cisco created. This feature enhances switch network reliability, manageability, and security.

#### FEATURE DESCRIPTION

STP configures meshed topology into a loop-free, tree-like topology. When the link on a bridge port goes up, STP calculation occurs on that port. The result of the calculation is the transition of the port into forwarding or blocking state. The result depends on the position of the port in the network and the STP parameters. This calculation and transition period usually takes about 30 to 50 seconds. At that time, no user data pass via the port. Some user applications can time out during the period.

In order to allow immediate transition of the port into forwarding state, enable the STP PortFast feature. PortFast immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.

As long as the port participates in STP, some device can assume the root bridge function and affect active STP topology. To assume the root bridge function, the device would be attached to the port and would run STP with a lower bridge priority than that of the current root bridge. If another device assumes the root bridge function in this way, it renders the network suboptimal. This is a simple form of a denial of service (DoS) attack on the network.

The temporary introduction and subsequent removal of STP devices with low (0) bridge priority cause a permanent STP recalculation.

The STP PortFast BPDUs guard enhancement allows network designers to enforce the STP domain borders and keep the active topology predictable. The devices behind the ports that have STP PortFast enabled are not able to influence the STP topology. At the reception of BPDUs, the BPDUs guard operation disables the port that has PortFast configured. The BPDUs guard transitions the port into errdisable state, and a message appears on the console. This message is an example:

```
2000 May 12 15:13:32 %SPANTREE-2-RX_PORTFAST:Received BPDU on PortFast
enable port.
Disabling 2/1
2000 May 12 15:13:32 %PAGP-5-PORTFROMSTP:Port 2/1 left bridge port 2/1
```

Consider this example:

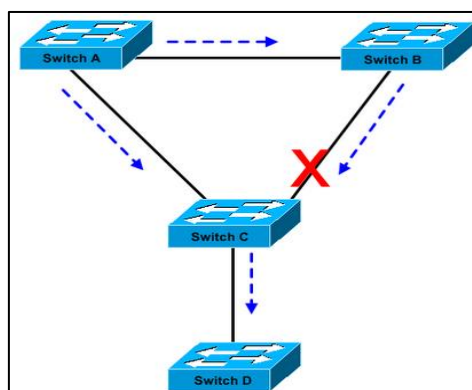


Figura C.1.

Bridge A has priority 8192 and is the root for the VLAN. Bridge B has priority 16384 and is the backup root bridge for the same VLAN. Bridges A and B, which a Gigabit Ethernet link connects, make up a core of the network. Bridge C is an access switch and has PortFast configured on the port that connects to device D. If the other STP parameters are default, the bridge C port that connects to bridge B is in STP blocking state. Device D (PC) does not participate in STP. The dashed arrows indicate the flow of STP BPDUs.



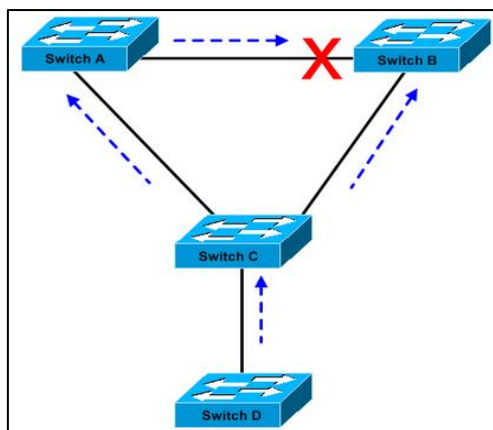


Figura C.2.

In Figure C2, device D has started to participate in STP. For example, a Linux-based bridge application is launched on a PC. If the priority of the software bridge is 0 or any value below the priority of the root bridge, the software bridge takes over the root bridge function. The Gigabit Ethernet link that connects the two core switches transitions into blocking mode. The transition causes all the data in that VLAN to flow via the 100-Mbps link. If more data flow via the core in the VLAN than the link can accommodate, the drop of frames occurs. The frame drop leads to a connectivity outage.

The STP PortFast BPDU guard feature prevents such a situation. The feature disables the port as soon as bridge C receives the STP BPDU from device D.

## CONFIGURATION

You can enable or disable STP PortFast BPDU guard on a global basis, which affects all ports that have PortFast configured. By default, STP BPDU guard is disabled. Issue this command in order to enable STP PortFast BPDU guard on the switch:

### CatOS Command

```
Console> (enable) set spantree portfast bpdu-guard enable
```

Spantree portfast bpdu-guard enabled on this switch.

Console> (enable)

### **Cisco IOS Software Command**

```
CatSwitch-IOS(config)# spanning-tree portfast bpduguard
```

```
CatSwitch-IOS(config)
```

When STP BPDU guard disables the port, the port remains in the disabled state unless the port is enabled manually. You can configure a port to reenble itself automatically from the errdisable state. Issue these commands, which set the errdisable-timeout interval and enable the timeout feature:

### **CatOS Commands.**

```
Console> (enable) set errdisable-timeout interval 400
```

```
Console> (enable) set errdisable-timeout enable bpdu-guard
```

### **Cisco IOS Software Commands.**

```
CatSwitch-IOS(config)# errdisable recovery cause bpduguard
```

```
CatSwitch-IOS(config)# errdisable recovery interval 400
```

Note: The default timeout interval is 300 seconds and, by default, the timeout feature is disabled.

## **MONITORING**

In order to verify whether the feature is enabled or disabled, issue this command:

### **COMMAND OUTPUT**

#### **CatOS Command**

```
Console> (enable) show spantree summary
```

```

CatOS Command

Console> (enable) show spantree summary
Root switch for vlans: 3-4.
Portfast bpdu-guard enabled for bridge.
Uplinkfast disabled for bridge.
Backbonefast disabled for bridge.

Summary of Connected Spanning Tree Ports By VLAN:

Vlan  Blocking Listening Learning Forwarding STP Active
-----
      1         0         0         0         1         1
      3         0         0         0         1         1
      4         0         0         0         1         1
     20         0         0         0         1         1

Blocking Listening Learning Forwarding STP Active
-----
Total         0         0         0         4         4

Console> (enable)

```

Figura C.3.

## Cisco IOS Software Command

CatSwitch-IOS# show spanning-tree summary totals

```

Cisco IOS Software Command

CatSwitch-IOS# show spanning-tree summary totals
Root bridge for: none.
PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short

Name
-----
 1 VLAN          Blocking Listening Learning Forwarding STP Active
-----
                   0         0         0         1         1

CatSwitch-IOS#

```

Figura C.4.

## **ANEXO D**

### **SPANNING-TREE PROTOCOL ENHANCEMENTS USING LOOP GUARD AND BPDU SKEW DETECTION FEATURES**

#### **INTRODUCTION**

Spanning Tree Protocol (STP) resolves physically redundant topologies into loop-free, tree-like topologies. The biggest issue with STP is that some hardware failures can cause it to fail. This failure creates forwarding loops (or STP loops). Major network outages are caused by STP loops.

This document describes the loop guard STP feature that is intended to improve the stability of the Layer 2 networks. This document also describes Bridge Protocol Data Unit (BPDU) skew detection. BPDU skew detection is a diagnostic feature that generates syslog messages when BPDUs are not received in time.

Refer to Cisco Technical Tips Conventions for more information on document conventions.

#### **FEATURE AVAILABILITY**

##### **CatOS**

- The STP loop guard feature was introduced in CatOS version 6.2.1 of the Catalyst software for Catalyst 4000 and Catalyst 5000 platforms and in version 6.2.2 for the Catalyst 6000 platform.
- The BPDU skew detection feature was introduced in CatOS version 6.2.1 of the Catalyst software for Catalyst 4000 and Catalyst 5000 platforms and in version 6.2.2 for the Catalyst 6000 platform.

## Cisco IOS

- The STP loop guard feature was introduced in Cisco IOS Software Release 12.1(12c)EW for Catalyst 4500 switches and Cisco IOS Software Release 12.1(11b)EX for Catalyst 6500.
- The BPDU skew detection feature is not supported in Catalyst switches running Cisco IOS system software.

## BRIEF SUMMARY OF STP PORT ROLES

Internally, STP assigns to each bridge (or switch) port a role that is based on configuration, topology, relative position of the port in the topology, and other considerations. The port role defines the behavior of the port from the STP point of view. Based on the port role, the port either sends or receives STP BPDUs and forwards or blocks the data traffic. This list provides a brief summary of each STP port role:

- Designated—One designated port is elected per link (segment). The designated port is the port closest to the root bridge. This port sends BPDUs on the link (segment) and forwards traffic towards the root bridge. In an STP converged network, each designated port is in the STP forwarding state.
- Root—The bridge can have only one root port. The root port is the port that leads to the root bridge. In an STP converged network, the root port is in the STP forwarding state.
- Alternate—Alternate ports lead to the root bridge, but are not root ports. The alternate ports maintain the STP blocking state.
- Backup—This is a special case when two or more ports of the same bridge (switch) are connected together, directly or through shared media. In this case, one port is designated, and the remaining ports block. The role for this port is backup.

## STP LOOP GUARD

### FEATURE DESCRIPTION

The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs.

When one of the ports in a physically redundant topology no longer receives BPDUs, the STP conceives that the topology is loop free. Eventually, the blocking port from the alternate or backup port becomes designated and moves to a forwarding state. This situation creates a loop.

The loop guard feature makes additional checks. If BPDUs are not received on a non-designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the designated port role. The port moves to the STP forwarding state and creates a loop.

When the loop guard blocks an inconsistent port, this message is logged:

- **CatOS**

```
%SPANTREE-2-LOOPGUARDBLOCK: No BPDUs were received on port 3/2 in  
vlan 3. Moved to loop-inconsistent state.
```

- **Cisco IOS**

```
%SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port
FastEthernet0/24 on VLAN0050.
```

Once the BPDU is received on a port in a loop-inconsistent STP state, the port transitions into another STP state. According to the received BPDU, this means that the recovery is automatic and intervention is not necessary. After recovery, this message is logged:

- **CatOS**

```
%SPANTREE-2-LOOPGUARDUNBLOCK: port 3/2 restored in vlan 3.
```

- **Cisco IOS**

```
%SPANTREE-2-LOOPGUARD_UNBLOCK: Loop guard unblocking port
FastEthernet0/24 on VLAN0050.
```

Consider this example in order to illustrate this behavior: Switch A is the root switch. Switch C does not receive BPDUs from switch B due to unidirectional link failure on the link between switch B and switch C.

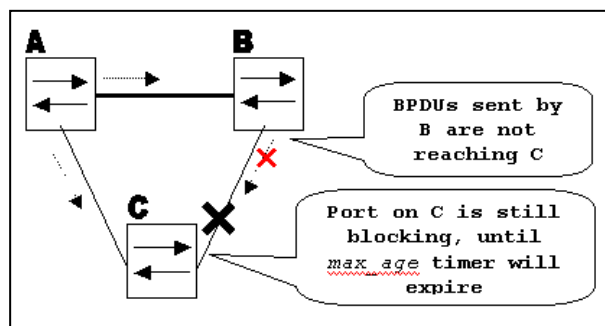


Figura D.1.

Without loop guard, the STP blocking port on switch C transitions to the STP listening state when the `max_age` timer expires, and then it transitions to the forwarding state in two times the `forward_delay` time. This situation creates a loop.

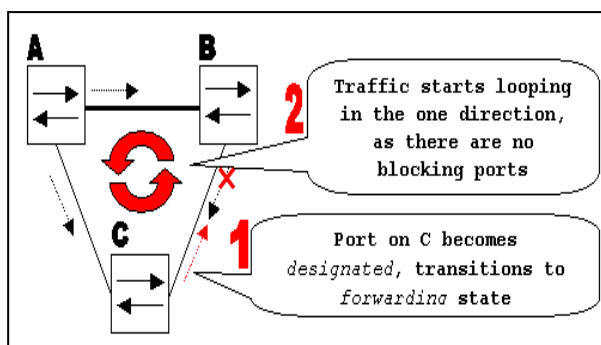


Figura D.2.

With loop guard enabled, the blocking port on switch C transitions into STP loop-inconsistent state when the `max_age` timer expires. A port in STP loop-inconsistent state does not pass user traffic, so a loop is not created. (The loop-inconsistent state is effectively equal to blocking state.)

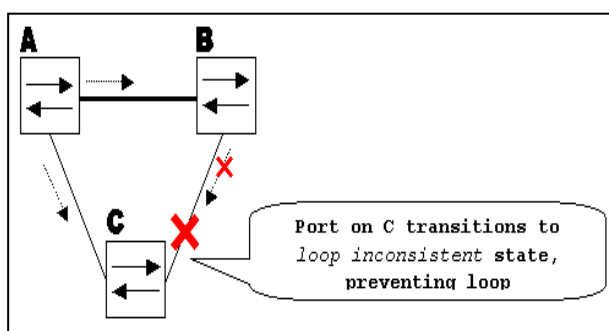


Figura D.3.

## CONFIGURATION CONSIDERATIONS

The loop guard feature is enabled on a per-port basis. However, as long as it blocks the port on the STP level, loop guard blocks inconsistent ports on a per-VLAN basis (because of per-VLAN STP). That is, if BPDUs are not received on the trunk port for only one particular VLAN, only that VLAN is blocked (moved to loop-inconsistent STP state). For the same reason, if enabled on an EtherChannel interface, the entire channel is blocked for a particular VLAN, not just one link (because EtherChannel is regarded as one logical port from the STP point of view).



On which ports should the loop guard be enabled? The most obvious answer is on the blocking ports. However, this is not totally correct. Loop guard must be enabled on the non-designated ports (more precisely, on root and alternate ports) for all possible combinations of active topologies. As long as the loop guard is not a per-VLAN feature, the same (trunk) port might be designated for one VLAN and non-designated for the other. The possible failover scenarios should also be taken into account.

Consider this example:

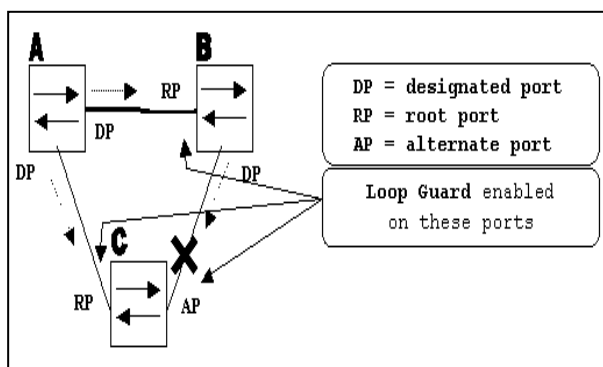


Figura D.4.

By default, loop guard is disabled. This command is used to enable loop guard:

- **CatOS**

```
set spantree guard loop <mod/port>
```

```
Console> (enable) set spantree guard loop 3/13
```

Enable loopguard will disable rootguard if it's currently enabled on the port(s).

```
Do you want to continue (y/n) [n]? y
```

```
Loopguard on port 3/13 is enabled.
```

- **Cisco IOS**

```
spanning-tree guard loop
```

```
Router(config)#interface gigabitEthernet 1/1
```

```
Router(config-if)#spanning-tree guard loop
```

With version 7.1(1) of the Catalyst software (CatOS), loop guard can be enabled globally on all ports. Effectively, loop guard is enabled on all point-to-point links. The point-to-point link is detected by the duplex status of the link. If duplex is full, the link is considered point-to-point. It is still possible to configure, or override, global settings on a per-port basis.

Issue this command in order to enable loop guard globally:

- **CatOS**

```
Console> (enable) set spantree global-default loopguard enable
```

- **Cisco IOS**

```
Router(config)#spanning-tree loopguard default
```

Issue this command in order to disable loop guard:

- **CatOS**

```
Console> (enable) set spantree guard none <mod/port>
```

- **Cisco IOS**

```
Router(config-if)#no spanning-tree guard loop
```

Issue this command in order to globally disable loop guard:

- **CatOS**

```
Console> (enable) set spantree global-default loopguard disable
```

- **Cisco IOS**

Router(config)#no spanning-tree loopguard default

Issue this command in order to verify loop guard status:

- **CatOS**

```

show spantree guard <mod/port>

Console> (enable) show spantree guard 3/13
Port                VLAN Port-State   Guard Type
-----
3/13                2    forwarding    loop
Console> (enable)

```

Figura D.5.

- **Cisco IOS**

```

show spanning-tree

Router#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfig guard is enabled
Extended system ID      is disabled
Portfast Default        is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default       is enabled
UplinkFast              is disabled
BackboneFast            is disabled
Pathcost method used    is short

Name                    Blocking Listening Learning Forwarding STP Active
-----
Total                    0          0          0          0          0

```

Figura D.6.

## LOOP GUARD VERSUS UDLD

Loop guard and Unidirectional Link Detection (UDLD) functionality overlap, partly in the sense that both protect against STP failures caused by unidirectional links. However, these two features differ in functionality and how they approach the problem. This table describes loop guard and UDLD functionality:

Tabla D.1

Functionality Configuration Action granularity Autorecover	Loop Guard Per-port Per-VLAN Yes	UDLD Per-port Per-port Yes, with err-disable timeout feature
Protection against STP failures caused by unidirectional links	Yes, when enabled on all root and alternate ports in redundant topology	Yes, when enabled on all links in redundant topology
Protection against STP failures caused by problems in the software (designated switch does not send BPDU)	Yes	No
Protection against miswiring.	No	Yes

Based on the various design considerations, you can choose either UDLD or the loop guard feature. In regards to STP, the most noticeable difference between the two features is the absence of protection in UDLD against STP failures caused by problems in software. As a result, the designated switch does not send BPDUs. However, this type of failure is (by an order of magnitude) more rare than failures caused by unidirectional links. In return, UDLD might be more flexible in the case of unidirectional links on EtherChannel. In this case, UDLD disables only failed links, and the channel should remain functional with the links that remain. In such a failure, the loop guard puts it into loop-inconsistent state in order to block the whole channel.

Additionally, loop guard does not work on shared links or in situations where the link has been unidirectional since the link-up. In the last case, the port never receives BPDU and becomes designated. Because this behaviour could be normal, this particular case is not covered by loop guard. UDLD provides protection against such a scenario.

As described, the highest level of protection is provided when you enable UDLD and loop guard.

## **INTEROPERABILITY OF LOOP GUARD WITH OTHER STP FEATURES**

### **ROOT GUARD**

The root guard is mutually exclusive with the loop guard. The root guard is used on designated ports, and it does not allow the port to become non-designated. The loop guard works on non-designated ports and does not allow the port to become designated through the expiration of max\_age. The root guard cannot be enabled on the same port as the loop guard. When the loop guard is configured on the port, it disables the root guard configured on the same port.

### **UPLINK FAST AND BACKBONE FAST**

Both uplink fast and backbone fast are transparent to the loop guard. When max\_age is skipped by backbone fast at the time of reconvergence, it does not trigger the loop guard. For more information on uplink fast and backbone fast, refer to these documents:

- [Understanding and Configuring the Cisco Uplink Fast Feature](#)
- [Understanding and Configuring Backbone Fast on Catalyst Switches](#)

### **PORTFAST AND BPDU GUARD AND DYNAMIC VLAN**

Loop guard cannot be enabled for ports on which portfast is enabled. Since BPDU guard works on portfast-enabled ports, some restrictions apply to BPDU guard. Loop guard cannot be enabled on dynamic VLAN ports since these ports have portfast enabled.

### **SHARED LINKS**

Loop guard should not be enabled on shared links. If you enable loop guard on shared links, traffic from hosts connected to shared segments might be blocked.

### **MULTIPLE SPANNING TREE (MST)**

Loop guard functions correctly in the MST environment.

## **BPDU SKEW DETECTION**

Loop guard should operate correctly with BPDU skew detection.

## **BPDU SKEW DETECTION**

### **FEATURE DESCRIPTION**

STP operation relies heavily on the timely reception of BPDUs. At every hello\_time message (2 seconds by default), the root bridge sends BPDUs. Non-root bridges do not regenerate BPDUs for each hello\_time message, but they receive relayed BPDUs from the root bridge. Therefore, every non-root bridge should receive BPDUs on every VLAN for each hello\_time message. In some cases, BPDUs are lost, or the bridge CPU is too busy to relay BPDU in a timely manner. These issues, as well as other issues, can cause BPDUs to arrive late (if they arrive at all). This issue potentially compromises the stability of the spanning tree topology.

BPDU skew detection allows the switch to keep track of BPDUs that arrive late and to notify the administrator with syslog messages. For every port on which a BPDU has ever arrived late (or has skewed), skew detection reports the most recent skew and the duration of the skew (latency). It also reports the longest BPDU delay on this particular port.

In order to protect the bridge CPU from overload, a syslog message is not generated every time BPDU skewing occurs. Messages are rate-limited to one message every 60 seconds. However, should the delay of BPDU exceed max\_age divided by 2 (which equals 10 seconds by default), the message is immediately printed.

Note: BPDU skew detection is a diagnostic feature. Upon detection of BPDU skewing, it sends a syslog message. BPDU skew detection takes no further corrective action.

This is an example of a syslog message generated by BPDU skew detection:

```
%SPANTREE-2-BPDU_SKEWING: BPDU skewed with a delay of 10 secs (max_age/2)
```

## CONFIGURATION CONSIDERATIONS

BPDU skew detection is configured on a per-switch basis. The default setting is disabled.

Issue this command in order to enable BPDU skew detection:

```
Cat6k> (enable) set spantree bpdu-skewing enable
```

Spantree bpdu-skewing enabled on this switch.

In order to see BPDU skewing information, use the `show spantree bpdu-skewing <vlan>|<mod/port>` command as demonstrated in this example:

```
Cat6k> (enable) show spantree bpdu-skewing 1
Bpdu skewing statistics for vlan 1
Port Last Skew (ms) Worst Skew (ms) Worst Skew Time
-----
3/12 4000 4100 Mon Nov 19 2001, 16:36:04
```

*Figura D.7.*

## **ANEXO E**

### **SPANNING TREE PROTOCOL ROOT GUARD ENHANCEMENT**

#### **INTRODUCTION**

This document explains the Spanning Tree Protocol (STP) root guard feature. This feature is one of the STP enhancements that Cisco created. This feature enhances switched network reliability, manageability, and security.

#### **FEATURE DESCRIPTION**

The standard STP does not provide any means for the network administrator to securely enforce the topology of the switched Layer 2 (L2) network. A means to enforce topology can be especially important in networks with shared administrative control, where different administrative entities or companies control one switched network.

The forwarding topology of the switched network is calculated. The calculation is based on the root bridge position, among other parameters. Any switch can be the root bridge in a network. But a more optimal forwarding topology places the root bridge at a specific predetermined location. With the standard STP, any bridge in the network with a lower bridge ID takes the role of the root bridge. The administrator cannot enforce the position of the root bridge.

Note: The administrator can set the root bridge priority to 0 in an effort to secure the root bridge position. But there is no guarantee against a bridge with a priority of 0 and a lower MAC address.

The root guard feature provides a way to enforce the root bridge placement in the network.



The root guard ensures that the port on which root guard is enabled is the designated port. Normally, root bridge ports are all designated ports, unless two or more ports of the root bridge are connected together. If the bridge receives superior STP Bridge Protocol Data Units (BPDUs) on a root guard-enabled port, root guard moves this port to a root-inconsistent STP state. This root-inconsistent state is effectively equal to a listening state. No traffic is forwarded across this port. In this way, the root guard enforces the position of the root bridge.

The example in this section demonstrates how a rogue root bridge can cause problems on the network and how root guard can help.

In Figure E. 1, Switches A and B comprise the core of the network, and A is the root bridge for a VLAN. Switch C is an access layer switch. The link between B and C is blocking on the C side. The arrows show the flow of STP BPDUs.

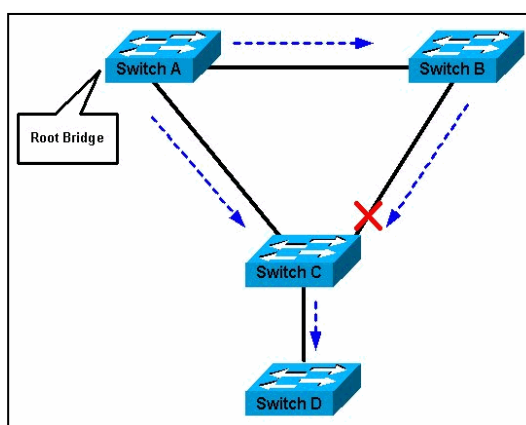


Figura E.1.

In Figure E.2, device D begins to participate in STP. For example, software-based bridge applications are launched on PCs or other switches that a customer connects to a service-provider network. If the priority of bridge D is 0 or any value lower than the priority of the root bridge, device D is elected as a root bridge for this VLAN. If the link between device A and B is 1 gigabit and links between A and C as well as B and C are 100 Mbps, the election of D as root causes the Gigabit Ethernet link that connects the two core switches to block.

This block causes all the data in that VLAN to flow via a 100-Mbps link across the access layer. If more data flow via the core in that VLAN than this link can accommodate, the drop of some frames occurs. The frame drop leads to a performance loss or a connectivity outage.

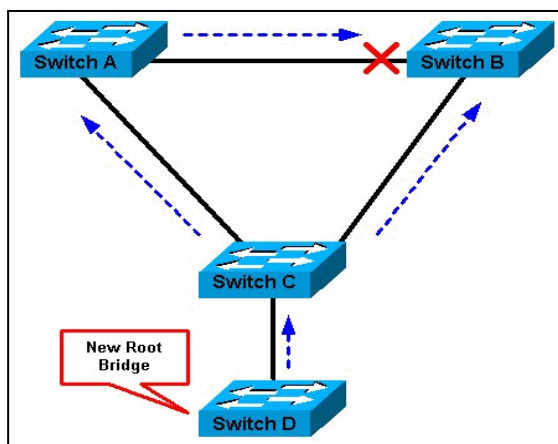


Figura E.2.

The root guard feature protects the network against such issues.

The configuration of root guard is on a per-port basis. Root guard does not allow the port to become an STP root port, so the port is always STP-designated. If a better BPDU arrives on this port, root guard does not take the BPDU into account and elect a new STP root. Instead, root guard puts the port into the root-inconsistent STP state. You must enable root guard on all ports where the root bridge should not appear. In a way, you can configure a perimeter around the part of the network where the STP root is able to be located.

In Figure E.2. Enable root guard on the Switch C port that connects to Switch D.

Switch C in Figure E.2 blocks the port that connects to Switch D, after the switch receives a superior BPDU. Root guard puts the port in the root-inconsistent STP state. No traffic passes through the port in this state. After device D ceases to send superior BPDUs, the port is unblocked again. Via STP, the port goes from the listening state to the learning state, and

eventually transitions to the forwarding state. Recovery is automatic; no human intervention is necessary.

This message appears after root guard blocks a port:

```
%SPANTREE-2-ROOTGUARDBLOCK: Port 1/1 tried to become non-designated in VLAN 77.
```

```
Moved to root-inconsistent state
```

## **AVAILABILITY**

Root guard is available in Catalyst OS (CatOS) for Catalyst 29xx, 4500/4000, 5500/5000, and 6500/6000 in software version 6.1.1 and later. For the Catalyst 6500/6000 that runs Cisco IOS® system software, this feature was first introduced in Cisco IOS Software Release 12.0(7)XE. For the Catalyst 4500/4000 that runs Cisco IOS system software, this feature is available in all releases.

For the Catalyst 2900XL and 3500XL switches, root guard is available in Cisco IOS Software Release 12.0(5)XU and later. The Catalyst 2950 series switches support the root guard feature in Cisco IOS Software Release 12.0(5.2)WC(1) and later. The Catalyst 3550 series switches support the root guard feature in Cisco IOS Software Release 12.1(4)EA1 and later.

## **CONFIGURATION**

### **CATOS CONFIGURATION**

The root guard configuration is on a per-port basis. On Catalyst switches that run CatOS, configure root guard in this way:

```
vega> (enable) set spantree guard root 1/1
```

```
Rootguard on port 1/1 is enabled.
```

Warning!! Enabling rootguard may result in a topology change.

vega> (enable)

In order to verify whether the root guard is configured, issue this command:

```
vega> (enable) show spantree guard
Port                VLAN Port-State   Guard Type
-----
1/1                 1    forwarding    root
1/2                 1    not-connected  none
3/1                 1    not-connected  none
3/2                 1    not-connected  none
3/3                 1    not-connected  none
3/4                 1    not-connected  none
5/1                 1    forwarding     none
5/25                1    not-connected  none
15/1                1    forwarding     none
vega> (enable)
```

Figura E.3.

### Cisco IOS Software Configuration for Catalyst 6500/6000 and Catalyst 4500/4000

On the Catalyst 6500/6000 or Catalyst 4500/4000 switches that run Cisco IOS system software, issue this set of commands in order to configure STP root guard:

```
Cat-IOS# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Cat-IOS#(config)# interface fastethernet 3/1
```

```
Cat-IOS#(config-if)# spanning-tree guard root
```

Note: Cisco IOS Software Release 12.1(3a)E3 for the Catalyst 6500/6000 that runs Cisco IOS system software changed this command from spanning-tree rootguard to spanning-tree guard root. The Catalyst 4500/4000 that runs Cisco IOS system software uses the spanning-tree guard root command in all releases.

### **CISCO IOS SOFTWARE CONFIGURATION FOR CATALYST 2900XL/3500XL, 2950, AND 3550**

On the Catalyst 2900XL, 3500XL, 2950, and 3550, configure switches with root guard in interface configuration mode, as this example shows:

```
Hinda# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Hinda(config)# interface fastethernet 0/8
```

```
Hinda(config-if)# spanning-tree rootguard
```

```
Hinda(config-if)# ^Z
```

```
*Mar 15 20:15:16: %SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Rootguard  
enabled on
```

```
port FastEthernet0/8 VLAN 1.^Z
```

```
Hinda#
```

## **WHAT IS THE DIFFERENCE BETWEEN STP BPDU GUARD AND STP ROOT GUARD?**

BPDU guard and root guard are similar, but their impact is different. BPDU guard disables the port upon BPDU reception if PortFast is enabled on the port. The disablement effectively denies devices behind such ports from participation in STP. You must manually reenabling the port that is put into errdisable state or configure errdisable-timeout.

Root guard allows the device to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic. Recovery occurs as soon as the offending device ceases to send superior BPDUs.

For more information about BPDU guard, refer to this document:

Spanning Tree PortFast BPDU Guard Enhancement

## **DOES THE ROOT GUARD HELP WITH THE TWO ROOTS PROBLEM?**

There can be a unidirectional link failure between two bridges in a network. Because of the failure, one bridge does not receive the BPDUs from the root bridge. With such a failure, the root switch receives frames that other switches send, but the other switches do not receive the BPDUs that the root switch sends. This can lead to an STP loop. Because the other switches do not receive any BPDUs from the root, these switches believe that they are the root and start to send BPDUs.

When the real root bridge starts to receive BPDUs, the root discards the BPDUs because they are not superior. The root bridge does not change. Therefore, root guard does not help to resolve this issue. The UniDirectional Link Detection (UDLD) and loop guard features address this issue.

For more information on STP failure scenarios and how to troubleshoot them, refer to this document:

- [Spanning Tree Protocol Problems and Related Design Considerations](#)

## ANEXO F

# UNDERSTANDING AND CONFIGURING THE UNIDIRECTIONAL LINK DETECTION PROTOCOL FEATURE

## INTRODUCTION

This document explains how the Unidirectional Link Detection (UDLD) protocol can help to prevent forwarding loops and blackholing of traffic in switched networks.

## PROBLEM DEFINITION

Spanning-Tree Protocol (STP) resolves redundant physical topology into a loop-free, tree-like forwarding topology.

This is done by blocking one or more ports. By blocking one or more ports, there are no loops in the forwarding topology. STP relies in its operation on reception and transmission of the Bridge Protocol Data Units (BPDUs). If the STP process that runs on the switch with a blocking port stops receiving BPDUs from its upstream (designated) switch on the port, STP eventually ages out the STP information for the port and moves it to the forwarding state. This creates a forwarding loop or STP loop.

Packets start to cycle indefinitely along the looped path, and consumes more and more bandwidth. This leads to a possible network outage.

How is it possible for the switch to stop receiving BPDUs while the port is up? The reason is unidirectional link. A link is considered unidirectional when this occurs:

The link is up on both sides of the connection. The local side is not receiving the packets sent by the remote side while remote side receives packets sent by local side.

Consider this scenario. The arrows indicate the flow of STP BPDUs.

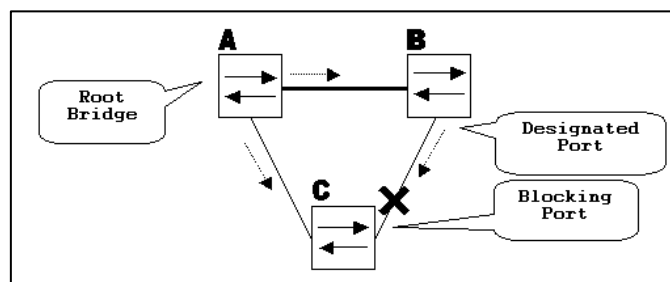


Figura F.1.

During normal operation, bridge B is designated on the link B-C. Bridge B sends BPDUs down to C, which is blocking the port. The port is blocked while C sees BPDUs from B on that link.

Now, consider what happens if the link B-C fails in the direction of C. C stops receiving traffic from B, however, B still receives traffic from C.

C stops receiving BPDUs on the link B-C, and ages the information received with the last BPDUs. This takes up to 20 seconds, depending on the maxAge STP timer. Once the STP information is aged out on the port, that port transitions from the blocking state to the listening, learning, and eventually to the forwarding STP state. This creates a forwarding loop, as there is no blocking port in the triangle A-B-C. Packets cycle along the path (B still receives packets from C) taking additional bandwidth until the links are completely filled up. This brings the network down.

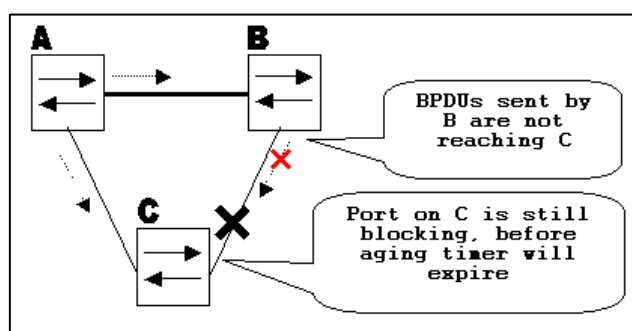


Figura F.2.



Another possible issue that can be caused by a unidirectional link is traffic blackholing.

### **How Unidirectional Link Detection Protocol Works**

In order to detect the unidirectional links before the forwarding loop is created, Cisco designed and implemented the UDLD protocol.

UDLD is a Layer 2 (L2) protocol that works with the Layer 1 (L1) mechanisms to determine the physical status of a link. At Layer 1, auto-negotiation takes care of physical signaling and fault detection. UDLD performs tasks that auto-negotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When you enable both auto-negotiation and UDLD, Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

UDLD works by exchanging protocol packets between the neighboring devices. In order for UDLD to work, both devices on the link must support UDLD and have it enabled on respective ports.

Each switch port configured for UDLD sends UDLD protocol packets that contain the port's own device/port ID, and the neighbor's device/port IDs seen by UDLD on that port. Neighboring ports should see their own device/port ID (echo) in the packets received from the other side.

If the port does not see its own device/port ID in the incoming UDLD packets for a specific duration of time, the link is considered unidirectional.

This echo-algorithm allows detection of these issues:

- Link is up on both sides, however, packets are only received by one side.

- Wiring mistakes when receive and transmit fibers are not connected to the same port on the remote side.

Once the unidirectional link is detected by UDLD, the respective port is disabled and this message is printed on the console:

```
UDLD-3-DISABLE: Unidirectional link detected on port 1/2. Port disabled
```

Port shutdown by UDLD remains disabled until it is manually reenabled, or until `errdisable` timeout expires (if configured).

## UDLD MODES OF OPERATION

UDLD can operate in two modes: normal and aggressive. In normal mode, if the link state of the port was determined to be bi-directional and the UDLD information times out, no action is taken by UDLD. The port state for UDLD is marked as undetermined. The port behaves according to its STP state.

In aggressive mode, if the link state of the port is determined to be bi-directional and the UDLD information times out while the link on the port is still up, UDLD tries to re-establish the state of the port. If not successful, the port is put into the `errdisable` state.

Aging of UDLD information happens when the port that runs UDLD does not receive UDLD packets from the neighbor port for duration of hold time. The hold time for the port is dictated by the remote port and depends on the message interval at the remote side. The shorter the message interval, the shorter the hold time and the faster the detection. Recent implementations of UDLD allow configuration of message interval.

UDLD information can age out due to the high error rate on the port caused by some physical issue or duplex mismatch. Such packet drop does not mean that the link is unidirectional and UDLD in normal mode will not disable such link.

It is important to be able to choose the right message interval in order to ensure proper detection time. The message interval should be fast enough to detect the unidirectional link before the forwarding loop is created, however, it should not overload the switch CPU. The default message interval is 15 seconds, and is fast enough to detect the unidirectional link before the forwarding loop is created with default STP timers. The detection time is approximately equal to three times the message interval.

For example:  $T_{\text{detection}} \sim \text{message\_interval} \times 3$

This is 45 seconds for the default message interval of 15 seconds.

It takes  $T_{\text{reconvergence}} = \text{max\_age} + 2 \times \text{forward\_delay}$  for the STP to reconverge in case of unidirectional link failure. With the default timers, it takes  $20 + 2 \times 15 = 50$  seconds.

It is recommended to keep  $T_{\text{detection}} < T_{\text{reconvergence}}$  by choosing an appropriate message interval.

In aggressive mode, once the information is aged, UDLD will make an attempt to re-establish the link state by sending packets every second for eight seconds. If the link state is still not determined, the link is disabled. Aggressive mode adds additional detection of these situations:

- The port is stuck (on one side the port neither transmits nor receives, however, the link is up on both sides).

- The link is `up` on one side and `down` on the other side. This issue might be seen on fiber ports. When transmit fiber is unplugged on the local port, the link remains `up` on the local side. However, it is `down` on the remote side.

Most recently, fiber FastEthernet hardware implementations have Far End Fault Indication (FEFI) functions in order to bring the link `down` on both sides in these situations. On Gigabit Ethernet, a similar function is provided by link negotiation. Copper ports are normally not susceptible to this type of issue, as they use Ethernet link pulses to monitor the link. It is important to mention that in both cases, no forwarding loop occurs because there is no connectivity between the ports. If the link is `up` on one side and `down` on the other, however, blackholing of traffic might occur. Aggressive UDLD is designed to prevent this.

## CONFIGURATION AND MONITORING

These commands detail the UDLD configuration on Catalyst switches that run CatOS. UDLD needs to first be enabled globally (default is disabled) with this command:

```
Vega> (enable) set uddl enable
```

```
UDLD enabled globally
```

Issue this command: to verify whether the UDLD is enabled

```
Vega> (enable) show uddl
```

```
UDLD: enabled
```

```
Message Interval: 15 seconds
```

UDLD also needs to be enabled on necessary ports with this command:

```
Vega> (enable) set uddl enable 1/2
```

```
UDLD enabled on port 1/2
```

Issue the `show uddl port` command to verify whether UDLD is enabled or disabled on the port and what the link state is:

```
Vega> (enable) show udld port
UDLD          : enabled
Message Interval : 15 seconds

Port      Admin Status  Aggressive Mode  Link State
-----
1/1       enabled        disabled         undetermined
1/2       enabled        disabled         bidirectional
```

Figura F.3.

Aggressive UDLD is enabled on a per-port basis with the `set udld aggressive-mode enable <module/port>` command:

```
Vega> (enable) set udld aggressive-mode enable 1/2
Aggressive UDLD enabled on port 1/2.
Vega> (enable) show udld port 1/2
UDLD          : enabled
Message Interval : 15 seconds

Port      Admin Status  Aggressive Mode  Link State
-----
1/2       enabled        enabled          undetermined
```

Figura F.4.

Issue this command to change the message interval:

```
Vega> (enable) set udld interval 10
```

UDLD message interval set to 10 seconds

The interval can range from 7 to 90 seconds, with the default being 15 seconds.

Refer to these documents for more information on the IOS UDLD configuration:

- For Catalyst 6500/6000 switches that run Cisco IOS system software, refer to *Configuring UDLD*.
- For Catalyst 2900XL/3500XL switches, refer to the *Configuring UniDirectional Link Detection* section of *Configuring the Switch Ports*.
- For Catalyst 2940 switches, refer to *Configuring UDLD*.
- For Catalyst 2950/2955 switches, refer to *Configuring UDLD*.
- For Catalyst 2970 switches, refer to *Configuring UDLD*.
- For Catalyst 3550 switches, refer to *Configuring UDLD*.
- For Catalyst 3560 switches, refer to *Configuring UDLD*.
- For Catalyst 4500/4000 running Cisco IOS, refer to *Configuring UDLD*.

## REFERENCIAS BIBLIOGRÁFICAS

- Cayuqueo, S. (2012). *Cayu- Monitoreo de red con Nagios*. Obtenido de <http://wiki.cayu.com.ar/doku.php?id=manuales:nagios>
- CISCO. (2010). *Cisco Catalyst 4500 Series Switches*. Obtenido de <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4000-series-switches/65591-cat4500-high-cpu.html>
- Cisco Systems. (2010). *Switch : Switch Cisco Catalyst de la serie 4500*. Obtenido de [http://www.cisco.com/cisco/web/support/LA/7/77/77440\\_cat4500\\_high\\_cpu.html](http://www.cisco.com/cisco/web/support/LA/7/77/77440_cat4500_high_cpu.html)
- Douglas, M., & Schmidt, K. (2005). *Essential SNMP*. Sebastopol,Ucrania: O'Reilly.
- Frisch, E. (2002). *Essential System Administration*. Sebastopol,Ucrania: O'Reilly.
- Horizons Vertical. (2010). *SNMP Message Format*. Obtenido de Vertical Horizons - SNMP <http://verticalhorizons.in/snmp-message-format-snmp-pdu-format/>
- Huidobro, J. M., Blanco, A., & Jordán, J. (2008). *Redes de Area Local - Administracion de Sistemas Informaticos*. Madrid, España: Thomson Paraninfo, S.A.
- Martí, A. (2009). *Gestion de Red*. Cataluña, España: UPC.
- NAGIOS. (2010). *Nagios Exchange*. Obtenido de <http://exchange.nagios.org/>
- Nagios. (2012). *Nagios Chile community site*. Obtenido de [http://www.nagios-cl.org/?page\\_id=47](http://www.nagios-cl.org/?page_id=47)
- Nagios Core. (2012). *Nagios- Documentation*. Obtenido de <http://nagios.sourceforge.net/docs/nagioscore/3/en/toc.html>
- NAGIOSQL. (2010). *NAGIOSQL*. Obtenido de <http://www.nagiosql.org/>
- PNP4NAGIOS. (2010). *PNP4NAGIOS*. Obtenido de <http://docs.pnp4nagios.org/>
- Stallings, W. (2004). *Comunicaciones y redes de computadoras*. Madrid, España: Pearson educacion, S.A.
- UIT-T. Recomendación M.3010. (2000). *Principios de gestion de la TMN*. Obtenido de [http://www.itu.int/net/itu\\_search/index.aspx?cx=001276825495132238663%3Anqzm45z846q&cof=FORID%3A9&ie=UTF-8&q=M3010](http://www.itu.int/net/itu_search/index.aspx?cx=001276825495132238663%3Anqzm45z846q&cof=FORID%3A9&ie=UTF-8&q=M3010)
- UIT-T. Recomendación X.700. (1992). *Marco de gestion para la interconexion de sistemas abiertos para aplicaciones del CCITT*. Obtenido de <http://www.itu.int/rec/T-REC-X.700-199708-I/e>
- UIT-T. Recomendacion X.701. (1997). *Tecnologia de la informacion- Interconexion de sistemas abiertos (OSI)*. Obtenido de <http://www.itu.int/rec/T-REC-X.701-199708-I/e>

