UNIVERSIDAD POLITÉCNICA SALESIANA FACULTAD DE INGENIERÍAS SEDE QUITO-CAMPUS SUR CARRERA DE INGENIERÍA ELECTRÓNICA MENCIÓN (TELECOMUNICACIONES)

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

TESIS PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERO ELECTRÓNICO

AUTORES:

GINA ALEJANDRA OJEDA OJEDA DIANA ALEXANDRA VALDIVIESO CARRIÓN

DIRECTOR: ING. VERÓNICA SORIA

QUITO, NOVIEMBRE 2011

DECLARACIÓN

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

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

Gina Alejandra Ojeda

Diana Alexandra Valdivieso

CERTIFICACIÓN

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

> Verónica Soria DIRECTORA DE TESIS

AGRADECIMIENTO

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

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

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

DIANA VALDIVIESO

DEDICATORIA

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

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

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

DIANA VALDIVIESO

AGRADECIMIENTO

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

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

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

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

GINA OJEDA

DEDICATORIA

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

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

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

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

A mis amigas las quiero y las extrañaré siempre.

GINA OJEDA

CONTENIDO

PRESENTACIÓN RESUMEN	
	1
	1
SITUACION ACTUAL	1
1.1 ANTECEDENTES	1
1.2 ESTRUCTURA GENERAL DE LA CORPORACIÓN NACIONAL DE	
TELECOMUNICACIONES	2
1.3 ESTRUCTURA ANTERIOR DEL ÁREA IP/MPLS	
1.4 NUEVA ESTRUCTURA DEL ÁREA O&M IP/MPLS	4
1.5 IDENTIFICACIÓN DE FUNCIONES DE LAS NUEVAS ÁREAS	4
1.5.1 ÁREA DE OPERACIÓN Y MANTENIMIENTO	4
1.5.2 ÁREA DE INGENIERÍA	5
1.5.3 ÁREA DE GESTIÓN	б
1.5.4 ÁREA DEL NOC	7
1.6 POLÍTICAS	
1.6.1 ESCALAMIENTO INTERNO BACKBONE	
1.6.2 TIEMPOS DE RESPUESTA	9
1.7 INDICADORES DE GESTIÓN	9
1.7.1 BENEFICIOS DE LOS INDICADORES DE GESTIÓN	
1.7.1.1 SATISFACCIÓN DEL CLIENTE	
1.7.1.2 MONITOREO DEL PROCESO	
1.7.1.3 GERENCIA DEL CAMBIO	
1.8 CONOCIMIENTO TÉCNICO DEL PERSONAL	13
CAPÍTULO 2	16
ARQUITECTURA MPLS Y MODELOS DE SISTEMAS DE GESTIÓN	16
2.1 INTRODUCCIÓN	
2.2 MPLS (MULTIPROTOCOL LABEL SWITCHING)	17
2.2.1 ELEMENTOS DE MPLS	17
2.2.1.1 DOMINIO MPLS	17
2.2.1.2 LER (LABEL EDGE ROUTER)	
2.2.1.3 LSR (LABEL SWITCHING ROUTER)	
2.2.1.4 FEC (FORWARDING EQUIVALENCE CLASS)	
2.2.1.5 LSP (LABEL SWITCHED PATH)	
2.2.1.5.1 ENRUTAMIENTO HOP BY HOP	20
2.2.1.5.2 ENRUTAMIENTO EXPLÍCITO (ER-LSP)	20
2.3 TUNELIZACIÓN EN MPLS	

2.4 ETIQUETA	20
2.4.1 ASIGNACIÓN Y DISTRIBUCIÓN DE ETIQUETAS	21
2.4.1.1 ASIGNACIÓN DE ETIQUETAS DOWNSTREAM	21
2.4.1.1.1 DOWNSTREAM ON DEMAND	22
2.4.1.1.2 UNSOLICITED DOWNSTREAM	22
2.4.1.2 ASIGNACIÓN DE ETIQUETAS UPSTREAM	22
2.4.2 FORMATO DE LA CABECERA MPLS	23
2.4.3 PILA DE ETIQUETAS (LABEL STACK)	24
2.5 DISTRIBUCIÓN DE LA CAPA DE RED EN PLANOS	25
2.5.1 PLANO DE CONTROL	25
2.5.1.1 TABLA DE ENRUTAMIENTO	25
2.5.2 PLANO DE DATOS	26
2.6 FUNCIONAMIENTO DE MPLS	26
2.7 PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS	28
2.7.1 PROTOCOLO LDP (LABEL DISTRIBUTION PROTOCOL)	29
2.7.2 PROTOCOLO BGP (BORDER GATEWAY PROTOCOL)	29
2.7.3 PROTOCOLO CR-LDP (CONSTRAINT-BASED ROUTING LDP)	30
2.7.3.1 CR-LSP	30
2.7.4 PROTOCOLO RSVP-TE (RSVP - TRAFFIC EXTENSION)	31
2.7.4.1 RSVP-TE	31
2.8 APLICACIONES DE MPLS	31
2.8.1 INGENIERÍA DE TRÁFICO	32
2.8.2 CALIDAD DE SERVICIO (QOS)	32
2.8.3 SOPORTE DE REDES VIRTUALES PRIVADAS	33
2.8.3.1 FUNCIONAMIENTO DE UNA VPN	34
2.8.3.2 MODELO DE ENRUTAMIENTO VPN EN MPLS	34
2.8.3.3 REDES PRIVADAS VIRTUALES MPLS	35
2.8.3.3.1 VPNS MPLS DE CAPA 3 (VPNS BGP / MPLS)	35
2.8.3.3.2 VPNS MPLS DE CAPA 2	36
2.9 VENTAJAS MPLS	36
2.10 MODELOS DE SISTEMAS DE GESTIÓN	37
2.10.1 GESTIÓN DE REDES	37
2.10.2 ELEMENTOS DE GESTIÓN DE REDES	37
2.10.3 MODELO DE GESTIÓN OSI	38
2.10.4 MODELO DE GESTIÓN INTERNET	40
2.10.4.1 VERSIONES SNMP	43
2.10.5 MODELO DE GESTIÓN INTERNET TMN	44
2.10.5.1 MODELO DE CAPAS TMN	44
2.10.5.1.1 ELEMENTOS DE RED	44
2.10.5.1.2 GESTIÓN DE ELEMENTOS DE RED	45

2	.10.5.1.3 GESTIÓN DE RED	. 45
2	.10.5.1.4 GESTIÓN DE SERVICIOS	. 45
2	.10.5.1.5 GESTIÓN EMPRESARIAL	. 46
2.10	.5.2 CONJUNTOS DE FUNCIONES DE GESTIÓN TMN	. 46
2.10	.5.3 INTERFAZ Q3	. 46
CAPITULO	3	47
PLATAFOR	MAS DE CESTIÓN V MONITOREO DE UN BACKBONE: ANA WHAT`S U	Р
CACTL NA	GIOS. IP SOLUTION CENTER. ACS	. 47
2.1 INIT	PODUCCIÓN	17
3.1 INT		. 47
3.2 AN	COMPATIBILIDAD OUE PRESENTA ANA	. 47
3.2.1		. 40
2.2.2	NIVELES EUNCIONALES DE ANA	. 40
3.2.5	NIVELES FUNCIONALES DE ANA	. 49
3.2.2	3.1 OESTION DE ELEMENTOS	. 49
2.2.2	2.2 SERVICIO DE ACTIVACIÓN	51
5.2.3 2.2.4	DENEELCIOS DE ANA	. 51
3.2.4	DENEFICIOS DE ANA	. 52
2.2.1		. 52
3.3.1	EUNCIONALIDADES DE WHATS UD	. 52
3.3.2	DESCRIPCIÓN DE LAS EUNCIONES BÁSICAS	. 52
3.3.3 3.4 CAC	TI	. 55
3.4 CAC		. 54
3.4.1		. 54
3.4.2 2.4.2		. 54
5.4.5 2.4.4		. 54
5.4.4 2.4.5	DASE DE DATOS	. 54
5.4.5 2.4.6		. 55
3.4.0 3.5 NAC	MONTORED DE UN EQUITO CON CACIT	. 50
3.5 NAC	Ω Δ Ρ Δ C ΤΕΡΊ STIC Δ S ΡΡΙΝCΙΡΔΙ ΕS	. 57
3.5.1	DESCRIPCIÓN DEL SERVIDOR NACIOS	58
3.5.2 3.6 IP St	OLUTION CENTER	. 50
3.6 1	APLICACIONES	60
3.6.2	CAPACTERÍSTICAS V VENTALAS	. 00
37 409	CARACTERISTICAS I VENTASAS	. 02
371	CARACTERÍSTICAS	. 0 <i>5</i>
3.7.1	FUNCIONALIDAD DE ACS	. 0 4 6/
373	POR OLIÉ ES NECESARIO USAR ACS?	. 07
3.7.5	NUEVAS CARACTERÍSTICAS	. 05
5.7.4		. 05

CAPÍTULO 4	66
ITIL FOUNDATION (INFORMATION TECHNOLOGY INFRAESTRUCT	URE LIBRARY 66
4.1 INTRODUCCIÓN	66
4.2 DESCRIPCIÓN	66
4.3 OBJETIVOS DE ITIL	67
4.4 ÁREAS ADMINISTRADAS POR ITIL	67
4.5 ESTRUCTURA ITIL	68
4.6 GESTIÓN DE SERVICIO	69
4.7 SOPORTE DE SERVICIOS	
4.7.1 COMPONENTES DE LA METODOLOGÍA DE SOPORTE AL S	SERVICIO 70
4.7.2 GESTIÓN DE INCIDENCIAS	
4.7.3 GESTIÓN DE PROBLEMA	
4.7.4 GESTIÓN DE CAMBIO	
4.7.5 GESTIÓN DE CONFIGURACIONES	
4.7.6 GESTIÓN DE VERSIONES	
4.8 PROVISIÓN DE SERVICIOS	
4.8.1 GESTIÓN DE NIVELES DE SERVICIOS	
4.8.2 GESTIÓN FINANCIERA DE LOS SERVICIOS TI	
4.8.3 GESTIÓN DE CAPACIDAD	
4.8.4 GESTIÓN DE LA CONTINUIDAD DEL SERVICIO	
4.8.5 GESTIÓN DE DISPONIBILIDAD	
4.8.6 GESTIÓN DE LA SEGURIDAD	
CAPÍTULO 5	
I EVANTAMIENTO V DOCUMENTACIÓN DE PROCESOS NECESARIO	IS PARA I A
ADMINISTRACIÓN DE UNA RED BACKBONE IP/MPLS	
5.1 MANUAL CACTI	
5.1.1 OBJETIVO	
5.1.2 INTRODUCCION	
5.1.3 INGRESO AL SISTEMA	
5.1.4 PANTALLA INICIAL	
5.1.5 TAB CONSOLE	
5.1.5.1 DEVICES	
5.1.5.2 ANADIK UN EQUIPO	
5.1.5.5 EDITAR UN EQUIPO	
5.1.5.5 MANAGEMENT	
5.1.5.5.1 GRAPH MANAGEMENT	
5.1.5.5.2 CREACIÓN DE UN GRAPH TREE	
5.1.6 TAB GRAPH	

5.1.6.1 VISUALIZACIÓN DE GRÁFICOS	103
5.1.6.2 EJEMPLO DE ANÁLISIS DE GRÁFICOS	104
5.1.7 TAB MONITOR	106
5.1.8 TAB GPS MAP	107
5.1.8.1 MAPA	107
5.1.8.2 SATÉLITE	108
5.1.8.3 RELIEVE	108
5.1.9 TAB WEATHERMAP	109
5.1.10 TAB NPC	115
5.1.10.1 HOSTS	115
5.1.10.1.1 HOST	116
5.1.10.1.2 HOSTSGROUP PROBLEMS	117
5.1.10.1.3 HOSTSGROUP OVERVIEW	117
5.1.10.1.4 HOSTSGROUP GRID	118
5.1.10.2 SERVICES	118
5.1.10.2.1 SERVICES	118
5.1.10.2.2 SERVICES PROBLEMS	119
5.1.10.3 PROCESS INFORMATION	119
5.1.10.4 EVENT LOG	120
5.1.10.5 REPORTING	120
5.1.11 TAB THOLDS	121
5.1.11.1 THRESHOLDS	121
5.1.11.2 HOST STATUS	122
5.1.12 TAB CLOG	123
5.1.13 TAB CEREOUS	124
5.1.14 TAB NECTAR	128
5.1.14.1 CREACIÒN DE UN REPORTE	129
5.1.14.1.1 ITEMS	131
5.1.14.1.2 PREVIEW	132
5.1.14.1.3 EVENTS	132
5.2 MANUAL DE ADMINISTRACIÓN DE ANA (ACTIVE NETWORK ABSTRAC	ГION) 134
5.2.1 OBJETIVO	134
5.2.2 INTRODUCCIÓN	134
5.2.3 ANA MANAGE	135
5.2.3.1 FUNCIONES PRINCIPALES	135
5.2.3.2 INICIALIZACIÓN DE ANA MANAGE	136
5.2.3.3 BARRA DE HERRAMIENTAS	138
5.2.3.4 ADMINISTRACIÓN DE SERVIDORES ANA	139
5.2.3.4.1 ADMINISTRACIÓN DE ANA UNITS	139
5.2.3.4.1.1 CREACIÓN UN NUEVO UNIT	140

5.2.3.4.2	2 Al	DMINISTRACIÓN DE LOS AVMS	
5.2.3	3.4.2.1	CREACIÓN DE UNA AVM	
5.2.3.4.	3 Al	DMINISTRACIÓN DE VNES	
5.2.3	3.4.2.2	CREACIÓN DE UNA VNE	
5.2.3.5	GLO	BAL SETTINGS	153
5.2.3.5.	1 D	ATABASE SEGMENTS	154
5.2.3.5.2	2 EV	VENT MANAGEMENT SETTINGS	155
5.2.3.5.	3 M	ESSAGE OF THE DAY	156
5.2.3.5.4	4 PC	DLLING GROUPS	156
5.2.3	8.5.4.1	CREAR UN NUEVO POLLING GROUP	157
5.2.3.5.	5 PF	ROTECTION GROUPS	158
5.2.3	8.5.5.1	CREAR UN NUEVO PROTECTION GROUPS	158
5.2.3.5.	6 RI	EPORT SETTINGS	159
5.2.3.5.	7 SE	ECURITY SETTINGS	159
5.2.3	8.5.7.1	AUTHENTICATION METHOD	159
5.2.3	8.5.7.2	PASSWORD SETTINGS	160
5.2.3	8.5.7.3	USER ACCOUNT SETTINGS	161
5.2.3.5.	8 Al	NA SECURITY	161
5.2.3	8.5.8.1	ADMINISTRACIÓN DE DISPOSITIVOS	161
5.2.3	8.5.8.2	APLICACIÓN DE FUNCIONALIDADES	162
5.2.3	3.5.8.3	FUNCIONES DE SEGURIDAD	162
5.2.3	3.5.8.4	ADMINISTRACIÓN DE SEGURIDAD	163
5.2.3.5.	9 T(OPOLOGY	167
5.2.3	8.5.9.1	CREACIÓN DE NUEVO ENLACE ESTÁTICO	168
5.2.4 EVE	ENTVIS	SION (VISOR DE SUCESOS ANA)	169
5.2.4.1	INIC	IALIZACIÓN DE EVENTVISION	169
5.2.4.2	DET	ALLES EVENTVISION	172
5.2.4.3	DET	ALLES -SPLIT SCREEN	173
5.2.4.4	TAB	ALL	173
5.2.4.5	TAB	AUDIT	174
5.2.4.6	TAB	PROVISIONING	175
5.2.4.7	TAB	SECURITY	175
5.2.4.8	TAB	SERVICE	176
5.2.4.9	TAB	SYSLOG	178
5.2.4.10	TAB	SYSTEM	179
5.2.4.11	TAB	TICKET	
5.2.4.12	TAB	SNMP TRAPS	180
5.2.5 CISC	CO AN	IA NETWORKVISION	
5.2.5.1	FUN	CIONALIDAD DE NETWORKVISION	
5.2.5.2	INIC	IALIZACIÓN DE NETWORKVISION	

	5.2.5.	.3 WORKSPACE	183
	5.2.5.	.4 TAB STARTUP	184
	5.2.5.	.5 TAB DISPLAY	184
	5.2.5.	.6 TAB AUDIO	186
	5.2.5.	.7 BARRA DE HERRAMIENTAS NETWORKVISION	186
	5.2.5.	.8 CREACIÓN DE UN MAPA	187
	5.2.5.	.9 CREACIÓN DE DISPOSITIVOS	188
	5.2.5.	.10 AÑADIR VPNS A UN MAPA	189
	5.2.5.	.11 MAP VIEW	190
	5.2	2.5.11.1 ÍCONOS DE LOS DISPOSITIVOS	191
	5.2	2.5.11.2 ÍCONOS Y SÍMBOLOS	192
	5.2	2.5.11.3 NIVELES DE GRAVEDAD	193
	5.2	2.5.11.4 ESTADOS VNE	194
	5.2.5.	12 LIST VIEW	195
	5.2.5.	13 LINK VIEW	195
	5.2.5.	.14 OVERLAYS	196
	5.2.5.	.15 LAYOUT MAP	197
	5.2.5.	.16 TICKET PANE	198
	5.2.5.	.17 VENTANA INVENTORY	199
	5.2.5.	18 BUSSINES TAG	200
		5.2.3.5.9.2 CREACIÓN DE UN BUSSINESS TAG	200
	5.2.5.	.19 REPORTS OVERVIEW	201
	5.2	2.5.19.1 TIPOS DE REPORTES	201
	5.2	2.5.19.2 GENERACIÓN DE INFORMES	201
	5.2	2.5.19.3 CREACIÒN DE UN REPORTE	203
5.3	MAN	IUAL WHATSUP	208
5.	.3.1	OBJETIVO	208
5.	.3.2	INTRODUCCIÓN	208
5.	.3.3	INGRESO A LA PLATAFORMA	208
5.	.3.4	CREACIÓN DE UN MAPA	210
	5.3.4.	.1 GENERAL	211
	5.3.4.	.2 DISPLAY	212
	5.3.4.	.3 NETWORK	213
5.	.3.5	TAB MAP	213
5.	.3.6	TAB EDIT	214
5.	.3.7	TAB DEPENDENCIES	219
5.	.3.8	TAB STATISTICS	220
5.	.3.9	TAB NOTIFICATIONS	221
5.	.3.10	TAB MINI STATUS	223
5.	3.11	TAB STATUS	224

5	.3.12	Μ	IONITOREO DEL ESTADO DE LOS EQUIPOS	225
	5.3.12	2.1	STATUS	225
	5.3.12	2.2	HISTORY	225
	5.3.12	2.3	UP-TIME	226
	5.3.12	2.4	LOG	227
5	.3.13	V	ERIFICACIÓN DE CONECTIVIDAD	230
	5.3.13	3.1	CONNECT	230
	5.3.13	3.2	PING	230
	5.3.13	3.3	TRACEROUTE:	231
	5.3.13	3.4	BROWSER	232
5.4	MAN	UAL	IPSOLUTIONC	234
5	5.4.1	OBJ	ETIVO	234
5	5.4.2	INTI	RODUCCIÓN	234
5	5.4.3	ING	RESO A LA PLATAFORMA	234
5	6.4.4	OPC	IÓN SERVICE INVENTORY	235
	5.4.4.	.1	CREACIÓN DE CUSTOMERS	236
	5.4.4.	.2	ELIMINAR UN CUSTOMER	238
	5.4.4.	.3	CREACION DE PROVIDERS	239
	5.4.4.	.4	RESOURCE POOLS	241
	5.4.4.	.5	CE ROUTING COMMUNITIES	243
	5.4.4.	.6	VRFS	246
	5.4.4.	.7	VLANS	250
	5.4.4.	.8	MPLS VPN	252
	5.4.4.	.9	CREACIÓN DE SERVICIO MPLS-VPN	260
	5.4.4.	.10	BORRAR VRF'S	263
5	5.4.5	OPC	IÓN SERVICE DESING	265
	5.4.5.	.1	OPCIÓN POLICIES	266
	5.4.5.	.2	OPCIÓN TEMPLATES	267
5	.4.6	OPC	IÓN MONITORING	267
5	6.4.7	OPC	IÓN DIAGNOSTICS	268
5	.4.8	OPC	IÓN ADMINISTRATION	269
5.5	MAN	UAL	NAGIOS	270
5	5.5.1	OBJ	ETIVO	270
5	5.5.2	INST	TALACIÓN DEL SERVIDOR NAGIOS	270
5	5.5.3	CRE	ACIÓN DE EQUIPOS PARA NAGIOS	271
5	5.5.4	CRE	ACIÓN DE SERVICIOS PARA NAGIOS	272
5	5.5.5	CRE	ACIÓN DE ALERTAS POR EMAIL DE NAGIOS	274
5	5.5.6	INST	TALACIÓN DE HERRAMIENTAS DE NAGIOS - NDOUTILS	275
5	5.5.7	CON	IFIGURACIÓN DE DISPOSITIVOS	276
5	5.5.8	CON	IFIGURACIÓN DE SERVICIOS	276

5.6	MAN	NUAL ACS (ACCESS CONTROL SERVER)	277
5	5.6.1	OBJETIVOS	277
5	5.6.2	INTRODUCCIÓN	277
5	5.6.3	INGRESO A LA PLATAFORMA	277
5	5.6.4	PANTALLA PRINCIPAL	278
5	5.6.5	TAB USER SETUP	279
	5.6.5	CONFIGURACIÓN DE USUARIOS EN UNA BASE DE DATOS EXTE	RNA
		279	
	5.6.5	ENCONTRAR UN USUARIO ESPECÍFICO EN LA BASE DE DATOS	280
	5.6.5	LISTADO DE NOMBRES QUE EMPIEZAN CON UN CARACTER	
	PAR	TICULAR	280
	5.6.5	CAMBIO DE UN NOMBRE DE USUARIO EN LA BASE DE DATOS	281
	5.6.5	5.5 CONFIGURACIÓN DE UN USUARIO	281
5	5.6.6	TAB GROUP SETUP	286
	5.6.6	5.1 CREACIÓN DE UN GRUPO DE USUARIO	286
	5.6.6	5.2 RENOMBRAR UN GRUPO	288
5	5.6.7	TAB SHARE PROFILE COMPONENTS	289
	5.6.7	2.1 CONJUNTO DE COMANDOS DE AUTORIZACIÓN	290
	5.6.7	AÑADIR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN	290
	5.6.7	2.3 EDITAR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN	291
	5.6.7	AÑADIR Y EDITAR UN CONJUNTO DE COMANDOS DE	
	AUT	ORIZACIÓN	291
	5.6.7	2.5 ELIMINAR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN	292
5	5.6.8	TAB NETWORK CONFIGURATION	292
	5.6.8	3.1 CONFIGURACIÓN DE DISPOSITIVOS	293
5	5.6.9	TAB SYSTEM CONFIGURATION	295
	5.6.9	0.1 SERVICE CONTROL	296
	5.	6.9.1.1 SERVICES LOG FILE CONFIGURATION	297
5	5.6.10	TAB INTERFACE CONFIGURATION	298
	5.6.1	0.1 CONFIGURACION DEL PROTOCOLO TACAS+ (CISCOIOS)	298
	5.6.1	0.2 CONFIGURACIÓN DEL PROTOCOLO RADIUS (ALCATEL)	299
5	5.6.11	TAB ADMINISTRATION CONTROL	300
	5.6.1	1.1 ADD ADMINISTRATOR	301
	5.6.1	1.2 ACCESS POLICY	302
	5.6.1	1.3 SESSION POLICY	304
5	5.6.12	TAB EXTERNAL USER DATABASE	305
5	5.6.13	TAB REPORT AND ACTIVITY	306
	5.6.1	3.1 TACACS+ ACCOUNTING	307
	5.6.1	3.2 TACAS+ ADMINISTRATION	307
	5.6.1	3.3 LOGGED IN USERS	308

5	.6.13.4	ADMINISTRATION AUDIT	
5	.6.13.5	ACS SERVICE MONITORING	
5.7 P	ROCESO	DS O&M/MPLS	
5.7.1	DIA	GRAMA GENERAL DE LOS PROCESOS Y USO DE LAS PLATA	FORMAS.
	311		
5.7.2	2 PÉR	DIDAS DE PAQUETES POR INTERMITENCIAS DE ENLACES	
5.7.3	B FAL	LO DE EQUIPOS DE ACCESO	
5.7.4	CON	NECTIVIDAD LIMITADA O NULA	
5.7.5	5 PRC	BLEMAS DE CONFIGURACIÓN EN PLATAFORMAS	
CAPÍTUI			
CONCLU	SIONES	S Y RECOMENDACIONES	
CONCLU 6.1 C	SIONES	S Y RECOMENDACIONES	336
CONCLU 6.1 C 6.2 R	SIONES ONCLU ECOME	S Y RECOMENDACIONES SIONES NDACIONES	
CONCLU 6.1 C 6.2 R REFERE	SIONES ONCLU ECOME NCIAS I	S Y RECOMENDACIONES SIONES NDACIONES BIBLIOGRÁFICAS	
CONCLU 6.1 C 6.2 R REFERE BIBLIOG	SIONES ONCLU ECOME NCIAS I RAFÍA	S Y RECOMENDACIONES SIONES NDACIONES BIBLIOGRÁFICAS CAPITULO UNO	
CONCLU 6.1 C 6.2 R REFERE BIBLIOG BIBLIOG	ONCLU ECOME NCIAS I RAFÍA	S Y RECOMENDACIONES SIONES NDACIONES BIBLIOGRÁFICAS CAPITULO UNO CAPITULO DOS	
CONCLU 6.1 C 6.2 R REFERE BIBLIOG BIBLIOG BIBLIOG	SIONES ONCLU ECOME NCIAS I RAFÍA RAFÍA	S Y RECOMENDACIONES SIONES NDACIONES BIBLIOGRÁFICAS CAPITULO UNO CAPITULO DOS CAPÍTULO TRES	

ÍNDICE DE FIGURAS

CAPITULO 1

FIGURA 1.1: ESTRUCTURA GENERAL DE CNT	2
FIGURA 1.2: ESTRUCTURA DEL ÁREA IP/MPLS ANTERIOR	3
FIGURA 1.3: NUEVA ESTRUCTURA DEL ÁREA O&M DE LA CNT	4

CAPITULO 2

FIGURA 2.1: DOMINIO MPLS, LER, LSR	18
FIGURA 2.2: FEC	19
FIGURA 2.3: LSP	19
FIGURA 2.4: UPSTREAM, DOWNSTREAM	21
FIGURA 2.5: ASIGNACIÓN DE ETIQUETAS DOWNSTREAM	21
FIGURA 2.6: DOWNSTREAM ON DEMAND	22
FIGURA 2.7: UNSOLICITED DOWNSTREAM	22
FIGURA 2.8: ASIGNACIÓN UPSTREAM	23
FIGURA 2.9: CABECERA MPL	23
FIGURA 2.10: PLANOS MPLS	26
FIGURA 2.9: CABECERA MPL	23
FIGURA 2.10: PLANOS MPLS	26
FIGURA 2.11: FUNCIONAMIENTO MPLS	27
FIGURA 2.12: CR-LSP	31
FIGURA 2.13: COMPONENTES DE UNA VPN	33
FIGURA 2.14: ARQUITECTURA MPLS VPN	35
FIGURA 2.15: ELEMENTOS DE GESTIÓN DE RED	38
FIGURA 2.16: ENTORNO DE GESTIÓN	41
FIGURA 2.17: ESTRUCTURA JERÁRQUICA DE LOS OBJETOS ADMINISTRADOS POR	10
SNMP	43

CAPITULO 3

FIGURA 3.1: MONITOREO DE UN EQUIPO	
FIGURA 3.2: DIAGRAMA DE RED NAGIOS	60

CAPITULO 4

FIGURA 4.1: ÁREAS ADMINISTRADAS POR ITIL67
FIGURA 4.2: SOPORTE DE SERVICIO70
FIGURA 4.3: GESTIÓN DE INCIDENCIAS72
FIGURA 4.4: GESTIÓN DE PROBLEMA74
FIGURA 4.5: GESTIÓN DE CAMBIOS75
FIGURA 4.6: GESTIÓN DE CONFIGURACIÓN76
FIGURA 4.7: GESTIÓN DE VERSIONES79
FIGURA 4.8: PROVISIÓN DE SERVICIOS80
FIGURA 4.9: GESTIÓN DE NIVELES DE SERVICIO81
FIGURA 4.10: GESTIÓN FINANCIERA82
FIGURA 4.11: GESTIÓN DE CAPACIDAD83
FIGURA 4.12: GESTIÓN DE CONTINUIDAD DEL SERVICIO
FIGURA 4.13: EVALUACIÓN DE RIESGOS
FIGURA 4.14: GESTIÓN DE DISPONIBILIDAD86
FIGURA 4.15: GESTIÓN DE LA SEGURIDAD88

CAPITULO 5

FIGURA 5.1.1: INGRESO AL SISTEMA	90
FIGURA 5.1.2: PANTALLA INICIAL	90
FIGURA 5.1.3: DEVICES	91
FIGURA 5.1.4: AÑADIR UN NUEVO EQUIPO	92
FIGURA 5.1.5: MENÚ DEVICES	94
FIGURA 5.1.6: EDICIÓN DE UN EQUIPO	94

FIGURA 5.1.7: CREACIÓN DE GRÁFICOS	95
FIGURA 5.1.8: OPCIÓN GRAPH TYPE	96
FIGURA 5.1.9: FILTRO PARA BÚSQUEDA DE INTERFACES DE UN EQUIPO	96
FIGURA 5.1.10: SELECCIÓN DE INTERFACES	97
FIGURA 5.1.11: MENSAJE DE ÉXITO DE LA CREACIÓN DEL GRÁFICO	97
FIGURA 5.1.12: OPCIÓN GRAPH MANAGEMENT	98
FIGURA 5.1.13: SELECCIÓN DEL EQUIPO EN LA INTERFAZ	98
FIGURA 5.1.14: SELECCIÓN DEL GRÁFICO CREADO	99
FIGURA 5.1.15: EDICIÓN DE UNA INTERFAZ	99
FIGURA 5.1.16: UBICACIÓN DE UN GRÁFICO DENTRO DE UN ÁRBOL	100
FIGURA 5.1.17: ELECCIÓN DE LA UBICACIÓN DEL GRÁFICO	100
FIGURA 5.1.18: ADICIÓN DE UN NUEVO DIRECTORIO	101
FIGURA 5.1.19: PARÁMETROS DE CONFIGURACIÓN DEL EQUIPO	101
FIGURA 5.1.20: CREACIÓN DE SUBDIRECTORIOS	102
FIGURA 5.1.21: PARÁMETROS DE CONFIGURACIÓN DE UN SUBDIRECTORIO	102
FIGURA 5.1.22: INSERCIÓN DE GRÁFICAS EN UN SUBDIRECTORIO	102
FIGURA 5.1.23: SELECCIÓN DEL GRÁFICO EN LA OPCIÓN GRAPH	103
FIGURA 5.1.24: ACTUALIZACIÓN DE GRÁFICOS	103
FIGURA 5.1.25: VISUALIZACIÓN DE GRÁFICOS EN DIRECTORIOS Y SUBDIRECTORI	OS104
FIGURA 5.1.26: TRAFICO DEL CRECIMIENTO DEL ÚLTIMO AÑO DE LAS SALIDAS	
INTERNACIONALES DE CNT E.P	104
FIGURA 5.1.27: CONSUMO SEMANAL DE INTERNET	104
FIGURA 5.1.28: MONITOREO DE EQUIPOS	106
FIGURA 5.1.29: ESTADO DE LOS HOST	106
FIGURA 5.1.30: VISUALIZACIÓN DE PARÁMETROS DEL EQUIPO	107
FIGURA 5.1.31: OPCIÓN MAPA	108
FIGURA 5.1.32: OPCIÓN SATÉLITE	108
FIGURA 5.1.33: OPCIÓN RELIEVE	109
FIGURA 5.1.34: VISUALIZACIÓN DE LA INFORMACIÓN BÁSICA DE UN EQUIPO	109
FIGURA 5.1.35: OPCIÓN EDITOR	110

FIGURA 5.1.36: SELECCIÓN DEL MAPA A MODIFICAR	110
FIGURA 5.1.37: ADMINISTRACIÓN DE MAPAS	111
FIGURA 5.1.38: OPCIÓN PICK FROM	112
FIGURA 5.1.39: OPCIÓN ADD LINK	112
FIGURA 5.1.40: OPCIÓN MAP PROPERTIES	113
FIGURA 5.1.41: OPCIÓN MAP STYLE	113
FIGURA 5.1.42: OPCIONES DEL WEATHERMAP	114
FIGURA 5.1.43: EJEMPLO DE UN MAPA CREADO	114
FIGURA 5.1.44: MONITOREO DEL ESTADO DE LA PLATAFORMA NAGIOS	115
FIGURA 5.1.45: OPCIONES HOSTS DE NAGIOS	116
FIGURA 5.1.46: VISUALIZACIÓN DEL ESTADO DEL HOST	116
FIGURA 5.1.47: VISUALIZACIÓN DE PROBLEMAS QUE PRESENTA UN HOST	117
FIGURA 5.1.48: VISUALIZACIÓN DE LOS ESTADOS DE UN EQUIPO	117
FIGURA 5.1.49: VISUALIZACIÓN DEL PORCENTAJE DE PAQUETES PERDIDOS Y EL	
TIEMPO DE RESPUESTA	118
FIGURA 5.1.50: SERVICIOS ACTIVOS EN NAGIOS	119
FIGURA 5.1.51: VISUALIZACIÓN DE PROBLEMAS EN EL SERVICIO	119
FIGURA 5.1.52: VISUALIZACIÓN DE LA INFORMACIÓN DEL EQUIPO	120
FIGURA 5.1.53: VISUALIZACIÓN DE LOS LOGS DEL EQUIPO	120
FIGURA 5.1.54: INGRESO A LA PLATAFORMA NAGIOS	121
FIGURA 5.1.55: VISUALIZACIÓN DEL TRÁFICO QUE PASA POR LAS INTERFACES	
CONFIGURADAS EN LOS EQUIPOS	122
FIGURA 5.1.56: VISUALIZACIÓN DE GRÁFICOS DE LAS INTERFACES	122
FIGURA 5.1.57: VISUALIZACIÓN DE LA DISPONIBILIDAD DE LOS EQUIPOS	123
FIGURA 5.1.58: VISUALIZACIÓN DEL REGISTRO DE INCIDENCIAS	123
FIGURA 5.1.59: INGRESO A LA OPCIÓN MANAGE REPORT	124
FIGURA 5.1.60: SELECCIÓN DE LA OPCIÓN ADD	124
FIGURA 5.1.61: GUARDAR CONFIGURACIÓN MEDIANTE LA OPCIÓN SAVE	125
FIGURA 5.1.62: VISUALIZACIÓN DEL REPORTE CREADO	126

FIGURA 5.1.63: SELECCIÓN DEL NOMBRE DEL REPORTE	126
FIGURA 5.1.64: SELECCIÓN DE GRÁFICOS A INCLUIR EN EL REPORTE	126
FIGURA 5.1.65: OPCIÓN CEREOUS	127
FIGURA 5.1.66: PARÁMETROS DEL TIEMPO DE MONITOREO	127
FIGURA 5.1.67: DESCARGA DEL REPORTE	127
FIGURA 5.1.68: VISUALIZACIÓN DEL REPORTE	128
FIGURA 5.1.69: SELECCIÓN DE LA OPCIÓN NECTAR	128
FIGURA 5.1.70: CREACIÓN DE REPORTES	129
FIGURA 5.1.71: INSERCIÓN DE UN NUEVO ITEM	131
FIGURA 5.1.72: GUARDAR PARÁMETRO DE CONFIGURACIÓN	132
FIGURA 5.1.73: VISUALIZACIÓN PREVIA DEL REPORTE	132
FIGURA 5.1.74: REGISTRO DE REPORTES ENVIADOS	133
FIGURA 5.2.1: INICIO DE ANA MANAGE	136
FIGURA 5.2.2: VENTANA PRINCIPAL	137
FIGURA 5.2.3: BARRA DE HERRAMIENTAS	138
FIGURA 5.2.4: NUEVO UNIT	140
FIGURA 5.2.5: NUEVO ANA UNIT	141
FIGURA 5.2.6: PROPIEDADES DE ANA UNIT	142
FIGURA 5.2.7: NUEVO AVM	143
FIGURA 5.2.8: FUNCIONES EN LOS AVMS	144
FIGURA 5.2.9: PROPIEDADES AVMS	145
FIGURA 5.2.10: NUEVA VNE	146
FIGURA 5.2.11: TAB GENERAL	147
FIGURA 5.2.12: TAB SNMP	148
FIGURA 5.2.13: TAB TELNET/SSH	149
FIGURA 5.2.14: TAB ICMP	149
FIGURA 5.2.15: TAB POLLING	150
FIGURA 5.2.16: TABEVENT	151
FIGURA 5.2.17: FUNCIONES EN LOS VNES	152

FIGURA 5.2.18: FIND	
FIGURA 5.2.19: GLOBAL SETTINGS	
FIGURA 5.2.20: DATABASE SEGMENTS	
FIGURA 5.2.21: EVENTS MANAGEMENT SETTINGS	
FIGURA 5.2.22: MESSAGE OF THE DAY	
FIGURA 5.2.23: POLLING GROUP	
FIGURA 5.2.24: NEW POLLING GROUP	
FIGURA 5.2.25: PROTECTION GROUP	
FIGURA 5.2.26: REPORT SETTINGS	
FIGURA 5.2.27: AUTHENTICATION METHOD	
FIGURA 5.2.28: PASSWORD SETTINGS	
FIGURA 5.2.29: USER ACCOUNT SETTINGS	
FIGURA 5.2.30: SCOPES Y USERS	
FIGURA 5.2.31: NUEVO SCOPE	
FIGURA 5.2.32: NUEVO USUARIO	
FIGURA 5.2.33: TAB GENERAL	
FIGURA 5.2.34: TAB SECURITY	
FIGURA 5.2.35: TOPOLOGY	
FIGURA 5.2.36: NUEVO LINK	
FIGURA 5.2.37: INICIO EVENTVISION	
FIGURA 5.2.38: VENTANA PRINCIPAL EVENTVISION	
FIGURA 5.2.39: DETALLES EVENTVISION	
FIGURA 5.2.40: SPLIT SCREEN	
FIGURA 5.2.41: TAB ALL	
FIGURA 5.2.42: TAB AUDIT	
FIGURA 5.2.43: TAB PROVISIONING	
FIGURA 5.2.44: TAB SECURITY	
FIGURA 5.2.45: TAB SERVICE	
FIGURA 5.2.46: LOCATION	
FIGURA 5.2.47: INFORMACIÓN DE ALARMA ID	

FIGURA 5.2.48: INFORMACIÓN DE TICKET ID	178
FIGURA 5.2.49: PHISICAL INVENTORY	
FIGURA 5.2.50: TAB SYSLOG	
FIGURA 5.2.51: TAB SYSTEM	179
FIGURA 5.1.70: CREACIÓN DE REPORTES	
FIGURA 5.2.52: TAB TICKET	
FIGURA 5.2.53: TABS TRAPS	
FIGURA 5.2.54: INICIO NETWORKVISION	
FIGURA 5.2.55: PANTALLA PRINCIPAL DE NETWORKVISION	
FIGURA 5.2.56: PANTALLA DE OPCIONES	
FIGURA 5.2.57: DISPLAY	
FIGURA 5.2.58: AUDIO	
FIGURA 5.2.59: BARRA DE HERRAMIENTAS	
FIGURA 5.2.60: NUEVO MAPA	
FIGURA 5.2.61: LINK FILTER	
FIGURA 5.2.62: OPCIÓN ADDMAP	
FIGURA 5.2.63: SELECCIÓN DE DISPOSITIVOS	
FIGURA 5.2.64: ADICIÓN DE UNA VPN	
FIGURA 5.2.65: MAP VIEW	
FIGURA 5.2.66: ICONO DE DISPOSITIVO	
FIGURA 5.2.67: LIST VIEW	
FIGURA 5.2.68: LINK VIEW	
FIGURA 5.2.69: OVERLAY	
FIGURA 5.2.70: SELECCIÓN DE VLAN O VPN	
FIGURA 5.2.71: LAYOUTMAP	
FIGURA 5.2.72: TIPOS DE MAPAS	
FIGURA 5.2.73: TICKET PROPERTIES	
FIGURA 5.2.74: INVENTORY	
FIGURA 5.2.75: BUSSINESS TAG	201
FIGURA 5.2.76: REPORTES	

FIGURA 5.2.77: REPORTES EN ORDEN JERÁRQUICO	202
FIGURA 5.2.78: TIPO DE REPORTES	203
FIGURA 5.2.79: RUN REPORT	204
FIGURA 5.2.80: CNT MPLS NETWORK	205
FIGURA 5.2.81: CNT INTERNET TOPOLOGY	205
FIGURA 5.2.82: MPLS FASE I	206
FIGURA 5.2.83: CORE MPLS	206
FIGURA 5.2.84: VNES	207
FIGURA 5.3.1: RED ANDINATEL	209
FIGURA 5.3.2: EQUIPOS MPLS 6500	209
FIGURA 5.3.3: RED IP	209
FIGURA 5.3.4: EQUIPOS MPLS 7600	210
FIGURA 5.3.5: EQUIPOS BRAS-BORDERS	210
FIGURA 5.3.6: PROPIEDADES DE SONDEO DE LOS MAPAS	211
FIGURA 5.3.7: OPCIÓN GENERAL	212
FIGURA 5.3.8: OPCIÓN DISPLAY	212
FIGURA 5.3.9: OPCIÓN NETWORK	213
FIGURA 5.3.10: TAB MAP	214
FIGURA 5.3.11: TAB EDIT	214
FIGURA 5.3.12: PROPIEDADES DEL OBJETO	215
FIGURA 5.3.13: HABILITACIÓN DE LA OPCIÓN SNMP	215
FIGURA 5.3.14: OPCIÓN MONITOR	216
FIGURA 5.3.15: OPCIÓN SERVICES	217
FIGURA 5.3.16: OPCIÓN EVENTS	217
FIGURA 5.3.17: OPCIÓN ALERTS	218
FIGURA 5.3.18: OPCIÓN ENABLE ALERTS	218
FIGURA 5.3.19: OPCIÓN NOTES	219
FIGURA 5.3.20: OPCIÓN NOTES	219
FIGURA 5.3.21: TAB DEPENDENCIES	220
FIGURA 5.3.22: TAB STATISTICS	221

FIGURA 5.3.23: TAB NOTIFICATIONS	
FIGURA 5.3.24: NOTIFICATIONS LIBRARY	
FIGURA 5.3.25: SELECCIÓN DE LA OPCIÓN MINI STATUS	
FIGURA 5.3.26: MINI STATUS	
FIGURA 5.3.27: TAB STATUS	
FIGURA 5.3.28: STATUS	
FIGURA 5.3.29: HISTORY	
FIGURA 5.3.30: EQUIPO SIN RESPUESTA	
FIGURA 5.3.31: ESTADO UP DEL EQUIPO	
FIGURA 5.3.32: LOGS DEL EQUIPO	
FIGURA 5.3.33: ACTIVITY LOG	
FIGURA 5.3.34: CONNECT	
FIGURA 5.3.35: PING A UN EQUIPO	
FIGURA 5.3.36: TRACEROUTE	
FIGURA 5.3.37: BROWSE	
FIGURA 5.3.38: SERVICES	
FIGURA 5.4.1: INGRESO A LA PLATAFORMA	
FIGURA 5.4.2: OPCIÓN SERVICE INVENTORY	
FIGURA 5.4.3: OPCIÓN CUSTOMERS	
FIGURA 5.4.4: CREACIÓN DE UN NUEVO CUSTOMER	
FIGURA 5.4.5: COLOCACIÓN DEL NOMBRE Y DESCRIPCIÓN DEL CLIENTE	
FIGURA 5.4.6: VERIFICACIÓN DE LA CREACIÓN DEL CUSTOMER	
FIGURA 5.4.7: OPCIÓN DELETE CUSTOMER	
FIGURA 5.4.8: OPCIÓN PROVIDERS	
FIGURA 5.4.9: COLOCACIÓN DE LOS PARÁMETROS PARA LA CREACIÓN DEL PROVIDER2	40
FIGURA 5.4.10: OPCIÓN CREATE PROVIDER	
FIGURA 5.4.11: VERIFICACIÓN DE LA CREACIÓN DEL PROVIDER	
FIGURA 5.4.12: OPCIÓN RESOURCE POOLS	
FIGURA 5.4.13: OPCIÓN ROUTE TARGET	
FIGURA 5.4.14: VERIFICACIÓN DE CONFIGURACIONES	

FIGURA 5.4.15: OPCIÓN CE ROUTING COMMUNITIES	243
FIGURA 5.4.16: CREACIÓN DE UNA NUEVA COMMUNITY	244
FIGURA 5.4.17: SELECCIÓN DEL ISP	244
FIGURA 5.4.18: CONFIGURACIONES DE UNA COMUNIDAD RESPECTIVA	245
FIGURA 5.4.19: VERIFICACIÓN DE LA CREACIÓN DE LA COMUNIDAD	245
FIGURA 5.4.20: OPCIÓN VRF'S	246
FIGURA 5.4.21: CREACIÓN DE UNA NUEVA VRF	246
FIGURA 5.4.22: SELECCIÓN DE UN PROVEEDOR	247
FIGURA 5.4.23: PARÁMETROS DE CONFIGURACIÓN DE UNA VRF	247
FIGURA 5.4.24: PARÁMETROS OPCIONALES PARA LA CONFIGURACIÓN DE UNA VR	RF 248
FIGURA 5.4.25: GUARDAR LAS CONFIGURACIONES DE LA VRF	249
FIGURA 5.4.26: VERIFICACIÓN DEL CLIENTE AÑADIDO SATISFACTORIAMENTE	249
FIGURA 5.4.27: OPCIÓN DEVICE CONSOLE	250
FIGURA 5.4.28: OPCIÓN NEXT	250
FIGURA 5.4.29: BÚSQUEDA POR DISPOSITIVO	251
FIGURA 5.4.30: BÚSQUEDA POR GRUPO	251
FIGURA 5.4.31: SELECCIÓN DE PARÁMETROS EN EL COMANDO DE OPERACIÓN	252
FIGURA 5.4.32: VERIFICACIÓN DE LA CREACIÓN DE LA VLAN	252
FIGURA 5.4.33: OPCIÓN INVENTORY AND CONNECTION MANAGER	253
FIGURA 5.4.34: OPCIÓN SERVICE REQUESTS	253
FIGURA 5.4.35: SELECCIÓN DE LA OPCIÓN MPLS VPN	254
FIGURA 5.4.36: SELECCIÓN DE LA OPCIÓN POLICY	254
FIGURA 5.4.37: SELECCIÓN DEL CUSTOMER ANTERIORMENTE CREADO	255
FIGURA 5.4.38: ADICIÓN DE UN ENLACE	255
FIGURA 5.4.39: SELECCIÓN DEL EQUIPO DEL PROVEEDOR	255
FIGURA 5.4.40: OPCIÓN PE DEVICE	256
FIGURA 5.4.41: SELECCIÓN DE LA INTERFACE VLAN	256
FIGURA 5.4.42: ADICIÓN DE UNA VLAN CREADA	257
FIGURA 5.4.43: OPCIÓN INTERFACE DESCRIPTION	257
FIGURA 5.4.44: COLOCACIÓN DE LA IP WAN Y MÁSCARA A UN EQUIPO	258

FIGURA 5.4.45: COLOCACIÓN DE LA IP LAN Y MÁSCARA A UN EQUIPO	258
FIGURA 5.4.46: OPCIÓN USE_NEXT_HOP_IPADDR	259
FIGURA 5.4.47: COLOCACIÓN DE LA DIRECCIÓN IP WAN	259
FIGURA 5.4.48: OPCIÓN NEXT	259
FIGURA 5.4.49: OPCIÓN FINISH	260
FIGURA 5.4.50: ADVERTENCIA PARA GUARDAR CAMBIOS	260
FIGURA 5.4.51: ADICIÓN DE LA VRF A LA INTERFACE	261
FIGURA 5.4.52: OPCIÓN DEPLOY	261
FIGURA 5.4.53: GUARDAR CAMBIOS EFECTUADOS	262
FIGURA 5.4.54: REVISIÓN DE LOS CAMBIOS EFECTUADOS	262
FIGURA 5.4.55: VERIFICACIÓN DEL ESTADO DE LA INTERFACE	263
FIGURA 5.4.56: OPCIÓN DECOMMISSION	263
FIGURA 5.4.57: VALIDACIÓN DE CAMBIOS EFECTUADOS	264
FIGURA 5.4.58: OPCIÓN DEPLOY PARA ELIMINAR CONFIGURACIONES	264
FIGURA 5.4.59: GUARDAR NUEVOS CAMBIOS EFECTUADOS	265
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE	265
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING	265 266
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES	265 266 266
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA	265 266 266 267
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA FIGURA 5.4.64: OPCIÓN TEMPLATES	265 266 266 267 267
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA FIGURA 5.4.64: OPCIÓN TEMPLATES FIGURA 5.4.65: OPCIÓN MONITORING	265 266 266 267 267 268
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES. FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA. FIGURA 5.4.64: OPCIÓN TEMPLATES FIGURA 5.4.65: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN DIAGNOSTICS.	265 266 267 267 267 268
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA FIGURA 5.4.64: OPCIÓN TEMPLATES FIGURA 5.4.65: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN MONITORING FIGURA 5.4.67: OPCIÓN ADMINISTRATION	265 266 267 267 267 268 268 269
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA FIGURA 5.4.64: OPCIÓN TEMPLATES FIGURA 5.4.65: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN DIAGNOSTICS FIGURA 5.4.67: OPCIÓN ADMINISTRATION FIGURA 5.5.1: CREACIÓN DE EQUIPOS	265 266 267 267 267 268 268 269 272
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA FIGURA 5.4.64: OPCIÓN TEMPLATES FIGURA 5.4.65: OPCIÓN MONITORING FIGURA 5.4.65: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN DIAGNOSTICS FIGURA 5.4.67: OPCIÓN ADMINISTRATION FIGURA 5.5.1: CREACIÓN DE EQUIPOS FIGURA 5.5.2: CREACIÓN DE SERVICIOS	265 266 267 267 267 268 268 269 272 273
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA FIGURA 5.4.64: OPCIÓN TEMPLATES FIGURA 5.4.65: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN MITORING FIGURA 5.4.66: OPCIÓN DIAGNOSTICS FIGURA 5.4.67: OPCIÓN ADMINISTRATION FIGURA 5.5.1: CREACIÓN DE EQUIPOS FIGURA 5.5.2: CREACIÓN DE SERVICIOS FIGURA 5.5.3: CONFIGURACIÓN DE DISPOSITIVOS	265 266 267 267 267 268 268 269 272 273 273 276
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA FIGURA 5.4.64: OPCIÓN TEMPLATES FIGURA 5.4.65: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN DIAGNOSTICS FIGURA 5.4.67: OPCIÓN ADMINISTRATION FIGURA 5.5.1: CREACIÓN DE EQUIPOS FIGURA 5.5.2: CREACIÓN DE SERVICIOS FIGURA 5.5.4: CONFIGURACIÓN DE SERVICIOS	265 266 267 267 267 268 268 269 272 273 273 276 276
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA FIGURA 5.4.64: OPCIÓN TEMPLATES FIGURA 5.4.65: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN DIAGNOSTICS FIGURA 5.4.67: OPCIÓN ADMINISTRATION FIGURA 5.5.1: CREACIÓN DE EQUIPOS FIGURA 5.5.2: CREACIÓN DE SERVICIOS FIGURA 5.5.3: CONFIGURACIÓN DE DISPOSITIVOS FIGURA 5.5.4: CONFIGURACIÓN DE SERVICIOS FIGURA 5.6.1: PANTALLA DE INGRESO A LA PLATAFORMA	265 266 267 267 267 268 268 269 272 273 276 276 278
FIGURA 5.4.60: VERIFICACIÓN DE LA INACTIVIDAD DE LA VRF Y LA INTERFACE FIGURA 5.4.61: OPCIÓN SERVICE DESING FIGURA 5.4.62: OPCIÓN POLICIES FIGURA 5.4.63: SELECCIÓN DEL NOMBRE DE LA POLÍTICA FIGURA 5.4.64: OPCIÓN TEMPLATES FIGURA 5.4.65: OPCIÓN MONITORING FIGURA 5.4.66: OPCIÓN DIAGNOSTICS FIGURA 5.4.67: OPCIÓN ADMINISTRATION FIGURA 5.4.67: OPCIÓN ADMINISTRATION FIGURA 5.5.1: CREACIÓN DE EQUIPOS FIGURA 5.5.2: CREACIÓN DE SERVICIOS FIGURA 5.5.4: CONFIGURACIÓN DE DISPOSITIVOS FIGURA 5.5.4: CONFIGURACIÓN DE SERVICIOS FIGURA 5.6.1: PANTALLA DE INGRESO A LA PLATAFORMA FIGURA 5.6.2: PANTALLA PRINCIPAL	265 266 267 267 267 267 268 268 269 272 273 276 276 278 278

XXVII

FIGURA 5.6.4: UBICACIÓN DE USUARIOS EN LA BASE DE DATOS	280
FIGURA 5.6.5: LISTADO DE LOS NOMBRES DE USUARIO QUE EMPIEZAN CON UN CARÁCTER EN PARTICULAR	N 281
FIGURA 5.6.6: CONFIGURACIÓN DE UN USUARIO	
FIGURA 5.6.7: ELIMINACIÓN DE UN USUARIO	
FIGURA 5 6 8: OPCIÓN ADVANCED SETTINGS	285
FIGURA 5 6 9: CREACIÓN DE UN GRUPO DE USUARIO	287
FIGURA 5.6.10: OPCIÓN USER IN GROUP	207
FIGURA 5.6.11: OPCIÓN EDIT SETTINGS	288
FIGURA 5.6.12: RENOMBRAR UN GRUPO	200
FIGURA 5.6.12: NENOMBRAR ON OROLO MAND AUTHORIZATION	200
EICLIDA 5.6.14: COLIDOS CONEICLIDADOS DREVIAMENTE	200
FIGURA 5.0.14. UNUFOS CONFIGURADOS FREVIAMENTE E AUTORIZACIÓN	290
FIGURA 5.0.15: EDICIÓN DE UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN	291
FIGURA 5.0.16: CONFIGURACIÓN DE DISPOSITIVOS	293
FIGURA 5.6.17: OPCION SUBMIT	294
FIGURA 5.6.18: OPCION ADD ENTRY	294
FIGURA 5.6.19: CONFIGURACION DE LOS PARAMETROS DEL EQUIPO	295
FIGURA 5.6.20: TAB SYSTEM CONFIGURATION	296
FIGURA 5.6.21: OPCIÓN SERVICE CONTROL	297
FIGURA 5.6.22: TAB INTERFACE CONFIGURATION	298
FIGURA 5.6.23: CONFIGURACIÓN DEL PROTOCOLO TACAS+ (CISCO IOS)	299
FIGURA 5.6.24: CONFIGURACIÓN DEL PROTOCOLO RADIUS (ALCATEL)	300
FIGURA 5.6.25: OPCIÓN ADMINISTRATION CONTROL	301
FIGURA 5.6.26: OPCIONES ADMINISTRATION CONTROL	302
FIGURA 5.6.27: OPCIÓN ACCESS POLICY	303
FIGURA 5.6.28: OPCIÓN SESSION POLICY	304
FIGURA 5.6.29: OPCIÓN EXTERNAL USER DATABASE	305
FIGURA 5.6.30: OPCIÓN REPORT AND ACTIVITY	306
FIGURA 5.6.31: OPCIÓN TACACS+ ACCOUNTING	307
FIGURA 5.6.32: OPCIÓN TACAS+ ADMINISTRATION	308

FIGURA 5.6.33: OPCIÓN LOGGED IN USERS	
FIGURA 5.6.34: OPCIÓN ADMINISTRATION AUDIT	
FIGURA 5.6.35: OPCIÓN ACS SERVICE MONITORING	
FIGURA 5.7.1: SHOW INTERFACE	
FIGURA 5.7.2: SPANNING TREE	
FIGURA 5.7.3: MAC ADDRESS	
FIGURA 5.7.4: EJEMPLO DE FLAPEO POR MAC	314
FIGURA 5.7.5: PING EXTENDIDO	
FIGURA 5.7.6: CONEXIÓN WAN MPLS	
FIGURA 5.7.7: CONEXIÓN WAN DEL CLIENTE	
FIGURA 5.7.8: RUTA- CLIENTE	316
FIGURA 5.7.9: CONEXIÓN LAN	
FIGURA 5.7.10: CONEXIÓN LAN – WAN	
FIGURA 5.7.11: PROCESAMIENTO DEL EQUIPO	317
FIGURA 5.7.12: PROCESAMIENTO DEL CPU	
FIGURA 5.7.13: PARÁMETROS DE VLAN	
FIGURA 5.7.14: VERIFICACIÓN DE LA INTERFAZ	
FIGURA 5.7.15: RECEPCIÓN DE MAC	
FIGURA 5.7.16: VERIFICACIÓN CON LA DIRECCIÓN MAC	
FIGURA 5.7.17: SPANNING TREE	
FIGURA 5.7.18: VERIFICACIÓN DE PUERTOS	
FIGURA 5.7.19: MTU DE LA INTERFACES	
FIGURA 5.7.20: COMPROBACIÓN DE LA VLAN	
FIGURA 5.7.21: COMPROBACIÓN DE LA VRF	
FIGURA 5.7.22: VERIFICACIÓN DE INTERFAZ	
FIGURA 5.7.23: PING A LA VRF	
FIGURA 5.7.24: ENRUTAMIENTO VRF	
FIGURA 5.7.25: PING AL SIGUIENTE SALTO	
FIGURA 5.7.26: VERIFICACIÓN DE POLÍTICAS	
FIGURA 5.7.27: ESTADO ACTUAL VRF	

FIGURA 5.7.28: VERIFICACIÓN DE LA LAN	327
FIGURA 5.7.29: RUTA VRF	327
FIGURA 5.7.30: ESTADO DE LA INTERFAZ	328
FIGURA 5.7.31: SPANNING TREE	328

ÍNDICE DE TABLAS

CAPITULO 1

TABLA 1.1: INCIDENCIAS	
TABLA 1.2: CONOCIMIENTO TÉCNICO DEL PERSONAL	

CAPITULO 3

TABLA 3.1: CARACTERÍSTICAS Y BENEFICIOS DE CISCO IP SOLUTION CENTER.......63

CAPITULO 5

TABLA 5.2: INDICADORES DE ESTADO	172
TABLA 5.2.2: ÍCONOS Y SÍMBOLOS	193
TABLA 5.2.3: NIVELES DE GRAVEDAD	194
TABLA 5.2.4: ESTADOS DE UNA VNE	195
TABLA 5.4.1: ESTADOS DE UNA VNE TIPO DE SERVICIO	242

ACRÓNIMOS

AAA: Autenticación, Autorización y Administración

ATM: Asynchronous Transfer Mode

BGP: Border Gateway Protocol

CE: Customer Equipment

CMDB: Base de Datos para la Gestión de la Configuración

CMIP: Common Management Information protocol

CR-LDP: Constraint-Based Routing Ldp

CSV: Comma-Separated Values

DSL: Digital Subscriber Line

EAP: Extensible Authentication Protocol

FEC: Forwarding Equivalence Class

FIB: Forwarding Information Base

FR: Frame Relay

FTP: File Transferer Protocol

GPL: General Public License

HTTP: HyperText Transfer Protocol

ICMP: Internet Control Message Protocol

IETF: Internet Engineering Task Force

IP: Internet Protocol

IPX: Internetwork Packet Exchange

IS-IS: Intermediate System to Intermediate System

ISP: Internet Service Provider

ITIL: Information Technology Infraestructure Library

LAN: Local Area Network

LER: Label Edge Router

LFIB: Label Forwarding Information Base

LIB: Label Information Base

LSP: Label Switched Path

LSR: Label Switching Router

MIB: Management Information Base

MPLS: Multi -Protocol Label Switchin

MRTG: Multi Router Traphic Grapher

MySQL: My Structured Query Language

NM: Managed Nodes

NMS: Network Management Station

NOC: Network Operation Center

OSPF: Open Shortest Path First

PDU: Packet Data Unit

PE: Provider Equipment

PING: Packet INternet Groper

POP3: Post Office Protocol 3

RFC: Request For Comments

RRD: Round Robin Database

RSVP: Resource Reservation Protocol

RSVP-TE RSVP: Resource Reservation Protocol Traffic Engineering

SMS: Short Message Service

SNMP: Simple Network Management Protocol

SSH: Secure Shell

SSL: Secure Sockets Layer

TCP: Transmission Control Protocol

VLAN: Virtual Local Area Networks

VPN: Virtual Private Networks

RESUMEN

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

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

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

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

CAPÍTULO 1

SITUACIÓN ACTUAL

1.1 ANTECEDENTES^[1]

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

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

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

El área Backbone ha traspasado una serie de funciones a las nuevas áreas creadas para el desarrollo, administración, gestión y monitoreo de la red.
1.2 ESTRUCTURA GENERAL DE LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES



Figura 1.1: Estructura General de CNT^[1]

1.3 ESTRUCTURA ANTERIOR DEL ÁREA IP/MPLS

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



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

1.4 NUEVA ESTRUCTURA DEL ÁREA O&M IP/MPLS

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



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

1.5 IDENTIFICACIÓN DE FUNCIONES DE LAS NUEVAS ÁREAS

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

1.5.1 ÁREA DE OPERACIÓN Y MANTENIMIENTO

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

- ✓ Problemas de intermitencias en enlaces de internet.
- ✓ Problemas de lentitud en enlaces de datos.
- ✓ Problemas de intermitencias entre la matriz y sucursales de clientes.
- Mantenimientos coordinados con los ingenieros de soporte para clientes corporativos.
 - ✓ Implementación y pruebas de redundancia.
 - ✓ Implementación de sesiones BGP^1 .
 - ✓ Cambios de instalaciones de los clientes luego del mantenimiento.
- Instalación de nuevos nodos.
- > Verificación de transmisión para ingreso de un nuevo cliente.
- ➢ Coordinación con personal de DSLAM² para instalación de equipos.
 - ✓ Asignación de puertos.
 - \checkmark Pruebas de conectividad.
- > Factibilidad de transmisión hacia nodos para instalación de clientes.
 - ✓ Verificación de transmisión disponible para ingreso de un nuevo cliente.
- Procedimiento para el aprovisionamiento de clientes corporativos.
- Documentación con los datos de los equipos que se interconectan con otros proveedores.

1.5.2 ÁREA DE INGENIERÍA

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

¹ Véase Acrónimos.

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

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

1.5.3 ÁREA DE GESTIÓN

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

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

1.5.4 ÁREA DEL NOC⁴

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

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

1.6 POLÍTICAS

1.6.1 ESCALAMIENTO INTERNO BACKBONE

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

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

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

Escalamiento al área O&M PLATAFORMA MPLS:

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

Para el escalamiento de problemas realizar el siguiente procedimiento:

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

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

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

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

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

1.6.2 TIEMPOS DE RESPUESTA

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

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

1.7 INDICADORES DE GESTIÓN

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

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

Tabla 1.1- Incidencias

> FALLO DE EQUIPOS DE ACCESO

✓ INDICADOR DE EFICIENCIA

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

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

✓ INDICADOR DE EFICACIA

Fallos solucionados/ Fallos atendidos=7/9=0.7

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

✓ INDICADOR DE EFECTIVIDAD

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

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

> CONECTIVIDAD LIMITADA O NULA

✓ INDICADOR DE EFICIENCIA

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

Se atendió el 100% de los fallos presentados.

✓ INDICADOR DE EFICACIA

Fallos solucionados/ fallos atendidos=25/30=0.83

Se tiene un 83% de respuesta.

✓ INDICADOR DE EFECTIVIDAD

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

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

> PROBLEMAS DE CONFIGURACIÓN EN PLATAFORMAS

✓ INDICADOR DE EFICIENCIA

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

Se atendió el 93% de los fallos.

✓ INDICADOR DE EFICACIA

Fallos solucionados/ fallos atendidos=12/14=0.86

Se tiene un 86% de respuesta.

✓ INDICADOR DE EFECTIVIDAD

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

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

> PÉRDIDAS DE PAQUETES POR INTERMITENCIAS DEL ENLACE

✓ INDICADOR DE EFICIENCIA

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

Se atendió el 95% de los fallos.

✓ INDICADOR DE EFICACIA

Fallos solucionados/ fallos atendidos=34/38=0.89

Se tiene un 89% de respuesta.

✓ INDICADOR DE EFECTIVIDAD

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

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

1.7.1 BENEFICIOS DE LOS INDICADORES DE GESTIÓN

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

1.7.1.1 SATISFACCIÓN DEL CLIENTE

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

1.7.1.2 MONITOREO DEL PROCESO

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

1.7.1.3 GERENCIA DEL CAMBIO

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

1.8 CONOCIMIENTO TÉCNICO DEL PERSONAL

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

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

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

Tabla 1.2- Conocimiento Técnico del Personal^[2]

Como se muestra en la tabla 1.1 una parte de las causas del insuficiente manejo de las plataformas de gestión y monitoreo dentro del área es por la falta de conocimiento por ello nació la necesidad de generar un manual de usuario que contenga la información de todos los procesos de administración de estas herramientas con el fin de facilitar su uso, aprovechar todos los recursos posibles y dar solución a problemas existentes en la red.

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

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

CAPÍTULO 2

ARQUITECTURA MPLS Y MODELOS DE SISTEMAS DE GESTIÓN

2.1 INTRODUCCIÓN

El crecimiento del internet ha producido la innovación de una serie de tecnologías y sofisticados servicios. MPLS (Multi-Prototocol Label Switching) es una nueva arquitectura de red de reciente aparición que permitirá soportar las futuras aplicaciones multimedia y proporcionan una eficaz alternativa al ATM⁵ para multiplexar diversos servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de routers con funciones especializadas en el transporte de paquetes en el núcleo de las redes.

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

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

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

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

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

MPLS es un protocolo de transporte de datos estándar creado por $IETF^6$ y definido en la RFC⁷. 3031, para soluciones de conmutación multinivel. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

2.2.1 ELEMENTOS DE MPLS^{[2], [4]}

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

2.2.1.1 DOMINIO MPLS

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

2.2.1.2 LER (LABEL EDGE ROUTER)

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

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

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

2.2.1.3 LSR (LABEL SWITCHING ROUTER)

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



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

2.2.1.4 FEC (FORWARDING EQUIVALENCE CLASS) ^[4]

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

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



Figura 2.2: FEC^[1]

2.2.1.5 LSP (LABEL SWITCHED PATH)^[5]

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



Figura 2.3: LSP^[6]

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

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

2.2.1.5.1 Enrutamiento hop by hop^[1]

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

2.2.1.5.2 Enrutamiento explícito (ER-LSP)^[1]

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

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

2.3 TUNELIZACIÓN EN MPLS^{[1], [2], [4]}

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

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

2.4 ETIQUETA ^{[1], [2]}

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

Las operaciones que se realizan con una etiqueta son:

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

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

2.4.1 Asignación y distribución de etiquetas

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



Figura 2.4: Upstream, Downstream

2.4.1.1 Asignación de etiquetas Downstream

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



Figura 2.5: Asignación de etiquetas Downstream.

2.4.1.1.1 Downstream on Demand

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



Figura 2.6: Downstream on Demand

2.4.1.1.2 Unsolicited Downstream

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



Figura 2.7: Unsolicited Downstream

2.4.1.2 Asignación de etiquetas Upstream

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



Figura 2.8: Asignación Upstream

2.4.2 FORMATO DE LA CABECERA MPLS^{[1], [2]}

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



Figura 2.9: Cabecera MPLS^[9]

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

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

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

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

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

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

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

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

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

La arquitectura MPLS está formada por dos planos:

2.5.1 Plano de Control

El componte de control es la que se encarga de crear y mantener la información de etiquetas asignadas entre un grupo de LSR interconectados, por esto cada nodo de MPLS utiliza los protocolos de encaminamiento como lo son: OSPF, IS-IS y BGP-4⁸, realizando un intercambio de información con los enrutadores para la construcción y mantenimiento de las tablas de encaminamiento.

2.5.1.1 Tabla de Enrutamiento^{[1], [2]}

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

En MPLS, la tabla de enrutamiento puede ser:

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

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

⁸ Véase Acrónimos

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

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

2.5.2 Plano de Datos

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



Figura 2.10: Planos MPLS^[8]

2.6 FUNCIONAMIENTO DE MPLS ^{[1], [2], [7], [8]}

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

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



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

Figura 2.11: Functionamiento MPLS^[2]

- Antes de enviar la información se debe determinar un LSP y establecer los parámetros de calidad de servicio para dicho camino. Los parámetros de QoS sirven para comprobar:
 - \checkmark La cantidad de recursos a reservar al LSP.
 - ✓ Las políticas de descarte de paquetes y prioridades en colas en cada LSR.

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

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

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

- 2. Un paquete ingresa al dominio MPLS a través de un router de acceso (LER), este router determina los parámetros de QoS, le asigna un FEC específico al paquete el cual determina un LSP, se etiqueta y se envía el paquete. Si no existe un LSP para este FEC, el LER junto con los otros routers definen un nuevo LSP.
- 3. El paquete enviado por el LER es recibido por un router de tránsito (LSR), en este momento el paquete se encuentra dentro del dominio MPLS.
- El LSR realiza las siguientes funciones:
 - ✓ Desecha la etiqueta del paquete entrante y añade una nueva etiqueta al paquete saliente.
 - ✓ Envía el paquete al próximo LSR dentro del LSP.
 - 4. El LER de salida desecha la etiqueta, lee la cabecera del paquete IP y envía el paquete a su destino final.

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

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

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

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

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

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

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

2.7.1 PROTOCOLO LDP (LABEL DISTRIBUTION PROTOCOL)

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

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

2.7.2 PROTOCOLO BGP (BORDER GATEWAY PROTOCOL)

BGP es un protocolo vector distancia, que asigna a cada ruta a un valor de prioridad y selecciona la ruta que tenga mayor valor. La forma de configurar y definir la información que contiene e intercambia el protocolo BGP es creando un Sistema Autónomo2. Cada sistema autónomo (AS)⁹ tendrá sesiones internas "iBGP" y además sesiones externas "eBGP".

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

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

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

2.7.3.1 CR-LSP

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

Se pueden utilizar los CR-LSPs para:

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

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



Figura 2.12: CR-LSP ^[10]

2.7.4 PROTOCOLO RSVP-TE (RSVP - TRAFFIC EXTENSION)

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

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

2.7.4.1 RSVP-TE

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

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

MPLS ofrece las siguientes aplicaciones:

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

✓ Redes privadas virtuales (VPN)

2.8.1 INGENIERÍA DE TRÁFICO

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

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

2.8.2 CALIDAD DE SERVICIO (QoS)^[8]

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

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

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

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

2.8.3 SOPORTE DE REDES VIRTUALES PRIVADAS^[7]

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

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



Figura 2.13: Componentes de una VPN^[7]

- Customer Edge (CE) Routers: Son los routers localizados en la frontera de la red del cliente que solicita el servicio.
- Provider Edge (PE) Routers: Son los routers localizados en el borde del proveedor, estos routers actúan como los LERs.

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

2.8.3.1 Funcionamiento de una VPN^[7]

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

2.8.3.2 Modelo de enrutamiento VPN en MPLS

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

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

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

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



Figura 2.14: Arquitectura MPLS VPN^[7]

2.8.3.3 Redes privadas virtuales MPLS

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

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

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

La implementación de las VPNs BGP / MPLS se usa para distribuir la información de enrutamiento de la VPN a través del *backbone* del proveedor y MPLS para enviar el tráfico de un lugar a otro de la VPN. Se pueden proveer diferentes servicios a determinados usuarios dentro de la red. Las VPNs BGP / MPLS son IP / VPNs basadas en dispositivos *Provider Edge*, para intercambiar información utiliza el modelo *Peer to Peer¹¹* y realizan el enrutamiento VPN mediante el protocolo BGP.

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

2.8.3.3.2 VPNs MPLS de Capa 2

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

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

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

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

2.9 VENTAJAS MPLS^{[1], [11]}

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

¹² **Drafts:** Son los proyectos en estudio, no estandarizados por la IETF.

¹³**Modelo Overlay:** El proveedor de servicio y el cliente no intercambian información de enrutamiento de capa 3, puede implementarse con varias arquitecturas como: X.25, Frame Relay, ATM, etc.

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

2.10 MODELOS DE SISTEMAS DE GESTIÓN

2.10.1 GESTIÓN DE REDES

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

2.10.2 ELEMENTOS DE GESTIÓN DE REDES ^[12]

A continuación se describen los elementos de gestión de redes:

- GESTORES: Estaciones Gestoras (NMS, Network Management Station), nodo en el que se ejecuta la aplicación gestora. Es la parte de la aplicación que emite las directivas de operaciones de gestión y recibe notificaciones y respuestas.
- AGENTES: Nodos gestionados (NM, Managed Nodes), elementos de red como host, router, gateway, etc. En estos reside el agente gestor encargado de llevar a cabo las funciones de gestión requerida por la "Estación Gestora", actúan como servidores suministrando información al gestor.

¹⁴ T.Saydam and T. Magedanz, "From Networks and Network Management into Service and Service Management", *Journal of Networks and Systems Management*, Vol 4, No. 4 (Dic 1996).
- MIB: es una base de datos completa y bien definida, con una estructura en árbol, adecuada para manejar diversos grupos de objetos (información sobre variables/valores que se pueden adoptar), con identificadores exclusivos para cada objeto.
- Protocolo de Gestión de Red: Define la comunicación entre los nodos gestionados y las estaciones gestoras. El protocolo depende del modelo de gestión usado.

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



Figura 2.15: Elementos de Gestión de red^[12]

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

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

- ORGANIZACIÓN: Describe los componentes de la administración de red (administrador, agente, etc.) y sus relaciones.
- INFORMACIÓN: Se encarga de la estructura y el almacenamiento de la información de administración de los objetos de la red. Esta información se guarda en una base de datos llamada MIB (Base de Información de Administración, Management Information Base). El estándar de la industria se centra en la SMI (Estructura de la información de administración, Structure of Management Information) para definir las sintaxis y semánticas de la información de administración que se almacena en la MIB.
- COMUNICACIÓN: Indica la forma en que se comunica los datos de administración entre el agente y el proceso administrador. Tiene en cuenta los protocolos de transporte y aplicación y los comandos y respuestas entre iguales.
- FUNCIONALIDAD: Direcciona las aplicaciones de administración de red que residen en el NMS (Sistema de administración de la red, Network Management System).

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

- GESTIÓN DE FALLO: Comprende las tareas de detección, diagnóstico, asilamiento, reparación e información de las averías en los recursos y fallos de servicios de la red.
- GESTIÓN DE CONFIGURACIÓN: Facilita la optimización en el uso de los recursos manteniendo un inventario de los mismos (hardware y software), y estableciendo los cambios necesarios en los mismos para adaptarlos a las necesidades de los servicios.

- GESTIÓN DE CONTABILIDAD: Permite distribuir el coste de los recursos entre los usuarios y facilita información a los mismos sobre las tarifas aplicadas.
- GESTIÓN DE RENDIMIENTO: Efectúa la evaluación del comportamiento y eficacia de los recursos en relación con la prestación de los servicios a los usuarios, mediante el registro y análisis de los datos correspondientes a los parámetros de la red (demanda de tráfico, número de usuarios, rutas utilizadas, etc.).
- GESTIÓN DE SEGURIDAD: Se refiere a la protección contra el acceso no autorizado o accidental a las funciones de control de la red, a la red misma y a la información que circula por ella.

2.10.4 MODELO DE GESTIÓN INTERNET^[15]

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

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

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

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

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

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



Figura 2.16: Entorno de Gestión^[15]

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

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

Proceso de envío de un mensaje SNMP:

TRANSMISIÓN

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

RECEPCIÓN

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

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

AGENTE SNMP	Orga C Int	SO (1) I nización (3) I DOD (6) I ernet (1)	Estructu jerárquio Cada ob de forma	urado camente njeto está identificado a única
Directorio (1)	Administración (2)	Experim	Experimental (3) Privado (4)	
DID para sistema	/IB-2 (1)			Empresa (1)
Sistema (1)	TCP (6)	Pro	oteon (1)	Sun (42)
Interfaz (2)	UDP (7)	I	BM (2)	Apple (63)
Traducción de dirección (3)	EGP (8)	C	isco (9)	EGP (311)
IP (4)	CMOT (9)	н	IP (11)	
ICMP (5)	Transmisión (10)	Inalár	nbrico (18)	Sin asignar(9118)
1	SNMP (11)			SWN
IAB (Comité de arquitectura de Internet, Internet Architecture Board)		Adı	ninistrado	por el fabricante
	Identificadore	s de objet	0.	

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

2.10.4.1 VERSIONES SNMP

A continuación se describen las diferentes versiones de SNMP:

Versión 1:

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

Versión 2:

El avance más importante de SNMPv1, fue la introducción del tipo de mensaje GetBulkRequest y la incorporación de los contadores de 64 bits para reducir la carga de tráfico adicional para la monitorización y solucionar los problemas de monitorización remota o distribuida (con las RMON), ha dado paso a una nueva versión v2. Las versiones de SNMP son compatibles, en el sentido que SNMPv2 puede leer SNMPv1. Versión 3:

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

2.10.5 MODELO DE GESTIÓN INTERNET TMN^{[14], [16]}

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

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

2.10.5.1 MODELO DE CAPAS TMN

El modelo de capas presenta la siguiente estructura:

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

2.10.5.1.1 ELEMENTOS DE RED

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

2.10.5.1.2 GESTIÓN DE ELEMENTOS DE RED

El nivel de gestión de elementos tiene como responsabilidad.

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

2.10.5.1.3 GESTIÓN DE RED

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

2.10.5.1.4 GESTIÓN DE SERVICIOS

Es responsabilidad de este nivel:

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

2.10.5.1.5 GESTIÓN EMPRESARIAL

Es responsabilidad de este nivel:

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

2.10.5.2 CONJUNTOS DE FUNCIONES DE GESTIÓN TMN

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

2.10.5.3 INTERFAZ Q3

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

CAPITULO 3

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

3.1 INTRODUCCIÓN^[1]

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

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

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

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

3.2.1 COMPATIBILIDAD QUE PRESENTA ANA

ANA es compatible con todas las implementaciones IP-NGN¹⁵, particularmente con lo siguiente:

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

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

3.2.2 CARACTERÍSTICAS DE ANA

ANA posee las siguientes características:

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

¹⁵ NGN (Next Generation Network): Redes de nueva generación o redes de siguiente generación.

¹⁶ Véase Acrónimos

¹⁷ Véase Acrónimos

3.2.3 NIVELES FUNCIONALES DE ANA

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

ANA mantiene las siguientes funcionalidades:

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

3.2.3.1 GESTIÓN DE ELEMENTOS

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

> INVENTARIO Y GESTIÓN DE TOPOLOGÍA

- El descubrimiento de la red, el modelado físico y lógico del dispositivo y la representación física de la topología.
- ✓ Los datos obtenidos pueden incluir alarmas de aviso cuando se produzca fallos en el servicio.

> GESTIÓN DE FALLOS

- ✓ Detección de fallas
- ✓ Análisis de la causa principal de la falla
- ✓ Servicio de notificación de eventos a través de SNMP Trap¹⁸

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

> ADMINISTRACIÓN DE CONFIGURACIÓN

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

> SEGURIDAD

- ✓ Gestión de usuarios nuevos
- ✓ Ámbitos y roles
- ✓ Autenticaciones locales y externas (LDAP¹⁹)

> PERSONALIZACIÓN

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

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

3.2.3.2 RED Y MONITORIZACIÓN DE SERVICIOS

Presenta las siguientes características:

> SERVICIOS Y TECNOLOGÍAS

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

> SERVICIO DE MAPAS

✓ Topología estructurada y mapas de servicios para una mejor configuración de dispositivos.

> TRAYECTORIA

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

3.2.3.3 SERVICIO DE ACTIVACIÓN

> ACTIVACIÓN

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

3.2.4 BENEFICIOS DE ANA

Ana presenta los siguientes beneficios:

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

3.3 WHATS UP ^[9]

3.3.1 WHATS UP

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

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

3.3.2 FUNCIONALIDADES DE WHATS UP

Se tiene las siguientes funcionalidades

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

Monitoreo de dispositivos y servicios: El uso de protocolos estándar (TCP / IP, SNMP, NetBIOS²⁰ e IPX) ²¹para localizar y controlar la red.

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

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

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

Escuchar los eventos: Whats Up puede informar cuando se producen acontecimientos específicos. Por ejemplo, cuando se recibe una captura de SNMP²².

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

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

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

3.3.3 DESCRIPCIÓN DE LAS FUNCIONES BÁSICAS

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

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

²² Véase Acrónimos

3.4.1 CACTI

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

3.4.2 RRDTOOL

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

3.4.3 PHP

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

3.4.4 BASE DE DATOS

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

3.4.5 VENTAJAS

> Gráficos

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

> Fuentes de datos

✓ Permite utilizar todas las funciones de *rrcreate* y *rrdupdate*, incluyendo la definición de varias fuentes de datos por archivo RRD²³.

Colección de datos

- ✓ Las fuentes datos pueden ser actualizadas vía SNMP o mediante la definición de scripts.
- ✓ Soporte SNMP incluido utilizando *php-snmp* o *net-snmp*.
- ✓ Un componente opcional, *cactid*, implementa las rutinas SNMP en lenguaje C con multithreading²⁴.
- ✓ Muy importante para grandes números de dispositivos.

> Plantillas

 Permite crear plantillas para reutilizar las definiciones de gráficos, fuentes de datos y dispositivos.

²³ Véase Acrónimos

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

Gestión de usuarios

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

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

Debido a que CACTI es un desarrollo libre (GPL²⁵), requiere de un trabajo dedicado para lograr una buena gráfica de monitoreo. Para esto, es necesario, crear plantillas de Gráficas, plantillas de Equipos y plantillas de Datos, las cuales son en formato XML²⁶.



Figura 3.1: Monitoreo de un equipo

²⁵ Véase Acrónimos

²⁶ Véase Acrónimos

3.5 NAGIOS ^{[2], [3]}

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

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

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

3.5.1 CARACTERÍSTICAS PRINCIPALES^{[2], [3], [4]}

Entre sus características principales figuran la monitorización de servicios de red mediante protocolos como: (SMTP, POP3, HTTP, PING, Syslog²⁷ y Agentes Externos).²⁸

- ✓ La monitorización de los recursos de sistemas hardware.
- ✓ Independencia de sistemas operativos.
- ✓ Posibilidad de monitorización remota mediante túneles SSL²⁹ cifrados o SSH³⁰.
- ✓ Posibilidad de programar plugins específicos para nuevos sistemas.

²⁷ **Syslog:** Es un estándar para el envío de mensajes de registro en una red informática IP.

²⁸ Véase Acrónimos

²⁹ Véase Acrónimos

³⁰ Véase Acrónimos

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

Nagios se basa en una interfaz web donde se muestra información de los equipos que están siendo monitoreados además se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante correo electrónico, mensajes SMS³¹ y sonidos.

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

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

3.5.2 DESCRIPCIÓN DEL SERVIDOR NAGIOS

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

³¹ Véase Acrónimos

³² Véase Acrónimos

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



Figura 3.2: Diagrama de red Nagios^[2]

3.6 IP SOLUTION CENTER^[12]

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

Cisco IP Solution Center también ayuda a reducir los costos operacionales, proporcionando flujo de trabajo automatizado basado en la solución de problemas y capacidades de diagnóstico para redes VPN MPLS. Las aplicaciones pueden funcionar como aplicaciones independientes o como un conjunto, las funciones incluyen el aprovisionamiento y el diagnóstico automático de MPLS VPN, ATM, Frame Relay y Ethernet sobre MPLS VPN, ATM y Frame Relay³³.

3.6.1 APLICACIONES

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

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

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

> IP SOLUTION CENTER - MPLS VPN DE GESTIÓN

Presenta las siguientes funcionalidades:

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

> CISCO IP SOLUTION CENTER- MPLS VPN DE DIAGNÓSTICO

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

> CISCO IP SOLUTION CENTER DE GESTIÓN CAPA 2 VPN

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

> IP SOLUTION CENTER DE GESTIÓN- INGENIERÍA DE TRÁFICO

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

3.6.2 CARACTERÍSTICAS Y VENTAJAS

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

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

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

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

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

Tabla 3.1- Características y beneficios de Cisco IP Solution Center

3.7 ACS (ACCESS CONTROL SERVER)^[13]

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

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

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

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

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

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

3.7.1 CARACTERÍSTICAS

ACS presenta las siguientes características:

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

3.7.2 FUNCIONALIDAD DE ACS

ACS es altamente escalable y de alto rendimiento para el control de acceso que funciona como un servidor RADIUS³⁶ o TACACS³⁷ y los controles de autenticación, autorización y contabilidad (AAA³⁸) de los usuarios que acceden a los recursos corporativos a través de una red.

³⁵ Véase Acrónimos

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

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

³⁸ Véase Acrónimos

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

Cisco Secure ACS apoya el control de acceso y la contabilidad de los servidores de acceso telefónico, cable y soluciones de banda ancha DSL³⁹, firewalls, VPNs, Voz sobre IP (VoIP), el almacenamiento y conmutación LAN⁴⁰ y WLAN⁴¹.

3.7.3 ¿POR QUÉ ES NECESARIO USAR ACS?

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

3.7.4 NUEVAS CARACTERÍSTICAS

Añade las siguientes características:

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

³⁹ Véase Acrónimos

⁴⁰ Véase Acrónimos

⁴¹ Véase Acrónimos

CAPÍTULO 4

ITIL FOUNDATION (INFORMATION TECHNOLOGY INFRAESTRUCTURE LIBRARY

4.1 INTRODUCCIÓN^[3]

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

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

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

4.2 DESCRIPCIÓN^[3]

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

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

4.3 OBJETIVOS DE ITIL^[3]

- Diseminar las mejores prácticas en la gestión de servicios de Tecnologías de Información de forma sistemática basada en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos.
- Replanteamiento del área tecnológica y la definición de los elementos y procesos críticos dentro de la empresa.
- Los procesos de Administración de Servicios deben ser usados por las personas y herramientas efectivas y económicas para el desarrollo de la alta calidad y la innovación de los servicios de TI alineados con los procesos de negocio.

4.4 ÁREAS ADMINISTRADAS POR ITIL^[3]

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



Figura 4.1: Áreas administradas por ITIL^[3]

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

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

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

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

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

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

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

4.5 ESTRUCTURA ITIL ^{[1], [2], [3]}

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

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

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

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

SOPORTE DE SERVICIOS

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

PROVISIÓN DE SERVICIOS

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

4.6 GESTIÓN DE SERVICIO^[3]

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

4.7 SOPORTE DE SERVICIOS ^{[1], [3], [4], [5]}

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



Figura 4.2: Soporte de Servicio^[1]

4.7.1 COMPONENTES DE LA METODOLOGÍA DE SOPORTE AL SERVICIO

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

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

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

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

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

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

- ✓ Registrando y monitorizando incidentes.
- Aplicando soluciones temporales a errores conocidos en colaboración con la Gestión de Problemas.
- ✓ Colaborando con la Gestión de configuraciones para asegurar la actualización de CMDB⁴².
- ✓ Gestionando cambios solicitados vía peticiones de servicio en colaboración con la Gestión de Cambios y Versiones.

4.7.2 GESTIÓN DE INCIDENCIAS

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

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

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

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

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

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



Figura 4.3: Gestión de Incidencias^[1]

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

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

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

Los beneficios de una gestión eficaz de incidencias son:

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

4.7.3 GESTIÓN DE PROBLEMA

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

Las funciones principales de la Gestión de Problemas son:

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

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

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

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



Figura 4.4: Gestión de Problema^[1]

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

4.7.4 GESTIÓN DE CAMBIO

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

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

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

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



Figura 4.5: Gestión de Cambios^[1]

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

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

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

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

4.7.5 GESTIÓN DE CONFIGURACIONES

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

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



Figura 4.6: Gestión de Configuración^[1]

Las principales funciones de Gestión de Configuraciones son las siguientes:

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

- Proporcionar información precisa sobre la configuración TI a todos los diferentes procesos de gestión.
- Interactuar con las Gestiones de Incidentes, Problemas, Cambios y Versiones de manera que estas puedan resolver más eficientemente las incidencias, encontrar rápidamente la causa de los problemas, realizar los cambios necesarios para su resolución y mantener actualizada en todo momento la CMDB.
- Monitorizar periódicamente la configuración de los sistemas en el entorno de producción y contrastarla con la almacenada en la CMDB para subsanar discrepancias.
- Provee soporte al servicio, todos los procesos de Soporte al servicio dependen de gran manera de la CMBD:
 - ✓ Se necesita la información de los CLs^{43} para analizar incidentes y problemas.
 - ✓ La Gestión de Cambios y Versiones tiene que trabajar en estrecha colaboración con la Gestión de Configuraciones para mantener actualizada la CMBD.

Los CLs pueden ser:

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

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

4.7.6 GESTIÓN DE VERSIONES

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

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

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

Las versiones pueden clasificarse de acuerdo a la Infraestructura TI:

- Versiones mayores: que representan importantes despliegues de software y hardware y que introducen modificaciones importantes en la funcionalidad y características técnicas.
- Versiones menores: implica la corrección de varios errores conocidos puntuales y que a menudo son modificaciones que vienen a implementar de una manera correctamente documentada soluciones de emergencia.
- Versiones de emergencia: modificaciones que reparan de forma rápida un error conocido.

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



Figura 4.7: Gestión de Versiones^[1]

La **Gestión de Versiones** también debe mantener actualizada la Biblioteca de Software Definitivo (**DSL**), donde se guardan copias de todo el software en producción, y el Depósito de Hardware Definitivo (DHS⁴⁴), donde se almacenan piezas de repuesto y documentación para la rápida reparación de problemas de hardware en el entorno de producción.

4.8 PROVISIÓN DE SERVICIOS ^{[1], [3], [4], [5]}

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

⁴⁴**Biblioteca de Software Definitivo (DSL):** Donde se guardan copias de todo el software en producción.

Depósito de Hardware Definitivo (DHS): Donde se almacenan piezas de repuesto y documentación para la rápida reparación de problemas de hardware en el entorno de producción.



Figura 4.8: Provisión de Servicios^[1]

4.8.1 GESTIÓN DE NIVELES DE SERVICIOS

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

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

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

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



Figura 4.9: Gestión de Niveles de Servicio^[1]

La Gestión de Niveles de Servicio es la responsable de:

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

4.8.2 GESTIÓN FINANCIERA DE LOS SERVICIOS TI

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

⁴⁵ **SLAs (Service Level Agreement):** es un acuerdo de nivel de servicio contiene una descripción del servicio que abarca desde los aspectos más generales hasta los detalles más específicos del servicio.

⁴⁶**OLAs (Acuerdos de Nivel de Operación):** son documentos de carácter interno de la propia organización TI que determinan los procesos y procedimiento necesarios para ofrecer los niveles de servicio acordados con los clientes.

UC (Contratos de Soporte): es un acuerdo con un proveedor externo para la prestación de servicios no cubiertos por la propia organización TI.

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



Figura 4.10: Gestión Financiera^[1]

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

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

4.8.3 GESTIÓN DE CAPACIDAD

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

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

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



Figura 4.11: Gestión de Capacidad^[1]

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

- Predicción y provisión automatizada: ofrece una serie de herramientas para asegurar la efectividad de todos los aspectos relativos de la capacidad y rendimiento que afectan los servicios del negocio.
- Capacity Planning: contribuye a construir un proceso estructurado de la provisión de los recursos TI dependiendo de las necesidades.
- Informe históricos de uso y tendencia: proporciona herramientas de análisis que permiten identificar la relación entre el ciclo del negocio y la capacidad de los recursos.

4.8.4 GESTIÓN DE LA CONTINUIDAD DEL SERVICIO

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

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

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



Figura 4.12: Gestión de Continuidad del Servicio^[1]

Esta gestión debe combinar equilibradamente los siguientes procedimientos:

- Proactivos: buscan impedir o minimizar las consecuencias de una grave interrupción del servicio.
- **Reactivos:** su objetivo es reanudar el servicio tan pronto como sea posible.

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

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

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

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



Figura 4.13: Evaluación de Riesgos^[1]

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

4.8.5 GESTIÓN DE DISPONIBILIDAD

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

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

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



Figura 4.14: Gestión de Disponibilidad^[1]

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

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

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

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

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

4.8.6 GESTIÓN DE LA SEGURIDAD

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

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

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

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



Figura 4.15: Gestión de la Seguridad^[1]

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

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

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

CAPÍTULO 5

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

5.1 MANUAL CACTI

5.1.1 OBJETIVO

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

5.1.2 INTRODUCCIÓN

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

5.1.3 INGRESO AL SISTEMA

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

	User Login
lease enter v	our Cacti user name and password below:
Please enter y	your Cacti user name and password below:
Please enter y Jser Name:	rour Cacti user name and password below:
Please enter y Jser Name: Password:	rour Cacti user name and password below:

Figura 5.1.1: Ingreso al sistema^[1]

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

5.1.4 PANTALLA INICIAL

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



Figura 5.1.2: Pantalla Inicial^[1]

5.1.5 TAB CONSOLE

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

5.1.5.1 DEVICES

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

Cacti - Windows Int	ernet Explorer									
) 🕞 🔻 📙 http://:	172.16.19.152/cacti/host.php						🗙 🛃 🗶 🛃 🗠	ogle		
thivo Edición Ver	Favoritos Herramientas Ayuda									
Favoritos 🛛 🚖 🔰 N	lew Cacti 🙋 ACS 🙋 ISC 🙋 IPTV	/ 🙋 WhatsUp CNT 📴 Calculadora	IP - IP Subnetting	💐 Spyral 🙋 BRAS	🙁 Autenticació	in de usuarios 👔 AXI	5 🙋 ITELLIN 🔀 Ca	icti 🔌 Optus Looking	Glass	
10 cm	X Manual Carti					- A	<u> </u>	Página + Seguridad	 Herramientas 	- 6
1	Canada cota									
console gra	phs npc GPS	Map monitor weath	ermap							
and any David								Log	ced in as adm (Logo
										-
eate	Devices							-		A
w Graphs	Type: Any	Status: Any	V Rows:	30 Rows	Search:		go clear			
aph Management								-		_
aph Trees	<< Previous			Showing Row	s 1 to 30 of 1	22 [1,2,3,4,5]			Ne	ext
ta Sources	Description**	ID Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Availability	
vices	AMBCNTE01	123 6	6	Up	0	10.3.10.100	3.29	3.91	99.91	
athermaps	AMBSURE01	126 3	3	Up	0	10.8.0.76	5.89	9.71	99.89	
ection Methods	AMBSURP01	99 26	26	Up	0	10.3.1.100	7.89	35.14	99.79	
a Queries	AZGCNTE01	64 5	5	Up	0	10.6.20.100	8.27	10.63	99.59	
nlates	AZGCNTM01	65 4	4	Up	0	10.6.20.194	8.93	10.42	99.78	
h Templates	BBHCNTE01	40 9	9	Up	0	10.5.30.100	14.65	16.1	99.67	
: Templates	BBHCNTM01	77 1	1	Up	0	10.5.30.194	18.16	17.93	99.69	
Templates	BBHMTVM01	74 1	1	Up	0	10.5.30.196	7.15	13.59	99.02	
ort/Export	BBHQVDE01	78 2	2	Up	0	10.8.0.88	4.06	5.14	99.64	
ort Templates	BBHSJNM01	81 1	1	Up	0	10.5.30.200	12.74	15.85	98.44	
ort Templates	CACGLZM01	61 1	1	Up	0	10.6.10.199	13.19	14.99	99	
figuration	CACSIGM01	63 1	1	Up	0	10.6.10.197	16.81	34.23	90.13	
ngs	CACSTIM01	62 1	1	Up	0	10.6.10.205	10.24	15.45	97.77	
in Management	CCACNTE01	57 8	8	Up	0	10.6.10.100	7.91	10.76	99.57	
em Utilities	CCACNTM01	60 5	5	Up	0	10.6.10.195	8.9	12.49	99.62	
Management	CCACNTM02	59 9	9	Up	0	10.6.10.194	8.86	11.7	99.62	
Viewer	CCACNTP01	56 8	8	Up	0	10.6.1.100	8.11	199.45	98.99	
iut User	CCAJRTM01	105 2	2	Up	0	10.6.10.225	12.7	15.88	84.57	
	CCANNRM01	103 2	2	Up	0	10.6.10.221	10.7	13.64	98.58	
	CCASBLM01	104 4	4	Up	0	10.6.10.223	14.51	16.87	99.54	
	CCASPNM01	102 4	4	Up	0	10.6.10.220	9.48	12.95	99.49	
	ESMPALE01	29 6	6	Up	0	10.1.10.100	6.79	8.06	99.26	
	ESMPALE02	30 5	5	Up	0	10.8.0.87	24.74	8.02	99.23	
	ESMPALM01	31 6	6	Up	0	10.50.87.2	7.55	10.04	98.57	
	ESMPALP01	28 4	4	Up	0	10.1.1.100	7.27	246.77	99.27	
	ESMSNJM01	68 0	0	Disabled	0	10.1.10.197	0	0	100	
	GLPBLTM01	109 1	1	Up	0	10.20.158.110	551.75	534.32	89.65	
	GLPSCRE01	105 2	2	Up	0	10.8.0.95	511.69	512.14	98.8	
	GROCNTEDI	131 6	6	Up		10 5 40 100	10.22	10.03	99.81	
	STOCHTED'S	101 0		O P	•	10.0.40.100			20.0x	

Figura 5.1.3: Devices ^[1]

5.1.5.2 AÑADIR UN EQUIPO

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

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



Figura 5.1.4: Añadir un nuevo equipo^[1]

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

> DEVICE

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

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

> SECCIÓN AVAILABILITY/REACHABILITY OPTIONS:

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

SECCIÓN SNMP Options:

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

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

5.1.5.3 EDITAR UN EQUIPO

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

Create	Devices			1					1		Add
New Graphs	Type: Any	V Statu	a: Any	× Rows:	30 Rows	Search:		go clear			
Management											
Graph Management	<< Previous	/			Showing	Rows 1 to 30 of 12	2[12345]	/		Nov	4.55
Graph Trees	C C F C F C F C F C F C F C F C F C F C	10	Cranhe	Data Sources	Statur	Event Count	Hostopero	Current (mc)	Automagica (mm)	Availability	
Data Sources		10	Graphis	Data Sources	Status	Event count	nostname	Current (ms)	Average (ms)	Availability	
Devices	AMBCNIE01	123	0	0	Up	U	10.3.10.100	3.36	3.91	99.91	
Weathermaps	AMBSUREDI	126	3	3	Up	0	10.8.0.76	5.98	9.7	99.89	
Collection Methods	AMBSURP01	99	26	26	Up	0	10.3.1.100	8.17	35.19	99.79	
Data Queries	AZGCNTE01	64	5	5	Up	0	10.6.20.100	8.26	10.62	99.59	
Data Input Methods	AZGCNTM01	65	4	4	Up	0	10.6.20.194	8.95	10.4	99.78	
Tomplator	(

Figura 5.1.5: Menú Devices^[1]

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

Create New Graphs	AMBSURE01 (10.8.0.76)	*Create Granhs
Management	System: Cisco IOS Software, c7600rsp72043_rp Software (c7600rsp72043_rp-ADVIDSERVICESK9-W),	Version 12.2 (22) SRD2, RELEASE SOFTWARE (feg) Technical for this Host
Graph Management	Support: http://www.cisco.com/techsupport Copyright (c) 1986-2009 by Cisco Systems, Inc. Co	mpiled Thu 10-Sep-09 1
Graph Trees	Vpine: sci/istor (is avs, is nours, so minutes)	
Data Sources	Location: Quito	
Devices	Contact: Gestion IP/MPLS - 593-2-2540199	
Weathermans		
Collection Matheda	Devices [edit: AMBSURE01]	
Contraction Internet	Description	AMBSURE01
Data Quenes	Give this host a meaningful description.	
Data Input Methods	Hostname Fully gualified hostname or IP address for this device.	10.8.0.76
Templates	Host Template	
Graph Templates Host Templates	Choose what type of host, host template this is. The host template will govern what kinds of data should be gathered from this type of host.	Cisco Router
Data Templates		ROUTER C7600 NODO AMBATO SUR
Import/Export	Notes	
Import Templates	Enter notes to this host.	
Export Templates		
Configuration		
Settings	Disable Host Chesk this have to disable all sharks (as this heat	Disable Host
Plugin Management		
Utilities	Check this box to monitor this host on the Monitor Tab.	Monitor Host
System Utilities		POUTER CZEGO AMBATO SUR
User Management	Down Host Message	TUNGUBAHUA UNREACHEABLE
Flow Viewer	This is the message that will be displayed when this host is reported as down.	
Logout User		
	Latitude The devices latitude coordinates	0.000000000
	Longitude	
	The devices longitude coordinates	0.000000000
	Nagios Host Mapping	Nee
	Select the Naglos host that maps to this host.	None
	Availability/Reachability Options	
	Downed Device Detection	Disc and ONIND an
	The method Cacti will use to determine if a host is available for polling.	
	Pine Method	
	The type of ping packet to sent.	UDP Ping V
	NOTE: ICMP on Linux/UNIX requires root privileges.	
	Ping Port TCP or UDP port to attempt connection.	23
	Ping Timeout Value	100
	for SNMP pings.	400
	Ping Retry Count	
	The number of times Cacti will attempt to ping a host before failing.	

Figura 5.1.6: Edición de un equipo^[1]

5.1.5.4 CREACIÓN DE GRÁFICOS

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

Para la creación de los gráficos seguir los siguientes pasos:

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

😋 🕞 🔻 🚺 http://1	72:16:19:152/cacti/graphs_new.php	🛩 🔄 🔛 🚼 Google
Archivo Edición Ver F	Favoritos Herramientas Ayuda	
🚖 Favoritos 🛛 🙀 🔰 Ne	ew Cacti 🙋 ACS 🙋 ISC 🙋 IPTV 🙋 WhatsUp CNT 🔢 Calculadora IP - IP Subnetting 📈 Spyral 🙋 BRAS 🔀 Aut	enticación de usuarios 👔 AXIS 🙋 ITELLIN 🔯 Cacti 👟 Optus Looking Glass
La Carti		🏠 🔹 🕅 - 🖃 📾 🍷 Página 🔹 Seguridad 👻 Herramientas 🗙 🚱 🖛
console grap	hs npc GPS Map monitor weathermap	
Console -> Create New G	iraphs	Logged in as adm (Logout)
Create	AMBCNTE01 (10.3.10.100) Cisco Router	
New Graphs		*Edit this Host
Management	Host: AMBCNTE01 (10.3.10.100) Graph Types: Graph Temple	ate Based *Create New Host
Graph Trees		
Data Sources	Graph (AMBSURP01 (10.3.1.100)	
Devices	Graph T AZGCNTE01 (10.6.20.100)	
Weathermaps	Constan (A2.00(N1)(00.020.104)	
Collection Methods	BBHCNTE01 (10.5.30.100)	
Data Queries	Create: C BBHCN I M01 (10.5.30.194)	
Data Input Methods	Create: BBHOVDE01 (10.8.0.88)	
Templates	(Select a g BBHSJNM01 (10.5.30.200)	
Graph Templates	CACGLZM01 (10.6.10.199)	
Host Templates	CACSIGM01 (10.6.10.197)	cancel create
Data Templates	CACSTIMUT (10.6.10.205)	
Import/Export	CCACNTM01 (10.6.10.195)	
Export Templates	CCACNTM02 (10.6.10.194)	
Configuration	CCACNTP01 (10.6.1.100)	
Settings	CCAJRTM01 (10.6.10.225)	
Plugin Management	CCASELM01 (10.6.10.221)	
Utilities	CCASPNM01 (10.6.10.220)	
System Utilities	ESMPALE01 (10.1.10.100)	
User Management	ESMPALE02 (10.8.0.87)	
Flow Viewer	ESMPALMUT (10.50.87.2) ESMPAL 001 (10.1.1.100)	
Logout User	ESMSNJM01 (10.1.1.100)	
	GLPBLTM01 (10.20.158.110)	
	GLPSCRE01 (10.8.0.95)	
	GRDCNTE01 (10.5.40.100) GYEBLLP01 (10.5.2.100)	

Figura 5.1.7: Creación de gráficos^[1]

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

🖉 Cacti - Windows Inte	rnet E	cplorer										F 🗙
😋 🕞 🗢 🔰 http://1	72.16.19	.152/cacti	i/graphs_new.php?graph_I	:ype=18host_id	=1238filter=			~	🖌 🖌 🚼	Google		P-
Archivo Edición Ver P	avoritos	Herran	ientas Ayuda									
🚖 Favoritos 🛛 🖕 🔰 Ne	w Cacti	acs	🥫 ISC 🥫 IPTV 🏿 W	hatsUp CNT 🔢	Calculadora IP - IP	Subnetting 😹 Spyral	🖉 BRAS 🔀 Autentica	ción de usuarios 📓 AXIS	🦲 ITELLIN 🖂	Cacti 🔌 Optus Looking Gla	8	**
🔰 Catti								合 -	5 · 🗆 🖶	• Página • Seguridad •	Herramientas 🕶	@ - "
												_
console grap	hs	npo	GPS Map	monitor	weathermap							
Console -> Create New Gr	rapns									Logged	in as adm (Lo	gout)
Create	AM	BCNT	E01 (10.3.10.1	.00)	Cisco	Router						
Management	Host:	AM	BCNTE01 (10.3.10.10	D)		Graph Types:	SNMP - Interface S	Statistics ¥	*	Edit this Host		
Graph Management			(.,					*C	reate New Host		
Data Sources	Searc	h:		9	o clear							
Devices	Data	Ouerv	ISNMP - Interface St	atistics1								0
Weathermaps Collection Methods	<< P	revious				Showing Ro	ows 1 to 50 of 431 [1,2,3,4,5,6,7,8,9]			Nex	l>> =
Data Queries	Index	: Status	Description	Name (IF-M	IB) Alias (IF-MI	8)		Туре	Speed	Hardware Address	IP Address	
Data Input Methods	1	Up	GigabitEthernet1/1	Gi1/1	### MPLS -	LINK TO AMBSURP01	- Giga 0/2/0/5 ###	ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80	10.83.1.122	
Graph Templates	2	Up	GigabitEthernet1/2	Gi1/2	### MPLS -	LINK TO AMBSURP01	- Giga 0/6/0/4 ###	ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80	10.83.1.126	
Host Templates	3	Down	GigabitEthernet1/3	Gi1/3	DSLAM_PINU	LO		ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
Data Templates Import/Export	4	Down	GigabitEthernet1/4	Gi1/4				ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80		
Import Templates	5	Down	GigabitEthernet1/5	GI1/5				ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
Export Templates	6	Down	GigabitEthernet1/6	Gi1/6				ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
Settings	7	Down	GigabitEthernet1/7	Gi1/7				ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80		
Plugin Management	8	Down	GigabitEthernet1/8	Gi1/8				ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80		
System Utilities	9	Down	GigabitEthernet1/9	Gi1/9				ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80		
User Management	10	Down	GigabitEthernet1/10	Gi1/10				ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
Flow Viewer	11	Down	GigabitEthernet1/11	Gi1/11				ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
- cogour oser	12	Down	GigabitEthernet1/12	Gi1/12				ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
	13	Down	GigabitEthernet1/13	Gi1/13				ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
	14	Down	GigabitEthernet1/14	Gi1/14				ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
	15	Down	GigabitEthernet1/15	Gi1/15				ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
7	16	Down	GigabitEthernet1/16	Gi1/16				ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
	17	Down	GigabitEthernet1/17	Gi1/17				ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80		
_	18	Down	GigabitEthernet1/18	Gi1/18				ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80		
	19	Down	GigabitEthernet1/19	Gi1/19				ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80		
	20	Down	GigabitEthernet1/20	Gi1/20				ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80		
	21	Up	GigabitEthernet2/1	Gi2/1	eee MPLS -	LINK TO AMBONTPO1	- Giga 0/1/0/0 ###	ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80	10.83.2.18	
	22	Up	GigabitEthernet2/2	Gi2/2	eee MPLS -	LINK TO AMBONTPO1	- Giga 0/6/0/0 ###	ethernetCsmacd(6)	1000000000	00:00:26:CB:51:BE:80	10.83.2.22	
			-									- V

Figura 5.1.8: Opción Graph Type^[1]

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

console grap	hs	np	c GPS Map monitor w	eathermap			Ν		Logo	ged in as adm (Lo	gout)	
Create New Graphs Management Graph Management Graph Trees Date Sources	AM Host Sear	BCNT AN	E01 (10.3.10.100) IBCNTE01 (10.3.10.100) n	Cisco R clear	Cisco Router Graph Types: SNMP - Interface Statistics					*Edit this Host Create New Host		
Weathermaps	Data	Query	[SNMP - Interface Statistics]		Chausing D	awa 1 ka 50 of 272 [1 2 2 4 5	670]			Nov	0	
Collection Methods Data Queries	Inde	× Status	> Description	Name (IF-	Alias (IF-MIB)	JWS 1 to 30 01 373 [1,2,3,4,3,	0,7,0] Туре	Speed	Hardware Address	IP Address		
Data Input Methods Templates	45	Down	Vlan1	VI1			propVirtual (53)	1000000000	00:00:26:CB:51:BE:80			
Graph Templates	50	Up	unrouted VLAN 1	VLAN-1			propVirtual (53)	0	00:00:26:CB:51:BE:81			
Data Templates	51	Up	unrouted VLAN 1002	VLAN-1002			propVirtual (53)	0	00:00:26:CB:51:BE:80			
Import/Export Import Templates	52	Up	unrouted VLAN 1004	VLAN-1004			propVirtual (53)	0	00:00:26:CB:51:BE:80			
Export Templates	53	Up	unrouted VLAN 1005	VLAN-1005			propVirtual (53)	0	00:00:26:CB:51:BE:80			
Settings	54	Up	unrouted VLAN 1003	VLAN-1003			propVirtual (53)	0	00:00:26:CB:51:BE:80			
Plugin Management Utilities	55	Up	unrouted VLAN 100	VLAN-100			propVirtual (53)	0	00:00:26:CB:51:BE:80			
System Utilities	67	Up	GigabitEthernet2/3.ServiceInstance.304	GI2/3.SI.304			l2 <mark>vlan</mark> (135)	100000000				
Flow Viewer	68	Up	unrouted VLAN 304	VLAN-304			propVirtual (53)	0	00:00:26:CB:51:BE:80			
Logout User	70	Up	Vlan304	VI304	*** PPPoE TELYDA	TA ***	propVirtual (53)	100000000	00:00:26:CB:51:BE:80			
	71	Up	GigabitEthernet2/3.ServiceInstance.4029	Gi2/3.SI.4029			l2 <mark>vlan</mark> (135)	100000000				
	72	Up	unrouted VLAN 4029	VLAN-4029			propVirtual (53)	0	00:00:26:CB:51:BE:80			
	73	Up	Vlan4029	VI4029	PPPOE_UIOINQB0:	1_75K_AMB	propVirtual (53)	100000000	00:00:26:CB:51:BE:80			
	74	Up	GigabitEthernet2/3.ServiceInstance.100	Gi2/3.SI.100			12 <mark>vlan</mark> (135)	100000000				
	75	Up	Vlan100	VI100	eeee <mark>Vlan</mark> -ID eee		propVirtual (53)	100000000	00:00:26:CB:51:BE:80	10.3.10.193		

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

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

A	MBCN	TE01 (10.3.10.100)	Cisco R	outer				*Edit this Host	
Hos	st: /	AMBCNTE01 (10.3.10.100)		 Graph Types: 	SNMP - Interface Statistics		*(Create New Hos	at 🛛
Sea	arch: v	lan go	clear						
Dat	ta Que	ry [SNMP - Interface Statistics]							
thods <<	Previo	ous	News (TF	Showing Ro	ws 1 to 50 of 373 [1,2,3,4,5	,6,7,8]			N
Ind	lex Stat	us Description	MIB)	Alias (IF-MIB)		Туре	Speed	Hardware Address	IP Address
45	Dow	n Vlan1	VI1			propVirtual (53)	100000000	00:00:26:CB:51:BE:80	
50	Up	unrouted VLAN 1	VLAN-1			propVirtual (53)	0	00:00:26:CB:51:BE:81	
51	U.S.	unrouted VIAN 1002	VI 4N-1002			propVirtual		00-00-26-CB-51-BE-80	
						(53) propVirtual			
52	Up	unrouted VLAN 1004	VLAN-1004			(53)	0	00:00:26:CB:51:BE:80	
53	Up	unrouted VLAN 1005	VLAN-1005			propVirtual (53)	0	00:00:26:CB:51:BE:80	
54	Up	unrouted VLAN 1003	VLAN-1003			propVirtual (53)	0	00:00:26:CB:51:BE:80	
int 55	Un	uprouted VLAN 100	VLAN-100			propVirtual	0	00:00:26:CB:51:BE:80	
		Circle The sector of the secto	0.0/0.01.004			(53)	-		
int	Op.	olgabilitinena josef vicematance.304	012/ 31311304			propVirtual	1000000000		
68	Up	unrouted VLAN 304	VLAN-304			(53)	0	00:00:26:CB:51:BE:80	
70	Up	Vlan304	VI304	*** PPPoE TELYDAT	A ***	(53)	100000000	00:00:26:CB:51:BE:80	
71	Up	GigabitEthernet2/3.ServiceInstance.4025	Gi2/3.SI.4029			l2 <mark>vlan</mark> (135)	100000000		
	Un	unanted with to 20	10.00			propVirtual	0	00:00:26:CB:51:8E:80	

Figura 5.1.10: Selección de Interfaces^[1]

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

			CRS Map monit	una the							
Console -> Create New G	raphs	np		.or weath	lennap				Logged in	n as adm (Log	gout)
Create	+ Cre	ated gra	ph: AMBCNTE01 - Traffic - Gil/	20							
Management Graph Management	АМ	BCNT	E01 (10.3.10.100)	-	Cisco Router						
Graph Trees Data Sources	Host:	AM	BCNTE01 (10.3.10.100)		Graph Types:	SNMP - Interface Statistic	5 💙	*Ee *Cre	dit this Host ate New Host		
Devices Weathermaps	Searc	:h: Gi1	/2	go cle	ear						
Data Queries	Data	Query	[SNMP - Interface Statistics]								0
Data Input Methods	Index	< Status	Description	Name (IF-MI	IB) Alias (IF-MIB)		Туре	Speed	Hardware Address	IP Address	
Templates Graph Templates	2	Up	GigabitEthernet1/2	Gi1/2	### MPLS - LINK TO AMBS	JRP01 - Giga 0/6/0/4 ###	ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80	10.83.1.126	
Host Templates	20	Down	GigabitEthernet1/20	Gi1/20			ethernetCsmacd(6)	100000000	00:00:26:CB:51:BE:80		
Data Templates	59	Up	GigabitEthernet1/2-mpls layer	Gi1/2			mpls(166)	100000000			
Import/Export Import Templates	4						Selec	t a graph type	e: In/Out Bits		<
Configuration									cance	l creat	e

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

5.1.5.5 MANAGEMENT

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

5.1.5.5.1 GRAPH MANAGEMENT

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

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

🔰 Cacti		🐴 🔹 🔝 🛸 🖃 🌐 👻 Página 👻 Seguridad 👻 H	lerramientas 🔹 🔞 🕶
console graph	npc GPS Map monitor weathermup	Logged in	n as adm (Logout)
Create	Graph Management		bbA
New Graphs Management Graph Management CDEFs	Host: Any V Template: Any V Go Clear Rows: 30 Rows V Search:		
Colors	<< Previous Showing Rows 1 to 30 of 741 [1,2,3,4,5,6,7,8,9,10,11,12,13,1	4,15,16,17,18,19,20,21]	Next >>
GPRINT Presets	Graph Title**	ID Template Name	Size 📃
Oraph Trees	AMBCNTE01 - Traffic - Gi1/1 - LINK TO AMBSURP01 - Giga 0/2/0/5	632 Interface - Traffic (bits/sec)	120×500
Devices	AMBCNTE01 - Traffic - GI1/2 - LINK TO AMBSURP01 - Giga 0/6/0/4	633 Interface - Traffic (bits/sec)	120×500
Weathermaps	AMBCNTE01 - Traffic - Gi1/20	821 Interface - Traffic (bits/sec)	120×500
Collection Methods	AMBCNTE01 - Traffic - Gi2/1 - LINK TO AMBCNTP01 - Giga 0/1/0/0	634 Interface - Traffic (bits/sec)	120×500
Data Queries	AMBCNTE01 - Traffic - Gi2/2 - LINK TO AMBCNTP01 - Giga 0/6/0/0	635 Interface - Traffic (bits/sec)	120×500
Data Input Methods	AMBCNTE01 - Traffic - GI2/3 - LINK TO AMBCNTM01 - GI 0/2	636 Interface - Traffic (bits/sec)	120×500
Templates	AMBCNTE01 - Traffic - Gi2/3.SI.304	819 Interface - Traffic (bits/sec)	120×500
Graph Templates	AMBCNTE01 - Traffic - VI202 - PPPOE_AMBATO_CENTRO_UIOINQB01	664 Interface - Traffic (bits/sec)	120×500
Host Templates	AMBCNTE01 - Traffic - VLAN-1003	818 Interface - Traffic (bits/sec)	120×500
Data Templates	AMBCNTE01 - Traffic - VLAN-201	820 Interface - Traffic (bits/sec)	120×500
Import/Export	AMBCNTE01 - Traffic - VLAN-304	817 Interface - Traffic (bits/sec)	120×500
Export Templates	AMBSURE01 - Traffic - Fa3/2 - LINK LTCPJLM01 F0/8 30Mbps FO	655 Interface - Traffic (bits/sec)	120×500
Configuration	AMBSURE01 - Traffic - Fa3/38 - HACIA CALUMA	772 Interface - Traffic (bits/sec)	120×500
Settings	AMBSURE01 - Traffic - Fa4/24 - LINK LTCPJLM01 G0/1 20 Mbps BACKUP RADIO	654 Interface - Traffic (bits/sec)	120×500
Plugin Management	AMBSURP01 - GigabitEthernet0/2/0/2 - ### MPLS - LINK TO PUYCNTP01 - Giga 0/1/0/0 ### - DWDM	600 Interface - Traffic (bits/sec)	120×500
Utilities	AMBSURP01 - GigabitEthernet0/2/0/2 - ### MPLS - LINK TO PUYCNTP01 - Giga 0/1/0/0 ###	836 Interface - Traffic (bits/sec)	120×500
System Utilities	AMBSURP01 - GigabitEthernet0/2/0/6 - ### MPLS - LINK TO BBHCNTE01 - Giga 1/2 ### - DWDM	541 Interface - Traffic (bits/sec)	120×500
User Management	AMBSURP01 - GigabitEthernet0/2/2/1 - ### MPLS - LINK TO AZGCNTE01 - Giga 1/3 ###	837 Interface - Traffic (bits/sec)	120×500
Flow Viewer	AMBSURP01 - GigabitEthernet0/6/0/1 - ### MPLS - LINK TO PUYCNTP01 - Giga 0/2/0/0 ###	838 Interface - Traffic (bits/sec)	120×500
Logout User	AMBSURP01 - GigabitEthernet0/6/2/0 - ### MPLS - LINK TO AZGCNTE01 - Giga 1/1 ###	839 Interface - Traffic (bits/sec)	120×500
	AMBSURP01 - GigabitEthernet0/2/0/0 - ### MPLS - LINK TO GRDCNTE01 - Giga 2/1 ### - FO	537 Interface - Traffic (bits/sec)	120×500
	AMBSURP01 - GigabitEthernet0/2/0/1 - ### MPLS - LINK TO PUYCNTP01 - Giga 0/0/0/0 ### - FO	538 Interface - Traffic (bits/sec)	120×500
	AMBSURP01 - GigabitEthernet0/2/0/3 - ### MPLS - LINK TO LTCCNTE01 - Giga 2/2 ### - FO	539 Interface - Traffic (bits/sec)	120×500
	AMBSURP01 - GigabitEthernet0/2/0/4 - ### MPLS - LINK TO LTCCNTE01 - Giga 2/3 ### - DWDM	617 Interface - Traffic (bits/sec)	120×500
	AMBSURP01 - GigabitEthernet0/2/0/5 - ### MPLS - LINK TO AMBCNTE01 - Giga 1/1 ###	540 Interface - Traffic (bits/sec)	120×500
	AMBSURP01 - GigabitEthernet0/2/0/7 - ### MPLS - LINK TO BBHCNTE01 - Giga 1/3 ### - DWDM	542 Interface - Traffic (bits/sec)	120×500

Figura 5.1.12: Opción Graph Management^[1]

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

🔰 Cacti			🏠 • 🔝 - 🖃 🌐 • Página • Seguridad • H	terramientas 🔹 🔞 🕶
console grap	hs npc GPS Map moni	tor weathermap		
Console -> Graph Manag	ement		Logged i	n as adm (Logout)
Create	Graph Management			bbA
New Graphs		with a state of the state of th	1	
Management	Host: Any	V Template: Any V go clear]	
Graph Management	Rows: Any	<u>^</u>		
CDEFs	AMBCNTE01 (10 3 10 100)			
Colors	<< PrevAMBSUBE01 (10.8.0.76)	Showing Rows 1 to 30 of 741 [1,2,3,4,5,6,7,8,9,10,11,12,13	8,14,15,16,17,18,19,20,21]	Next >>
GPRINT Presets	Graph Ti AMBSURP01 (10.3.1.100)		ID Template Name	
Graph Trees	AMBCNT AZGCNTE01 (10.6.20.100)	(P01 - Giga 0/2/0/5	632 Interface - Traffic (bits/sec)	120×500
Data Sources	AMBCNT AZGCN I M01 (10.6 20.194)	P01 - Giga 0/6/0/4	633 Interface - Traffic (bits/sec)	120×500
Devices	AMBCNTE BRHCNITM01 (10.5.30.100)		821 Interface - Traffic (bits/sec)	120×500
Weathermaps	AMBONTE BBHMTVM01 (10.5.30.194)	P01 - Giga 0/1/0/0	634 Interface - Traffic (bits/sec)	120×500
Collection Methods	AMBONTE BBHQVDE01 (10.8.0.88)	P01 - Gina 0/6/0/0	635 Interface - Traffic (hits/sec)	120×500
Data Queries	AMBONTE BBHSJNM01 (10.5.30.200)	M01 - Gi 0/2	636 Interface - Traffic (bits/sec)	120×500
Data Input Methods	CACGLZM01 (10.6.10.199)	101-010/2	ete tu (Talle (bis/sec)	120,500
Templates	AMBCNTE CACSIGM01 (10.6.10.197)		819 Interrace - Inamic (bits/sec)	120x500
Graph Templates	CCACNITE01 (10.6.10.205)	CENIKO_DIDINQB01	664 Interface - Traffic (bits/sec)	120x500
Post Templates	CCACNTM01 (10.6.10.195)		818 Interface - Traffic (bits/sec)	120×500
Import/Export	AMBCNTE CCACNTM02 (10.6.10.194)		820 Interface - Traffic (bits/sec)	120×500
Import Templates	AMBCNTE CCACNTP01 (10.6.1.100)		817 Interface - Traffic (bits/sec)	120×500
Export Templates	AMBSURE CCAJRTM01 (10.6.10.225)	F0/8 30Mbps FO	655 Interface - Traffic (bits/sec)	120×500
Configuration	AMBSURE CCANNRM01 (10.6.10.221)	N CONTRACTOR OF CONTRACTOR	772 Interface - Traffic (bits/sec)	120×500
Settings	AMBSURE CCASPNM01 (10.6.10.220)	1 G0/1 20 Mbps BACKUP RADIO	654 Interface - Traffic (bits/sec)	120×500
Plugin Management	AMBSURI ESMPALE01 (10.1.10.100)	IPLS - LINK TO PUYCNTP01 - Giga 0/1/0/0 ### - DWDM	600 Interface - Traffic (bits/sec)	120×500
Utilities	AMBSURI ESMPALE02 (10.8.0.87)	APLS - LINK TO PUYCNTP01 - Giga 0/1/0/0 ###	836 Interface - Traffic (bits/sec)	120×500
System Utilities	AMBSURI ESMPALM01 (10.50.87.2)	4PLS - LINK TO BBHCNTE01 - Giga 1/2 ### - DWDM	541 Interface - Traffic (bits/sec)	120×500
User Management	AMBSURF OLDER TANDA (10.1.1.100)	APLS - LINK TO AZGCNTE01 - Giga 1/3 ###	837 Interface - Traffic (bits/sec)	120×500
Flow Viewer	GLPBLTM01 (10.20.158.110)	4PLS - LINK TO PUYCNTP01 - Giga 0/2/0/0 ###	838 Interface - Traffic (bits/sec)	120×500
Logout User	AMBSURI GBDCNTE01 (10.5.40.100)	MPLS - LINK TO AZGENTE01 - Gigs 1/1 ###	839 Interface - Traffic (bits/sec)	120x500
	AMBSURPO1 - GinabitEthernet0/2/0/0 - ##	# MPLS - LINK TO GROCNTED1 - Glos 2/1 ### - EO	537 Interface - Traffic (hits/sec)	120×500
	AMBSURPO1 - GigabitEthernet0/2/0/1 - ##	# MPLS - LTNK TO PULYENTPO1 - Gina 0/0/0/0 ### - EO	538 Interface - Traffic (hits/sec)	120×500
	AMPCUPPO1 - Ciashicthermato (2/0/2 - ##	# MDLS - LTMK TO LTCONTEG1 - Cime 2/2 ### - FO	520 Interface - Traffic (bits/sec)	120-500
	AMDCUDDO1 - GigabicEthernet0/2/0/3 - ##	# HPLS - LINK TO LICONTEGT - Giga 2/2 ### - FO	(17 Tabafasa - Traffic (bits/sec)	120,500
	APIDBORPOI - GigabitEthernet0/2/0/4 - ##	# MPLS - LINK TO LICCHTEDT - Giga 2/3 ### - DWDM	err interface - frattic (bits/sec)	1208300
	AMBSURPU1 - GigabitEthernet0/2/0/5 - ##	# MPLS - LINK TO AMBENTEUT - Giga 1/1 ###	540 Interface - Traffic (bits/sec)	120×500
	AMBSURP01 - GigabitEthernet0/2/0/7 - ##	# MPLS - LINK TO BBHCNTEU1 - Giga 1/3 ### - DWDM	542 Interface - Traffic (bits/sec)	120×500

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

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

🔰 Cacti			🏠 🔹 🔝 🕤 🖃 🌧 🔹 Página 🕶	Seguridad 🔹 Herramientas 🔹 🕢 🔹
console grap	hs npc GPS Map monitor weathermap			Logged in as adm (Logout)
Create	Graph Management			bbA
New Graphs Management Graph Management CDEFs	Host: AMBCNTE01 (10.3.10.100) V Template: Any Rows: 30 Rows V Search:	go clear		
Colors	<< Previous	Showing Rows 1 to 11 of 11 [1]		Next >>
GPRINT Presets	Graph Title**		Template Name	Size
Graph Trees	AMBCNTE01 - Traffic - Gi1/1 - LINK TO AMBSURP01 - Giga 0/2/0/5	632	Interface - Traffic (bits/sec)	120×500
Data Sources	AMBCNTE01 - Traffic - Gi1/2 - LINK TO AMBSURP01 - Giga 0/6/0/4	633	Interface - Traffic (bits/sec)	120×500
Devices	AMBCNTE01 - Traffic - Gi1/20	821	Interface - Traffic (bits/sec)	120×500
Weathermaps Collection Mathede	AMBCNTE01 - Traffic - Gi2/1 - LINK TO AMBCNTP01 - Giga 0/1/0/0	634	Interface - Traffic (bits/sec)	120×500
Collection Methods	AMBCNTE01 - Traffic - Gi2/2 - LINK TO AMBCNTP01 - Giga 0/6/0/0	635	Interface - Traffic (bits/sec)	120×500
Data Input Methods	AMBCNTE01 - Traffic - Gi2/3 - LINK TO AMBCNTM01 - Gi 0/2	636	Interface - Traffic (bits/sec)	120×500
Templates	AMBCNTE01 - Traffic - Gi2/3.5I.304	819	Interface - Traffic (bits/sec)	120×500
Graph Templates	AMBOUTCOL T - (C - MOOD - DODOC AMBATO_CENTRO_UIOINQB01	664	Interface - Traffic (bits/sec)	120×500
Host Templates	AMBCNTE01 - Traffic - VLAN-1003	818	Interface - Traffic (bits/sec)	120×500
Data Templates		820	Interface - Traffic (bits/sec)	120×500
Import/Export	AMBCNTE01 - Traffic - VLAN-3 AMBCNTE01 - Traffic - VLAN-1003	817	Interface - Traffic (bits/sec)	120×500
Import Templates	<< Previous	Showing Rows 1 to 11 of 11 [1]		Next >>
Export Templates	L		Delete	
Configuration	7	Choose an action:	Delete	yo go
Settings				
Utilities				
System Utilities				
User Management				
Flow Viewer				
Logout User				
Ŷ				

Figura 5.1.14: Selección del gráfico creado^[1]

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

la Carti		🦄 🔹 🗟 🕤 🚍 🔹 Página + Seguridad + Herramientas + 👰 +
P coco		
console grap	hs npc GPS Map monitor weathermap	
tonsole -> Graph Manage	ement -> (Edit)	Logged in as adm (Logout)
2	AMPONTENT T 45- 011 (20	The Original Deliver Made
Create	AMBCNTE01 - Traffic - Gi1/20	*Turn On Graph Debug Mode.
Management	Graph Template Selection (edit: AMBCNTE01 - Traffic - Gi1/20)	
Graph Management	Selected Graph Template	
CDEFs	Choose a graph template to apply to this graph. Please note that graph data may be lost if you	Interface - Traffic (bits/sec)
Colors	change the graph template after one is already applied.	
GPRINT Presets	Choose the host that this graph belongs to.	AMBCNTE01 (10.3.10.100)
Graph Trees		
Data Sources	Supplemental Graph Template Data	
Devices	Graph Fields	
Weathermaps	Title (title)	host_description - Traffic - query_ifName
Collection Methods	Graph Item Eiglds	
Data Queries	Inhound Data Source	
Data Input Methods	The data source to use for this graph item.	AMBONTEUT-Tramc-GI1/20 (tramc_in)
Templates	Outbound Data Source	AMBCNTE01 - Traffic - Gi1/20 (traffic out)
Host Tomplates	The data source to use for this graph item.	
Data Templates	AMPONTEOI	Traffic Gil/20
Import/Export	AMBONIEUI	ITALIC - GI1/20
Import Templates		
Export Templates	겉 0.8	Iot
Configuration	§ 0.6	e e e e e e e e e e e e e e e e e e e
Settings	5 04	
Plugin Management	8	17 m
Utilities	.2 0.2	
System Utilities	0.0	00 00 00 02:00 04:00 06:00 08:00 10:00
User Management	Inbound Current: 0.00 Average:	0.00 Maximum: 0.00
Flow Viewer	 Outbound Current: 0.00 	Average: 0.00 Maximum: 0.00
Logout User	prive red by ad	revels, ing 2011
		cancel save

Figura 5.1.15: Edición de una interfaz^[1]

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

10 Cacti			🐴 🔹 🔝 🐇 🖃 🌧 🔹 Página 🕶	Seguridad + Herramientas + 🔞	-
console grapi	hs npc GPS Map monitor weathermap				
Console -> Graph Manage	ement			Logged in as adm (Logout	rt)
Create	Eavo Succosoful				
New Graphs	Save Succession.				-
Management	Graph Management			Add	
Graph Management	Host: AMBCNTE01 (10 3 10 100) Template: Any	y go clear			
CDEFs	20 Down W County				
Colors	Kows: JU Rows V Search:				
Graph Trees	<< Previous	Showing Rows 1 to 11 of 11 [1]		Next >>	5
Data Sources	Granh Title**	ID	Template Name	Size	1
Devices	AMBCNTE01 - Traffic - Gi1/1 - LINK TO AMBSURP01 - Giga 0/2/0/5	632	Interface - Traffic (bits/sec)	120×500	1
Weathermaps	AMBCNTE01 - Traffic - Gi1/2 - LINK TO AMBSURP01 - Giga 0/6/0/4	633	Interface - Traffic (bits/sec)	120×500	i.
Collection Methods	AMBCNTE01 - Traffic - Gi1/20	821	Interface - Traffic (bits/sec)	120×500	٦l
Data Queries	AMBCNTE01 - Traffic - Gi2/1 - LINK TO AMBCNTP01 - Giga 0/1/0/0	634	Interface - Traffic (bits/sec)	120×500	ī.
Templates	AMBCNTE01 - Traffic - Gi2/2 - LINK TO AMBCNTP01 - Giga 0/6/0/0	635	Interface - Traffic (bits/sec)	120×500	٦I
Graph Templates	AMBCNTE01 - Traffic - Gi2/3 - LINK TO AMBCNTM01 - Gi 0/2	636	Interface - Traffic (bits/sec)	120×500	Ξl.
Host Templates	AMBCNTE01 - Traffic - Gi2/3.SI.304	819	Interface - Traffic (bits/sec)	120×500	ā.
Data Templates	AMBCNTE01 - Traffic - VI202 - PPPOE_AMBATO_CENTRO_UIOINQB01	664	Interface - Traffic (bits/sec)	120×500	
Import/Export	AMBCNTE01 - Traffic - VLAN-1003	818	Interface - Traffic (bits/sec)	120×500	2
Import Templates	AMBCNTE01 - Traffic - VLAN-201	820	Interface - Traffic (bits/sec)	120×500	
Export Templates	AMBCNTE01 - Traffic - VLAN-304	817	Interface - Traffic (bits/sec)	120×500	
Settings	<< Previous	Showing Rows 1 to 11 of 11 [1]		Next >>	5
Plugin Management	L,	Choose an action:	Delete	v go	Π.
Utilities			Delete		-
System Utilities			Change Graph Template		
User Management			Change Host		
Flow Viewer			Reapply Suggested Names Resize Graphs		
Logout User			Duplicate		
-			Convert to Graph Template		
			Place on a Tree (CONSUMO INTER	RNET PROVINCIAS)	
			Place on a Tree (Local Host)		
			Place on a Tree (PROYECTO)		
			Place on a Tree (RED BRAS NACIO	NAL)	
			Place on a Tree (RED DE INTERNE	-1)	
			Place on a Tree (RED MPLS NACIO	INAL)	

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

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

🔰 Cacti			🏠 💌 🔝 🐇 📼 Página	a • Seguridad • Herramientas • 🔞 •
console graphs npc GPS Map	monitor weathermap			
Console -> Graph Management -> Actions				Logged in as adm (Logout)
Graate	Diaco on a Troo (RED MDI S NACT			
New Graphs	Place of a free (KED MPES MACE	ONAE)	1.1.11.1	
new oraphs	when you click save, the following	graphs will be placed under the branch s	elected below.	
Careb Management	AMPONTED1 Tartes MAN 1000			
Graph Hanagement	AMBCINTEUT - Trainc - VLAN-1003	•		
CDEFS	Dectination Branch			
Colors	feed			
GPRINT Presets	Itool			
Graph Trees	[root]	^	no yes	
Data Sources	ANUINA			
Devices	MPLS Andina Azuay			
Weathermaps	MDLS Andina Canar MDLS Andina Chimborozo			
Collection Methods	MPLS Andina Mariasal			
Data Queries	MPLS Andina Pichincha			
Data Input Methods	MPLS Andina Tungurahua			
Templates	Mols Andina Carchi			
Graph Templates	Mpls Andina Esmeraldas			
Host Templates	Mpls Andina Imbabura			
Data Templates	Mpls Andina Inaquito			
Import / Export	Mpls Andina Loja			
Import Templates	Mpls Andina Quito Centro	3		
Event Templater	Mpls Andina Zamora			
Configuration	Mpls Santo Domingo Tsachilas			
Configuration	MDLS Andina Bolivar			
ol i ta i	INCLUAD			
Plugin Management	ORIENTE			
otilities	MPLS Oriente Morona Santiago			
system utilities	Mpls Oriente Napo			
User Management	Mpls Oriente Orellana			
Flow Viewer	Mpls Oriente Pastaza			
Logout User	Mpls Oriente Sucumbios			
	PACIFICO			
	Mpls Pacifico Bellavista	-		
	Mpls Pacifico Correos			
	Mpls Pacifico El Oro	120		
	MpIs Pacifico Finansur	×		

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

5.1.5.5.2 CREACIÓN DE UN GRAPH TREE

Los gráficos pueden ser organizados de forma jerárquica.

- 1. Seleccionar en el menú la opción Graph Tree
- 2. En la parte superior dar clic en *Add* para añadir o crear un nuevo directorio como se muestra en la figura 5.1.18:



Figura 5.1.18: Adición de un nuevo directorio^[1]

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

🖉 Cacti - Windows Internet Explorer	
🚱 🕙 🔹 🔰 http://172.16.19.152/cattl/tree.php?action=edit	V 🔶 🗶 Google
Archivo Edición Ver Favoritos Herramientas Ayuda	
🖕 Favoritos 🛛 🎭 🐌 New Cacti 🙋 ACS 🙋 ISC 🙋 IPTV 🙋 WhatsUp CNT 📭 Calculadora IP - IP Subnetting 🗷 Spyral 🖉 BRAS 🕺 Autentic	zación de usuarios 📓 AXIS 🔊 ITELLIN 🖾 Cacti 🗞 Optus Looking Glass 👋
🕼 Cacti	🛅 🔻 🔝 👘 🐨 Página 🖌 Seguridad 👻 Herramientas 🕶 🔞 👻 ≫
console graphs npc GPS Map monitor weathermap	
Console -> Graph Trees -> (Edit)	Logged in as adm (Logout)
Create Graph Trees (new)	
New Graphs Name Management A useful name for this graph tree.	
Graph Management Sorting Type Choose how items in this tree will be sorted.	rdering (No Sorting)
Graph Trees Manual Or	dering (No Sorting)
Devices Natural On	dering cancel create
Weathermaps Numeric O	rdering
Collection Methods	
Data Queries	

Figura 5.1.19: Parámetros de configuración del equipo^[1]

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



Figura 5.1.20: Creación de subdirectorios^[1]

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

console grap Console -> Graph Trees	phs npc GPS Map monitor weathermap		Logged in as adm (Logaut)
Create	Tree Items		
New Graphs	Parent Item	Iroot	
Management	Choose the parent for this header/graph.	frood	
Graph Management	Tree Item Type Choose what type of tree item this is.	Header 💌	
Graph Trees	Tree Item Value		
Data Sources	Title	La mutad	
Devices	If this item is a header, enter a title here.	AZUAY	
Weathermaps			
Collection Methods		e	cancel save
Data Queries			

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

Nota: Los subdirectorios se deben configurar como Header.

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

🔰 Cacti		💁 • 🔝 🐇 🖶 • Página • Seguridad	• Herramientas • 🔞 •
console gra	phs npc GPS Map monitor weathermap		
Console -> Graph Trees	-> (Edit)	Log	ged in as adm (Logout)
Create	Graph Trees [edit: CONSUMO INTERNET PROVINCIAS]		
New Graphs Nanacement	Name A useful name for this graph tree.	CONSUMO INTERNET PROVINCIAS	
Graph Management	Sorting Type Choose how items in this tree will be sorted.	Alphabetic Ordering	
Graph Trees Data Sources	Tree Items		Add
Devices Weathermans	++		
Collection Methods	Item	Value	
Data Queries	B AZI AY (Add)	Heading	x
Data Input Methods	E BO	Heading	×
Templates	E CARCHI (Add)	Heading	×
Graph Templates	CANAR (Add)	Heading	×
Host Templates	CHIMBORAZO (Add)	Heading	×

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

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

🔰 Cacti		🏠 - 🗋 - 📑 🖶 - Página - Seguridad - Herramientas - 👔 -
console grap	hs npc GPS Map monitor weathermap	
Console -> Graph Trees	-> (Edit) -> Graph Tree Items	Logged in as adm (Logout
Consta	The Research	
Greate	Tree Items	
wew Graphs	Parent Item Choose the parent for this header/graph.	AZUAY 🗸
Graph Management	Tree Item Type Choose what type of tree item this is.	Graph 🖌
Graph Trees	Tree Item Value	
Data Sources	Graph	
Devices	Choose a graph from this list to add it to the tree.	INTERNET AZUAT DOWINSTREAM
Weathermaps	Round Robin Archive	INTERNET AZUAY DOWNSTREAM
Collection Methods	Choose a round robin archive to control now this graph is displayed.	INTERNET AZUAT UPSTREAM
Data Queries		INTERNET BOLIVAR UPSTREAM
Data Input Methods		ipingb01
Templates		lps
Graph Templates		ISP_UIOINQSW02 - Traffic - Gi7/1 to GG01 Po1
Host Templates		ISP_UI0INQSW02 - Traffic - Gi7/2 to GGC1 Po1
Data Templates		ISP_UIOINQSW02 - Traffic - Gi7/3 to GGC2 Po2
Import/Export		ISP_UIUINUSWU2 · Traffic · GI7/4 to GGC2 Po2
Import Templates		ISP_UIDINGSW02 - Traffic - Gi7/6 to GGC3 Po3
Export Templates		ISP_UIQINQSW02 - Traffic - Gi7/7 to GGC4 Po4
Configuration		ISP_UIOINQSW02 - Traffic - Gi7/8 to GGC4 Po4
Settings		LBTSLNE01 - Gi1/7 - SW ERICSSON SALINAS
Plugin Management		LBTSLNE01 · Gi2/11 · ### MPLS · LINK TO LBTSTEM01 · 100M · NGSDH · ###
Utilities		LBTSLNE01 · Gi2/3 · ### MPLS · LINK TO GYEFNSE01 G12/19 1G_NGSDH ###
System Utilities		LBTSLNE01 · Po2 · ### MPLS · LINK TO GYEPLYM01 · Po2 ###
User Management		LBTSLNE01 - G(2/1 - ### MPLS - LINK TO GYEPLYM01 - G(g) 1/32 - 1G - FO ###
Flow Viewer	1	ILB I SENEUT · GI2/20 · ### MPLS · LINK TO LB I SENM01 · GIQ 0/2 · 1G ###

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

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

🔰 Cacti		🚹 👻 🔂 🕤 🖃 👾 🎽 Página 👻 Seguridad 👻 Herramientas 💌 🚱 👻 🏸
console grap	hs npc GPS Map monitor weathermap	
Console -> Graph Trees -	-> (Edit) -> Graph Tree Items	Logged in as adm (Logout)
Create	Tree Items	
New Graphs Management	Parent Item Choose the parent for this header/graph.	AZUAY
Graph Management	Tree Item Type Choose what type of tree item this is.	Graph 💌
Graph Trees	Tree Item Value	
Devices	Graph Choose a graph from this list to add it to the tree.	INTERNET AZUAY DOWNSTREAM
Weathermaps	Round Robin Archive	Daily (5 Minute Average)
Collection Methods		Hourly (1 Minute Average)
Data Input Methods		Daily (5 Minute Average) cancel save
Templates		weeky (so minute Average)
Graph Templates		Yearly (1 Day Average)
Host Templates		

Figura 5.1.24: Actualización de gráficos^[1]

5.1.6 TAB GRAPH

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

5.1.6.1 VISUALIZACIÓN DE GRÁFICOS

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

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



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

5.1.6.2 EJEMPLO DE ANÁLISIS DE GRÁFICOS

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



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

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

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



Figura 5.1.27: Consumo semanal de internet^[1]

En estos gráficos se observa de manera más detallada el consumo de tráfico de internet de una semana, donde se puede observar que de lunes a jueves el pico de tráfico alcanzado es similar mientras que de viernes a domingo este disminuye, esto se debe al comportamiento de los clientes y a pesar que se puede generar un perfil puede haber días en los que los picos sean diferentes ya que depende del número de clientes conectados así como del tipo de uso que estos le den.

5.1.7 TAB MONITOR

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



Figura 5.1.28: Monitoreo de equipos^[1]

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



Figura 5.1.29: Estado de los host^[1]

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



Figura 5.1.30: Visualización de parámetros del equipo^[1]

5.1.8 TAB GPS MAP

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

Presenta tres opciones de visualización que se indican a continuación:

5.1.8.1 MAPA

En la parte izquierda del mapa se muestran dos opciones:

- 1. La primera opción permite reducir o ampliar el mapa.
- 2. La segunda opción permite realizar una vista panorámica de los nodos ya sea hacia la derecha, izquierda, arriba y abajo como se muestra en la figura 5.1.31:



Figura 5.1.31: Opción Mapa^[1]

5.1.8.2 SATÉLITE

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



Figura 5.1.32: Opción Satélite^[1]

5.1.8.3 **RELIEVE**

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



Figura 5.1.33: Opción Relieve^[1]

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



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

5.1.9 TAB WEATHERMAP

Permite generar esquemas de red donde se pueden añadir gráficos que CACTI tiene por defecto.
Para crear un nuevo Weathermap se debe seguir los pasos descritos a continuación:

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



Figura 5.1.35: Opción Editor^[1]

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



Figura 5.1.36: Selección del mapa a modificar^[1]

- 3. En la ventana que aparece a continuación se encuentran las siguientes opciones que permitirán administrar los mapas de las redes de mejor manera:
 - ✓ Change File: Permite escoger el nombre de un equipo para poder ser editado como se muestra en la figura 5.1.37
 - ✓ Add node: Permite añadir un nodo y colocar los datos correspondientes además incluye la opción para escoger la imagen deseada en la mapa ya sea un router, switch, nube,etc, como se muestra en la figura 5.1.37



Figura 5.1.37: Administración de mapas^[1]

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

	🧷 Pick a graph - Windows Internet Explorer 📃 🗖 🔀
	🙋 http://186.46.85.2/cacti/plugins/weathermap/cacti-pick.php?command=
Node Properties	Pick a graph:
Position 698 ,320	
Internal Name node03993	Host: Anv
Label	Filter: (case-sensitive)
Info URL /cacti/graph.php?rra_id	Set both OVERLIBGRAPH and INFOURL.
'Hover' Graph URL <mark>/cacti/graph_image.php</mark>	
Icon Filename images/cisco_catalyst_sw_cnt.PNG 👻	*INSTITUTO NACIONAL DE PREINVERSIA N - Traffic - VIA
Move Delete Clone Edit	"INSTITUTO NACIONAL DE PREINVERSIÃ"N - Traffic - VI446
This is where help appears for podes	*MIN DE MINAS Y PETROLEOS - Traffic - VI1
	*MIN DE MINAS Y PETROLEOS - Traffic - VI1522
	*MIN DE MINAS Y PETROLEOS - Traffic - VI1523
	*MIN DEFENSA NACIONAL - Traffic - Fa0/0.506
	*MIN DEFENSA NACIONAL - Traffic - Fa0/0.507
	*MIN DEFENSA NACIONAL - Traffic - Fa0/1
DA	*MIN RELACIONES EXTERIORES Y COMERCIO - Traffic -
	×
	😌 Internet 🦓 🕶 🔩 100% 💌 🔬

Figura 5.1.38: Opción Pick from^[1]

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



Figura 5.1.39: Opción Add Link^[1]

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

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

Map Properties					
					Cancel Submit
Map Title	MPLS LOS	S RIOS			
Legend Text	Traffic Loa	ad			
Timestamp Text	Created: 9	%b %d %Y	%H:%M		
Default Link Width	2	pixels			
Default Link Bandwidth	1G	bit/sec in,	1G	bit/sec out	
Map Size	800	× 600	pixels		
Output Image Filename					
Output HTML Filename					
Background Image Filename	NONE				~
This is where help appears fo	r maps				

Figura 5.1.40: Opción Map Properties^[1]

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

Map Style		
	Cancel Sul	bmi
Link Labels	Percentage 🛩	
HTML Style	Overlib (DHTML) 💌	
Arrow Style	Classic 🔽	
Node Font	3 (GD builtin) 💌	
Link Label Font	2 (GD builtin) 💌	
Legend Font	4 (GD builtin) 💌	
	Abc123% Abc123% Abc123% Abc123% Abc123%	
Font Samples:	Font 1 Font 2 Font 3 Font 4 Font 5	
	(Drawn using your PHP install)	
Helpful text will	appear here, depending on the current item selected. It should wrap	
onto several ini		

Figura 5.1.41: Opción Map Style^[1]

- ✓ Manage Colors: Ésta opción no se encuentra habilitada todavía en la plataforma. Permite administrar los colores de cada uno de elementos insertados en el mapa.
- ✓ Manage images: Esta opción no se encuentra habilitada todavía. Permite administrar las imágenes insertadas en el mapa.
- ✓ Editor settings: Es un editor de configuraciones dependiendo de los requerimientos.

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



Figura 5.1.42: Opciones del Weathermap^[1]



Figura 5.1.43: Ejemplo de un mapa creado^[1]

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

5.1.10 TAB NPC

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

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



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

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

5.1.10.1 HOSTS

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

console graphs n	ectar npc	Cereus monitor	clog thold	GPS Map weath	ermap	settings	
Nagios Status Nagios Notifications On Enabled	Host Checks Service C Enabled Enable	Host Status Sur hecks Down	umary Unreachable U 0 3	p Pending 0	Service Status Summar Critical Warning	Unknown Ok	es admin (Logo Pending D
avigation 😽	Deshboard Senices	Hosts ^					
Monitoring	Hosts × Host Problems	B Hostgroup Overview 8	Hastgroup Grid 🖾				
Mosts	Host . St	Gr. Lest Check 2011-04-08 09:50	Viext Check	Pugin Output ECO OK - Paquetes perdidor	a - 0%, RTA - 0.86 ma		
mil Hostgroup Overview	AGENCIA NACIONAL POSTAL						
Services	DRECTOR GENERAL SRI	2011-04-08 09:50	50 2011-04-08 09:56:00	ECO OK - Paquetes perdidor	a = 0%, RTA = 0.96 ma		
Service Problems	EMPRESA NACIONAL DE FARMACOS	2011-04-08 09:51	00 2011-04-08 09:58:14	ECO OK - Paquetes pertition	a = 0%, RTA = 0.59 ma		
(IIII) Comments	gateway	2011-04-08 09:49	50 2011-04-08 09:55:00	ECO OK - Paquetes perdidor	s = 0%, RTA = 0.03 ms		
Im Scheduled Downtime	GERENTE FONDO	2011-04-08 09:51	00 2011-04-08 09:58:14	ECO OK - Paquetes perdidor	s = 0%, RTA = 0.76 ms		
Reporting ILN2C	GERENTE GENERAL BEDE	2011-04-08 09:50	40 2011-04-08 09:55:50	ECO OK - Paquetes perdido	s = 0%, RTA = 0.96 ms		
II Nagos	NCOP	2011-04-08 09:50	00 2011-04-08 09:55:10	ECO OK - Paquetes perdidor	s = 0%, RTA = 0.58 ms		
	iccahost	2011-04-08 09:50	2011-04-08 09:55:10	ECO OK - Paquetes perdidor	s = 0%, RTA = 0.02 ms		
		2011-04-08 09:50	40 2011-04-05 09:55:50	ECO OK - Paquetes perdidor	s = 0%, RTA = 0.50 ms		
	MN. COORDINACION SEG. INTERNA	2011-04-08 09:50	40 2011-04-08 09:55:50	ECO OK - Paquetes perdidor	a - 0%, RTA - 0.94 ma		
	MN.	2011-04-08 09:50	30 2011-04-08 09:55:40	ECO OK - Paquetes perdidor	s = 0%, RTA = 0.78 ms		
	C Seach	× 0				, Do	playing 1 - 10 of

Figura 5.1.45: Opciones Hosts de Nagios^[1]

5.1.10.1.1 HOST

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

console graphs ne	ctar npc Cer	eus monitor	clog thold	GPS Map weathermap	Settings P
Nagios Status Nagios Notifications On Enabled	Host Checks Service Check Enabled Enabled	Host Status Summa	Unreachable Up 0 32	Pending Critical Warni 0 1 1	ng Unknown Ok Pendin 2 93 0
avigation स	Dashboard Services	losts ×			
Monitoring	Hosts × Host Problems (3)	Hostgroup Overview (2) Host	group Grid 🕄		
House H	Host . Sta.	Or Last Check 2011-04-08 09:50:50	Next Check 2011-04-08 09:56:00	Plugin Output ECO OK - Paquetes percisios = 0%, RTA = 0.85 ms	
Mostgroup Grid	DIRECTOR GENERAL SRI	2011-04-08 09:50:50	2011-04-08 09:56:00	ECO OK - Paquetes percidos = 0%, RTA = 0.86 ms	
	NACIONAL DE	2011-04-05 98(51)-04	2011-04-06 09:56:1+	ECO OK - Paquetes percidos + pro, ktiel + piso me	1
JIII Status Map JIII Convients	pateway	2011-04-08 09:49:50	2011-04-08 09:55:00	ECO OK - Paquetes perdidos = 0%, RTA = 0.03 ms	
IIII Scheduled Downtine IIII Process Information IIII Event Log	GERENTE FONDO SOLIDARIDAD / MINTEL	2011-04-08 09:51:00	2011-04-08 09:58:14	ECO OK - Paquetes perdidos = 0%, RTA = 0.78 ms	
Reporting In N2C	GERENTE GENERAL BEDE	2011-04-08 09:50:40	2011-04-08 09:55:50	ECO OK - Paquetes perdidos = 0%, RTA = 0.96 ma	
II yagoa	NCOP	2011-04-06 09:50:00	2011-04-08 09:55:10	ECO OK - Paquetes perdidos = 0%, RTA = 0.58 ms	
	localhost	2011-04-08 09:50:00	2011-04-08 09:55 10	ECO OK - Paquetes perdidos = 0%, RTA = 0.02 ms	
	AORICULTURA	2011-04-08 09:50:40	2011-04-08 09:55:50	ECO OK - Paquetes perdidos = 0%, RTA + 0.50 ms	
	MR. COORDINACION SEG. INTERNA	2011-04-08 09:50:40	2011-04-08 09:55:50	ECO OK - Paquetes perdidos = 0%, RTA = 0.94 ms	
		2011-04-08 09:50:30	2011-04-08 09:55:40	ECO OK - Paquetes perdidos = 0%, RTA = 0.78 ms	
	Provide Statements	200			Distances 1 -

Figura 5.1.46: Visualización del estado del host^[1]

5.1.10.1.2 HOSTSGROUP PROBLEMS

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

D Cacti							👌 • 🖻	· 🗆 🌐	• Página • S	ieguridad + He	erramientas 🕶 🔞 🕶
console graphs ne	ectar npc	Cereus	monitor	clog t	thold	PS Map wea	thermap		sett	Logged in a	s admin (Logout)
Nagios Status			Host Status Sumr	nary			Service State	is Summary			
Nagios Notifications On Enabled	Host Checks Ser	vice Checks Enabled	Down 1	Unreachable 0	Up 32	Pending 0	Critical 1	Warning 1	Unknown 2	Ok 93	Pending 0
Ravigation Key Implementation Implementation Implementation Implementation	Denhoerd Servi	StaGr	2011-04-08 09:59:10	Next Check 2011-04-08 10:	Pugi 0420 ECO	i Outout	. perdicios + 100%				

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

5.1.10.1.3 HOSTSGROUP OVERVIEW

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

console graphs pecta					CD CD alle	Fayilla + Degui	uau • rierranilerkas • 🐨
	npc Cereus mo	nitor clog	thold GPS N	lap weathermap		settings	gged in as admin (Logout)
Nagios Status Nagios Notifications On Enabled Navigation C	Host Checks Service Checks Dr Enabled Enabled	tatus Summary own Unreachable 1 0	Up 32	Pending Critical 0 1	tatus Summary Warning 1	Unknown 2	Ok Pending 93 0
Montoring Hosts Mosts Mosts	Hosts 🕮 Host Problems 🕮 Hostgroup Over Host 🛦	rview × Hostgroup Grid 🙁 Status	Critical	Warning	Unknown	Ok	Pending
Hostgroup Overview Hostgroup Grid Services Services	AGENCIA NACIONAL POSTAL DRECTOR GENERAL SRI	•	0	0	0	3	0
Service Problems G Servicegroup Overview G Servicegroup Grid	GERENTE FONDO SOLIDARIDAD / MINTEL GERENTE GENERAL BEDE NCOP	•	0 0	0 0 0	0 0	3 3 3	0 0 0
Comments Comments Scheduled Downtime Process Information Event Log	IIN. AGRICIU TURA IIN. COORDINACION SEG. INTERNA IIIN. COORDINADOR DE LA POLITICA INTERNA		0	0 0	0	3	0
Reporting Naglos	MN. CULTURA MN. DE AMBIENTE MN. DE COORDINACION GABINETE DE LO SECT.		0	0	0	1 3 3	0
9 (c	pateway ocalhost	•	0	0	0	1	0

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

5.1.10.1.4 HOSTSGROUP GRID

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

🗿 🕢 🔹 🔰 http://186.46.85.2/cor			💌 🗟 🎋 🗙 🛃 scope	
wohivo Edición Ver Favoritos Her	rranientas Avuda			
Favoritos	CS @ ISC @ IPTV @ Wheelb CNT	Calculadora IP - IP Submetting A Source & BRAS Autoritización de um	arios 🔐 AUDS 🖉 ITELLIN 🦳 Cacti 🛸 Option Looking Glass	
in cas			A . El . Cl an . Biena . Securitad . Here	miertas +
console graphs ne	ctar npc Cereus	monitor clog thold GPS Map wea	thermap settings 💡	M
			Legged in as i	admin (Lo
Ragios Status		Host Status Summary	Service Status Summary	
Nagios Notifications	Host Checks Service Checks	Down Unreachable Up Pending	Critical Warning Unknown Ok	Pending
On Enabled	Enabled Enabled	0 32 0	1 2 85	0
Navigation 🕿	Destboard Services C Hosts ×			
a 📴 Nentering	Hastarous Grid *			
a lis Ress	Contraction of the local distance of the loc	Deschart		_
IIII Hoata	191 A 0000	Page Output		
III) Hostproup Overview	Host Group: All Servers (15 Hosts)			
Hostgroup Grid	DSTAL	ELU UK - Hagsetes perdicos + UN, RIA + USI Ins		
A TO Services	RECTOR GENERAL SRI	ECO OK - Paquetes perdidos = 0%, RTA = 0.99 ms		
IIII Dervices	ENPRESA NACIONAL DE	ECO OK - Paquetes perdidos = 0%. RTA = 0.54 ms		
I Servicegroup Overview	GERENTE FONDO	ECO OK - Paquetes perdidos = 0%. RTA = 1.11 ms		
Servicegroup Grid	SOLDARDAD / HINTEL			
IIII Status Map	GERENTE GENERAL BEDE	ECO OK - Paquetes perdidos = 0%, RTA = 0.95 ms		
Comments	NCOP O	ECO OK - Paquetes perdidos = 0%, RTA = 0.74 ms		
Process Information	MN. AORICULTURA	ECO OK - Paquetes perdicios = 0%, RTA = 0.56 ms		
JELEvent Log	NNL COORDINACION SEG.	ECO OK - Paquetes perdidos + 0%, RTA + 0.69 ms		
Reporting	NNL COORDNADOR DE LA	ECO OK - Paquetes perdicios + 0%, RTA + 0.74 ms		
Nagios	NNL CULTURA	ECO OK - Paquetes perdidos = 0%, RTA = 0.70 ms		
	MRL DE AMBENTE	ECO OK - Paquetes perdidos = 0%, RTA = 0.84 ms		
	MRL DE COORDNACIÓN GABNETE DE LO SECT.	ECO OK - Paquetes perdidos = 0%, RTA + 0.45 ms		
	INN. DE COORDNICACIÓN DE SECT. ESTR.	ECO OK - Paquetes perdidos + 0%, RTA + 0.93 ms		
	gateway 🕒	ECO OK - Paquetes perdidos = 0%. RTA = 0.03 ms		
	incalitost 6	ECO OK - Paquetes pertitios = 0% RTA = 0.02 ma		

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

5.1.10.2 SERVICES

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

5.1.10.2.1 SERVICES

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

Services	Servicegroup Overviev	v 🖾 🛛 Serv	ice Probl	lems 🖾
Host 🔺	Service	Status	Graph	Plugin Output
AGENCIA NACIONAL POSTAL	DATOS AGENCIA NACIONAL POSTAL INTERMINISTERIAL	•		SNMP OK - up(1)
×	PING	•		ECO OK - Paquetes perdidos = 0%, RTA = 1.10 ms
AGENCIA NACIONAL POSTAL			_	
×	Uptime	•	L	SNMP OK - Timeticks: (3838642006) 444 days, 6:53:40.06
AGENCIA NACIONAL POSTAL				

Figura 5.1.50: Servicios activos en Nagios^[1]

5.1.10.2.2 SERVICES PROBLEMS

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

Gacti								6 • 6	· 🖻 🖶	▼ Página ▼ S	Seguridad + P	ierramientas + 🔞 +
console g	raphs ne	ctar np	c Cereus	monitor	clog	thold	GPS Map	eathermap		sett	ings	
											Logged in	as admin (Logout)
Nagios Status				Host Status Sur	nmary			Service Stat	us Summary			
Nagios	Notifications	Host Checks	Service Checks	Down	Unreachable	Up	Pending	Critical	Warning	Unknown	Ok	Pending
On	Enabled	Enabled	Enabled	0	0	33	0	0	1	0	96	0
Navigation	Navigation 🕅 Jashboard Services × Hosts 🖄 N2C 🕄 Naglos 🖾 Event Log 🖏 Process Info 🖏 Scheduled Downtine 🖏 Comments 🖏 Status Map 🖓											
🖨 🔚 Monitoring		Services 🕄 🔍	ervice Problems ×	Servicearoup Over	view 8 Servicearr	oup Grid 🖾						
Hosts	lems	Host + Se	rvice	Status Graph P	Augin Output						Notes	
- Hostgroup - Hostgroup	o Overview o Grid											
🕀 📴 Services												
- E Services												
- Service P	oblems											

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

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

5.1.10.3 PROCESS INFORMATION

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

Cacti - Windows Internet Explo	er 👘		
🔄 🕞 🔻 🔰 http://186.46.85.2/ca			💌 🗟 🕂 🗶 🛃 Google
erchivo Edición Ver Favoritos He	erramientas Ayuda		
Enverting	And R 192 R 1979 Whatel to CNT	Cale dations 10 - 10 Submettions (2) Stored (2) REAS (2) at	Analization de constantes 🖓 ANTS 🔊 TERLEN 🔛 Cardi 🗞 Ordens Londinos Glass
Lauras 30 Busican 61	12 6 DC 6 FLL 6 History on 1	Cachagara is - is providential for this and the	
Cacti			🖬 * 🖸 🛛 🔚 🐺 • Páginā • Segundau • Herramenkas • 📲
console graphs pe		monitor clog theid GR	Settings
console graphs in	ctar npc cercos	monitor clog those or	S Map weathermap Sectings and Longer in as admin (Longer in as admin (Longer in as admin (Longer in as admin (Longer in a statistical section
Nagios Status		Host Status Summary	Service Status Summary
Nagios Notifications	Host Checks Service Checks	Down Unreachable Up	Pending Critical Warning Unknown Ok Pending
On Enabled	Enabled Enabled	0 0 33	0 1 0 <mark>96</mark> 0
Savigation 📧	Dashboard Services 🔅 Hosts	□ N2C □ Nagios □ Event Log □ Process Info ×	Scheduled Downtime 🖾 Comments 🖾 Status Map 🖾
a 🔚 Monitoring	Parameter	Value	
🗃 🚞 Hosts	Naglos Version	32.0	
Hosts	instance D	1	
Host Problems	Process ID	2609	
Hostgroup Overview	Status Update Time	2011-04-08 10:39:26	
nosgroup one	Program Start Time	2011-04-06 09:47:19	
Services	Program Stop Time	NA	
	Last External Command Check	2011-04-08 10:39:26	
	Last Log Rotation	2011-04-08 00:00:00	
	Notifications Enabled	J.	
- Status Map	Active Service Checks Enabled		
Commenta	Passive Service Checks Enabled		
	Active Host Checks Enabled		
Process information	Passive Host Checks Enabled		
a ma Reporting	Event Handlers Enabled	*	
- mn N2C	Even Polastics Enabled		
Nagios	Plap Deteccon Enabled	×	
	Processing Performance Lata	*	
	Obsess Over Hosts	×	

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

5.1.10.4 EVENT LOG

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

🔰 Catti								🙆 • 🖻	· • 🖶	▪ Página • :	Seguridad + He	erramientas 🔹 🔞 🔹
console grap	hs ne	ctar npc	Cereus	monitor	clog	thold G	PS Map weat	hermap		sett	ings	
Nagios Status				Host Status Sum	mary			Service Stat	us Summary			
Naglos On	Notifications Enabled	Host Checks Se Enabled	ervice Checks	Down 0	Unreachable 0	Up 33	Pending 0	Critical 0	Warning 1	Unknown 0	0k 96	Pending 0
Ravigation Khorking Koots Koots Kastyno Dr. Kastyno	erview d Dverview Grid Sind	Dathbard Ser Date 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.05 10. 2011.04.06 10. 2011.04.06 10. 2011.04.06 10. 2011.04.06 10. 2011.04.06 10.	Vides All Hosts Al	NIZC (3) Nagios fry DE ALERT: MIN. ECON NOTFICATION: admin ALERT: MIN. ECON MIN. ECON DE ALERT: MIN. ECON ave of retention data DE ALERT: MIN. ECON DE ALERT: MIN. ECON DE ALERT: MIN. ECON DE ALERT: Mocanosi, DE ALERT: MOCANOSI, MIN. MIN. MIN. MIN. MIN. MIN. MIN. MIN.	Comparent Log > Comparent Log	PROCESS INFO 33 PROCESS INFO 33 PROCESS INFO 34 PROCESS INFO 34 PROCES	Scheduled Downter 0 OK - Paquetes percent obt hu any ECO OK aquetes perdidos = 0 ⁴ NIZAS:0K:HARD;1;5N obt/y-service-by-am CS AVS0:254 procet S AVIS0:254 procet S AVIS0:253 procet	Comments Com	33 Status Ma 0.57 ma - a = 055, DTA = 1 - 068 = 0%, RTA = - 54 procesos - 54 procesos -	р 23 9.57 ma 0.57 п		
N2C		0 2011-04-08 08: ∅ 2011-04-08 08: ▲ 2011-04-08 08: ♠ 2011-04-08 08: ♠ 2011-04-08 08:	47:20 Auto-s 14:50 SERVIX 13:50 SERVIX 48:56 SERVIX	ave of retention data CE ALERT: localhost;7 CE ALERT: localhost;7 CE NOTIFICATION: roc	completed success Total Processes;OK; Total Processes;WA ot;localhost;Total Pro	fully. SOFT;2;PROCS ACE RNING;SOFT;1;PROC cesses;OK;notify-se	PTAR: 247 procesos CS AVISO: 251 proces ervice-by-email;PROC!	sos S ACEPTAR: 247 p	rocesos			

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

5.1.10.5 REPORTING

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

Decti		🦄 🔹 🔝 🕤 🚍 💌 Página - Seguridad - Herramientas - 🚷 -
console graphs nectar npc Cereus	monitor clog thold GPS Map we	eathermap settings S and A
Nagios Status Nagios Notifications Host Checks Service Checks	Host Status Summary Down Unreachable Up Pending	Service Status Summary Critical Warning Unknown Ok Pending
Unit Leaders Leaders Leaders Lavegation (*) Deskboord Not C (*) Rayoux (*) Controls Interference (*) Deskboord Not C (*) Rayoux (*) Interference Interference (*) Deskboord Not C (*) Rayoux (*) Interference Interfere	Contrasería: es 1964-66.85.2 (P) El servidor 1964-66.52 en llagos Access require un nombre de usuaro y una contrasería. Adventerios: esta servidor está solcitando que su nombre de dutenticación básica sin conexión esgura). Usuario: Usuario: Contrasería: Recordar contrasería	

Figura 5.1.54: Ingreso a la plataforma Nagios^[1]

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

5.1.11 TAB THOLDS

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

5.1.11.1 THRESHOLDS

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

🖉 Console -> Thresholds - Windows Internet	Explorer						_ • ×
🔄 🕞 🔻 🔰 http://186.46.85.2/cacti/plugins/thol	d/thold_graph.php?tab=thold		v 🗟 (🔊 🗙 🚼 Google			P -
Archivo Edición Ver Favoritos Herramientas	Ayuda						
🖕 Favoritos 🛛 🍰 🔰 New Cacti 🖉 ACS 🙋 ISC	🦲 IPTV 🙋 WhatsUp CNT 胆 Calculadora IP	- IP Subnetting 😹 Spyral 🙋 BRAS 😣 Au	tenticación de usuarios 📓 AXIS 🙋	, ITELLIN 📴 Cacti 🔌	Optus Looking Glass	5	»
🙁 🔹 🔰 Console -> Thresholds 🛛 🗙 🔰 Cacti - V	Weathermap - BRAS		🟠 • 🖻	- 🖃 🌐 - Página	a + Seguridad + F	Herramientas	• 🔞 •
console graphs nectar	npc Cereus monitor	clog thold GPS	Map weathermap		settings	PE	
Console -> Thresholds					Logged	J in as admir	n (Logout)
Thresholds Host Status							
Threshold Status							
Template: All 💽 Status: Trigger	:ed 💙 Rows: 30 💙 Search:	go clear					
de Bravious		Showing Rows 1 to 2 of	2[1]				Next >>
Actions Name**				Type High	Low Cu	urrent	Enabled
MIN. AGRICULTURA - Traffic - 10.80.60	.2 - 3i1/26.1506 [traffic_in]		3	Aigh/Low 1.5	21	1832.7333	Enabled
MIN. AGRICULTURA - Traffic - 10.80.60	.2 - 311/26.1506 [traffic_out]		4	Aigh/Low 1.5	13	5288.8233	Enabled
<< Previous		Showing Rows 1 to 2 of	2 [1]				Next >>
Alarm	Warning	Notice	Ok		Disal	bled	
Time: 0.01 seconds, User: 0.01 seconds, System	: 0 seconds, Swaps: 0 swaps, Pages: 0 pa	iges					

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

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

🙁 🔹 🔰 Console -> Three	holds 🛛 🗴 🔰 Cacti - Weathermap - BRAS	🏠 * 🔊 - 🖃 🌐 Y Página + Seguridad + Herramientas + 😢 + 🎽					
console graph Console -> Thresholds	ns nectar npc Cereus monitor clog thold	GPS Map weathermap Logged in as admin (Logout)					
Create New Graphs Management Graph Management Graph Trees Data Sources Devices Thresholds Weathermaps	Data Source Description: MIN. ACRICULTURA - Traffic - 10.80.60.2 - GI1/26.1506 Associated Graph (graphe that use this RRD): 17 - MIN. AGRICULTURA - Traffic - GI1/26.1506 V	HIN. AGRICULTURA - Traffic - Gil/26.1506					
Data Queries Data Input Methods	1: traffic_in 2: traffic_out Hi: 1.5 Lo: n/a BL: off Hi: 1.5 Lo: n/a BL: off Data Source Item (traffic in) - Current value: [27219.8862]						
Templates Graph Templates Host Templates Data Templates	Template settings Template settings Template Propagation Enabled Whether or not these settings will be propagates from the threshold template.	Template Propagation Enabled					
Threshold Templates Map Templates Import/Export	Mandstory settings Threshold Name Provide the Thold a meaningful name Threshold reakhor	MIN. AGRICULTURA - Traffic - 10.80.60.2 - Gi1					
Import Templates Export Templates	Whether or not this threshold will be checked and alerted upon. Weekend Exemption If this is checked, this Threshold will not alert on weekends.	Threshold Enabled Weekend Exemption					
Settings Plugin Management	Disable Restoration Email If this is checked, Thold will not send an alert when the threshold has returned to normal status. Threshold Type	Disable Restoration Email					
System Utilities User Management	The type of Threshold that will be monitored. High / Low Sattings High Threshold	High / Low Values					
Logout User NMID Manage Reports	If set and data source value goes above this number, alert will be triggered Low Threahold If set and data source value goes below this number, alert will be triggered						
Backup/Restore Support Info	Breach Duration The amount of time the data source must be in breach of the threshold for an alert to be raised. Data Manipulation	5 Minutes V					
	Data Type Special formatting for the given data. Other setting	Exact Value 🗸					
T	Repeat sider the amount of time has pasted since the last alert. Notify account for the second side of the s	Never V					

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

5.1.11.2 HOST STATUS

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

😁 🔹 🔰 Console -> Thresholds	🗙 🔰 Cacti - Weathermap - BRAS	i					<u>a</u>	• 🗟 · 🖻 🌐 •	Página • Segurio	ad • Herrar	nientas • 🔞 •	. ×
console graphs	nectar npc	Cereus monitor	clog		thold	GPS Map	weathermap		settings	ged in as a	dmin (Logout)
Thread all a literate Charles												
Device Status												
	Status: Not Lin	Search				go cle	ar					
// E.B.												4
<< Previous			Sh	nowing R	lows 1 t	o 29 of 29 [1]	1				Next >>	
Actions Description**		1	D (D Graphs S	ata ources S	itatus	Event Count	Hostname	Current (ms)	Average (ms)	Availability	
*EMPRESA NACIONAL DE	FARMACOS ENFARMA	E	80 8	0 0	L. L	Inknown	0	10.80.75.1	0	0	100	
INCOP *INCOP		7	6 (0 0		Inknown	0	10.80.5.1	0	0	100	
INSTITUTO NACIONAL I	E PREINVERSIÓN	8	33 .	3 3		lown	236	10.80.38.1	1.48	1.65	9.2	
MIN DE DESARROLO UR	BANO Y VIVIENDA	9	95 (0 0		Inknown	0	10.80.8.1	0	0	100	
CEMPRESA NACIONAL DE	FARMACOS ENFARMA	8	31 (0 0	L. L	Inknown	0	201.219.62.77	0	0	100	
CINSTITUTO NACIONAL	DE PREINVERSIÓN	e	35 4	0 0		Inknown	0	201.219.62.156	0	0	100	
MIN DEFENSA NACIONA		9	94 (0 0	, u	Inknown	0	190.152.88.250	0	0	100	
MIN. DE COORDINACIÓ	N DE POLÍTICA ECONÓMICA	9	93 (0 0	L. L	Inknown	0	201.219.62.165	0	0	100	
MIN. INCLUSION ECON	MICA Y SOCIAL	7	5 (0 0	, c	Inknown	0	190.152.88.233	0	0	100	
@MIN.CULTURA		7	18 4	0 0	L. L	Inknown	0	190.152.88.237	0	0	100	
MINISTERIO DE AMBIEN	те	9	9 (0 0		Inknown	0	201.219.62.54	0	0	100	
@PRESIDENCIA DE LA RE	PUBLICA	7	11 (0 0	L. L	Inknown	0	201.219.63.129	0	0	100	
REGISTRO CIVIL		9	90 4	0 0		Inknown	0	201.219.40.2	0	0	100	
SECRETARIA DE INTELI	SENCIA	e	36 (0 0	L. L	Inknown	0	201.219.62.32	0	0	100	
BANCO CENTRAL		5	57 (0 0	c	Disabled	0	10.80.73.161	0	0	100	
CONTRALORIA GENERAL	DEL ESTADO	e	ie :	1 1	0	lown	5	10.80.73.85	1.25	19.66	53.83	
DIR. GENERAL DEL CONS	JO NACIONAL	3	35 (0 0	c	lisabled	0	10.80.73.25	0	0	100	11
INEC INEC			56 (0 0	c	Disabled	0	10.80.73.153	0	0	100	
MIN. COORDINADOR DE	A POLITICA INTERNA	4	ie :	1 1	0	Down	5	10.80.73.93	2.75	3.78	67.57	
MIN. DE JUSTICIA		4	8	1 1		Down	3	10.80.73.109	2.18	2.59	67.04	
MIN. DEL LITORAL		2	20 4	0 0	c	lisabled	0	10.80.18.1	0	0	100	
MIN. DESARROLLO URBA	NO Y VIVIENDA	:	10 0	0 0	c	Disabled	0	10.80.69.2	0	0	100	
MIN. ELECTRIFICACION	ENERGIAS RENOV.	2	21 (0 0		isabled	0	10.80.63.1	0	0	100	
MIN. TRABAJO Y EMPLEO		:	5 (0 0	c	Disabled	0	10.80.13.1	1.08	1.34	96.55	
POLICIA NACIONAL			52 (0 0		isabled	0	10.80.73.141	0	0	100	
PRESIDENTE DIRECTORI	0 GYE 8000	4	11 0	0 0	c	Disabled	0	10.80.73.53	0	0	100	
SEC. NACIONAL DE TRAN	PARENCIA	2	28 3	1 1		lown	621	10.80.70.2	5.48	13.75	0.7	
SEC NACIONAL PLANTETO	ACTON - RACKUP	-	6 1	0 0		licablad	0	10 80 68 2	0	0	100	~

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

5.1.12 TAB CLOG

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

😤 🔹 🔰 Casti		🗙 🚺 Cacti	Weathern	nap - BRAS									0 · 6	· 🖾	👘 • Pi	igina • Se	guridad -	Herramient	:as + 🔞 ·
console	graphs	nectar	npo	Cere	us mo	onitor	clog	th	bld	GPS M	ap	eatherm							
ien Cacti Log																	2	Logged in	as admir
Log File Filter	s										-	-							-
Tail Lines:	500 Lines	Message Ty	Al		Go Clea	er Purge	1		_										
Refresh:	1 Minute	 Display Ord 	TI N	ewest First 💌			-												
Search/Recext	-																		
I am Film (Tata)	10000 500	A design a design of	o Other	Tiber in Alle	5														
4/08/2011 11:1	15-20 4M - W	FATHERMAD: Dolla	TO1 STA	TS: Weathern	0.974 (10)	complete :	Eri 08 And	11.11.35	20 -0500-	53 mea		10.74	roade uit	R installe					
04/08/2011 11:1	35:20 AM - W	EATHERMAP: Polle	r[0] [Ma	p 8] PRES1111	Wrote map to	to /usr/share	re/cacti/site	/plugins/w	athermag	o/output/s	caffb95c3	753de79	Seel.ong						
and /usr/share/c	cacti/site/plug	ins/weathermap/e	utput/ca	ffb95c3753de7	H66e1.thumb	p.png													
04/08/2011 11:3	35:20 AM - W	EATHERMAP: Polk	(0) (Ma;	p 8] PRES111/	4bout to write	e image file	e. If this is	the last m	issage in ;	your log.	increase	memory	limit in p	hp.ini [Wa	(POLL01]				
04/08/2011 11:1 1./usr/share/cad	35:20 AM - W ti/site/plugins	EATHERMAP: Poll- /weathermap/out	Jut/ceffb	p 8] PRE\$1111 /95c3753de796	Aep: /usr/sh Jel.png	iare/casti/ait	ite/plugins/	/weatherma	p/configs/	/PRES111	··> /uer/	ibare/ca	ti/site/plu	pins/weat	hermep/o	utput/caff	b95c3753	de7966e1.	.html
04/08/2011 11/3 and /usr/share/s	35:20 AM - W cacti/site/plug	EATHERMAP: Polisina/weathermap/s	r[0] [Mas utput/do	p 9] PRES12: V 359782ada6e	rote map to of998.thumb	/usr/share/ b.png	/cacti/site/p	plugins/wes	ithermap/i	output/cf	0369782	ada6e30	998.png						
4/08/2011 11:1	35:19 AM - W	EATHERMAP: Polle	r[0] [Mag	p 9] PRES12: A	bout to write	image file.	. If this is th	he last me	usage in yo	our log, i	increase r	nemory_	imit in ph	p.ini (WM	POLLS:]				
4/08/2011 11:1 k/usr/share/cad	25:19 AM - W ti/site/plugins	EATHERMAP: Polle	r[0] [Mag sut/cf03b	p 9] PRES12: 5 9782ada6e30	ep: /usr/sha 998-png	ere/cecti/site	e/plugins/w	eathermap	/configs/P	PRES12 ->	> /usr/sh	ere/cecti/	site/plugi	s/weathe	map/out	put/cf03b1	782ede64	e30f998.ht	tml
04/08/2011 11:3 and /usr/share/o	35:19 AM - W catti/site/plug	EATHERMAP: Polle	r[0] [Map utput/e4	p 10] PRE513: 43e84ad92980	Wrote map to 873d22.thum	to /usr/share	re/cacti/site	/plugins/w	iethermap	o/output/e	e443e84;	d9298c8	73d22.pn						
4/08/2011 11:1	35:19 AM + W	EATHERMAP: Pole	[0] [Mar	p 10] PRES13;	About to write	e image file	e. If this is	the last m	assage in r	your log.	increase	memory	limit in p	hplini (sus	(POLL01]				
14/08/2011 11:3 //usr/share/cad	35:19 AM - W ti/site/plugins	EATHERMAP: Polic /weathermap/out	r[0] [Mag aut/e443	p 10] PRES13: Je84ad9298c87	Mapi /usr/sh 3d22.png	nare/cacti/sit	ite/plugins/	weatherma	p/configs/	PRES13	-> /usr/s	nare/cact	/site/plug	ins/weath	ermap/ou	tput/e443	e84ad929	P8c873d22	.html
04/08/2011 11:3 end /uar/share/c	35:19 AM - W cecti/site/plug	EATHERMAP: Polk ins/weathermap/r	(0) (Mas utput/42	p 11) PRES15: 6367436568:5	Wrote map 5 01197d.thum	to /usr/share nbipng	e/cacti/site	t/plugina/w	athermap	p/output/4	42636743	b5dBc50	1197d.pn	\$					
4/08/2011 11:1	35:19 AM - W	EATHERMAP: Polle	r[0] [Mar	p 11] PRES15:	About to write	e image file	e. If this is	the last m-	assage in .	your log.	increase	memory	limit in p	hp.ini [Wi	POLL01]				
/4/08/2011 11:1 /usr/share/cad	35)19 AM - W ti/site/plugins	EATHERMAP: Polic //weathermap/out	(0) [Mag out/42b3	p 11] PRES13: 674355d8:501	Mapi /usr/sh 197d.png	are/cacti/s?	ite/plugins/	/weatherma	p/configs/	PRESIS -	-> /usr/s	hare/cact	/site/plug	ins/weath	ermag/ou	tput/42b3	67435568	lc301197d	.html
4/08/2011 11:1 and /usc/share/c	35:19 AM - W cacti/site/plug	EATHERMAP: Polk ins/weathermap/r	r[0] [Ma; utput/72	p 12] PRES16: (b63e4f9439tb	Arote map b fa129.thumb	to /ust/share b.png	e/cacti/site	e/plugins/w	athermap	o/output/1	72663+4	9439cb7	a129.png						
4/08/2011 11:3	35119 AM - W	EATHERMAP: Polle	r[0] [Map	0 12] PRES16:	About to write	is image file	e. If this is	the last m	issage in i	your log.	increase	memory	limit in p	hp.ini [Wi	(POLLO1]				
04/08/2011 11:3 //usr/share/cad	35:19 AM - W ti/site/plugins	EATHERMAP: Polls /neathermap/out	r[0] [Mag aut/72b6	p 12] PRES16: 3+4/9439cb7/s	vtap: /usr/sh 129.png	iare/cacti/s?	ite/plugins/	/weatherma	p/configs/	PRES16	-> /usr/s	hare/cact	/site/plug	ins/weath	ermap/ou	tput/72b6	3e4f9439	cb7fa129.)	html
4/08/2011 11:1 nd /usr/share/c	35:19 AM - W cscti/site/plug	EATHERMAP: Polk ins/weathermap/r	r[0] [Ma: utput/s4	p 13] PRES14: 61158462f2c3	Wrote map b 3633c.thumi	o /ust/shere b.ong	e/cacti/site	e/olugins/w	athermap	p/output/s	a461158-	+62f2c33	1633c.png						
4/08/2011 11:1	35:18 AM - W	EATHERMAP: Polle	r[0] [Mas	p 13] PRES14:	About to write	e image file	e. If this is	the last m-	assage in i	your log.	increase	memory	limit in p	p.ini (wa	(POLLO1]				
04/08/2011 11:3 //usr/share/cad	35:18 AM - W ti/site/plugins	EATHERMAP: Polls	(0) [Mas out/#461	p 13] PRES14: 158462f2:333	Aap: /uar/ah 33c.png	are/cacti/si	ite/plugins/	weatherma	p/configx/	PRES14 -	-> /ust/s	hare/cact	/site/plug	ins/weath	ermap/ou	tput/a461	158462/2	t333633t.)	html
4/08/2011 11:1 nd /usr/share/c	35:18 AM - W cacti/site/plug	EATHERMAP: Polis ins/weathermap/o	/[0] [Mag utput/cl/	p 14] PRES17: 81743fa53b1a	Wrote map to b2d78.thum	.o /ust/share ib.png	re/cacti/site	s/plugins/w	.ethermap	p/output/o	c181745f	e53b1e5	2d78.png	0					
4/08/2011 11:1	35:18 AM - W	EATHERMAD: Poll	(0) [Mas	p 14] PRES171	About to write	e image file	e. If this is :	the last m	ssage in :	your log.	Increase	memory	limit in p	hp.ini [Wit	POLLO1]				
04/08/2011 11:1 k/usr/share/cad	35:18 AM - W ti/site/plugins	EATHERMAP: Polk	/[0] [Mag put/c181	p 14] PRES17: 745fa53b1a3b	Asp: /usr/sh d78.png	/are/cacti/sit	ite/plugins/	/neatherma	p/confige/	PRES17 -	-> /ust/s	nere/cect	/site/plug	ing/weath	ermap/ou	tput/c181	745fa53b;	1#5b2d78.	html
4/08/2011 11:1 nd /usr/share/c	35:18 AM - W cacti/site/plug	EATHERMAP: Policins/weathermap/o	(0) [Mag utput/14	o 13] PRES18: 356936cd/2fas	Wrote map to Braee thumb	o /ust/shan s.png	e/cacti/site	s/plugins/w	athermap	p/output/:	1e35693	icdf2fa99	face.pnp						
04/08/2011 11:1	35:18 AM - W	EATHERMAP: Polle	r[0] [6ta:	0 15] PRES18:	About to write	e image file	e. If this is	the last m	assage in -	your log.	increase	memory	limit in p	hplini (Wit	POLLO1]				

Figura 5.1.58: Visualización del registro de incidencias^[1]

5.1.13 TAB CEREOUS

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

Para la creación de estos reportes seguir los siguientes pasos:

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

console graphs n	ectar npc	Cereus monitor	clog thold GPS Ma	p weathermap		
Console -> CereusReporting Reports					Logged in as adm	in (Logout)
Create	CereusRend	orting - Reports				
New Graphs	Corcubicope	intering interportes				
Management	Reports					Add
Graph Management	ReportId					
Graph Trees	1	REPORTE	Disponibilidad	Graph Report	1 Day	
Data Sources	2	Reporte Prueba		Graph Report	On Demand	
Devices	La.					
Thresholds	-				Choose an action: Delete	S0
Weathermaps						
Collection Methods						
Data Queries						
Data Input Methods						
Templates						
Graph Templates						
Host Templates						
Data Templates						
Threshold Templates						
Map Templates						
Import/Export						
Import Templates						
Export Templates						
Configuration						
Settings						
Plugin Management						
Utilities						
System Utilities						
User Management						
and the second se						
NMID						
Manage Reports						
Backup/Restore						
Support Info						

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

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

console graphs	nectar npc	Cereus monitor	clog thold GPS Ma	p weathermap		min (Logout)
Create	CereusRep	orting - Reports			cogges in as at	(cogoot)
New Graphs Management	Reports					Add
Graph Management	ReportId	Name	Description	Report Type	Schedule Type	
Graph Trees	1	REPORTE	Disponibilidad	Graph Report	1 Day	
Data Sources	2	Reporte Prueba		Graph Report	On Demand	
Devices	L.					
Thresholds					Choose an action: Dele	e 🎽 Go
Weathermaps						

Figura 5.1.60: Selección de la opción Add^[1]

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

✓ *Report Name:* Nombre del nuevo reporte

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

Con la opción On Demand se obtiene reportes continuamente.

- ✓ *Report Page Size:* Permite escoger el tamaño de la hoja del reporte se sugiere usar la opción A4.
- *Report Page Orientation:* Permite escoger la orientación de la página del reporte se sugiere escoger la opción *Portrait*.
- *Report Graph Format:* Permite establecer el orden de los gráficos ya sea
 2 gráficos en columnas o la opción Default que permite colocar un gráfico en una columna.
- ✓ *Report Output Format:* Permite establecer el reporte en dos tipos de formato ya sea en PDF o en HTML, se sugiere usar el formato PDF ya que es de fácil manejo para el usuario.
- 3. Finalmente escoger la opción *Save* para guardar los parámetros creados como se muestra en la figura 5.1.61:

console gra	phs nectar npc Cereus monitor clog	thold GPS Map weathermap	
Console -> CereusRepo	rting Reports -> (Add)		Logged in as admin (Logout
Create	CereusReporting - Add Report		
New Graphs			
Management	Report [new]		
Graph Management	Report Name	REPORTE PRUEBA	
Graph Trees	The name of the report.		
Data Sources		DESCRIPCIÓN DEL GRÁFICO	<u>^</u>
Devices	Report Description		
Thresholds	The detailed describtion of this report. This will be also be displayed in the report.		
Weathermaps			
Collection Methods			<u>×</u>
Data Queries	Report Type Select if this is a normal report a graph report or a special DSSTATE report	Graph Report 💌	
Data Input Methods	Default Report Timecoan		
Templates	The default report timespane of this report.	On Demand 🚩	
Graph Templates	Report Page Size	Δ4 🔍	
Host Templates	The default report timespane of this report.		
Data Templates	Report Page Orientation The default report timespane of this report	Portrait 💌	
Threshold Templates	Report Crank Format		
Map Templates	The default report timespane of this report.	Default 💌	
Import/Export	Report Output Format	PDF V	
Import Templates	The Output Format can be PDF or HTML	PDF	
Export Templates		HTM	
Configuration			Save
Settings			

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

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



Figura 5.1.62: Visualización del reporte creado^[1]

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

console graphs no Graphs -> Tree Mode	ectar npc Cereus monitor clog thold GPS Map weathermap	settings
- Default Tree	Graph Filters	
E Localhost	Presets: Last Day Y From: 2011-04-07 11:31 To: 2011-04-08 11:31 🖬 📢 1 Day Y 🔶 Refresh Clear	
B-Monitoreo	Search: Grants per Paper 10 V Thumbnails: Go Clear	
B-PRESIDENCIA		
"Host: BANCO CENTRAL		
Host: CAE	REPORTE PRUEBA V Add to Report 10 V Ad V Portrait V Default	Include Sub-Leafs
Host: DESPACHO PRESIDENTE MIN LITORAL	Please choose	
- Host: DIR, GENERAL DEL	REPORTE Showing All Graphs	
-Host: EMPRESA NACIONAL DE	T REPORTE PRUEBA DESPACHO PRESIDENTE MIN LITORAL	
Host: GERENTE FONDO	Cranh Tomolatos Interface, Traffic (bits/sec)	

Figura 5.1.63: Selección del nombre del reporte^[1]

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



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

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



Figura 5.1.65: Opción Cereous^[1]

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

console graphs nectar npc Cereus monitor clog	thold GPS Map weathermap	settings
CereusReporting - Generate Report		
Report		
Report Name The name of the report.	REPORTE PRUEBA	
Report Description The detailed describtion of this report. This will be also be displayed in the report.	DESCRIPCIÓN DEL GRÁFICO	
Report Type Select if this is a normal report, a graph report or a special DSSTATs report.	Graph Report	
Report includes sub leafs The report can include sub leafs. This is only valid for non graph reports.	false	
Default Report Timespan The default report timespane of this report.		
Report Timespan Timespan for this report to use	From: 2011-04-08 11:00	
		Cancel

Figura 5.1.66: Parámetros del tiempo de monitoreo^[1]

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



Figura 5.1.67: Descarga del reporte^[1]

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

		007 5000					
DES	CRIPCIA'N DEL	GRAIFICO					
DES	PACHO PRESIE	ENTE MIN LITO	RAL - Traffic	VI677			
	DESPA	CHO PREST	DENTE M		I. Tra	ffic . Vl	677
	DESFA	CHU FRESI		IN LIIUKA	L - 11a	1110 - 40	077
Pu	500	ر الا الا ال					
eco	400						
5	300						
ě.	200						5
bit	100						
	0-	11:10	11:20	11:30	11:40	11:50	12:00
		From 2011/	/04/08 11:	00:00 To 20	11/04/08	12:00:00	
	Outbound	Current:	544.91 443.40	Average:	554.43 447 78	Maximum:	5/1.6/ 471_40
	ourbound	current.	445.40	Average.	447.70	nax indir.	471.40
		ENTE MIN LITO	RAL - Traffic	VI677			
DES	PACHO PRESIE						
DES		CHO PREST	DENTE M	TN L TTORA	I - Tra	ffic - Vl	677
DES		CHO PRESI	IDENTE M	IN LITORA	L - Tra	ffic - Vl	677
DES		CHO PRESI	EDENTE M	IN LITORA	L - Tra	ffic - Vl	677
DES	DESPA	CHO PRESI	IDENTE M	IN LITORA	L - Tra	ffic - Vl	677 FOR 100 1
er second	DESPACHO PRESID	CHO PRESI	EDENTE M	IN LITORA	ıL - Tra∙	ffic - Vl	677 real of a
s per second	DESPA 500 400 300 200	CHO PRESI	EDENTE M	IN LITORA	L - Tra	ffic - Vl	677 PORT OF A LAND
bits per second	DESPA 500 400 300 200 100	CHO PRESI	EDENTE M	IN LITORA	L - Tra∙	ffic - Vl	677 WILLIAM
bits per second	DESPA 500 400 300 200 100 111:00	CHO PRESI	ILL 20	IN LITORA	L - Tra	ffic - Vl	12:00
bits per second \$	DESPA 500 400 300 200 100 11:00	CH0 PRES	DENTE M	11:30 00:00 To 20	L - Tra 11:40 11/04/08	ffic - Vl	677 12:00
bits per second \$	DESPA 500 400 300 200 100 11:00	CH0 PRES	DENTE M	IN LITORA 11:30 00:00 To 20	L - Tra 11:40 11/04/08	ffic - Vl	677 12:00

Figura 5.1.68: Visualización del reporte^[1]

5.1.14 TAB NECTAR

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

Cacti - Microsoft Internet Explorer											
Archivo Edición Ver Favoritos Herramier	ntas Ayuda							A			
🄇 Atrás 🔹 🐑 - 💌 🖻 🏠 🍃	🔎 Búsqueda 📩	Favoritos 🥝	🔗• 🍓 🔳 · 📮	K 🗱 🦓							
Directión 🕘 http://192.172.10.234/cartilek.mine	ubertar/hectar.php						~	🔁 🕼 Vinculos			
console graphs nectar npc Cereus monitor thold GPS Map clog weathermap											
Nectar Logged in as admin (Lo											
Reports [Administrator Level] Add											
Searchi	Ste	itusi Any N	Pagei 30 V G	io Clear							
<< Previous				Showing Ro	ows 1 to 4 of 4 [1]			Next >>			
Report Title**	Owner	Interval (c:i)	Last Run	Next Run	From	То	Туре	Enabled			
Nuevo Reporte CNT	Administrator	Day(s) (1:0)	2011/05/04 16:40:10	2011/05/05 16:40:00	CNT	fabricio10ec@yahoo.com	Inline JPEG Image	Enabled			
REPORTE PRUEBA AGRI	Administrator	Day(s) (1:0)	2011/05/05 12:30:09	2011/05/06 12:30:00	interministerial.monitoreo@andinanet.net	jhairos@gmail.com	Inline JPEG Image	Enabled 🔲			
Reporte Semanal	Administrator	Week(s) (1:0)	2011/05/04 13:00:18	2011/05/11 13:00:00	Monitoreo Interministerial		Inline JPEG Image	Enabled			
Reporte Semanal Trafico Presidencia	Administrator	Week(s) (1:0)	2011/05/04 14:55:08	2011/05/11 14:55:00	Monitoreo Interministerial	Multiple	Inline JPEG Image	Enabled			
<< Previous				Showing Ro	ows 1 to 4 of 4 [1]			Next>>			
Ļ						Choose	an action: Send Now	✓ Go			

Figura 5.1.69: Selección de la opción Nectar^[1]

5.1.14.1 CREACIÓN DE UN REPORTE

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

A Carti Hirtereeft Internet Explorer	
Archivo Edición Ver Favoritos Herramientas Avuda	
🔾 Arás • 🔘 - 🙁 😰 🏠 🔎 Búsqueda 👷 Feroritos 🤣 🎯 - چ 📓 - 📴 🔣 鑬 🚳	
Dirección 🜒 http://192.172.10.234/cacti/plugins/nectar/nectar.php?action=edit8tab=detais	🔽 🏹 Ir Vinclos 🎽
console graphs nectar npc Cereus monitor thold GPS Map Netur-> Report Edit	Clog weathermap Logged in as admin (Logged)
Details	
Report Details (new) General Settings	
Report Name Give this Report a descriptive Name	New Report
Enable Report Check this box to enable this Report.	Enable Report
Dutput Formatting Use Custom Format HTML	
Check this box if you want to use custom html and CSS for the report. Default Text Font Size Default Text Font Size	Use Custom Format HTML
Defines the default from size for all text in the report inducing the report line. Default Object Alignment Defines the default Alignment for Text and Graphs.	
Graph linked Should the Graphs be linked ?	Graph linked
Graph Settings	
The number of Graph columns.	
Graph Width The Graph Height in Pixels.	300 🔽
Graph Height The Graph Height in Pixels.	125 🗸
Thumbnails Should the Graphs be rendered as Thumbnails?	Thumbnails
Email Frequency	
Next Timestamp for sending Mail Report Start time for [first]next] mail to take place. All future mailing times vill be based upon this start time. A good example vould be 2:004M.	2011/05/0512:40:00
Report Interval Defines a schedule pattern, relative to given start time, e.g. "Day" or "Month". e.g. "Weak" for reporting interval with a veekly repeat cycle	Dey(s)
Number of Intervals Defines a the number of intervals (see above) to pass until next schedule.	1
Report Offset [seconds] The Offset in Seconds with respect to the (interval, count) base. 	0
Email Sender/Receiver Details	
Subject This value will be used as the Email subject. The report name will be used if left blank.	
This Hame will be used as the E-mail Senders name From Final Address	
This Adress vill be used as the E-mail Senders address	
To Email Address(es) Please separate multiple adresses by comma (.)	
Image attach type Select one of the given Types for the Image Attachments	Inline JPEG Image
	Cancel

Figura 5.1.70: Creación de reportes^[1]

Los parámetros a configurar presentan las siguientes opciones:

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

> OUTPUT FORMATTING

En esta opción se debe colocar los siguientes parámetros:

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

> GRAPH SETTINGS

En esta opción se debe colocar los siguientes parámetros:

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

EMAIL FREQUENCY

En esta opción se debe colocar los siguientes parámetros:

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

> EMAIL SENDER/RECEIVER DETAILS

En esta opción se debe colocar los siguientes parámetros:

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

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

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

5.1.14.1.1 ITEMS

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

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



Figura 5.1.71: Inserción de un nuevo Item^[1]

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



Figura 5.1.72: Guardar parámetro de configuración^[1]

5.1.14.1.2 PREVIEW

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



Figura 5.1.73: Visualización previa del reporte^[1]

5.1.14.1.3 EVENTS

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

console graphs nectar npc Cereus monitor thold GPS Map clog weathermap	
Nectar -> Report Edit	Logged in as admin (Logout)
Details Items Preview Events	Send Report
Scheduled Events [edit: Nuevo heppend cint_	
2011/05/06 16:40:00 - Friday	
2011/05/07 16:40:00 - Saturday	
2011/05/08 16:40:00 - Sunday	
2011/05/09 16:40:00 - Monday	
2011/05/10 16:40:00 - Tuesday	
2011/05/11 16:40:00 - Wednesday	
2011/05/12 16:40:00 - Thursday	
2011/05/13 16:40:00 - Friday	
2011/05/14 16:40:00 - Saturday	
2011/05/15 16:40:00 - Sunday	
2011/05/16 16:40:00 - Monday	
2011/05/17 16:40:00 - Tuesday	
2011/05/18 16:40:00 - Wednesday	
2011/05/19 16:40:00 - Thursday	

Figura 5.1.74: Registro de Reportes enviados^[1]

5.2 MANUAL DE ADMINISTRACIÓN DE ANA (Active Network Abstraction)

5.2.1 OBJETIVO

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

5.2.2 INTRODUCCIÓN

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

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

La arquitectura ANA consiste en dos tipos de servidores:

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

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

 Cisco ANA Unit: El objetivo principal de ANA Units es contener VNEs (Virtual Network Element; es un modelo de elemento de red tanto en lo físico como en lo lógico) y formar con ellas una red para poder interconectarse con otras independientemente de la unidad en la cual se ejecuten, además permite la distribución óptima de dichas VNEs.

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

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

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

5.2.3 ANA MANAGE

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

5.2.3.1 FUNCIONES PRINCIPALES

Las funciones principales de administración soportadas por ANA Manage son:

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

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

5.2.3.2 INICIALIZACIÓN DE ANA MANAGE

- 1. Ejecutar la aplicación.
- 2. Ingresar la información en el cuadro de diálogo de inicio de sesión:
 - ✓ Nombre de usuario
 - ✓ Contraseña
 - ✓ Host (ANA GW dirección IP del servidor o nombre de host)

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

ANA	Manage	
Version 3.7	X.	
User Name	ifonte	
Password:		
Server:	10.8.33.3	
	OK Cancel	

Figura 5.2.1: Inicio de Ana Manage^[1]

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

- Panel de Navegación: Este panel se encuentra en el lado izquierdo de la pantalla y contiene algunos elementos de ANA (ejemplo: Gateway, Units y AVMs) y funciones administrativas que pueden ser ejecutadas usando ANA Manage.
- Panel de Visualización: Este panel se encuentra en el lado derecho de la pantalla y presenta todos los detalles relacionados a la opción que se haya seleccionado en el panel de navegación en la parte izquierda de la pantalla.

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



Figura 5.2.2: Ventana Principal^[1]

5.2.3.3 BARRA DE HERRAMIENTAS

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



Figura 5.2.3: Barra de Herramientas^[1]



NEW: Depende del elemento seleccionado.

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

Properties

PROPERTIES: Muestra las propiedades de un elemento seleccionado.



DELETE: Borra un elemento seleccionado.



START: Carga los AVM/VNE seleccionados.



STOP: Descarga los AVM/VNE seleccionados.



MAINTENANCE: Mueve los VNE para su mantenimiento.



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

5.2.3.4 ADMINISTRACIÓN DE SERVIDORES ANA

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

Los administradores pueden realizar las siguientes funciones:

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

5.2.3.4.1 ADMINISTRACIÓN DE ANA UNITS

A continuación se describirá la creación de ANA Unit.

5.2.3.4.1.1 CREACIÓN UN NUEVO UNIT

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

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

M Cisco ANA Manage - jfonte@10.8.33.3							
File Tools Reports Help							
New Properties							
ANA Serve ANA Lint	ANA Servers						
ANA GLOTTE, SOLOTON	Find :	2		₩	,	,	
ANA Unit 10.8.33.12	e.	IP Address	Status	Up Since	Physical Memory	Memory/Up 🗎	Memory/All AVMs
	-	10.8.33.3	Up	21/04/11 15:48:07	32640M	1302M	1608M
DB Segments	3	10.8.33.6	Up	21/04/11 15:52:06	32640M	19300M	24364M
Event Management Settings	3	10.8.33.12	Up	21/04/11 15:50:58	16384M	11116M	11422M
Poling Groups	3	10.8.33.15	Up	21/04/11 15:51:14	32768M	15988M	16294M
Protection Groups							
- Report Settings							
Security Settings Security Settings							
Topology							
Users							
🖮 🛐 Workflow Engine							

Figura 5.2.4: Nuevo Unit^[1]

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

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

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

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

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

New ANA Unit		X
Add a new ANA Unit. If the n start automatically. Click OK when you're done.	ew unit is installed and reachable i	it will
IP Address:		
Standby Unit		
Protection Group:	default-pg 🛛 👻	
Gateway IP:	10.8.33.3	
	ОК	Cancel

Figura 5.2.5: Nuevo Ana Unit^[1]

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

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

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

M ANA Unit 10.8.3	3.6 - Properties
Displays ANA Unit p	roperties.
IP Address:	10.8.33.6
Status:	Up
Up Since:	Thu Apr 21 15:52:06 COT 2011
Physical Memory:	32640M
Memory/All AVMs:	24364
Memory/Up AVMs:	19300
Protection Group:	default-pg
🔽 Enable Unit Prot	ection
	OK Cancel

Figura 5.2.6: Propiedades de ANA Unit^[1]

5.2.3.4.2 ADMINISTRACIÓN DE LOS AVMs

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

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

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

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

5.2.3.4.2.1 CREACIÓN DE UNA AVM

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

- 1. Seleccionar el elemento de jerarquía de la ANA Units en el panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y seleccionar *New AVM*.
- 2. Colocar el *Id* del AVM, en la cual se debe ubicar números del 101 hasta el 999 los mismos que son únicos para cada servidor.
- Colocar una clave significativa que es una cadena que identifica de forma única un AVMs en el sistema, independientemente de su ubicación en la unidad para que un escenario de conmutación por error en el sistema sea transparente.
- 4. Especificar el tamaño de la memoria
- 5. Habilitar o deshabilitar la opción OnCreation
- 6. Habilitar o deshabilitar la protección AVM.

Todos estos parámetros se muestran en la figura 5.2.7.

ANA Unit:	10.8.33.6	5		
D:	T.			
(ey:				
Allocated Memory:	256	MB		
Activate on cre	ation			
Fnable AVM Pro	tection			

Figura 5.2.7: Nuevo AVM^[1]

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

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

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

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

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

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

M Cisco ANA Manage - jfonte@10.8.33.3				
File Tools Reports Help				
Rew Properties				
ANA Servers ANA Gateway 10.8.33.3	ID:	100	Status:	Down
🖃 💆 ANA Unit 10.8.33.6	Max. Memory:	256		
A B New VNE A A Actions A Actions A Actions A Actions A B Start C A A Delete Stop				
C A/ Properties 5 C A/ Properties 5 C AVM405_7600_CE_MPLS C AVM505 7600 CarrierE_INT				
AVM501_7600_CarrierE_INT AVM502_7600_CarrierE_INT				

Figura 5.2.8: Funciones en los AVMs^[1]

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

M A'	VM 100 - Prop	oerties		
Gene	ral			
	Key:			
	Status:	Down		
	Location:			
	ANA Unit:	10.8.33.6		
	Max. Memory:	256	МВ	
	🗹 Enable AVM	1 Protection	1	
	ок		Cance	
	Memory:	4%		Conn

Figura 5.2.9: Propiedades AVMs^[1]

5.2.3.4.3 ADMINISTRACIÓN DE VNES

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

5.2.3.4.2.2 CREACIÓN DE UNA VNE

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

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


Figura 5.2.10: Nueva VNE^[1]

A continuación se despliega el asistente VNE.

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

> TAB GENERAL

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

En la opción Scheme se sugiere colocar la opción Default.

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

GYECNTP01 - Properties				
General NMP Telnet / SSH IC	MP Polling Events			
Cisco ANA uses this information to	p identify the VNE.			
-Identification:				
Name:	GYECNTP01			
IP Address:	10.5.1.100			
Туре:	Cisco CR585			
Scheme:	IpCore 💌			
Orbus				
-Status:				
Status:	Up			
	Start Ston Maintenance			
Location				
ANA LINE	10.8.33.6			
AVM:	201			
AVIII.	201			
	Secondary			
	OK Cancel Apply			
Choose WAV	Memory: 6% Connected			

Figura 5.2.11: Tab General^[1]

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

➤ TAB SNMP

- Seleccionar la opción SNMP versión para gestionar la información de acceso SNMP.
- 2. Seleccionar la versión SNMP soportada por cada elemento de la VNE que está siendo administrada como se indica en la figura 5.2.12.

У GYECNTP01	- Properties		
Gene al SNMP	Tenet / SSH ICMP Polling Eve	ents	
▼ Enable SNMP	SNMP V1	◯ SNMP V2	⊙ SNMP V3
SNMP V1/V2 Sett	ings:		
Community:	Read:		
	Write:		
-SNMP V3 Setting: Authentication:	nd5		
	User: user_can	a363	
	Password:	•••••	
Encryption:	des		
	Password:		
		ок	Cancel Apply
Choose WAV	,,	femory: 6%	Connected

Figura 5.2.12: Tab SNMP^[1]

> TAB TELNET / SSH

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

- 1. Seleccionar Telnet, puerto 23 o SSH, puerto 22.
- Para añadir una nueva secuencia de comandos; colocar el valor del *Prompt/Run* en la tabla, dando clic en el campo *Prompt* y finalmente seleccionar *Add*, como se indica en la figura 5.2.13.

GYECNTP01 - Proj	perties		
General S IMP Telnet /	SSH ICMP Polling	g Events	
✓ Enable	-		
Protocol: SSHv2	*	Port: 22	
Prompt		Run	
GYECNTP01#			
		Line 0 (Size 1)	1
Promot		Rur	dack
			nuon
		Add	nove
User Name:	anauser		
Client Authentication:	password	v	
	Password:	•••••	Ξ
	Private Key:		
		< >>	
	Public Key:		
		Cenerate	
Server Authentication:	save-first-auth	 Image: A start of the start of	
<			>
		OK Cancel A	pply
Choose WAV		Memory: 7% Connected	

Figura 5.2.13: Tab Telnet/SSH^[1]

> TAB ICMP

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

GYECNTP01 - Properties	
General SNMP Telnet / SS	
Enable	
Polling Rate: sec.	

Figura 5.2.14: Tab ICMP^[1]

> TAB POLLING

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

- 1. Colocar los intervalos de sondeo para la VNE.
- 2. Seleccionar la opción *Group* que define un grupo específico de sondeo como se indica la figura 5.2.15:

Group Group			Instance	
Polling Intervals:				
Status:	180	sec.		
Configuration:	900	sec.		
System:	86400	sec.		
Topology:				
Layer 1:	30	sec.		
Layer 2:	30	sec.		
Adaptive Polling:				
ANA Settings	 Device Type 	e Settings	🔘 Local Sett	ings
🖌 Enable				
Upper Threshold:	90	%		
Lower Threshold:	60	%		
Lower Threshola:	60	%		

Figura 5.2.15: Tab Polling^[1]

Adaptative polling

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

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

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

> TAB EVENTS

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

GYECNTP01	- Properties	JX
General SNMP 1	Telnet / SSH ICMP Poling Events	_
Specify the IP addr	resses for which SNMP syslog and trap events will be generated	
Enter IP Address	s: Event-Generating IP Addresses:	
	Add	
	Remove	
	OK Cancel Apply	,
Choose WAV	Memory: 7% Connected	

Figura 5.2.16: TabEvent^[1]

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

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

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

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

M Cisco ANA Manage - ifonte⊘10.8.33.3								_ ð 🗙
File Tools Reports Help								
New Properties								
ANA Servers	ID:	202	Status:	Up				
ANA Gateway 10.8.33.5	Up Since:	14/01/11 21:36:52	Max. Memory:	750				
AVM 100 AVM200_CRS1_P_INT AVM201_CRS1_P_MPLS	Key:	AVM202_CR51_LAB						
AVM202_CR51_LAB	VNEs							
AWM301_GSRXR_PE_MPLS	Find :							
AVM404_7600_CE_MPLS	Key			1	SNMP	Telpet	Element Class	Element
AVM405_/600_CL_MPLS	UIOLAE !	10.2.97.100		14/01/11 2	." true	true	Auto Detect	Cisco CR:
AVM501_7600_cerrintE_INT AVM501_7500_cerrintE_INT AVM502_7000_cerrintE_INT AVM502_7000_cerrintE_INTLS AVM504_7500_cerrintE_MPLS		Actions Delete Poperti Properti	KEs Stop					
AVM50b_r/60U_carrierE_MPL5 AVM509_r600_carrierE_MPL5 AVM509_r600_carrierE_MPL5 AVM510_r600_carrierE_MPL5	L							

Figura 5.2.17: Funciones en los VNEs^[1]

> FUNCIONALIDAD FIND

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

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

Find:	a l
Proper(Any)	1
(Any) AVM	
VNE	
	1
Direction	1
A	

Figura 5.2.18: Find^[1]

5.2.3.5 GLOBAL SETTINGS

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

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

Todas estas opciones se muestran en la figura 5.2.19:



Figura 5.2.19: Global Settings^[1]

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

5.2.3.5.1 DATABASE SEGMENTS

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

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

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

M Cisco ANA Manage - jfonte@10.8.33.3							
File Tools Reports Help							
New Properties							
ANA Servers	A Servers 06 Segments						
ANA Gateway 10.8.33.3							
ANA UNIC 10.6.33.6		1			(
ANA Unit 10.8.33.15	Na € ∧ `	Туре	Tablespace	Partti	Extent	Next E	Bytes
E Concersorarigo				-		-	
DB Segments	ALARM_OID	INDEX PARTI"	ANA37	8	19	0	1245184
Message of the Day	ALARM_TA1	INDEX PARTI	ANA37	8	46	0	4980736
O Poling Groups	ALARM_TICK.	INDEX PARTI"	ANA37	8	19	0	1245184
Protection Groups	AUDITEVENT	TABLE PARTI.	ANA:37	7	53	0	5439488
Report Settings	AUDITEVENT	INDEX PARTI	ANA37	7	12	0	786432
Scones	AUDITEVENT.	INDEX PARTI	ANA37	7	14	0	917504
Topology	AUDITEVENT.	INDEX PARTI	ANA:37	7	12	0	786432
🙀 Users	BIN\$kEno5TA.	TABLE	ANA37	1	1	0	65536
E Workflow Engine	BIN\$koB3ZFZ	TABLE	ANA37	1	1	0	65536
	BOSRESULTS	TABLE	ANA37	1	1	0	65536
	BOSUSER	TABLE	ANA37	1	1	0	65536
	BOSUSER_N	INDEX	ANA37	1	1	0	65536
	BOSUSER_OI	INDEX	ANA37	1	1	0	65536
	BUSINESSOB.	TABLE	ANA37	1	1	0	65536
	BUSINESSOB.	INDEX	ANA37	1	1	0	65536
		TADLE	4514.07			0	05520

Figura 5.2.20: Database Segments^[1]

5.2.3.5.2 EVENT MANAGEMENT SETTINGS

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

- Para cada partición de la base de datos: se debe colocar los días en los que su información va a ser eliminada.
- ✓ Para cada partición: se debe colocar el tamaño (en días) de la partición de la base de datos como se indica en la figura 5.2.21:



Figura 5.2.21: Events Management Settings^[1]

5.2.3.5.3 MESSAGE OF THE DAY

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

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



Figura 5.2.22: Message of the day^[1]

5.2.3.5.4 POLLING GROUPS

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

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

M Cisco ANA Manage - jfonte@10.8.33.3	
File Tools Reports Help	
🔞 New 🔳 Properties 📋 🖿 🔳 🌌 🏠	
🖶 🔂 🛛 ANA Servers	Poling Groups
ANA Gateway 10.8.33.3 ANA Unit 10.8.33.6	Find:
ANA Unit 10.8.33.12 ANA Unit 10.8.33.15	Polling e A T Description
🖶 👸 🛛 Global Settings	default
- DB Segments	slow
Event Management Settings Message of the De Defing Groups Define Groups Define Groups	
Report Settings	
in and security Settings → [1] Scores → [2] Topology → [2] Workflow Engine 34 [2] Workflow Engine	

Figura 5.2.23: Polling Group^[1]

5.2.3.5.4.1 CREAR UN NUEVO POLLING GROUP

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

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

New Polling Group		X
Create a customized pollir instead of the default gro	ng group, which can then be used by a VNE up.	
Name:		
-Polling Intervals:		
Status: Configuration:	sec.	
System:	sec.	
-Topology:		
Layer 1:	sec.	
Layer 2:	sec.	
	ок Са	ancel

Figura 5.2.24: New Polling Group^[1]

 Colocar el nombre y los valores para cada uno de los 5 intervalos del *Polling Group*. Cualquier cambio realizado en la opción Global Settings se guarda automáticamente y se registra en el registro de Cisco ANA, como se indica en la figura 5.2.24.

5.2.3.5.5 PROTECTION GROUPS

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

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

5.2.3.5.5.1 CREAR UN NUEVO PROTECTION GROUPS

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

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



Figura 5.2.25: Protection Group^[1]

5.2.3.5.6 REPORT SETTINGS

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

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

M Cisco ANA Manage - jfonte@10.8.33.3	
File Tools Reports Help	
AWA Servers AWA Gateway 10.8.33.3 AWA Unit 10.8.33.6 AWA Unit 10.8.33.15 AWA Unit 10.8.33.15 Child Settings D Segments	Purge Settings Purge reports after: 9 days Store reports up to: 30 MB (Current: 0.0 KB) Security Settings
Create Analoguement - Scourge Poling Groups Poling Groups Report Settings Scopes Topology Users Users	

Figura 5.2.26: Report Settings^[1]

5.2.3.5.7 SECURITY SETTINGS

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

5.2.3.5.7.1 AUTHENTICATION METHOD

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

M Cisco ANA Manage - jfonte@10.8.33.3			
File Tools Reports Help			
麗 纳			
AMA Servers AMA Servers AMA Line 100.3.3.3 AMA Line 100.3.3.3 AMA Line 100.3.3.16 AMA Line 100.3.3.12 AMA Line 100.3.3.12 AMA Line 100.3.3.12 AMA Line 100.3.3.12 AMA Line 100.3.3.12 AMA Line 100.3.3.12 AMA Line 100.3.3.12 AMA Line 100.3.3.14 AMA Line 100.3.3.12 AMA Line 100.3.3.15 AMA Line 100.3.112 AMA Line 100.3.112 AMA Line 100.3.112 AMA Line 100.3.12 AMA Line 100.3.112 AMA Service 100.3.11 AMA Service 100.3.11 AMA Service 100.3.11 AMA Service 100.3.11 <th>ANA Authenticidion LDAP Authentication LDAP Authentication LDAP Ret.s: Distinguished Name Prefix: Distinguished Name Suffix: ANA-LDAP Protocot</th> <th>Map://forever-name.dl.d27656 ON ON-Unters,OC=dl.DC=d2 SSR V</th> <th></th>	ANA Authenticidion LDAP Authentication LDAP Authentication LDAP Ret.s: Distinguished Name Prefix: Distinguished Name Suffix: ANA-LDAP Protocot	Map://forever-name.dl.d27656 ON ON-Unters,OC=dl.DC=d2 SSR V	
		l	Apply Restore

Figura 5.2.27: Authentication Method^[1]

5.2.3.5.7.2 PASSWORD SETTINGS

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



Figura 5.2.28: Password Settings^[1]

5.2.3.5.7.3 USER ACCOUNT SETTINGS

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

Eile Tools Reports Help	
INT AN	
ANA Servers	Millser Account Settings - User Account Settings Properties
🕀 🎬 🛛 ANA Gateway 10.8.33.3	
🕞 🎒 🛛 ANA Unit 10.8.33.6	
🖶 🎒 🛛 ANA Unit 10.8.33.12	
🖻 🗿 ANA Unit 10.8.33.15	Usable account if inactive for 30 days.
🔂 AVM 100	
AVM302_GSRXR_PE_MPL	
AVM303_GSRXR_PE_MPL	
AVM401_7600_CE_MPLS	
AVM410_7600_CE_MPLS	
AVM411_7600_CE_MPLS	
AVM412_7600_CE_MPLS	
AVM506_7600_CamerE_N	
AVM507_7600_CarrierE_	
AVM6UU_ME6524_CE_MP	
AVM604_ME6524_CE_MP	
AVMOD5_ME6524_CE_MP	
AVM/UU_ASR_RR_INT	
AMM/03_ASK_RK_MPLS	
AVMBUU_6513_PE_MPLS	
AVIMOUD_/304_PE_MPLS	
AVIMI902_ME6524_CE_MM	
DR Segmente	
Event Management Settings	
Mossage of the Day	
Boling Groups	
Protection Groups	
Report Settings	
Security Settings	
Authentication Method	
User Account Settings	Apply Restore
- fill	(the second sec
Topology	
Users	
🗴 🛅 Workflow Engine	
_	Memory 5% Connected
	i i inquesto i i inquesto i i i i i i i i i i i i i i i i i i i

Figura 5.2.29: User Account Settings^[1]

5.2.3.5.8 ANA SECURITY

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

5.2.3.5.8.1 ADMINISTRACIÓN DE DISPOSITIVOS

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

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

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

APLICACIÓN DE FUNCIONALIDADES 5.2.3.5.8.2

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

5.2.3.5.8.3 **FUNCIONES DE SEGURIDAD**

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

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

\mathcal{T}	
[⊉	_)

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



Configurator: Activa los servicios y configura la red.



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



Operator: Muestra información de la red.



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

5.2.3.5.8.4 ADMINISTRACIÓN DE SEGURIDAD

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

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



Figura 5.2.30: Scopes y Users^[1]

> ADMINISTRACIÓN DE SCOPES

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

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

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

➤ CREACIÓN DE UN SCOPE

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

- Seleccionar la opción *Scope* en el panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y elegir *New Scope*.
- 2. Colocar el nombre del Scope y añadir el dispositivo que va a ser parte del Scope como se indica en la figura 5.2.31.

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



Figura 5.2.31: Nuevo Scope^[1]

> ADMINISTRACIÓN DE USUARIOS

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

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

> CREAR USUARIOS

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

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

- Seleccionar la opción Users en el panel de navegación y dar clic en la opción New o a su vez dar clic derecho y elegir New User.
- 2. En el cuadro de dialogo colocar el nombre, contraseña y la descripción.
- 3. Seleccionar la función del usuario por defecto.

Todos estos parámetros se indican en la figura 5.2.32:

🖌 Cisco ANA Manage - root@	172.18.229.155			🛛
File Taols Help				
🥵 New 📜 Properties 👔				
ANA Servers Global Settings Global Settings Topology Users Guidantinue Forme	-ANA Users Find : Us ⊋ / ``	Description Det	ast Login	
a 🕁 Honnow Englie	New User Name: User Name: Full Name: Description: Password: Confirm password. Role I Force Password	I a construit de la construit	Cancel	

Figura 5.2.32: Nuevo Usuario^[1]

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

A continuación se muestra dos tablas de propiedades:

> TAB GENERAL

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

lobo 5 - Prope	rties	
General Security	1	
User Name:	John_S	
Last Login:	Jan 1, 1970 2:00:0	
Full Name:	John Smith	
Description:	Marketing Dept.	
🔽 Enable Acc	ount	
🔽 Limit Conne	ctions to:	
Force Pass	word Change After: 30 days.	
Force Pass	vord Change at Next Login	
	or l court	1 A1-
ady		Connected

Figura 5.2.33: Tab General^[1]

> TAB SECURITY

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

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

efault Active Rights	Configurator
Scope Name	Security Level
Router	Configurator
	Line 1 (1 / 1 Selecte
Add	Line 1 (1 / 1 Selecte Remove

Figura 5.2.34: Tab Security^[1]

5.2.3.5.9 **TOPOLOGY**

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

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



Figura 5.2.35: Topology^[1]

5.2.3.5.9.1 CREACIÓN DE NUEVO ENLACE ESTÁTICO

Para crear un nuevo enlace estático seguir los siguientes pasos:

- 1. Seleccionar la opción Topology en el panel de navegación y dar clic en la opción *New* o a su vez dar clic derecho y elegir New Static Link.
- 2. Seleccionar el sitio de A y Z del enlace estático, expandir el inventario físico de cada elemento y seleccionar la interfaz.
- 3. Dar clic en *Created*.

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

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



Figura 5.2.36: Nuevo Link^[1]

5.2.4 EVENTVISION (VISOR DE SUCESOS ANA)

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

5.2.4.1 INICIALIZACIÓN DE EVENTVISION

- 1. Ejecutar la aplicación.
- 2. Ingresar la información en el cuadro de diálogo de inicio de sesión:
 - \checkmark Nombre de usuario
 - ✓ Contraseña
 - ✓ Host(ANA GW dirección IP del servidor o nombre de host)

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

EventVision
Version 3.7.X
User Name: ifonte
Password:
Server: 10.8.33.3 💌
OK Cancel

Figura 5.2.37: Inicio EventVision^[1]

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

Las categorías de eventos son las siguientes:

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

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

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

E) c	isco ANA E	ventVision - jfont	e@10.8.33.3					
<u>F</u> ile	Edit ⊻jew	Tools Reports H	Page, Refre	esh, Filt	er, Auto	-Refresh, Spl	it Screen	
	Event ID	Time	Description	Command N	Command Si	Command P Originating	IP User Name	
	1077622	10-may-11 11:19:10	Command:GetEventViewerP.	GetEventVie	com.sheer.m	172.16.19.1	41 jfonte	<u> </u>
	1077621	10-may-11 11:19:10	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
•	1077620	10-may-11 11:19:08	Command:Find was execut	Find	com.sheer.m	172.16.19.1	41 jfonte	
. ا	1077619	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
. ا	1077618	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
. ا	1077617	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
. ا	1077616	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr.			
. ا	1077615	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr.	Event Infor	mation	
. ا	1077614	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	_
. ا	1077613	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	_
. ا	1077612	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
. ا	1077611	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
	1077610	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
. ا	1077609	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
. ا	1077608	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
. ا	1077607	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
. ا	1077606	10-may-11 11:19:00	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
. ا	1077605	10-may-11 11:18:59	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
	1077604	10-may-11 11:18:59	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
	1077603	10-may-11 11:18:59	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
	1077602	10-may-11 11:18:59	Command:Get was execute	Get	com.sheer.fr	172.16.19.1	41 jfonte	
•	4077004	10	· · · · · · · · · · · · · · · · · · ·	~- -	l 4 🤻	470.40.4	44 14-14-	Celected)
Audi	Provisionin	q Security Service	Syslog System Ticket V1 1	Trap V2 Trap	V3 Trap	Event Cate	egories	Sciecteu)
Result	ts 1 - 50						501105	

Figura 5.2.38: Ventana Principal EventVision^[1]

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

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

ICONO	COLOR	GRAVEDAD
*	ROJO	CRITICO
+	NARANJA	MAYOR
<u> </u>	AMARILLO	MENOR

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

Tabla 5.2.1- Indicadores de estado^[1]

5.2.4.2 DETALLES EVENTVISION

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

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

seveni	the second state of the se	Look Mandidia atian Time V	Description		0 also as side data al	Current Course	
	ty Ticket ID	Last Modification Time	Description	Location	Acknowledged	Event Count	Affected Devices Cour
	024920	10-may-11 11:20:16	CPU utilization ex*	UIUCKDEU1	NO	5	i.
	017002	10-may-11 11.26.16	E 824926 - 1	licket Proper	ties		
	024845	10-may-11 11.22.27	Betresh		Clear		
	824949	10-may-11 11:22:27		1 House Houge			
	824877	10-may-11 11:22:27	824926				Cleared
	824871	10-may-11 11:20:04	CDU uniteratio		فاستحاد والعا		
L	824928	10-may-11 11:20:00	CPO Udiizadio	mess man lower	urresnoid		
	824941	10-may-11 11:19:59	UIOCRDE01				
	824927	10-may-11 11:19:53					
L I	824873	10463					
		D.1.1.	711.				
	824940	10-ma DODIE C	_11C				
	824940 824939	10-ma 10-ma	_IIC	n of 6% less than	the lower thresh	old of 40%.	
L	824940 824939 824938	10-ma 10-ma 10-may-11 11:18:39	_11C jiizatio	n of 6% less than	the lower thresh	old of 40%.	
	824940 824939 824938 824937	10-ma 10-ma 10-may-11 11:18:39 10-may-11 11:18:37		n of 6% less thar	the lower thresh	old of 40%.	
L L L	824940 824939 824938 824937 824936	10-ma 10-ma 10-may-11 11:18:39 10-may-11 11:18:37 10-may-11 11:18:36		n of 6% less thar	the lower thresh	old of 40%.	
L L L L	824940 824939 824938 824937 824936 824935	10-ma 10-ma 10-ma 10-may-11 11:18:39 10-may-11 11:18:37 10-may-11 11:18:36 10-may-11 11:18:34	LIIC ilization	n of 6% less than	the lower thresh	old of 40%. Advanced Notes	
	824940 824939 824938 824937 824935 824935 824935	10-ma 10-may-11 11:18:39 10-may-11 11:18:37 10-may-11 11:18:34 10-may-11 11:18:34 10-may-11 11:18:33	C IIC Ilization	n of 6% less than	the lower thresh correlation	old of 40%. Advanced Notes 4%	Connected
	824940 824939 824938 824937 824936 824935 824935 824934 824932	10-may 10-may-11 11:18:39 10-may-11 11:18:37 10-may-11 11:18:36 10-may-11 11:18:33 10-may-11 11:18:33 10-may-11 11:18:26	General History	Affected Parti	es Correlation , Memory:	old of 40%. Advanced Notes 4%	Connected
L L L L L	824940 824939 824938 824937 824936 824935 824934 824934 824932 824933	10-ma 10-ma 10-may-11 11:18:39 10-may-11 11:18:37 10-may-11 11:18:36 10-may-11 11:18:36 10-may-11 11:18:25 10-may-11 11:18:25	General History	Affected Parti	the lower thresh es Correlation , Memory: No No	old of 40%. Advanced Notes 4% 2	Connected

Figura 5.2.39: Detalles EventVision^[1]

5.2.4.3 DETALLES -SPLIT SCREEN

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

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

٥	Cisco ANA I	iventVision - jfont	e@10.8.33.3				l.	
File	Edit View	Tools Reports H	elp					
<	> 🕲	📡 🛃 📃						
	Event ID	Time	Description	Location	Event Type			
۰	1077666	10-may-11 11:34:43	Command:Get was execute		Audit			^
۰	1077665	10-may-11 11:30:58	Command:Get was execute		Audit			
۰	1077664	10-may-11 11:30:34	Command:Get was execute		Audit			
4	1077663	10-may-11 11:30:15	Command:Get was execute!		Audit			
۰	1077662	10-may-11 11:29:54	Command:Get was execute		Audit			
۰	1077622	10-may-11 11:19:10	Command:GetEventViewerP		Au			
۰	1077621	10-may-11 11:19:10	Command:Get was execute		Au Infor	mació	n Gener	a1
۰	1077620	10-may-11 11:19:08	Command:Find was execut		Au	macio		ui –
۰	1077619	10-may-11 11:19:00	Command:Get was execute.		Audit			
۰	1077618	10-may-11 11:19:00	Command:Get was execute		Audit			
۰	1077617	10-may-11 11:19:00	Command:Get was execute		Audit			
۰	1077616	10-may-11 11:19:00	Command:Get was execute.		Audit			
۰	1077615	10-may-11 11:19:00	Command:Get was execute		Audit			
۰	1077614	10-may-11 11:19:00	Command:Get was execute		Audit			~
							Line 4 (1 / 50	Selected)
Pr	operties:							
Γ						_		^
	ID:	1077663				Severity:	Cleared	
	Description:	Command:Get was ex	ecuted by jfonte from IP:172.16	19.141 L	Detalles	Time:	10-may-11 11:30:15	
	Location:	N/A				Туре:	Audit Event	~
<								>
Au	dit Provisioni	ng Security Service	Syslog System Ticket V1 T	rap V2 Trap V3 Ti	ap All			
kes	ults 1 - 50				Memor	y: 10%	Connected	

Figura 5.2.40: Split Screen^[1]

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

5.2.4.4 TAB ALL

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

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

- ✓ Tiempo
- \checkmark Tipo de evento

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

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

Severity 🗸 🗸	Event ID	Short Description	Time	Event Type
3206		Link down	8/31/04 - 10:56:57	Service
L.	2649	Link down	8/31/04 - 07:53:57	Service
L	24793	Link down	9/6/04 - 12:47:25	Service
L	24315	Link down due to Card event	9/6/04 - 10:37:44	Service
k i	24256	Link down due to Card event	9/6/04 - 10:25:48	Service
L	24055	Link down due to Card event	9/6/04 - 09:44:23	Service
L.	10663	Link down	9/2/04 - 11:50:57	Service
	4090	Link down due to Card event	8/31/04 - 15:57:45	Service
£ 1	21562	Link down	9/5/04 - 17:17:57	Service
	3355	Link down	8/31/04 - 11:23:57	Service
	24839	Link down due to Card event	9/6/04 - 12:57:35	Service
L	24633	Link down due to Card event	9/6/04 - 12:05:05	Service
I.	0.1100	123 J. C. C. M. C. S.		· ·

Figura 5.2.41: Tab All^[1]

5.2.4.5 TAB AUDIT

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

E Ci		ventVision - ifont	e@10.8.33.3					
File	-dit View	Tools Reports H						
	ത്തി		ada.					
	<u>~ @</u>							
Sev.	Event ID	Time	Description	Command N	Command Si	Command P Origi	nating IP	User Name
۰	1077699	10-may-11 11:50:49	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
	1077698	10-may-11 11:50:44	Command:Get was execute.	Get	com.sheer.fr	172.1	6.19.141	jfonte
4	1077697	10-may-11 11:50:29	Command:InternalGet was e	InternalGet	com.sheer.m"	172.1	6.19.141	jfonte jfonte
۰	1077696	10-may-11 11:50:27	Command:GetReportParame	GetReportPar 🚬	com.sheer.m	172.1	6.19.141	jfonte
*	1077695	10-may-11 11:49:19	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
	1077694	10-may-11 11:49:19	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
۰	1077693	10-may-11 11:49:07	Command:Update was exec	Update	com.sheer.m	172.1	6.19.141	jfonte
*	1077692	10-may-11 11:48:14	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
*	1077691	10-may-11 11:47:56	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
۰	1077690	10-may-11 11:47:56	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
	1077689	10-may-11 11:47:56	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
	1077688	10-may-11 11:47:56	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
۰	1077687	10-may-11 11:47:29	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
	1077686	10-may-11 11:47:27	Command:Get was execute.	Get	com.sheer.fr	172.1	6.19.141	jfonte
	1077685	10-may-11 11:47:25	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
۰	1077684	10-may-11 11:47:21	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
	1077683	10-may-11 11:46:10	Command:Get was execute.	Get	com.sheer.fr	172.1	6.19.141	jfonte
	1077682	10-may-11 11:46:09	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
۰	1077681	10-may-11 11:46:08	Command:Get was execute.	Get	com.sheer.fr	172.1	6.19.141	jfonte
	1077680	10-may-11 11:46:03	Command:Get was execute.	Get	com.sheer.fr?	172.1	6.19.141	jfonte
۰	1077679	10-may-11 11:45:58	Command:Get was execute	Get	com.sheer.fr	172.1	6.19.141	jfonte
	4077070	10		~		470.4	C 4 0 4 44	Line 3 (1 (50 Selected)
			Sudan Sustan Tislat V1.7	Van V2 Tran	2 Trans			Line 5 (17 50 Selected)
Audit	rovisionir	ig [securicy [service]	systog system licket vi i	rap v2 trap				
Results	:1-50					Memory: 6	76	Connected

Figura 5.2.42: Tab Audit^[1]

5.2.4.6 TAB PROVISIONING

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

	Event ID	Event	User Name	Time	Status	Source
1	1238	Execution of script ShowConfiguration succeeded	toot	2/10/04 - 14:36:25	Success	BB1800-47
l.	1231	Execution of script ShowConfiguration succeeded	root	2/10/04 - 14:18:41	Success	RB1800-Sim
L.	985	Execution of script ShowRunningConfig succeeded	root	2/10/04 - 13:49:17	Success	PE-206
L.	973	Execution of script RemoveVrf succeeded	root	2/10/04 - 13:35:43	Success	PE-206
6	972	Execution of script RemoveVrf succeeded	root	2/10/04 - 13:35:29	Success	PE-206
4	951	Execution of script AddVrf succeeded	root	2/10/04 - 11:25:13	Success	PE-206
	942	Execution of script RemoveVrf succeeded	foot	2/10/04 - 10:16:10	Success	PE-209
1	941	Execution of script AddVrf succeeded	root	2/10/04 - 10:14:38	Success	PE-209
	864	Execution of script AddVrfSite succeeded	root	2/9/04 - 17:06:25	Success	PE-206
1	860	Execution of script AddRouteTargetExport succeeded	root	2/9/04 - 17:05:23	Success	PE-206 VRF 5.7
L.	858	Execution of script AddRouteTargetImport succeeded	root	2/9/04 - 17:05:22	Success	PE-206 VRF 5
1	855	Execution of script AddVrf succeeded	toot	2/9/04 - 17:04:20	Success	PE-206
	841	Execution of script RemoveRouteTarget succeeded	root	2/9/04 - 14:57:46	Success	PE-208 VRF BLT
	458	Execution of script RemoveVrf succeeded	root	2/8/04 - 10:27:15	Success	PE-209
	456	Execution of script RemoveVrf succeeded	root	2/8/04 - 10:27:13	Success	PE-208
	454	Execution of script RemoveVrf succeeded	root	2/8/04 - 10:27:12	Success	PE-207
	451	Execution of script RemoveVrf succeeded	root	2/8/04 - 10:27:09	Success	PE-206
	1902	Execution of script ChangePortStatus succeeded	root	2/10/04 - 16:00:37	Success	PE-208#3:AT*

Figura 5.2.43: Tab Provisioning^[1]

5.2.4.7 TAB SECURITY

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

E Ci	SCO ANA E	ventVision - jfont	e@10.8.33.3					
File	Edit View	Tools Reports H	elp					
$\langle \langle \rangle$	>	📡 🔛 🖽						
	Event ID	Time	Description	Location	User Name	Client Type	Originating IP	
۰	1077421	10-may-11 11:18:44	Successful login jfonte	Avm 11	jfonte	Unknown	172.16.19.141	~
۰	1077420	10-may-11 11:18:43	Successful login jfonte	Avm 11	jfonte	Unknown	172.16.19.141	
	1076560	10-may-11 11:16:57	Successful login root	Avm 11	root	Unknown	10.8.33.202	
	1076513	10-may-11 11:16:31	Successful login root	Avm 11	root	Unknown	10.8.33.202	
۰	1076512	10-may-11 11:12:31	User root logged off	Avm 11	root	Unknown	10.8.33.214	
۰	1076511	10-may-11 11:12:18	User root logged off	Avm 11	root	Unknown	10.8.33.214	
	1076406	10-may-11 09:02:59	Successful login noc	Avm 11	noc	Unknown	172.16.7.130	
	1076299	10-may-11 08:45:30	Successful login root	Avm 11	root	Unknown	10.8.33.214	
	1076280	10-may-11 08:45:06	User root logged off	Avm 11	root	Unknown	10.8.33.213	
۰	1076246	10-may-11 08:44:49	User root logged off	Avm 11	root	Unknown	10.8.33.213	_
۰	1076095	10-may-11 08:44:13	Successful login root	Avm 11	root	Unknown	10.8.33.214	
۰	1070790	10-may-11 08:39:01	Successful login root	Avm 11	root	Unknown	10.8.33.213	
	1070788	10-may-11 08:38:59	Successful login root	Avm 11	root	Unknown	10.8.33.213	
	1070748	09-may-11 19:00:29	User noc logged off	Avm 11	noc	Unknown	172.16.7.130	
۰	1070745	09-may-11 17:12:21	User root logged off	Avm 11	root	Unknown	10.8.33.211	
۰	1070744	09-may-11 17:12:14	User root logged off	Avm 11	root	Unknown	10.8.33.211	
۰	1070640	09-may-11 14:55:43	Successful login root	Avm 11	root	Unknown	10.8.33.211	
	1069835	09-may-11 14:52:34	Successful login root	Avm 11	root	Unknown	10.8.33.211	
.	1069834	09-may-11 12:21:48	User darcos logged off	Avm 11	darcos	Unknovvn	172.16.9.76	
۰	1069443	09-may-11 12:13:15	Successful login darcos	Avm 11	darcos	Unknown	172.16.9.76	
۰	1069442	09-may-11 12:13:04	User gestion logged off	Avm 11	gestion	Unknown	172.16.9.76	
•	4000007	00 mm 44 44 20 04	Current di la cia ana	0		1.1=1.= =	470.40 7.400	(50 Salacted)
Quidit	Brouiciou		Suclea Sucteen Ticket VI	Trap V2 Trap V2 1	Trap OI		Line 13(1	/ 50 50/80led)
Addit	Provision	Ig Security Service	Sysing System Ticket VI	Trap v2 Trap V3				
Results	1 - 50					Memory:	9% Connect	ed

Figura 5.2.44: Tab Security^[1]

5.2.4.8 TAB SERVICE

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

		-40 8 22 2							
	Cisco ANA Eventvision - Jiont	e@10.8.33.3						والعام	
File	Edit View Tools Reports He	qls							
<	: 🔊 🕲 🚺 🛃 📖	1	_	_	-				1
	Event ID Time	Description	Location	Alarm ID	Ticket ID	Causing Event ID	Duplication Count	Reduction C	\Box
	147619 27-abr-11 07:50:10	Interface status up	And the second s				1	1	^
۰	147576 27-abr-11 07:50:10	Interface status up	UIOINQE02 VRF d.	816512	816490		1	1	1
۰	426144 27-abr-11 00:35:36	Device unreacha	GYECNTB01	782950	782950		1	1	1
+	426134 27-abr-11 00:32:57	MPLS interface re	GYECNTB01:LSE	792888	792888		1	1	1
+	426134 27-abr-11 00:32:57	MPLS interface re	GYECNTB01:LSE	792887	792887		1	1	
۰	426129 27-abr-11 00:31:20	Device unreacha	MIANAPB02	772857	772857		1	1	
+	426121.27-abr-11 00:29:04	Device unreacha	UIOINQB01	772848	772848		1	1	
+	426116.27-abr-11 00:27:29	Device unreacha	MIANAPB01	772851	772851		1	1	
	426107 27-abr-11 00:24:12	MPLS interface a?	GYECNTB01:LSE	792888	792888		1	1	
	426107 27-abr-11 00:24:12	MPLS interface a	GYECNTB01:LSE	792887	792887		1	1	
	426105 27-abr-11 00:23:38	Device reachable	MIANAPB01	772851	772851		1	1	
	426105.27-abr-11 00:23:37	Device reachable	MIANAPB02	772857	772857		1	1	
	426105 27-abr-11 00:23:37	Device reachable	UIOINQB01	772848	772848		1	1	
	426105 27-abr-11 00:23:37	Device reachable	GYECNTB01	782950	782950		1	1	
+	425624 26-abr-11 22:27:53	Device unreacha	UIOINQB01	772848	772848		1	1	
+	425608 26-abr-11 22:23:48	Device unreacha	MIANAPB01	772851	772851		1	1	
+	425601 26-abr-11 22:21:21	Device unreacha	MIANAPB02	772857	772857		1	1	
+	425596 26-abr-11 22:20:13	Device unreacha	GYECNTB01	782950	782950		1	1	
+	425590 26-abr-11 22:18:35	MPLS interface re	GYECNTB01:LSE	792888	792888		1	1	
+	425590 26-abr-11 22:18:35	MPLS interface re	GYECNTB01:LSE	792887	792887		1	1	
-	425588 26-abr-11 22:17:16	MPLS interface a	GYECNTB01:LSE	792888	792888		1	1	
	400000 00 alm 44 004740		OVERNTDOM OF	700007	TODOOT	_		Line 0 (Size	50)
Au		ivslog System T	ficket V1 Trap V2	Trap V3 T	rap All				-
Res	eutre 1 - 50					Memory:	6%) c	oppected	

Figura 5.2.45: Tab Service^[1]

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

UIOINQE02 [129M+]					
Comparing a set of the second se	Route Distinguisher: 28006/201293 Name: dat1293 IPv4 IPv6 Stes Econd: Route Targets 20006.201293	Import Route Targets 20006:201203	Floute Mr	aps	
EMAAP@UIOINQE02 EMELNORTE@UIOINQE02	Routing Tables				
	Find :				
	Destination	Prefix	Outgoing Interface	Туре	Routing Protocol
ESPE@UIOINQE02	172.27.21.40			Indirect	BOP
ETAFASHION@UIOINQE02	172.27.12.128			Indirect	BGP
ETAPA@UIOINQE02	172.26.117.240			Indirect	BGP
FARMAENLACE@UIOINQE02	IT2.26.121.36			Indirect	BGP
FINSISTEMAS@UIOINOE02	172.26.108.88			Indirect	BGP
	# 172,26,150.0			Indirect	BOP
	172.27.8.200			Indirect	BGP
Device Zoom 🔀 Best Fit	172.26.121.32			Indirect	BGP
	172,26,108,92			Indirect	BGP
	172.27.12.136			Indirect	BGP
	# 172.26.121.44			Indirect	BGP
	172 26 108 80			Indirect	RGP
	<				>
					Line U (Size 719)

Figura 5.2.46: Location^[1]

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

E 816499	Alarm Properties		
(P) Retreet	Alarmi Properties		
Co Refresh			
Alarm ID:	816499	Severity:	Cleared
Description:	Interface status up	Time:	27-abr-11 07:50:10
Location:	UIOINQE02 VRF DHCPNET IP:Vlan326	Open Alarms:	0/0
Ticket ID:	816490		
-Details:			
IP Interface	Vlan326 (10.10.1.93) changed status to up		
General Histo	ry Affected Parties Correlation		
		Mem	ory: 13% Connected

Figura 5.2.47: Información de Alarma Id^[1]

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

E 816490 - Ti	cket Propertie	5								
(Refresh	Acknowledge	L Clear								
Alarm ID:	816490					Severity:		Major		
Description:	Port up					Time:	27-8	abr-11 07:50:21		
Location:	LIOINGE02#11:0	GigabitEtherne	11/13			Open Alarms:	22/2	26		
Acknowledged:	No									
Details:										
Port Up										
General History	Affected Parties	Correlation	Advanced	Notes						
						Memo	ey:	9%	Connecte	nd br

Figura 5.2.48: Información de Ticket Id^[1]

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

UIOINQE02 [129M+]							
	-Location Information						~
Image: Barrier And American Structure (108M+) Image: Barrier (108M+) Image: Barrier (108M+) Im		Thus Only	Langellan -	11 discharthese shi tha			
E Weight Physical Inventory [21M+]	Type:	mber Optic	Location:	11. agabittinernet11/15			
Chassis [21M+]	Pluggable Type:	GBIC	Connector Description:	1000BaseLH			
Slot 1: Card - WS-X6148-R3-45 [6]	Part ID:	WS-G5486	Connector Serial Num:	H11L325			
Slot 7: Card - WS-SI IP720-38	Sending Alarmer	brum.	Port Alian	GrabitEthernet11/13			
Slot 8: Card - WS-SUP720-38	Jonaing Marines	crub	Porcession.	cagazite (normal 1975)			
Slot 9: Card - WS-X6582-2PA	Managed:	true	Status:	OK			
🖨 🛲 🐥 Slot 11: Card - WS-X6724-SFP [12]							
ma Subslot 6: Subcard - WS-F6700							
GigabitEthernet11/1 - Missing F	\delta Disable Sendir	g Alarms					
GigabitEthernet11/2	WI AN Interface						
GigabitEthernet11/4	TENT Incorrace						
GigabitEthernet11/5	Mode:	Trunk			VLAN Type:		Layer
GigabitEthernet11/6 - Missing F	Native VLAN ID:	1			VLAN Encapsulation	n Type:	IEEEE
GigabitEthernet11/7 - Missing F	Allowed VLANs:	32, 296, 302-	304, 306, 307, 309-316, 3	318-326, 328-330, 493, 2904, 39	87 VLAN Encapsulatio	n Admin Type:	IEEEE
GigabitEthernet11/8							
GigabitEthernet11/10 - Missing							
GigabitEthernet11/11 - Missing	Circle B Block						
GigabitEthernet11/12 - Missing	Gigable Ethernet						
🚛 👫 GigabitEthernet11/13	MAC Address:	00 16 C8 CD D0	90				
GigabitEthernet11/14 - Missing							
GigabitEthernet11/15 - Missing							
GigabitEthernet11/15	21 D. I. I.						×
GigabitEthernet11/18 - Missing	N						
GigabitEthernet11/19 - Missing	Find :	🔛 🖄					
	Address 👻 🚈		Mask	VLAN Type	Operational State	VLAN ID	Inne
Q Device Zoom 🔀 Best Fit				Bridge		(1) default	^
				Bridge		(319) VLAN"	
				Bridge		(3987) VLA"	~
	<						>
						Line 0 (Size 29)
	Sub Interfaces						
					9	en Port Utilization	Graph
				Men	nory: 11%	Connected	

Figura 5.2.49: Phisical Inventory^[1]

5.2.4.9 TAB SYSLOG

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

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

E Cisco	ANA Event	'ision - root@172.18.229.155					
File Edit	View Tools	: Help					
« »	0 🖸 🚺	2 🔳					
7	Alarm ID	Short Description	Location	Time			
*	256405	Generic syslog	CRS4A-SDR	1/31/09 - 00:01:3	19		^
4	256404	Generic syslog	CRS4A-SDR	1/31/09 - 00:01:3	39		
A	256403	Generic syslog	CRS4A-SDR	1/31/09 - 00:01:3	39		
	256402	Generic syslog	CRS4A-SDR	1/31/09 - 00:01:3	19		
4	256401	Generic syslog	CRS4A-SDR	1/31/09 - 00:01:3	19		=
.	256400	Generic syslog	CRS4A-SDR	1/31/09 - 00:01:3	39		
	256128	Cleared due to ForceClear	CRS4A#0.0 -Back.1:GigabitEth?	1/30/09 - 23:22:	51		
*	256127	Cleared due to ForceClear	CRS4A#0.0 -Back.1:GigabitEth?	1/30/09 - 23:22:	51		
A	256126	Cleared due to ForceClear	CRS4A : 11.31.101.16	1/30/09 - 23:22:	51		
A	256125	Cleared due to ForceClear	PE12	1/30/09 - 23:22:	51		
*	256124	Cleared due to ForceClear	CRS4A#0.0 -Back.0: GigabitEth?	1/30/09 - 23:22:	51		
4	256123	Cleared due to ForceClear	CRS4A#0.0 -Back.0: GigabitEth?	1/30/09 - 23:22:	51		
A	256122	Cleared due to ForceClear	CRS4A#0.0 -Back.1:GigabitEth	1/30/09 - 23:22:	51		
A	256121	Cleared due to ForceClear	CRS4A#0.0 -Back.1:GigabitEth?	1/30/09 - 23:22:	51		
4	256120	Cleared due to ForceClear	CRS4A-SDR : 11.31.101.14	1/30/09 - 23:22:	51		
4	256119	Cleared due to ForceClear	PE11	1/30/09 - 23:22:	51		
A	256118	Cleared due to ForceClear	PE21#0.4 -Back.1:TenGigE0/4/*	1/30/09 - 23:22:	51		
4	256117	Cleared due to ForceClear	PE21#0.4 -Back.1:TenGigE0/4/	1/30/09 - 23:22:	51		
4	256116	Cleared due to ForceClear	CRS4A#0.0 -Back.1:GigabitEth?	1/30/09 - 23:22:	51		
A	256115	Cleared due to ForceClear	CRS4A#0.0 -Back.1:GigabitEth*	1/30/09 - 23:22:	51		~
							Line 1 (Size 50)
Audit P	rovisioning Se	curity Service Syslog ystem Ticket V1 T	rap V2-V3 Trap				
Results 1	- 50					Memory: 12%	Connected

Figura 5.2.50: Tab Syslog^[1]

5.2.4.10 TAB SYSTEM

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

E) Cis	co ANA Event	Vision - root@172.18.229.155			
File E	dit View Tool	s Help			
< (» 🕲 🚺				
	> Event ID	Short Description	Location	Time	
٨	256186	Agent 11.16.254.43 is starting BOS Unit = 172.18.229.156 AVM = 400	CRS4A-SDR	1/30/09 - 23:27:24	^
۰	256185	Agent 11.16.254.40 is starting BOS Unit = 172.18.229.156 AVM = 400	CRS4A	1/30/09 - 23:27:24	
۰.	256184	Agent 11.16.254.30 is starting.BOS Unit = 172.18.229.156 AVM = 400	iox1-sdr0-p	1/30/09 - 23:27:23	
.	256183	AVM 400 started.BOS Unit = 172.18.229.156	Avm 400	1/30/09 - 23:27:23	
۰.	256182	AVM 400 is starting.BOS Unit = 172.18.229.156	Avm 400	1/30/09 - 23:27:16	
۰.	256179	AVM 400 is shutting down.BOS Unit = 172.18.229.156	Avm 400	1/30/09 - 23:26:50	
۰.	256178	AVM 400 shut down.BOS Unit = 172.18.229.156	Avm 400	1/30/09 - 23:26:50	
<u>.</u>	256177	AVM 400 shut down.BOS Unit = 172.18.229.156	Avm 400	1/30/09 - 23:26:50	
٩	256166	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
A	256165	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
A	256164	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
A	256163	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
۰	256162	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
٩	256161	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
٩	256160	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
٩	256159	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
A	256158	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
A	256157	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
٨	256156	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	
٩	256155	Table statistics are too old	Avm 11	1/30/09 - 23:24:07	<u>~</u>
					Line 1 (Size 50)
Audit	Provisioning Se	ecurity Service System sket V1 Trap V2-V3 Trap			
Results	1 - 50			Memo	ry: 12% Connected

Figura 5.2.51: Tab System^[1]

5.2.4.11 TAB TICKET

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

Ticket ID							
Ticket ID							
	Last Modification Time	Description	Location	Acknowledged	Event Count	Affected Devices Coun	ıt
825009	10-may-11 12:36:48	Port down	STDCNTE01#	No	12	1	-
824946	10-may-11 12:35:41	Port up	UIOLPZE01#2.	Yes	8	1	
824927	10-may-11 12:35:41	CPU utilization les	UIOEEPE01	Yes	6	1	
824945	10-may-11 12:35:41	CPU utilization les	UIOLLZE02	Yes	2	1	
825001	10-may-11 12:35:09	Dropped packet r	UIOQCNE01#	No	4	1	
825000	10-may-11 12:35:07	Dropped packet r	UIOQCNE01#	No	4	1	
824999	10-may-11 12:35:06	Dropped packet r	UIOQCNE01#	No	4	1	
824998	10-may-11 12:35:04	Dropped packet r	UIOQCNE01#	No	4	1	
824997	10-may-11 12:35:04	Dropped packet r	UIOQCNE01#	No	4	1	
824995	10-may-11 12:34:56	Dropped packet r	UIOGCNE01#	No	4	1	
824996	10-may-11 12:34:56	Dropped packet r	UIOQCNE01#	No	4	1	
825003	10-may-11 12:34:53	CPU utilization les	UIOEEPE01	No	2	1	
824994	10-may-11 12:34:50	Dropped packet r	UIOQCNE01#	No	4	1	
825004	10-may-11 12:32:09	Port down	UIOLPZE01#2.	No	9	1	
824959	10-may-11 12:31:13	CPU utilization les	UIOCRDE01	No	6	1	
825002	10-may-11 12:29:28	Discarded packet	UIOQCNE01#	No	2	1	
823001	10-may-11 12:29:17	Layer 2 tunnel up	303@UIOGJL."	No	2	1	
817802	10-may-11 12:26:38	Port up	UIOLPZE01#2.	Yes	16 2	1	
824989	10-may-11 12:26:30	Port down	UIOLPZE01#2.	No	9	1	
824984	10-may-11 12:24:10	Port down	UIOLPZE01#2.	No	10	1	
824982	10-may-11 12:21:26	Laver 2 tunnel do	323/20UIOQC	No	1	2	1
							2
	224986 224927 224927 224927 225000 224999 224999 224999 224995 224997 224995 224995 224995 224994 225002 225002 225002 225002 225002 224999 224999 224999 224999 224994 224992 224992	24398 10-may-11 12:35:41 234927 10-may-11 12:35:41 23495 10-may-11 12:35:41 23495 10-may-11 12:35:09 25001 10-may-11 12:35:09 25009 10-may-11 12:35:00 23498 10-may-11 12:35:04 23498 10-may-11 12:35:04 23498 10-may-11 12:35:04 23498 10-may-11 12:34:55 23498 10-may-11 12:34:55 23498 10-may-11 12:34:55 23498 10-may-11 12:34:55 23600 10-may-11 12:34:55 23600 10-may-11 12:32:09 23498 10-may-11 12:32:09 23498 10-may-11 12:20:17 23600 10-may-11 12:20:17 23601 10-may-11 12:20:17 23602 10-may-11 12:20:10 23498 10-may-11 12:20:10 23498 10-may-11 12:24:10 23498 10-may-11 12:24:10 23498 10-may-11 12:24:10 23498 10-may-11 12:24:10 23498 10-may-11 12:24:10	224396 10-may-11 12:35:41 PDt utilization les 234927 10-may-11 12:35:41 CPU utilization les 234945 10-may-11 12:35:09 Dropped packet r 235001 10-may-11 12:35:00 Dropped packet r 232499 10-may-11 12:35:04 Dropped packet r 234999 10-may-11 12:34:50 Dropped packet r 234999 10-may-11 12:34:50 Dropped packet r 234996 10-may-11 12:34:50 Dropped packet r 234996 10-may-11 12:32:09 Port down 234995 10-may-11 12:32:09 Port down 234995 10-may-11 12:32:09 Port down 234995 10-may-11 12:32:09 Port down 234991 10-may-11 12:24:10 Port down 234992 10-may-11 12:24:10 Port down 234994 10-may-11 12:24:10 Port down <td< td=""><td>224396 10-may-11 12:35:41 Put up 0000-2201/2: 234927 10-may-11 12:35:41 CPU utilization les.", UDOE-201/2: 123495 10-may-11 12:35:41 CPU utilization les.", UDOE-201/2: 123501 10-may-11 12:35:09 Dropped packet r.", UDOC/NE01/2: 124399 10-may-11 12:35:00 Dropped packet r.", UDOC/NE01/2: 124399 10-may-11 12:35:04 Dropped packet r.", UDOC/NE01/2: 124399 10-may-11 12:35:04 Dropped packet r.", UDOC/NE01/2: 124395 10-may-11 12:35:04 Dropped packet r.", UDOC/NE01/2: 125001 10-may-11 12:35:05 CPU utilization les.", UDOC/NE01/2: 125003 10-may-11 12:35:05 Dropped packet r.", UDOC/NE01/2: 125004 10-may-11 12:20:09 Port down UDOL/DE01/2: 125001 10-may-11 12:21:20 Port down UDOL/DE01/2: 125002</td><td>Status Tortup District No Status Tormay-11 12:35:41 CPU dilization les.", UIGCEE012-, 149 Status Tormay-11 12:35:41 CPU dilization les.", UIGCEE012-, No Status Tormay-11 12:35:41 CPU dilization les.", UIGCEE012-, No Status Tormay-11 12:35:09 Dropped packet r.", UIGCEE012-, No Status Tormay-11 12:35:06 Dropped packet r.", UIGCEE012-, No Status Tormay-11 12:35:07 Dropped packet r.", UIGCEE012-, No Status Tormay-11 12:35:200 Port down UIGCEE012-, No Status Tormay-11 12:21:21 L</td><td>States Tormay-11 12:35:41 Orbit Up DioDe2D12:01:22:01 /22:00 /22:01 /22:00 /22:01 /22:00</td><td>Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Di</td></td<>	224396 10-may-11 12:35:41 Put up 0000-2201/2: 234927 10-may-11 12:35:41 CPU utilization les.", UDOE-201/2: 123495 10-may-11 12:35:41 CPU utilization les.", UDOE-201/2: 123501 10-may-11 12:35:09 Dropped packet r.", UDOC/NE01/2: 124399 10-may-11 12:35:00 Dropped packet r.", UDOC/NE01/2: 124399 10-may-11 12:35:04 Dropped packet r.", UDOC/NE01/2: 124399 10-may-11 12:35:04 Dropped packet r.", UDOC/NE01/2: 124395 10-may-11 12:35:04 Dropped packet r.", UDOC/NE01/2: 125001 10-may-11 12:35:05 CPU utilization les.", UDOC/NE01/2: 125003 10-may-11 12:35:05 Dropped packet r.", UDOC/NE01/2: 125004 10-may-11 12:20:09 Port down UDOL/DE01/2: 125001 10-may-11 12:21:20 Port down UDOL/DE01/2: 125002	Status Tortup District No Status Tormay-11 12:35:41 CPU dilization les.", UIGCEE012-, 149 Status Tormay-11 12:35:41 CPU dilization les.", UIGCEE012-, No Status Tormay-11 12:35:41 CPU dilization les.", UIGCEE012-, No Status Tormay-11 12:35:09 Dropped packet r.", UIGCEE012-, No Status Tormay-11 12:35:06 Dropped packet r.", UIGCEE012-, No Status Tormay-11 12:35:07 Dropped packet r.", UIGCEE012-, No Status Tormay-11 12:35:200 Port down UIGCEE012-, No Status Tormay-11 12:21:21 L	States Tormay-11 12:35:41 Orbit Up DioDe2D12:01:22:01 /22:00 /22:01 /22:00 /22:01 /22:00	Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Discrete Status Discrete Status Discrete Status Discrete Status Status Discrete Status Di

Figura 5.2.52: Tab Ticket^[1]

5.2.4.12 TAB SNMP TRAPS

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

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

	lisco	ANA EventV	'ision - root@172.18.229.155					
File	Edit	View Tools	Help					
«	»	0 📡	2 📖					
	7	Alarm ID	Short Description	Location	Time			
4		256399	Cisco Configuration management event notifica.	CRS4A-SDR	1/31/09 - 00:01:3	36		^
4		256398	Cisco Configuration management event notifica.	CRS4A-SDR	1/31/09 - 00:01:3	36		
		256397	Cisco Configuration management event notifica.	CRS4A	1/31/09 - 00:01:3	35		
4		256396	Cisco Configuration management event notifica.	CRS4A	1/31/09 - 00:01:3	35		
4		256395	Cisco Configuration management event notifica.	CRS4A	1/31/09 - 00:01:3	35		
4		256394	Cisco Configuration management event notifica.	CRS4A	1/31/09 - 00:01:3	35		
		255796	Cleared due to ForceClear	132@PE21	1/30/09 - 23:22:5	51		
4		255795	Cleared due to ForceClear	CRS4A P: GigabitEthernet0/0/0/.3	1/30/09 - 23:22:5	51		
		255794	Cleared due to ForceClear	CRS4A IP:GigabitEthernet0/0/0/.3	1/30/09 - 23:22:5	51		
4		255793	Cleared due to ForceClear	CRS4A IP: GigabitEthernet0/0/0/.5	1/30/09 - 23:22:5	51		
4		255792	Cleared due to ForceClear	222@PE11	1/30/09 - 23:22:5	51		
4		255791	Cleared due to ForceClear	112@PE11	1/30/09 - 23:22:5	51		
		255790	Cleared due to ForceClear	222@PE21	1/30/09 - 23:22:5	51		
		255789	Cleared due to ForceClear	PE11 VRF srvcs	1/30/09 - 23:22:5	51		
		255788	Cleared due to ForceClear	CRS4A-SDR IP:Loopback0	1/30/09 - 23:22:5	51		
		255787	Cleared due to ForceClear	CRS4A-SDR IP:tunnel-te1005	1/30/09 - 23:22:5	51		
		255786	Cleared due to ForceClear	CRS4A-SDR IP:tunnel-te1000	1/30/09 - 23:22:5	51		
4		255785	Cleared due to ForceClear	CRS4A-SDR IP:GigabitEthernet	1/30/09 - 23:22:5	51		
4		255784	Cleared due to ForceClear	136@PE12	1/30/09 - 23:22:5	51		
		255783	Cleared due to ForceClear	134@PE22	1/30/09 - 23:22:5	51		×
								Line 1 (Size 50)
Aud	it Pro	ovisioning Sec	curity Service Syslog System Tic <mark>e</mark> t V1 Tr	ap V2-V3 Trap				
lesu	ts 1 -	50				Me	mory: 14%	Connected

Figura 5.2.53: Tabs Traps^[1]
5.2.5 CISCO ANA NETWORKVISION

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

5.2.5.1 FUNCIONALIDAD DE NETWORKVISION

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

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

5.2.5.2 INICIALIZACIÓN DE NETWORKVISION

Seguir los pasos que se indican:

- 1. Ejecutar la aplicación.
- 2. Ingresar la información en el cuadro de diálogo de inicio de sesión:
 - ✓ Nombre de usuario
 - ✓ Contraseña
 - ✓ Host(ANA GW dirección IP del servidor o nombre de host)

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

Cisco Active I	Network Abstra	iction	
Network	Vision		
VEISION J.F.A			
User Name:			
Password:		-	
Server: 10.	8.33.3	•	
	OK Car	and D	
	UK Cark	.ei	

Figura 5.2.54: Inicio NetworkVision^[1]

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

5.2.5.3 WORKSPACE

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



Figura 5.2.55: Pantalla principal de NetworkVision^[1]

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

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

Options 🛛 🔀
Startup Display Audio
Workspace Info
🗹 Load Workspace on Startup
·
OK Cancel Apply

Figura 5.2.56: Pantalla de Opciones^[1]

5.2.5.4 TAB STARTUP

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

5.2.5.5 TAB DISPLAY

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

Options 🔀		
Startup Display Audio		
Preferences Map Labels Font Size: 12 💌		
Severity Show Severity Text (e.g. [3M+])		
Show Acknowledged		
Show Propagated		
Display Name		
🔘 Do not use Business Tag		
 Add Business Tag to name 		
O Replace name with Business Tag		
OK Cancel Apply		

Figura 5.2.57: Display^[1]

Las siguientes son las configuraciones que se pueden cambiar:

> SEVERITY

Se recomienda habilitar las siguientes opciones:

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

> DISPLAY NAME

Se recomienda habilitar la siguiente opción:

✓ AddbusinessTag: Muestra el nombre original del elemento de red y el nombre del Business Tag.

5.2.5.6 TAB AUDIO

Permite seleccionar archivos de sonido para ser mostrados cuando una alarma se activa.

Estos archivos de sonidos pueden ser para alarmas de nivel crítico, mayor o menor como se muestra en la figura 5.2.58:

Options	X
Startup Display Audi	•
Enable Audio R	esponse for Alarm
Critical:	,/sounds/critical.wav
Major:	
Minor:	v 🖻 🛛
Loop Sound o	n Critical Alarm
ОК	Cancel Apply

Figura 5.2.58: Audio^[1]

5.2.5.7 BARRA DE HERRAMIENTAS NETWORKVISION

La barra de herramientas NetworkVision permite a los usuarios de manera fácil y rápida realizar operaciones diarias. La información sobre las herramientas se muestra al desplazar el puntero del mouse sobre los íconos de la barra de herramientas.

Las opciones disponibles dependen del nivel de permisos de usuario. Las opciones de la barra de herramientas varían dependiendo de su elección. Los ejemplos incluyen: Añadir túnel, inventario, cambio de tamaño, etc. Como indica la figura 5.2.59:



Figura 5.2.59: Barra de herramientas^[1]

5.2.5.8 CREACIÓN DE UN MAPA

Para la creación de un mapa seguir los siguientes pasos:

- 1. En la barra de herramientas dar clic en *New Map* o seleccionar *New Map* del menú *File* como se indica en la figura 5.2.60.
- 2. Colocar el nombre del mapa el cual debe constar de entre 1 a 65 caracteres.

🛛 Cisco ANA NetworkVision -	jfonte@10.8.33.3 (Core MI	PLS)					
File Edit View Node Tools Network Inventory Reports Window Help							
Core MPLS [1C+]	Network Elements	Network Elements					
AMBCNTP01 [17M+]	Find :	ind:					
GYEBLLP01 [8M+]	Name		IP Address €∠	System Name	Comm		
GYECNTE99 [9M+]	III + UIOMSCE9	9 [24M+]	10.2.98.100		Device		
GYECNTP01 [2M+]	III 🖊 UIOINGE99	[8M+]	10.2.99.100		Device		
UIOINQE01 [123M+]	SF AMBSURPO	11 [5M+]	10.3.1.100	AMBSURP01.cnt	Device		
		1 [17M+]	10.3.2.100		Device		
UIOINQP01 [7M+]	😬 🐥 GYECNTPO	1 [2M+]	10.5.1.100	GYECNTP01.cnt.c	Device		
	🥑 🍠 GYEBLLPO	1 [8M+]	10.5.2.100	GYEBLLP01.cnt.c	Device		
UIOMSCP01	🔟 🐥 GYEBLLE9	9 [7M+]	10.5.98.100		Device		
	III + GYECNTE9	9 [9M+]	10.5.99.100		Device		
	🥮 🍠 Uloinqpoi	[7]/ ·	10001		evice		
	UIOMSCP01	Create Map		2	svice		
		[🧿 Map Name:			vice		
	🥶 🐥 UIOMSCED	ı 💙			vice		
		[1: MAPA		Advanced	evice		
	USE GYEFNSED	1 (vice		
			OK Cancel				
	<						

Figura 5.2.60: Nuevo Mapa^[1]

3. El botón *Avanced* permite filtrar los enlaces que aparecen en el panel del mapa como se indica en la figura 5.3.60:

Link Fi	lter	X
Group	All	
✓ ATIO ✓ ATIO ✓ BFLO ✓ BGLO ✓ BULO ✓ Ethe	All Custom Data Link None Physical IVPN	
	pp S II	
Phy Phy Server Tun	vice nel	<
	OK Cancel Apply	

Figura 5.2.61: Link Filter^[1]

4. Se puede seleccionar los tipos de enlaces que van a ser filtrados de un grupo predefinido de tipos de enlaces como se indica en la figura 5.2.61. Al colocar el mouse sobre el dispositivo se desplegarán los enlaces establecidos en el mismo.

5.2.5.9 CREACIÓN DE DISPOSITIVOS

Para la creación de un dispositivo seguir los siguientes pasos:

1. En la barra de herramientas dar clic en la opción *AddtoMap* y elegir el elemento de red o dar clic en *File/AddtoMap/Network Element*, como se indica en la figura 5.2.62:

V Cisco ANA N	etworkVisior	- jfonte@10.8.33.3 (Core MPL
File Edit View	Node Tools	Network Inventory Reports Window
🔛 New Map	Ctrl+N	
Close	Curto	Network Elements
Load MultiPa	ath	Find :
🗾 🛃 Add to Map		Network Element
Save Map	Ctrl+5	Add a network element to the map (
Print Previe	W	AMBSURP01
Print	Ctrl+P	
[X] Exit	Ctrl+Alt+>	
	MSCE99 [24M+ _. MSCP01	M + GYEBLLE99

Figura 5.2.62: Opción AddMap^[1]

 En la lista de dispositivos seleccionar el dispositivo que se desee incluir en el mapa. Se puede seleccionar y añadir múltiples dispositivos mediante CTRL o CTRL+, como indica la figura 5.3.63:

Madd Network Element		×			
◯ Search Element Category 🕑		Go			
• Show All					
Find :	III - 1				
Name	IP Address	System Name			
ESMPALP01	10.1.1.100	<u> </u>			
ESMPALE01	10.1.10.100	=			
SMREFM01	10.1.10.194	ESMREFM01.c			
BRCNTE01	10.1.20.100	IBRCNTE01.cn			
■	10.1.20.194	IBROTVM01.ci			
■	10.1.20.195	IBRATUM01.cr			
TLCCNTE01	10.1.30.100				
STLCANGM01	10.1.30.194	TLCANGM01.c			
S NVLCNTE01	10.1.40.100	NVLCNTE01.c			
PFOCNTE01	10.2.10.100	PFOCNTE01.ai			
S TENCNTE01	10.2.20.100	TENCNTE01.ar			
UIOTBCM01	10.2.54.194	UIOTBCM01.ar			
UIOLABP01	10.2.97.100				
UIOINQX01	10.2.255.100				
SF PUYCNTP01	10.3.3.100	PUYCNTP01.c			
MBCNTE01	10.3.10.100	~			
<		>			
	Line 1	(1 / 123 Selected)			
		Cancel			

Figura 5.2.63: Selección de dispositivos^[1]

5.2.5.10 AÑADIR VPNs A UN MAPA

Para la adición de VPNs a un mapa seguir los siguientes pasos:

- 1. En la barra de herramientas dar clic en AddtoMap / VPN / EXISTING.
- 2. Seleccionar las VPNs que se requieran incluir en el mapa como se indica en la figura 5.3.64:

Cisco ANA NetworkVision - jfonte@10.8.33.3	(MPLS ATP Topology)						- a 🗙
File Edit View Node Tools Network Inventory Report	rts Window Help						×
			87				
AMBGREDI (S9M+) A MOSREDI (S9M+) A MOSREDI (S9H) AMBGREDI (S0H) COCKIEUS ORLUDI (MH) COCKIEUS (MH) A ORCUTEDI (MH) A ORCUTEDI (MH) A ORCUTEDI (MH) A ORCUTEDI (MH)	Add VPN Search Description Show All Available VPNs as of [0 Find*	3.may.11 15:42]		©		٦	^
GYEFNEE0 [30M+] JERATUM01 [1M] JERATUM01 [1M] JERATUE0 [47M+]	Name	Descrip	ption				
- ● ↓ LTCCNTEDI [19M+] - ● ↓ LTCSLCMOI [16M+] - ● PRUEBAS_ANA - ● ▲ RBECNTED (197M+)	X 1337					00-1	
RBBNORMOI [1M]	ACTIVANET				10/10/10/10/1		
TLCANGON [M] TLCANGON [M] TLCANGON [M] TLCCNTEOI [36M+] UIOCBYEOI [13M+]	ALEGRO ALEGRO_EXT				101		
UIOCCLEDI [26M+] UIOCTCEDI [30M+] UIOETTEDI [20M+] ✓	AMANDA_GUJARF	80					
Find:	BCE_EXT						
Severity Ticket ID Last Modification Time Ticket ID Dev ▲ 820399 03-may-11 15:40:13 Po	reso 🕺 BCO_PICH			Line 5 (1 / 644 Selected)	cation Count	Reduction Count	Alarm Count 4
A 820423 03-may-11 15:39:08 Dr	rope			OK Cancel			1
820394 03-may-11 15:17:28 Dr	ropt					2	1
* 820357 03-may-11 15:15:05 CP	PU utilization les UKUMSCEUT	110 4	1	4	•	1	1
820375 03-may-11 15:06:37 Tx	<utilization be="" is="" td="" uiomsce01#<=""><td> No 2</td><td>1</td><td>2</td><td>:</td><td>2</td><td>1</td></utilization>	No 2	1	2	:	2	1
820333 03-may-11 14:43:12 Po	ort up AMBSURE01	." No 9	1	2		9	4
		•				Lin	e 3 (1 / 1.565 Selected)
Add VPN					Memory:	6%	Connected

Figura 5.2.64: Adición de una VPN^[1]

5.2.5.11 MAP VIEW

Proporciona un panel de árbol jerárquico de los elementos de red incluido en el mapa, así como el diseño topológico de la NEs, los enlaces y las agregaciones.

Cisco Ana Networkvision ofrece la elección de diversas herramientas de visualización que se pueden utilizar para conocer y analizar los mapas y su contenido. Los elementos de la red pueden ser agregados y la información se puede mostrar al colocar el mouse sobre un elemento de enlace o de la red, como se indica en la figura 5.3.65:



Figura 5.2.65: Map View^[1]

El mapa topológico es la principal herramienta utilizada por Cisco ANA Network Vision para mostrar los vínculos y las relaciones entre los elementos de red y los nodos agregados.

5.2.5.11.1 ÍCONOS DE LOS DISPOSITIVOS

Cada elemento de red tiene cinco componentes que conforman el ícono y cada componente representa el estado o los atributos del elemento como se muestra en la figura 5.2.66:



Figura 5.2.66: Icono de dispositivo^[1]

- ✓ **Icono del dispositivo:** Indica el tipo de dispositivo.
- Color del ícono del dispositivo: Indica el estado y la gravedad del dispositivo.
- ✓ **Icono de las alarmas:** Indica la presencia de nuevas alarmas.

Si no hay alarmas, o todas las alarmas activas se reconocen, entonces no se muestra el icono alarmas

✓ Icono del estado de VNE: Indica el estado de gestión.

Si una VNE está en pleno funcionamiento entonces el icono VNE no se muestra.

Etiqueta del dispositivo: Consiste en el nombre del dispositivo y la notación.

Indica el número de alarmas con la mayor severidad.

El signo + se utiliza para indicar alarmas adicionales de menor gravedad que también existen.

5.2.5.11.2 ÍCONOS Y SÍMBOLOS

A continuación se presentan los diversos íconos y su representación en el mapa.

ÍCONO	REPRESENTACIÓN
	Red no conocida
1	Red, subred o agregación
	lógica
	Router
	SNMP genérico
	Switch Ethernet

	DSLAM
X	ATM switch
	BRAS
8	Visible para usuarios con
	más altos niveles de
	permiso
	Dispositivo fantasma
X	VPN
	Router Virtual
	Site business element

Tabla 5.2.2- Íconos y Símbolos

5.2.5.11.3 NIVELES DE GRAVEDAD

A continuación se muestran en la tabla 5.2.3 los niveles de gravedad que puede presentar un equipo o dispositivo.

ÍCONO	COLOR	GRAVEDAD
X	ROJO	CRITICO
X .	NARANJA	MAYOR
	AMARILLO	MENOR
	CELESTE	ADVERTENCIA
	VERDE	AUTORIZADO,

		NORMAL Ó OK.
X	AZUL	INFORMACIÓN
X.	BLANCO	DESCONOCIDO

 Tabla 5.2.3- Niveles de gravedad
 [1]

5.2.5.11.4 ESTADOS VNE

En la tabla 5.2.4 se muestran los distintos estados que pueden presentar una VNE.

ESTADO	ÌCONO DEL	DESCRIPCIÓN
	МАРА	
6	VNE Inalcanzable	El Gateway no recibió ninguna
		respuesta de la VNE.
B	Inicialización VNE	
	Equipo	La VNE no logró alcanzar el
	Inalcanzable	equipo.
None	Operacional	
8	Parcialmente	Algunos elementos de la VNE
	Soportado	no son soportados en su
		totalidad.
8	No compatible	La VNE no es compatible con
		el hardware del elemento de
		red, con la versión del software
		o el módulo del equipo.
	Equipo	El tipo del equipo es
	desconocido	desconocido o la VNE ha sido

		detenida.
19	Mantenimiento	El elemento de red se encuentra
		en up pero no ha sido
		monitoreada.

Tabla 5.2.4 -Estados de una VNE^[1]

5.2.5.12 LIST VIEW

Para desplegar *List View* dar clic en *Show List View* de la barra de herramientas. Muestra los detalles de todos los dispositivos incluidos en el mapa actual de la red o subred como indica en la figura 5.2.67:

Cisco ANA NetworkVision - ¡fonte@10.8.33.3 (Core MPLS)						
File Edit View Node Tools Network Invento	ry Reports Window Help					,
Gre MPLS [1C+]	Network Elements					
AMBCNTP01 [17/H+] AMBSURP01 [5/H+] CYERLEOD [7/H+]	Find:	<u></u>				
	Name	IP Address €/	System Name	Communication State	Investigation State	Element Category
	UIOMSCE99 [24M+]	10.2.98.100		Device Reachable		
GYECNTPO1 [2M+]	III 🖊 UIOINQE99 [8M+]	10.2.99.100		Device Reachable		
UIOINQEDI [20M+]		10.3.1.100	AMBSURP01.cnt	Device Unreachable	Currently Unsynchroni	Router
	MBCNTP01 [17M+]	10.3.2.100		Device Unreachable	Currently Unsynchroni	
UIOINQP01 [7M+]	😬 🐥 GYECNTP01 [2M+]	10.5.1.100	GYECNTP01.cnt.c	Device Reachable	Operational	Router
	SYEBLLP01 [8M+]	10.5.2.100	GYEBLLP01.cnt.c.	Device Unreachable	Currently Unsynchroni	Router
UIOMSCP01	I A GYEBLLE99 (7M+)	10.5.98.100		Device Reachable		
	III 📕 GYECNTE99 [9M+]	10.5.99.100		Device Reachable		
		10.8.0.1	UIOINQP01.cnt.co	Device Unreachable	Preparing for Maintena	Router
	UIOMSCP01	10.8.0.2		Device Reachable		
	III 🖊 UIOQCNP01 [1C+]	10.50.0.3		Device Reachable		
	😬 🐥 UIOMSCE01 [55M+]	10.50.0.10	UIOMSCE01.cnt.c"	Device Reachable	Operational	Router
	😂 🌾 UIOINGED1 [123M+]	10.50.0.18	UIOINGE01.cnt.co	Device Unreachable	Discovering	Router
	UFFNSE01 [30M+]	10.50.0.22		Device Unreachable	Initializing	
			-			
	• • • • • • • • • • • • • • • • • • •					>

Figura 5.2.67: List View^[1]

5.2.5.13 LINK VIEW

Para desplegar *Link View* dar Clic en Show *List View* de la barra de herramientas como se indica en la figura 5.2.68.

Link View muestra los enlaces dependiendo de las configuraciones realizadas en el *Link Filter*, cualquiera de los enlaces añadidos o removidos en el mapa son automáticamente añadidos o removidos al *Link View*.

Cisco ANA NetworkVision - jfonte@10.	8.33.3 (Core MPLS)						
File Edit View Node Tools Network Invento	ry Reports Window H	elp					
			1 🛛 - 🖸 🕞 🍳 🕐				
Gre MPLS [1C+] Show Links we	wind :	1	🗸 🎫 🖷 🛱 🖗	3			
- AMBSURP01 [SM+]	Context	Severity	A End-Point	Bi Dire	Z End-Point	Link Type 😌 λ	
GYEBLLE99 [7M+]	Core MPLS [1C+]		GYEBLLP01#0.7:TenGigE0/7/0/3	true	GYEBLLE99#0.0:TenGigE0/0/0/0	Physical Layer	
GYECINTE99 [9M+]	Core MPLS [1C+]	٨	GYECNTP01#0.7:TenGigE0/7/0/0	true	UIOINGP01#0.1:TenGigE0/1/0/2	Physical Layer	
- e + GYECNTP01 [2M+]	Core MPLS [1C+]		UIOMSCP01#0.0.TenGigE0/0/0/2	true	UIOMSCE01#12.0.TenGigabitEt?	Physical Layer	
GYEFNSE01 [30M+]	Core MPLS [1C+]	٨	LIOINGP01#0.1:TenGigE0/1/0/0	true	UIOINGE01#9: TenGigabitEthern	Physical Layer	
	Core MPLS [1C+]	<u>0</u>	UIOINGP01#0.2 TenGigE0/2/0/1	true	UIOINGE01#9:TenGigabitEthern	Physical Layer	
UIOINQP01 [7M+]	Core MPLS [1C+]		GYECNTP01#0.0.TenGigE0/0/0/0	true	GYEBLLP01#0.7:TenGigE0/7/0/0	Physical Layer	
UIOMSCEDI [55M+]	Core MPLS [1C+]		AMBSURP01#0.0: TenGigE0/0/0/1	true	AMBCNTP01#0.0:TenGigE0/0/0/0	Physical Layer	
UIOMSCP01	Core MPLS [1C+]		LIOMSCE99#0.0.TenGigE0/0/0/0	true	UIOMSCP01#0.1:TenGigE0/1/0/3	Physical Layer	
	Core MPLS [1C+]		LIOINGP01#0.0:TenGigE0/0/0/0	true	UICMSCP01#0.0:TenGigE0/0/0/0	Physical Layer	
	Core MPLS (1C+)		GYEBLLP01#0.1.0:GigabitEther.	true	UIOMSCP01#0.6.0.GigabitEther	Physical Layer	
	Core MPLS [1C+]		AMBSURP01#0.0: TenGigE0/0/0/2	true	GYECNTP01#0.6:TenGigE0/6/0/1	Physical Layer	
	Core MPLS (1C+)		GYECNTP01#0.6:TenGigE0/6/0/2	true	GYECNTE99#0.0:TenGigE0/0/0/0	Physical Layer	
	Core MPLS [1C+]		LIOINGE99#0.0.TenGigE0/0/0/0	true	UICINGP01#0.6:TenGigE0/6/0/0	Physical Layer	
							Line 0 (Siz
Find :	N						

Figura 5.2.68: Link View^[1]

5.2.5.14 OVERLAYS

Para desplegar *overlays* dar clic en *Choose overlay Type* de la barra de herramientas como se indica en la figura 5.2.69.

Permite visualizar que dispositivos y enlaces son parte de un servicio específico (VPN ó VLAN).

V Cisco ANA NetworkVision - jfonte	@10.8.33.3 (Core MPLS)		
File Edit View Node Tools Network	Inventory Reports Window H		
🖃 📲 🐥 Core MPLS [1C+]	None		
	VLAN		
	VPN ext		
	Core MPLS [1C+]		
	Core MPLS [1C+]		
- 🥌 🐥 GYECNTP01 [2M+]	Core MPLS [1C+]		
GYEFNSE01 [30M+]	Core MPLS [1C+]		

Figura 5.2.69: Overlay^[1]

Escoger una VPN ó VLAN específica de acuerdo a los requerimientos como indica la figura 5.2.70:

V Se	lect VPN Overlay		X			
O Se	arch Description 🕑	Go				
💿 Sh	 Show All 					
Availa	Available VPNs as of [03-may-11 13:54] 🛞					
Find :		# - -				
Name		Description				
X	29_BRAVCO		^			
X	1337					
X	ABAD_MENDIETA					
X	ABB					
X	ACTIVANET					
X	ADITMAQ					
X	AGRIPAC					
Ø	ALEGRO					
쓰	ALEGRO_EXT					
X	ALIANZANET2					
X	AMANDA_GUIJARRO					
X	ANDINANET					
X	ANETGYE					
X	BCE_EXT					
X	BCENT					
X	BCO_PICH		~			
		Line 8 (1 / 644 Select	ed)			
		OK Cance				

Figura 5.2.70: Selección de Vlan o Vpn^[1]

5.2.5.15 LAYOUT MAP

En este mapa se realiza el posicionamiento de la NEs (Network Element) y sus agrupaciones (grupos de NE). Las NEs pueden ser reposicionadas en el mapa. Los elementos pueden ser organizados automáticamente seleccionando el ícono del diseño del mapa, los diseños predefinidos para el mapa son: Circular, Symmetric, Tree, Hierarchical.

Escoger de la barra de herramientas *Layout Map* para elegir cada una de las opciones de mapas que se requiera como se indica en la figura 5.2.71:



Figura 5.2.71: LayoutMap^[1]

A continuación se presentan los distintos tipos de topologías que se pueden establecer como se muestra en la figura 5.2.72:



Figura 5.2.72: Tipos de mapas^[1]

5.2.5.16 TICKET PANE

Ticket pane muestra todos los tickets abiertos (por causa de alarma). La jerarquía completa de alarmas aparece al visualizar la ventana de *Ticket Properties* dando doble clic en cualquiera de los *ticket ID* como se indica en la figura 5.2.73.

La gravedad se propaga hacia arriba en la jerarquía de la red.

						G	YEBLLE99 [7	7M+]	UIOINGE01 [123M+	UIOMSC	P01
				75462	9 - Ti	cket Properti	es				
				Refres	h 🔍	Acknowledge	🜔 Clear				
				Alarm ID:		754629				Severity:	Minor
			<	Descriptio	n:	Layer 2 tunnel	down			Time:	01-mar-11 11:59:03
Find :		1		Location:		346@UIOINGE	01			Open Alarms:	0/0
Severity	Ticket ID	Last Modification Time	e 0 ∀	Acknowle	dged:	No					
4	754629	01-mar-11 11:59:03	L.	Details:]
A .	754626	01-mar-11 11:59:02	L	tunnel	PTPLay	er2MplsTunnel: v	cid 346 chang	e state to dowr	ו		
A	754627	01-mar-11 11:59:01	L								
A	748761	01-mar-11 11:36:52	F								
4	739680	16-feb-11 15:56:14	L		ictoru	Affected Darting	Correlation	Advanced N	inter		
4	739679	16-feb-11 15:56:10	1	General II	NAV I	File	Correlation	Advanced		Memory	9% Connected

Figura 5.2.73: Ticket Properties^[1]

5.2.5.17 VENTANA INVENTORY

Para visualizar esta ventana dar doble clic en el elemento de red del mapa o seleccionar el elemento de red y seleccionar de la barra de menú *Node/Inventory* ó a su vez dar clic derecho en elemento de red del mapa y seleccionar *Inventory*.

A continuación aparecerá la siguiente pantalla como se muestra en la figura 5.2.74:

TLC	ANGM01 [1M]					
₽- 50 ⊕-	CLCANGMOI [110] Logical Inventory Physical Inventory	Communication Investigation S	n State: Device Unreachable State: Discovering TLCANGM01 [1M]	3		
		Vendor:	Cisco			
		Product:	4 Eth-Switch		ANEL DE	
		Memory Usage	89491132	PR		
		Element Name	TLCANGM01			
		Serial Number: TP Address:	SAL1333WF0E			•
		Syctem Name:	TLCONGM01 cpt cc	mer		
	PANEL DE	Up Since:	11-mar-11 09:51:0	4		
		Contact:	Gestion IP/MPLS - 5	593-2-2540199		
	NAVEGACIÓN	Location:	Angel			
		DRAM Free:	55465392			
		DRAM Used:	11643472			
		Flash Device S	ize: Boot Flash = 66322 1061076	2432, Supervisor's Boot Flash = 133	3431296, Flash disk0 = 51207	3728
		Coffeend Unit	1901970			
		Software vers	Cieco IOS Softwar	a e6572 na Soffwara (e6572 na A	DVIDSERVICESKO M. Varair	12 2(22) CVI2 RELEASE COL
		System Descrip	btion: Technical Support: Copyright (c) 1986 Compiled Mon 26-C	http://www.cisco.com/techsuppor -2009 by Cisco Systems, Inc. -2009 21:18 by prod_rel	t	1112.2(33)3XI3, NEELMSE 301
		Processor DRA	M: 1006632960			
		Sending Alarm	s: true			
(27X)		Element Type:	Cisco ME 6524G5-8	S Ethernet Switch	_	
De De	vice Zoom			PANEL DE		
1	3 2	×	VIS	SUALIZACIÓN		<u>></u>
		General	DEL	DISPOSITIVO	J	

Figura 5.2.74: Inventory^[1]

Permite visualizar los componentes físicos y lógicos de un dispositivo y su estado.

- ✓ Physical Inventory: Incluye los diferentes componentes del dispositivo como son chasis, tarjetas, subslots entre otros.
- ✓ Logical Inventory: Incluye información tal como tráfico ATM, Access list y entidades de enrutamiento.

5.2.5.18 BUSSINES TAG

Un *bussiness tag* puede ser usado para etiquetar un componente de un elemento de red. Es un registro que se almacena en la base de datos del Gateway y está asociado con el elemento que se ha configurado.

Un *Bussines Tag* es una construcción u organización de ciertos elementos de la red y sus propiedades en una entidad lógica, para proporcionar capacidad y realizar el seguimiento con una mejor perspectiva, esto incluye elementos de capa 2, capa 3 y routers virtuales.

5.2.3.5.9.2 CREACIÓN DE UN BUSSINESS TAG

Para la creación de un Bussiness Tag realizar los siguientes pasos:

- 1. Elegir un elemento de red y dar clic derecho y escoger Attach bussiness tag.
- 2. En el cuadro de diálogo colocar la información requerida:
 - ✓ Una clave única
 - ✓ Nombre del bussiness tag
 - ✓ Tipo de bussiness tag: Suscriber, Provider Connection o Label
- 3. Guardar los cambios generados

Todos estos parámetros se muestran en la figura 5.2.75.

	Attach Business	Tag to GYECNTB01	X
	Unique Key :		
GYECNTA01	Name :		
GTECHIAG (1014) GTECHIAG (1014	Type :	Label	
		Save	Cancel

Figura 5.2.75: Bussiness Tag^[1]

5.2.5.19 REPORTS OVERVIEW

Cisco ANA proporciona un informe de gestión que le permite generar, visualizar y exportar informes de la información administrada por Cisco ANA.

Se puede guardar los reportes generados en cualquiera de los siguientes formatos: PDF, CSV, HTML, XLS y XMLL.

5.2.5.19.1 TIPOS DE REPORTES

- ✓ **Eventos:** La información relativa de eventos syslog y tickets abiertos.
- ✓ Inventory (Inventario): Versión de Software, resumen de la información.

5.2.5.19.2 GENERACIÓN DE INFORMES

En la barra de menú de Networkvision elegir la opción *Reports* en la cual existen dos opciones *Report Manager* y *RunReport* para crear, generar y administrar todos los reportes como se muestra en la figura 5.2.76:

Cisco ANA NetworkVision - jfonte@10.8.33.3 (CNT Internet Topology)						
File Edit View Node Tools Network Inve	ntor Reports Window Help					
	Report Manager					
GYECNTA01	Inventory Reports >	e e e e e e e e e e e e e e e e e e e				
		UIOMSCC01 [1m]				
- CYECNTB01 [72M+]	<u>_</u>					

Figura 5.2.76: Reportes^[1]

El gestor de informes está disponible en Cisco ANA Networkvision, ANA Manage y EventVision para la elección de informes, escogiendo la opción *Reports/ReportManage*.

Report manage permite ejecutar informes estándar como el número de syslogs por equipo o para definir informes adaptados a su entorno.

El panel de navegación muestra la representación jerárquica de los reportes y sus diferentes tipos como se muestra en la figura 5.2.77:



Figura 5.2.77: Reportes en orden jerárquico^[1]

Las carpetas de informes normalizadas que figuran en el gestor ANA son de eventos y de inventario. Cada carpeta contiene los tipos de informes que se proporcionan con CISCO ANA, además el usuario definen los mismos.

5.2.5.19.3 CREACIÒN DE UN REPORTE

Para generar un reporte del Menu Reports seguir los siguientes pasos:

 Escoger *Reports/Run, Report/folder/report-type*, donde: *Folder* es el requerimiento del archivo como se indica en la figura 5.2.78: *Report-type* es el requerimiento del tipo de reporte.



Figura 5.2.78: Tipo de reportes^[1]

- 2. Dar clic derecho en el tipo de reporte y elegir Run.
- En el cuadro de diálogo del *RunReports* colocar la información requerida y dar clic en Ok.
- 4. En la opción *Report Settings*, especificar el nombre del reporte la descripción y la seguridad del reporte la misma que puede ser pública o privada.

Prívate: El reporte puede ser visualizado o usado únicamente por el creador del reporte o el administrador.

Public: El reporte puede ser visualizado o usado por otros usuarios.

- 5. En la opción *Data Selection*, especificar el tiempo de concurrencia de los reportes ya sea en segundos, minutos, horas, días, meses y años.
- 6. En la opción *DeviceSelction*, especificar el equipo que se requiera añadir al reporte mediante la opción *Add*.

Todos estos parámetros se muestran en la figura 5.2.79:

🛛 Run Report - De	tailed Syslogs			
Report Settings				
Report Name:				
Description:				
Report Security:	Private Public			
Data Source:	Event Archive			
Date Selection				
 Last: 	1	Days 💌	·	
From date:	Mon 30 / May / 2011	10 : 43 : 12		
To date:	Mon 30 / May / 2011 📻 💌	10 : 43 : 12		
Device Selection				
 Select Devices 	Selected Devices:			
All Devices		Add		
		Remove]	
		Clear		
L			ок	Cancel
	Me	mory 7%	Conne	cted

Figura 5.2.79: Run Report^[1]

A continuación se presentan los mapas que se encuentran levantados en la red de la Corporación Nacional de Telecomunicaciones:

> CNT MPLS NETWORK



Figura 5.2.80: CNT MPLS NETWORK^[1]

> CNT INTERNET TOPOLOGY



Figura 5.2.81: CNT INTERNET TOPOLOGY^[1]

> MPLS FASE I



Figura 5.2.82: MPLS FASE I^[1]

> CORE MPLS



Figura 5.2.83: CORE MPLS^[1]

> VNEs



Figura 5.2.84: VNEs^[1]

5.3 MANUAL WHATSUP

5.3.1 OBJETIVO

Conocer cada uno de los componentes que conforman la plataforma Whats Up para monitorear y administrar de manera correcta las redes y los servicios que prestan.

5.3.2 INTRODUCCIÓN

WhatsUp es una aplicación que permite mantener un correcto funcionamiento de la red. Con esta plataforma, se puede crear rápidamente un mapa de red, iniciar el monitoreo, y obtener retroalimentación sobre el desempeño de la misma.

Actualmente en esta plataforma se encuentra el mapa principal *Andinatel*, a partir del cual se puede ingresar a los mapas de los equipos 6500, 7600, red IP y BRAS.

5.3.3 INGRESO A LA PLATAFORMA

A continuación se muestran los pasos de ingreso a la plataforma What's Up y sus diferentes mapas como se muestra en la figuras 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5.

Para ingresar a la plataforma se debe colocar la correspondiente dirección del servidor.

- 1. Para ingresar a los mapas contenidos en *Andinatel* dar doble clic en uno de ellos.
- 2. Para regresar al mapa principal dar doble clic en la nube (que tiene el contenedor denominado Andinatel).



Figura 5.3.1: Red Andinatel^[1]



Figura 5.3.2: Equipos MPLS 6500^[1]



Figura 5.3.3: Red IP^[1]



Figura 5.3.4: Equipos MPLS 7600^[1]



Figura 5.3.5: Equipos BRAS-BORDERS^[1]

5.3.4 CREACIÓN DE UN MAPA

Para crear un nuevo mapa, en el menú principal, seguir los siguientes pasos:

- 1. Seleccionar File
- 2. New Map Wizard
- 3. Seleccionar Create a blank map

4. Clic en Finish

Se puede establecer las propiedades de sondeo para cada mapa de la red principal y el mapa de subred mediante los siguientes pasos:

- 1. En el menú principal, seleccionar Edit.
- Seleccionar la opción *Properties* o dar clic derecho en la red y elegir *Properties*, posteriormente aparecerá la siguiente pantalla como se muestra en la figura 5.3.6:

Map Properties [met	ro.wup]			X
Categories	General			
	Title:	Metro		
<u>Genera</u> l	Poll Frequency:	60	(seconds)	
	Default Timeout:	5	(seconds)	
Network				
		OK	Cancel	Help

Figura 5.3.6: Propiedades de sondeo de los mapas^[1]

Map Properties presenta 3 opciones: General, Display y Network.

5.3.4.1 GENERAL

Colocar la información general del mapa, nombre, tiempo de espera predeterminado y frecuencia de sondeo como se muestra en la figura 5.3.7:



Figura 5.3.7: Opción General^[1]

5.3.4.2 DISPLAY

Utilice esta configuración por defecto para los nuevos mapas. Si se selecciona esta opción, WhatsUp aplica esta configuración a todos los nuevos mapas creados como se muestra en la figura 5.3.8.



Figura 5.3.8: Opción Display^[1]

5.3.4.3 NETWORK

Permite configurar la red y subred del mapa principal, para ello escoger un método de escaneo como se indica en la figura 5.3.9:

Categories	Network		
General ABC Display	Subnet settings Parent map: <u>N</u> etwork: N <u>e</u> tmask: Active discovery sett <u>S</u> can method: Rescan intervat	MasterMap.wup 0.0.0.0 156.21.50.155 ings Scan at intervals 60 (minutes)	*
		Include new devices in goll Resolve hostnames	ncea

Figura 5.3.9: Opción Network^[1]

5.3.5 TAB MAP

Permite visualizar el mapa de la red con cada uno de los dispositivos que se encuentran en estado activo, inactivo o en reconexión como se muestra en la figura 5.3.10:

WhatsUp Gold - [Metro (metro.wup) : Map]	
File Edit View Monitor Configure Tools Reports Logs Window Help	_ 6 ×
	июзтренот
🖡 Map 💥 Sta 🗽 Dependencies 🕮 Statistics 🗮 Notifications 🗮 Status	80

Figura 5.3.10: Tab Map^[1]

5.3.6 **TAB EDIT**

Presenta una barra de herramientas que permitirá añadir y modificar una serie de dispositivos en el mapa como se muestra en la figura 5.3.11:



Figura 5.3.11: Tab Edit^[1]

Para agregar un objeto en el mapa, seleccionar y arrastrar dicho objeto sobre el mapa. Además se tiene la opción de mover y cambiar el tamaño del objeto. Para establecer las propiedades de objeto seleccionado realizar los siguientes pasos:

- 1. Dar clic con botón derecho y seleccione Item Properties.
- 2. En la opción *General*, colocar el nombre, tipo de dispositivo, dirección IP y en la opción *Polling Method*, se recomienda colocar ICMP para verificar la conectividad del equipo como se muestra en la figura 5.3.12:



Figura 5.3.12: Propiedades del Objeto^[1]

 Se puede habilitar la opción SNMP que permite gestionar los dispositivos que conforman la red, además activa la opción Logs SMNP para analizar los sucesos ocurridos como se muestra en la figura 5.3.13:

Item Properties : TL	.csgbm01
Categories	SNMP
	SNMP Manageable Device
General	Bead Community: public
SNMP	<u>₩</u> rite Community:
SNMP	Device Object ID:
	SNMP (Simple Network Management Protocol) support in devices is not
	managable devices. Community strings are usually treated like passwords within an organization.
Services	Device Object IDs are automatically filled in by the scan routines if you provide a valid community name during the scan.
Events	OK Cancel Help

Figura 5.3.13: Habilitación de la opción SNMP^[1]

4. En la opción *Monitor* habilitar *Monitor This Device* para especificar cuan a menudo se debe realizar el monitoreo a un dispositivo, además configurar el tiempo en segundos que se debe esperar para una respuesta y verificar si un dispositivo o dependencia se encuentre en up o down como se muestra en la figura 5.3.14:

em Properties:TL	CSGBM01	Þ
Categories	Monitor	
General SNMP SNMP Monitor	Monitor This Device Poll Frequency: 1 Poll Limeout: 5 Time Period 7 days a week, 24 hours a day Dependencies	
Services	Check only if this Device is <u>up</u> : (none) Check only if this Device is <u>d</u> own: (none)	
•	OK Cancel Help	

Figura 5.3.14: Opción Monitor^[1]

 Seleccionar la opción *Services* para añadir cualquier servicio que se desee que el equipo monitoree, se sugiere el servicio DNS, como se muestra en la figura 5.3.15:

Estos servicios son TCP/IP que incluye DNS, FTP, POP3, SMTP, HTTP, IMAP4, NNTP, SNMP.

Categories	Services		
34.	Services to monito	c	
General	Monitor	Comment	édd
SHMP	Manitor/Ser	vice Properties on this Dev	dee
SNMP			
(The second seco	DNS (Domain	Name Servicel	UK
	Arguments:		Cancel
27.000 million		1	Help
	Comment;	0	
Services			
. 🛃			

Figura 5.3.15: Opción Services^[1]

6. Seleccionar la opción *Events* para añadir cualquier evento que se desee solicitar, se sugiere elegir SNMP Trap como se muestra en la figura 5.3.16:

Categories	Events
- ⁶⁴ e	Events to solicit:
General	Device Event Properties
SNMP	Event Type: OK
	SNMP Trap Syslog Windows Log Help
-	Arguments:
Services	Comment: Association>>
E VOTAS	OK Cancel Help

Figura 5.3.16: Opción Events^[1]

- 7. Opcionalmente se puede elegir Association para seleccionar un servicio asociado a este evento en el equipo. Además, se puede definir si el servicio asociado entra en modo up o down en el mapa cuando se produce el evento, como se muestra en la figura 5.3.16:
- Seleccionar la opción *Alerts* y elegir *Enable Logging* el cual permitirá observar los logs del equipo en caso de que exista una incidencia, como se muestra en la figura 5.3.17:
| Item Properties : RE | BCLPM01 |
|----------------------|-----------------------------------|
| Categories | Alerts |
| SNMP 💻 | Enable alerts |
| SNMP | Alert Name Trigger Time Add |
| | Sound/Default 4 0:00 - 24:00 Edit |
| | Remove |
| Monitor | |
| | |
| Services | |
| | |
| | Device doining |
| Events | 🔽 Enable logging |
| | Logging aigger. |
| | |
| | OK Cancel Help |

Figura 5.3.17: Opción Alerts^[1]

9. Se puede seleccionar la opción *Enable Alerts* para añadir y activar la alerta con un sonido por default, como se muestra en la figura 5.3.18:

Regories	Alerts	
Monitor	Egable alerts Alert Name Trigger Scond/Default 4	Time <u>A</u> dd. 0.00 - 24.00 Edt
Add.	Mert	×
Note Trings Events Devi Time	cation: Sound/Detault / / / / / / / / / / / / / / / / / / /	Cancel Help
Alerts	7 days a week, 24 hours a day	Change
Notes	is uto send UP alert after sending DOWN alert alert mode Send UP alert after the device and all services are control devices.	10

Figura 5.3.18: Opción Enable Alerts^[1]

- 10. Si las alertas han sido habilitadas en el dispositivo seleccionado estas aparecerán en la lista de color blanco, si estas son deshabilitadas subsecuentemente la lista aparecerá de color gris.
- 11. Seleccionar *Notes* en el caso que se requiera colocar algún tipo de descripción del dispositivo o del servicio como se muestra en la figura 5.3.19:



Figura 5.3.19: Opción Notes^[1]

Seleccionar la opción *Menú* para configurar los comandos que permitan la verificación de conectividad del dispositivo en la red como se muestra en la figura 5.3.20:

alegories	Menu		
	Menu Name	Command	Add
Services	Connect Ping Traceroute Browse	[tehet] [ping] [trace] [browse]	EdR. Delete.
Events	Edit Menu Ite	m	×
6	Menu name.		OK
Alerts	Connect		Cancel
	Command		Help
Notes	(locite)		·
	- Sydneric		

Figura 5.3.20: Opción Notes^[1]

5.3.7 TAB DEPENDENCIES

Muestra las dependencias de la red como un árbol jerárquico e indica la secuencia de sondeo, el usuario define si las dependencias se encuentran en Up o Down. El valor entre paréntesis después del nombre del dispositivo es un elemento identificador para resolver nombres ambiguos de los equipos como se muestra en la figura 5.3.21:

Los dispositivos se enumeran en el orden en que son consultados. Se puede arrastrar un dispositivo dentro de la rama para cambiar el orden de sondeo del equipo.



Figura 5.3.21: Tab Dependencies^[1]

5.3.8 TAB STATISTICS

Provee un fácil acceso a las estadísticas de sondeo del mapa activo. Se puede verificar las estadísticas acumuladas de cada dispositivo en el mapa de la red activa como se muestra en la figura 5.3.22. Las estadísticas de sondeo se conservan al cerrar o abrir los mapas de la red. Cada mapa tiene un archivo asociado y se registran en el archivo denominado map_name.wui.

Las estadísticas para cada dispositivo son:

✓ **Dispositivo:** El nombre del dispositivo.

- Dirección: Dirección del dispositivo (si el método de votación es ICMP o de servicios solamente).
- ✓ Tipo: El método de sondeo o monitoreo (ICMP, Servicios solamente, NetBIOS o IPX), creado en el cuadro de diálogo General en las propiedades del dispositivo.
- ✓ Un estado de cero indica que el dispositivo está activo. Cualquier otro valor indica un error.

WhatsOp Cold :	(Netro (metro w	al I	Natiatio	J.								
The Edit Vew 1	Monitor Configure	Took	Reports	Logi	window	140						
0 # 8 # 1	6 < 8	8										
Centa	Address	3.04	944	Pet	el Ca	5.8	S., .	Qea	1	h.,	Hr.	Ha.
1,03461	10.1.30.197	174	0	1178	. Ø.,	96.57	1.00	11.52	1	3	3	14
ARCHEL	10.50.76.12	10#	0	1178.	. e.,	99.66	0.34	346	4	1	- 2	254
AMESURVEZ	10.50.76.4	10#	0	1176	. e.,	99.10	6.90	10:08		7	- 2	26
446942411	10.55.76.6	10#	0	1176	. Ø.,	轻频	2.00	2436	16	10		199
4465,6101	10.50.76.1	109		1176	÷ Ø.,	96.07	6.13	1.00	5)	1	19
CACEMEN	10.28.0.22	109	0	1178	ø.,	91.09	6.11	147		64	8	94
AND/THE	10.3.10.19H	139	11010	1178.	. Ø.,	\$3.43	46.57	\$21.09	12		3	58
PETRO ADDRES	10.21.0.27	10#	0	1178.	e.,	95.94	0.0	0.40	1	64	12	125
PYCHEEL	10.3.30.195	109	ė.	1176	. 0.	95.94	1.06	0.57	1	1	1	136
MERCODASA-	10.21.0.52	109	ů.	1176	0.	99.94	1.04	0.40	÷	ú	- 92	110
LAUSTERE	10.4.30.252	109	- i	1176	0	99,83	6.0	151	ŝ	ñ	- 2	544
ACCOUNTS A	10.81.04.2	100	- 1	1176	. 0.	9.0	10	1.40	÷	5	÷	176
LOCATION	10.2.4E.1H	108	ā	1176	. 10	96.02	1.04	14	ŝ	÷	- 1	10
UCON HEL	10.50.18.2	124	ä	1120	0	16.10	0.10	147	- 2	- 1	- 1	38
LOOPEDE	10.51.46.2	100	- i	1176	0	99.53	1.07	0.44	÷	- 2	- 1	345
BL/MAC	10.51.61.2	100	- 1	1176	. 6.	95.54	1.04	0.40	-	1	- 1	1477
and the second	net kaded	107	- 1	1176		10.	1.00	1.00	- 1	- 1	- 1	1
COMPO	10.40.76.8	100	100	1178.	. 0.	4.86	10.	1131		- 1	- 1	- 1
A REAL	10.80.76.17	104		1176		4.5	1.30	14.04	÷	ú	- i	131
170-1000	10.4.30.100	100	- 1	1176		10.10	141	6.00		- 1		12
10000000	10.4.00.005	100		11/8		14.16	1.44	43.15	4	- 2	- 1	1140
10000	10.4.00.000	100	- 1	1078	- 8		1.45	60.07		- 1	- 1	1140
212024940	10.4.20.197	1.79		1076	- 5-	95.00	1.78	1992		1	- 1	100
0040/0001	10.1.20.1%	1.79	- 1	1076	1.01	99.00	9.12	105		- 1	- 1	
1708040	10.50.79.5	1.77		1176	1.0	96.97	1.00	110			- !	00
1,00H0	10.1.30.196	104		1178	. 0	99.38	0.12	129	1	1	- 1	205
104,HO	10.4.30.199	104	0	1178.	. 0	99.22	6.78	84	1	1	3	104
SHATURO:	10.1.20.195	138	0	1178.	. e.	99.87	0.00	0.00		3	- 1	111
BRCYORL	10.51.42.5	13#	0	1176	. e.,	转用	1.25	2.50	0	4		2548
175,041	10.50.79.2	10#		1176	. Ø.,	96.87	1.65	11.52	0	,		140
EPW7041	10.51.47.5	10#		1174	÷.	99.40	6.40	6.43		,	5	685
(PR)ANO	10.50.87.4	174	. 0	1178	. Ø.,	99.45	4.99	604	0	7	5	9R
0980960	10.50.87.3	174	0	1178	. ø.,	99.32	1.68	7.40	ņ			2385
STOTOPHOL	10.4.30.200	10#	0	1178.	. Ø.,	96.51	1.49	36.44	0	- 1		н
PR0.094400	10.51.04.4	139	0	1176	. e.,	99.96	0.04	0.25	3	13	6	215
1755/0402	10.3.20.199	10#	0	1176	. Ø.,	99.34	6.96	1047	0	3	t	119
10074740	10.3.40.208	10#	- 0	1178	ø.,	99.86	0.14	1.04	11		- 1	26
1000000	10.3.40.201	10₽	- i	1178.	ø.,	99.89	6.11	6.42		- 4	- 1	18
ABRILING	10.3.40.203	109	- i	1176	. 0.	95.88	6.02	D14	ò	÷.	- 1	30
1000761	10.4.10.207	100	- i	1176		101.	0.00	0.00	ő	- í	- 6	- 6
BRIDUEL	10.51.42.8	100	- 2	1178	0	99.74	1.94	1105	ě	- 5	- 1	hi
UNIONE	10.8.0.49	100	- 1	1104		99.81	6.19	bite	ŝ	-1	- 1	14
OFMEN	10.80.10.8	100	- 1	100		99.10		240	1	1	- 1	144
LOCH N	10.20.100.100	100	- 1	108	1.1	110	11	0.00	1	1		1
- AND MI	HAR IN AN	Ű.	_	100		1.1	10.00	1.1		-	_	_
Ne Xia	Dependencies		Station	in 🗋	11 10	éoni 🛛	14	M I				
And in case of the local division of the loc		10		-			_	_				

Figura 5.3.22: Tab Statistics^[1]

5.3.9 TAB NOTIFICATIONS

Permite observar las notificaciones habilitadas para el mapa activo de la red. Las notificaciones son agrupadas por dispositivo.

Se puede alternar entre orden ascendente y descendente mediante un clic en cualquiera de las columnas como se indica en la figura 5.3.23.

WhatsUp G	old - [Metro [Metro.wup]	: Notifica	tions]		
File Edit V	iew Monitor Configure Too	is Reports	Logs Windo	r Help	
D 🚅 🖬 👌	3 🖪 🙆 🖌 🛞 🕲				
Device	Alert Name	Trigger	Start Time	End Time	Send UP E
APRONSPICI	SMTPMail/PROBLEMA	4	0000	2400	
AMBENSM01	Sound/Default	4	0000	2400	
AMBEN/SM01	Sound/Default		0000	2400	
AM8CNTM01	Sound/Default	4	0000	2400	
AMBIZAM01	Sound/Default	4	0000	2400	
AMBIZAM01*	Sound/Default	4	0000	2400	
AMBIZAM02	Sound/Default	4	0000	2400	
AM8128M01	Sound/Default	4	0000	2400	
AMBPELM01	Sound/Default	4	0000	2400	
AMEPELM01	Sound/Default	4	0000	2400	
AM85R5M01	Sound/Default	4	0000	2400	
AMBSTGM01*	Sound/Default	4	0000	2400	
AMBSURM01	Sound/Default	4	0000	2400	
AMESURM02	Sound/Default	4	0000	2400	
AM82M8M01	Sound/Default	4	0000	2400	
AZG88LM01	Sound/Default	4	0000	2400	
AZGCNRM01	Sound/Default	4	0000	2400	
AZGCNTM01	Sound/Default	4	0000	2400	
BALZARCENM01	Sound/Default	4	0000	2400	
BBHBUFEM01	Sound/Default	4	0000	2400	
BBHCNTM01	Sound/Default	4	0000	2400	
DEHMTVM01	Sound/Default	4	0000	2400	
BBHQVDE01	Sound/Default	4	0000	2400	
BBHQVDM01	Sound/Default	4	0000	2400	
BBHQVDM02	Sound/Default		0000	2400	
BBHQVDM02	Sound/Default	4	0000	2400	
BBH53NM01	Sound/Default	4	0000	2400	
CCACNTM01	Sound/Default		0000	2400	
CCACNTM02	Sound/Default	4	0000	2400	
CCAONTM03	Sound/Default	4	0000	2400	
CCAGLOM01	Sound/Default	4	0000	2400	
CCAGL2M01	Sound/Default	+	0000	2400	
CCA3RTM01	Sound/Default	4	0000	2400	
CCANNRM01	Sound/Default	4	0000	2400	
CCAPAUM01	Sound/Default	4	0000	2400	
CCASELM01	Sound/Default	4	0000	2400	
CCAS0GM01	Sound/Default	4	0000	2400	
CCASPNM01	Sound/Default	4	0000	2400	
CCASTIM01	Sound/Default	4	0000	2400	
CCASV0M01	Sound/Default	4	0000	2400	
CCASVT1M01	Sound/Default	4	0000	2400	
CUECENM01	Sound/Default	4	0000	2400	
DAULEM01	Sound/Default	4	0000	2400	
ECCCENM01	Sound/Default	4	0000	2400	
ECCCENM01	Sound/Default	4	0000	2400	
ESMATCM01	Sound/Default	4	0000	2400	
ESMATCM01	Sound/Default	4	0000	2400	
ESMREFM01	Sound/Default	4	0000	2400	
ESMREPM01	Sound/Default	4	0000	2400	
ESMREFM02	Sound/Default	4	0000	2400	
ESMSLRM01	Sound/Default	4	0000	2400	
ESMSN3M01	Sound/Default	4	0000	2400	
DOMESARA	CandPatak		1		
Map 🔏 i	Edit E Dependencies	Statisti	cs No	difications	Status
Ready					

Figura 5.3.23: Tab Notifications^[1]

Es importante mencionar que se puede definir los diferentes tipos de notificaciones usando la *Librería de Notificaciones*, para esto ingresar en Menú a la opción *Configure* y seleccionar *Notifications Library*, como se indica en la figura 5.3.24:

Beeper	New.
E VE Pager	Edit.
S 2 Program SMS	Delete
Sound WinPopup	Test
	Close
	Liose

Figura 5.3.24: Notifications Library^[1]

5.3.10 TAB MINI STATUS

Esta pequeña ventana permite supervisar el estado de la red. Esta es una alternativa para la ventana del mapa y puede ser usada en monitores de baja resolución o cuando se desee guardar espacio en el monitor.

Para visualizar la ventana escoger la opción *View/ Mini Status* como se muestra en la figura 5.3.25, mediante esta opción la ventana de WhatsUp principal se cierra y aparece la vista de los dispositivos en una ventana más pequeña como se indica en la figura 5.3.26.



Figura 5.3.25: Selección de la opción Mini Status^[1]

La opción *Mini Status* muestra el estado de todos los dispositivos en los mapas actualmente activos, utilizando los mismos colores de la ventana MAP.



Figura 5.3.26: Mini Status^[1]

- ✓ Cada mapa abierto es listado en una columna separada. Cualquier servicio que está siendo monitoreado en un dispositivo es mostrado.
- ✓ Dar doble clic en la ventana Mini Status para cerrar esta e ir de regreso a la ventana del mapa.

5.3.11 TAB STATUS

Muestra una lista de todos los equipos que se encuentran activos en el mapa e indica el status de cualquier servicio que está siendo monitoreado como se indica en la figura 5.3.27.

Esta opción presenta la posibilidad de ampliar la ventana de estado con el fin de leer toda la información de monitoreo.

En la barra de herramientas principal haga clic en el botón *Poll* para iniciar un chequeo de cada dispositivo en la ventana Status.

Ó

∢

Dar clic en el botón *Stopwatch* para iniciar un sondeo automático de cada dispositivo.



Figura 5.3.27: Tab Status^[1]

5.3.12 MONITOREO DEL ESTADO DE LOS EQUIPOS

Al dar clic derecho en el equipo, seleccionar la opción *Quick Status* la misma que despliega una barra de herramientas que muestra las siguientes opciones: *Status, History, Up-Time y Logs History* del equipo.

5.3.12.1 STATUS

Muestra el estado de los paquetes enviados por Whats'up, si el equipo está activo o inactivo y el tiempo de respuesta como se muestra en la figura 5.3.28:

Categories	Status					
	Status:	0		Active and	responding	
Status	COURT	23	<i></i>	811:	0	-
	-ICMP S	tatus				
	Down	Count	Total	Last Res	ponse Time:	
History	0		0	09.33.0	7	
	Service	Statu				
	Down	Count	Total	Last Res	ponse Time:	
Up-1me	0	-	0	Not sinc	e initialization	_
57			1	1.000		
Log						

Figura 5.3.28: Status^[1]

5.3.12.2 HISTORY

Muestra el tiempo de respuesta relativa del dispositivo sobre los treinta últimos chequeos como se muestra en la figura 5.3.29:

Quick Status : 10.3.	40.201
Categories	History
Saak Batar	This chart shows you the relative response times of this device over the last 30 pole. Red vertical bars indicate the device not responding.
Up Time Log	max 7 min 4 avg 4
	OK Cancel Help

Figura 5.3.29: History^[1]

En el caso de presentarse barras verticales de color rojo quiere decir que el equipo no está respondiendo como se indica en la figura 5.3.30:



Figura 5.3.30: Equipo sin respuesta^[1]

5.3.12.3 UP-TIME

Muestra el porcentaje en el cual el equipo se encuentra en estado up como se muestra en la figura 5.3.31.



Figura 5.3.31: Estado Up del equipo^[1]

5.3.12.4 LOG

Muestra los logs del equipo, el cual permite obtener información útil acerca del procesamiento del equipo y los respectivos sucesos en caso de presentarse un problema como se indica en la figura 5.3.32.



Figura 5.3.32: Logs del equipo^[1]

También se puede observar los Logs seleccionando en la barra de herramientas en el menú principal la opción *Activity Logs* como se muestra en la figura 5.3.33:

Activity Log - 4/17/2011-Today	Đ
File Direction Content Display Help	
⇔ 🖽 ⇒ 🎒 😨 🧟 😵 🤄 Raw ∩ Formatted	
20110418 121051 Alert successful process N: F:0 A:Sound/ 20110418 121051 Alert successful process N: F:0 A:Sound/ 20110418 121039 Alert successful process N: F:0 A:Sound/ 20110418 121029 Alert successful process N: F:0 A:Sound/ 20110418 12029 Alert successful process N: F:0 A:Sound/ 20110418 12029 Alert successful process N: F:0 A:Sound/ 20110418 12049 UP LTCSLCM01 10:50.78 2 missed 3 20110418 120749 UP LTCSLCM02 10.3.20.199 missed 2 20110418 120600 DOWN LTCSLCM02 10.50.78 z Timed Out 20110418 120600 DOWN LTCSLCM02 10.50.78 z Timed Out	
<	5

Figura 5.3.33: Activity Log^[1]

Para conocer las formas predeterminadas y configurar los colores para el monitoreo de los equipos escoger en el menú las opciones *Configuration /Program Options /Device States*.

Cada uno de los siguientes iconos presenta un estado diferente del equipo:



El color verde encendido indica que el equipo está respondiendo al sondeo.



El color predeterminado verde claro indica que el equipo no ha respondido a un sondeo.



El color predeterminado amarillo sólido indica el equipo no ha respondido a dos sondeos consecutivos.



El color predeterminado amarillo sólido indica que el equipo no ha respondido a tres sondeos consecutivos.



El color predeterminado rojo sólido indica que el equipo no ha respondido de cuatro a siete sondeos consecutivos.



El color predeterminado sólido rojo obscuro indica que el equipo no ha respondido a ocho o más sondeos consecutivos o tiene un error de red.



El color predeterminado sólido púrpura, indica que un servicio se encuentra down en el equipo.



El color predeterminado sólido de color gris obscuro indica que un equipo está inactivo.

5.3.13 VERIFICACIÓN DE CONECTIVIDAD

Al dar clic derecho en el ícono del equipo que se encuentra en el mapa se puede visualizar una serie de herramientas de diagnóstico de red para verificar la conectividad a un sistema particular de la red.

5.3.13.1 CONNECT

Permite realizar conexión remota a un equipo mediante telnet como indica la figura 5.3.34.



Figura 5.3.34: Connect^[1]

5.3.13.2 PING

Es una herramienta de diagnóstico para verificar la conectividad. Ping envía un ICMP en forma de un paquete de datos a un host remoto y muestra los resultados para cada uno. Este intercambio se conoce como "ping". El comando ping muestra

también el tiempo de respuesta de llegada en milisegundos (esto puede variar dependiendo de la carga de red) y depuración de información sobre la interfaz de red como se indica en la figura 5.3.35:

Count Size:	5 ÷	Delay (sec): 1 Timeout (ms): 50	1.	C ICMP	NetBe i	B
	Address	Sent 2 bytes	Receiv	ed: 2 Min: 8 M Status	ax:10 Avg. 3	
2	10.6.20.194 10.6.20.194	50 50	8 10	Success Success		

Figura 5.3.35: Ping a un equipo^[1]

5.3.13.3 TRACEROUTE:

Permite localizar y ver la ruta real de un paquete IP desde el equipo local a otro host en Internet. Los tiempos de respuesta se muestran en milisegundos y pueden variar dependiendo de la carga de la red. El comando *TraceRoute* es útil para encontrar los puntos donde existan posibles problemas en redes grandes y complejas que están conectadas entre sí por los routers como se indica en la figura 5.3.36:

faximum Hopcount: 32 Map Results Resolve Addresses 0 0 0 0 0 0 0	1 👰 💐
meoux (ms): 5000 .	
Completed	1
Hop RTT Diff Address Status	
0 0 17216.19.158	
2 0 0 1/2.16.0.125	
4 8 8 10.6.20.194	

Figura 5.3.36: Traceroute^[1]

5.3.13.4 BROWSER

Permite acceder a la cartografía, la vigilancia, y las funciones de notificación vía web de un equipo remoto como indica la figura 5.3.37:



Figura 5.3.37: Browse^[1]

Si los paquetes ICMP ping no pueden viajar en la red a su equipo, puede controlar este equipo, monitoreando los servicios configurados anteriormente.

El seguimiento de un servicio siempre implica un handshake⁴⁷, un protocolo también puede incluir un intercambio de información adicional entre WhatsUp y el servicio. Estos se pueden verificar en los Logs de los equipos y se pueden identificar los servicios supervisados en el cuadro Services como se indica en la figura 5.3.38:

Categories	Services		
- 1	Services to monitor.		
General	Monitor	Commont	Add
-	DNS (Domain Name Service) ETP (Ele Transfer Protocol)		Edt.
50.00	PDP3 (Post Office Protocol V3)	6 -	Bemov
SNMP	SMTP (Simple Mail Transfer Pro	stocol)	
	a nin corken scan		
Monitor			
42			Auto Disc
Services			
7		M	

Figura 5.3.38: Services^[1]

⁴⁷ Handshake: Es el proceso de negociación entre protocolos

Al realizar un mapa que posea un contenedor, dar clic derecho en propiedades y poner el nombre del mapa relacionado con este contenedor.

5.4 MANUAL IPsolutionC

5.4.1 OBJETIVO

Conocer las herramientas de la plataforma IPsolutionC para configurar y disponer de la conmutación de etiquetas por medio de MPLS y VPNs.

5.4.2 INTRODUCCIÓN

En este manual se mostrarán diversas características que son comunes entre varias aplicaciones, todos los pasos que se indican permitirán realizar múltiples configuraciones para la creación de políticas y otras características en común.

Las secciones tratadas en este manual son las siguientes:

- ✓ Service Inventory
- ✓ Service Desing
- ✓ Monitoring
- ✓ Diagnostics
- ✓ Administration

Es importante mencionar que de la lista de secciones mencionadas anteriormente la más utilizada es la sección *Service Inventory* porque permite realizar configuraciones de customers, providers etc. de forma amigable.

5.4.3 INGRESO A LA PLATAFORMA

Para ingresar a la plataforma colocar la dirección IP correspondiente en el browser, cuando se encuentre en la página principal ingresar el nombre de usuario y contraseña respectivamente, como se indicó anteriormente esta plataforma se encuentra conformada por diversas secciones las mismas que se muestran a continuación:

5.4.4 OPCIÓN SERVICE INVENTORY

Esta opción contiene herramientas para administrar los elementos del inventario, solicitudes de servicios y dispositivos, como se mencionó anteriormente esta es la sección más utilizada ya que aquí es donde se realizan configuraciones principales como se muestra en la figura 5.4.1.

Para proceder a realizar configuraciones en esta sección seguir los pasos que se muestrana continuación:

1. Dar clic en la sección Service Inventory como se muestra en la figura 5.4.1:

		Home Shortcuts Account Index Help About Logo
ahaha	IP Solution Center	
CISCO	Service Inventory ervice Design Monitoring Diagnostics Administration	User: jlope
You Are Here: •		Customer: No
	Welcome to IP Solution Center (ISC).	
	Service Inventory Tools to manage inventory elements, service requests, and devices.	
	Service Design Tools to create and manage policies and templates.	
	Monitoring Tools to manage tasks, ping parameters, and generate Service Level Agreement (SLA) probes and reports.	
	Tools for automated troubleshooting and diagnostics	
	Administration Tools to manage users and ISC configuration, servers and licensing.	
	NOTE: Use the Index link in the top-right corner at any time to view an indexed list of all ISC areas.	

Figura 5.4.1: Ingreso a la plataforma^[1]

 A continuación escoger la opción *Inventory and Connection Manager* para realizar las configuraciones correspondientes como se muestra en la figura 5.4.2:

	Home I Shortcuts I Acc	ount I Index I Help I About I Logout
1 alatha	IP_Solution_Center	
CISCO		
	Service Inventory Service Design Monitoring Diagnostics Administration	User: Zackarias
 Invento 	ory an <mark>t Connection Manager + Discov</mark> ary + Device Console +	
You Are Here: • Service In	Inventory	Customer: None
	Service Inventory	
	Tools to manage inventory elements, service requests, and devices.	
	Costs and manage inventory elements and Service Remises (SRs) for licensed services, and view translary mans	
	Discover devices, connections, and services.	
	Device Console	
	Download commands and configiets to devices and view device configuration.	

Figura 5.4.2: Opción Service Inventory^[1]

Dentro de la opción *Inventory and Connection Manager* se tiene más opciones las cuales permiten realizar configuraciones de usuarios dependiendo de las necesidades del administrador, las mismas que se indican a continuación:

5.4.4.1 CREACIÓN DE CUSTOMERS

Los customers se crean con el fin de poder administrar configuraciones individuales y los servicios que se le asigna a cada uno de ellos.

Para la creación de Customers realizar los siguientes pasos:

1. Elegir la opción *Customers* como se muestra en la figura 5.4.3:



Figura 5.4.3: Opción Customers^[1]

2. En la pantalla que aparece a continuación, crear un nuevo *Customer* mediante la opción *Create* como se muestra en la figura 5.4.4:

Cus	tom	ers				
			Show	v Customers with Customer Name match	ning *	Find
					S	showing 1 - 10 of 16 records
#		Ct	stomer Name			
1.		cu_geswimax				
2.		cu_sip				
3.		cu_vrf_etapa_internet				
- 4.		cu-datos				
5.		cu-gestion				
6.		cu-gesxdsl				
7.		cu-iptv				
8.		cu-netandina				
9.		cu-netcnt				
10.		cu-netdef				
	Rows	per page: 10 💌			🗐 🌒 Go to pag	e: 1 of 2 💿 🕞 🕅
					Create	Edit Delete

Figura 5.4.4: Creación de un nuevo Customer^[1]

3. Colocar el nombre del cliente y la respectiva descripción del mismo, en esta sección se debe colocar cualquier información pertinente sobre el cliente que podría ser útil para los proveedores de servicios, la información se encuentra limitada a 256 caracteres, como se muestra en la figura 5.4.5:

	cu_new
Customer Abbreviation:	cn
Contact Information:	Franklin Calderon fono 20223625

Figura 5.4.5: Colocación del nombre y descripción del cliente^[1]

Es importante mencionar que el formato utilizado por los administradores es el siguiente:

- ✓ El nombre se coloca de la siguiente manera: cu_ y el nombre del cliente que ha sido asignado a una VRF⁴⁸. Ejemplo: cu_banco_pichincha
- 4. Guardar las configuraciones realizadas mediante la opción *Save* y verificar que el customer fue creado y añadido satisfactoriamente como se muestra en la figura 5.4.6:



Figura 5.4.6: Verificación de la creación del customer^[1]

5.4.4.2 ELIMINAR UN CUSTOMER

Para proceder a eliminar un *Customer* seguir los pasos que se muestran a continuación:

- 1. Escoger las opciones: Service Inventory > Inventory and Connection Manager > Customers.
- 2. Seleccione uno o más clientes que desee eliminar marcando la casilla de verificación a la izquierda del nombre del cliente.
- 3. Dar clic en el botón *Delete*. Este botón se activa únicamente si uno o más clientes se han seleccionado, por lo tanto una ventana de confirmación de borrado aparecerá como se muestra en la figura 5.4.7:

⁴⁸ Véase Acrónimos

Delete (Customer	
	С	onfirm Delete
		Showing 1-1 of 1 records
#		Name
1.	Customer2	
Rows per	page: 10 💌	
		Delete

Figura 5.4.7: Opción Delete Customer^[1]

5.4.4.3 CREACION DE PROVIDERS

Los *providers* son entidades las cuales tienen asignados un ASN (Número de Sistema Autónomo), los mismos que son creados para que trabajen sobre MPLS. Para la creación de *Providers* seguir los siguientes pasos:

1. Elegir la opción *Providers* en la pantalla como se muestra en la figura 5.4.8:

ababa	IP Solution Center		
CISCO	Service Inventory Service Design Monitor	Ing Diagnostics Administration	User: jparedes
 Inventory a 	nd Connection Manager 👻 Discovery 👻 Device Console 👻		
You Are Here: Service Invento	ry> Inventory and Connection Manager		Customer: None
Selection - Service Requests	Inventory and Connection Manager Create and manage inventory elements and Service Requests (SRs) for	or licensed services, and view topology maps.	
Traffic Engineering Management Inventory Manager	Service Requests Create, deploy, and manage Service Requests (SRs).	Customers Create and manage Customers.	
Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Topology Tool Tool Topology Tool Tool	Traffic Engineering Management Create, deploy, and manage elements of Traffic Management.	Create and manage Providers.	
Customers Customer Sites CPE Devices	Buk-manage inventory elements.	Create and manage pools for IP address, Multicast address, Route Distinguisher, Route Target, Site of Origin, VC D, and VLAN.	
 Providers Provider Regions PE Devices 	View topology maps.	CE Routing Communities Create and manage CE Routing Communities.	
Access Domains Resource Pools CE Routing Communities	Create and manage Devices.	VRFs Create and manage VRFs.	
VRPS VPNs Named Physical Circuits NPC Place	Create and manage Device Groups.	Create and manage VPNs.	
· PseudoWireClass		Create and manage Named Physical Circuits (NPCs).	
		Create and manage PseudoWireClass.	

Figura 5.4.8: Opción Providers^[1]

2. Crear el Proveedor (VRF) con el nombre del ISP que va a utilizar como se muestra en la figura 5.4.9:

Providers		
	Shi	ow Providers with Provider Name matching * Find
		Showing 1 - 2 of 2 record
#	Provider	Provider BGP AS
1. CNT		28006
2. 🔲 ETAPA		28006
Rows per page: 10 💌		I∢
		Create Edit Delete

Figura 5.4.9: Colocación de los parámetros para la creación del Provider^[1]

3. Colocar el nombre del ISP que va a ocupar la VRF

A cada sistema autónomo BGP se le asigna un único número de 16 bits, es importante recalcar que para este manual el valor del BGP AS se encuentra establecido por defecto para las configuraciones de todas las VRFs. El rango establecido del BGP AS va desde el 1 al 65535.

4. Guardar los cambios efectuados en la configuración como se muestra en la figura 5.4.10:

	/	Valor	establecido p defecto	or
Create Pro	vider			
Name*:	ISP_NEW			
BGP AS*:	28006			(1 - 65535)
Contact Info:	FRANKLIN CALDERON		<	
			Save	Cancel
Note: * - Require	ed Field			

Figura 5.4.10: Opción Create Provider^[1]

5. Verificar que el Provider fue creado y añadido satisfactoriamente como se muestra en la figura 5.4.11:

Selection	Providers		
Service Requests Traffic Engineering		Show Providers with Provider Name match	ing * Find
Inventory Manager Tapalagy Tapal	*	Provider	Provider BGP AS
	1. CNT		28006
Device Groups			28006
Customers Customer Sites	3. SP NEW		28006
··· CPE Devices Providers	Rows per page: 10 💌	I	🛯 🕄 Go to page: 1 💿 🖉 🕅
Provider Regions PE Devices			Create Edit Delete
Access Domains Resource Pools			
CE Routing Communities VIDEe			
· VPNs			
NAmed Physical Circuits NPC Rings			
·· PseudoWireClass			
Status			
Operation: Create Provider Status: Succeeded			

Figura 5.4.11: Verificación de la creación del Provider^[1]

5.4.4.4 RESOURCE POOLS

Esta opción define un rango de direcciones IP para proporcionar servicios MPLS. Para la creación de *Resources Pools* seguir los pasos que se muestran a continuación:

		Home I Shortcuts	I Account I Index I Help I About I Logout
111111	IP Solution Center		
CISCO	Service Inventory Service Design Monito	ring Diagnostics Administration	
	service mentory service searging monito		User: jparedes
 Inventory and 	d Connection Manager		
You Are Here: . Service Inventor	Inventory and Connection Manager		Customer: None
	Inventory and Connection Manager		
Selection	Create and manage inventory elements and Service Requests (SRs) t	for licensed services, and view topology maps.	
Service Requests			
Management	Service Requests	Customers	
- Inventory Manager	(SRs).	Create and manage costoniers.	
 Topology Tool 	Testfie Consideration Management	Providers	
" Devices	Create, deploy, and manage elements of	Create and manage Providers.	
Device Groups	 Traffic Management. 		
> Customers	Inventory Manager	Resource Pools	
·· Customer Sites	Bulk-manage inventory elements.	Create and manage pools for IP address, Multicast address, Route Distinguisher, Rou of Ocioin VC ID, and VI AN	e Target, Site
·· CPE Devices	10×		
Providers Provider Regions	Topology Tool	CE Routing Communities	
·· PE Devices	View topology maps.		
·· Access Domains	Devices	VRFs	
Resource Pools	Create and manage Devices.	Create and manage VRFs.	
CE Routing Communities VDFe			
· VPNs	Device Groups	VPNs	
Named Physical Circuits	Create and manage Device Groups.	Create and manage VPNs.	
NPC Rings		Named Dissignal Circuits	
PseudoWireClass		Create and manage Named Physical Circuits (NPCs).	
		PseudoWireClass	
		Create and manage PseudoWireClass.	

1. Elegir la opción Resource Pools como se muestra en la figura 5.4.12:

Figura 5.4.12: Opción Resource Pools^[1]

 Reservar un recurso del pool para distinguir qué servicio se va a proporcionar, se recomienda usar la opción *Route Target* porque indica a MPLS cuando las rutas deben ser insertadas en la vrf apropiada, como se muestra en la figura 5.4.13:

I I I I I I I I I I I I I I I I I I I	IP Solution Center (Service Inventory) (Service Design (Monitoring) (Diagnostice) (Administration) Connection Manager = Olicovery = Device College =)	Home Shortcuts Account Index Heip About Logout User jparedes
You Are Here: • Service Inventory	Inventory and Connection Manager's Resource Rede Resource Pools	Customer: Hone
Service Requests Traffic Engineering Management Inventory Manager Topology Tool Topology Tool Devices	Pool Type: PV4 Address PV4 Address PV4 Addres PV4 Address PV4 Address PV4 Address PV4 Add	of Type All V Find Showing 0 of 0 records Pool Name
Device Groups Customers Customer Sites CPE Devices Providers Providers Provider Regions	Rows per pl VLAN	K Create Delete v
PE Devices Access Domains Resource Pools Cercourse Pools Vering Vering Vering Hermod Rhysical Crouts Hermod Rhysical Crouts Hermod Rhysical Crouts Hermod NyviceLass		

Figura 5.4.13: Opción Route Target^[1]

3. A continuación escoger un Start libre o disponible.

Tomar en cuenta que los identificadores de Vrfs están asignados o reservados del 101001 hasta el 101008 y los identificadores que se encuentran disponibles o libres van desde 101009 hasta el siguiente pool.

En la siguiente tabla se aprecia los tipos de servicios que se pueden proporcionar:

TIPO DE SERVICIO	
10xxx	Net Internet
20xxx	Datos
30xxx	Multicast
40xxx	VoIP
50xxx	Gestión

 Tabla 5.4.1 -Estados de una VNE Tipo de servicios
 [1]

4. Dentro de la opción *Route Target* verificar que las configuraciones son correctas como se muestra en la figura 5.4.14:

Resource	Pools					
Pool Type:	Route Target	▼				
				Show Ro	oute Target Pools with Pool Name matching	Find
		1				Showing 1 - 10 of 13 records
#	Start	Pool Size	Status		Pool Name	
1. 🔲 1		2	Allocated	28006:CNT		
2. 🔲 10	01001	8	Allocated	28006:CNT		
3. 🔽 10	01009	992	Available	28006:CNT		
4. 🗌 20	01001	2	Allocated	28006:CNT		
5. 📃 20	01003	3	Available	28006:CNT	1	
6. 🗌 20	01006	2	Allocated	28006:CN1	•	
7. 📃 20	01008	993	Available	28006:CNT		
8. 🔲 30	01001	1	Allocated	28006:CNT		
9. 🔲 30	01002	999	Available	28006:CNT		
10. 🔲 40	01001	2	Allocated	28006:CNT		
Rows per	rpage: 10 💌				IA 4	Go to page: 1 of 2 😡 🔉 🕼
						Create Delete

Figura 5.4.14: Verificación de configuraciones ^[1]

5.4.4.5 CE ROUTING COMMUNITIES

Una VPN puede ser organizada en subgrupos llamados CE Routing Communities, o Cercs. Un CERC describe cómo una VPN se puede comunicar con otra VPN. Por lo tanto, los Cercs describen la topología lógica de la VPN.

Para la creación de CE Routing Communities seguir los pasos que se muestran a continuación:

 Elegir la opción CE Routing Communities como se muestra en la figura 5.4.15 :

ahaha	IP Solution Center		Home Shortcuts Account Index Help About Logou
CISCO	Service Inventory Service Design Monito	oring Diagnostics Administration	User: jparede:
Inventory and	nd Connection Manager	•	
You Are Here: Service Inventor	y> Inventory and Connection Manager		Customer: Non
	Inventory and Connection Manager		
Service Requests	Create and manage inventory elements and Service Requests (SRs)) for licensed services, and view topology maps.	
Traffic Engineering Management Inventory Manager	Service Requests Create, deploy, and manage Service Requests (SRs).	Create and manage Customers.	
Topology Tool Devices Device Groups	Traffic Engineering Management Create, deploy, and manage elements of Traffic Management.	Providers Create and manage Providers.	
Customers Customer Sites CPE Devices	Buk-manage inventory elements.	Create and manage pools for IP address, Multicast address, Ro of Oribio MC ID, and MI AN	oute Distinguisher, Route Target, Site
 Providers Provider Regions PE Devices 	View topology maps.	CE Routing Communities Create and manage CE Routing Communities.	
Access Domains Resource Pools CE Routing Communities	Create and manage Devices.	Create and manage VRFs.	
VRFs VPNs Named Physical Circuits NPC Pings	Create and manage Device Groups.	Create and manage VPNs.	
- PseudoWireClass		Create and manage Named Physical Circuits (NPCs).	
		PseudoWireClass Create and manage PseudoWireClass.	

Figura 5.4.15: Opción CE Routing Communities^[1]

2. En la pantalla que aparece a continuación crear la nueva Community mediante la opción *Create* como se muestra en la figura 5.4.16:

						Hon	ne Shortcuts Account	I Index Help About Logout
ahaha	IP Solution Ce	nter						
CISCO	Service Inventory	Service Design	Monitoring Diagnos	tics Admini	stration			lines in an de s
Inventory and	Connection Manager +	Discovery + Device	Console 🔹					oser: jparedes
Man Are Here a Consistent and	Investment Concerning Mary	and CE Dautine Commu						Customer: Nano
Too Are here. • Service inventory.	CE Routing Commun	ties	1003					outonor, nono
Selection								
Service Requests Traffic Engineering						Show CERCs with Name	Matching *	Find
Management								Showing 1 - 10 of 17 records
Inventory Manager Topology Topi	2	Name	HRT	SRT		Provider		VPN
	1. 🔲 cerc-bnf		28006:201006	28006:201006	CNT			
Devices Device Groups	2. 🔲 cerc-dat001		28006:201001	28006:201001	CNT			
> Customers	3. 🔲 cerc-dat002		28008:201002	28006:201002	CNT			
Customer Sites CPE Devices	4. 🔲 cerc-dat007		28006:201007	28006:201007	CNT			
> Providers	5. 🔲 cerc-gestion		28008:501001	28006:501001	CNT		vpn-gestion	
Provider Regions PE Devices	6. 🔲 cerc-geswimax		28006:501003	28006:501003	CNT		vpn-ges.wimax	
·· Access Domains	7. 🔲 cerc-gesxdsl		28006:501002	28006:501002	CNT		vpn-gesxdsl	
·· Resource Pools	8. 🔲 cerc-iptv		28006:301001	28006:301001	CNT		vpn-iptv	
Communities	9. 🔲 cerc-netandina		28006:101005	28006:101005	CNT		vpn-netandina	
·· VRFs	10. 🔲 cerc-netcnt		28006:101004	28006:101004	CNT		vpn-netcnt	
VPNs Named Physical Circuits	David and 10						MA di Costor	and 1 of 2 m DDI
NPC Rings	Rows per page. 10						1 1 00103	
PseudoWireClass							Create	Edit Delete
Status								
Operation: Delete CE Routing								
Communities								
Status: M Succeeded								

Figura 5.4.16: Creación de una nueva Community^[1]

3. Escoger la opción *Select* y elegir el ISP⁴⁹ correspondiente como se muestra en la figura 5.4.17:

Create CE Routing C	ommunity		Select Provider - Windows Internet Explorer
Provider*:	ISP_NEW	Select	
Name*:			Show Providers with Provider Name matching * Find
CERC Type:	Hub and Spoke Fully Meshed		Showing 1 - 3 of 3 records Provider
Auto-pick route target values:			
Route Target 1:			3. () ISP_NEW
Route Target 2:			Rows per page: 10 💌 🛛 🗐 Go to page: 1 of 1 💷 🕞 🕅
	Save	Cancel	Select
Note: * - Required Field			

Figura 5.4.17: Selección del ISP^[1]

El nombre regido a la norma establecida: Cerc_datxxxx_nombreISP xxxx= Start de Resource Pool.

Ejemplo: Cerc_dat1424_ISP_NEW

4. Elegir Fully Meshed para que se puedan ver entre todos los equipos CEs

⁴⁹ Véase Acrónimos

- 5. Colocar el Start libre del Tipo de Servicio que se quiera configurar (Resource Pool).
- 6. Colocar el BGP AS asignado cuando se creó el PROVIDER
- 7. Guardar los cambios realizados como se muestra en la figura 5.4.18:

Create CE Routing	Community
Provider [*] :	ISP_NEW Select
Name*:	cerc_dat1009_new
CERC Type:	Hub and Spoke Fully Meshed
Auto-pick route target value	es:
Route Target 1:	28006 101009
Route Target 2:	
	Save Cancel
Note: * - Required Field	

Figura 5.4.18: Configuraciones de una comunidad respectiva^[1]

8. Verificar que se creó y añadió satisfactoriamente la Community como se muestra en la figura 5.4.19:

al. de					Hom	e Shortcuts Account Index	Help About Logout
CISCO	IP Solution Center Service Inventory Service Designed d Connection Manager + Discovery + Dev	gn Monitoring Diagno: ice Console •	atics Admini	stration			User: jparedes
You Are Here: Service Inventory	Inventory and Connection Manager CE Routing Con	nmunities					Customer: None
Selection	CE Routing Communities						
Service Requests Traffic Engineering					Show CERCs with Name	matching *	Find
Management ·· Inventory Manager			0.07			Showi	ng 1 - 10 of 18 records
·· Topology Tool		nki	SRI		Provider	VPN	_
Devices	1. Cerc datious new	28006:101009	28006:101009	ISP_NEW			
Device Groups		20006:201006	20006:201006	CNT			
Customers Customer Sites	a. Cerc-datori	20000.201001	28006.201001	ONT			
·· CPE Devices	Cerc-datooz	20000.201002	28006:201002	ONT			
Provider Regions		28008-501001	28006:501001	ONT		von-destion	
·· PE Devices	7 cerc-geswimax	28006:501003	28006:501003	ONT		von-geswimax	
Resource Pools	8. Cerc-gesxdsl	28006:501002	28006:501002	CNT		von-gesxdsl	
CE Routing Communities	9. cerc-iptv	28006:301001	28006:301001	CNT		vpn-lptv	
·· VRFs	10. Cerc-netandina	28006:101005	28006:101005	CNT		vpn-netandina	
•• VPNs Named Physical Circuits •• NPC Rings	Rows per page: 10 💌					I¶ Go to page: 1	of 2 🌀 🕽 🎝 🛛
PseudoWireClass						Create	Edit Delete
Status Operation: Save CE Routing Community Status: Succeeded							

Figura 5.4.19: Verificación de la creación de la comunidad^[1]

5.4.4.6 VRFs

Para la creación de una Vrf seguir los pasos que se muestran a continuación:

1. Elegir la opción VRFs como se muestra en la figura 5.4.20:



Figura 5.4.20: Opción VRF's^[1]

2. Crear la nueva VRF como se muestra en la figura 5.4.21:

CISCO • Inventory and	IP Solution Center Service Inventory Service Design Monitoring Diagnostics Adminis Connection Manager > Device Console >)	tration		User: jparedes
You Are Here: • Service Inventory>	Inventory and Connection Manager >> VRFs VRFs			Customer: None
Service Requests Traffic Engineering Management		Show VRF with VRF Name	matching *	Find
Inventory Manager Topology Tool	VRF Name		Provider	
Devices	1. bnf	ONT		
Device Groups Customers	3. dat1008	ETAPA		
Customer Sites CPE Devices	4. netont	CNT		
Providers ·· Provider Regions	Rows per page: 10 💌		【<】 Go to page 1	of 1 🎟 🕞 🕞 🛙
PE Devices Access Domains Resource Pools			Create Edit Co	opy Delete
CE Routing Communities VRFs				
VPNs Named Physical Circuits				
NPC Rings PseudoWireClass				

Figura 5.4.21: Creación de una nueva VRF^[1]

Escoger la opción Select para elegir el Provider como se muestra en la figura 5.4.22:

Create VRF			🖉 Select Provider - Windows Internet Explorer 💦 🔲 🕅 🔀
Name": Provider":	dat1009	Select	Show Providers with Provider Name matching Find Showing 1 - 3 of 3 records
VRF Attributes CE Routing Communities*: Import RT List:		Select	1. ○ CHT 2. ○ ETAPA 3. ○ ISP_HEW Rows per page: 10 ♥ 【《 ④ Go to page: 1 of 1 ▷ ▷】
Export RT List: Import Route Map: Export Route Map:			Select
Maximum Routes: 🎱 Threshold: 🔍 RD*:		(1 - 4294967295) (1 - 100) utopick RD	
Enable Multicast: Enable Auto Pick MDT Addresses: Default MDT Address*:		(a.b.c.d)	
Data MDT Subnet": Data MDT Size: Data MDT Threshold:		(a.b.c.d) (1 - 4294967 kilobita/sec)	
Default PIM Mode: MDT MTU: III	SPARSE_DENSE_MODE	(576 - 65535)	
SSM List Name*:			

Figura 5.4.22: Selección de un proveedor^[1]

- ✓ El nombre establecido: Datxxxx
- ✓ Dat: Para los servicios de datos, el tipo de servicios se muestra en la Tabla 5.4.1
- ✓ xxxx= Start de Resource Pool

Ejemplo: Dat1424, donde Dat=20 y 1424 es el Star de Resorce Pool

 Colocar el tipo de servicio que se va a implementar, además se puede ubicar datos adicionales como el nombre del cliente como se muestra en la figura 5.4.23:

Provider". ISP_NEW Select Description: Desc	Name":	dat1009
Description: VRF Attributes CE Routing Communities : Select Moot RT List: Export RT List: Show CERCs with Name ♥ matching * Find Export Route Map: Show CERCs with Name ♥ matching * Find Show Dest Route Map: Show Ser page 10 ♥ Widt @ On to page 1 or 1 @ 0 Ro*: Enable Multicast: Enable Multicast: Default MDT Addresses: Default MDT Addresses: Data MDT Stoe: Bab Multicast: Select Mot MDT Addresses: Select Mot MDT Addresses: Mot MDT Addresses: Select Mot MDT Addresses: Select Mot MDT Addresses: Mot MDT Addresses: Select Mot MDT Addresses: Select Mot MDT Addresses: Select Mot MDT Addresses: Select Mot MDT Addresses: Select Mot MDT Addresses: Select Sel	Provider [*] :	ISP_NEW Select
VRF Attributes CE Routing Communities : Export RT List: Export RT List: Brow Raute Map: Export Route M	Description:	datos new
CE Routing Communities : Select Import RT List: Export RT List: Moot RAUE Map: Export Route Map: Show CERCs with Name ▼ matching * Find Show DERCs With Addresses; P Default NDT Addresses; Default PIM Mode: SPARSE_DENSE_MODE ▼ MOT LITU ♥ (576 - 65535)	VRF Attributes	
Import RT List: Export RT List: Import Route Map: Export Route Map: Export Route Map: Show CERCs with Name ▼ matching * Find Show DERCs With Name ▼ Find Show DERCs With Addresses * Default NDT Addresses * Default NDT Addresses * MOT WIT With Name ▼ Find Show DERCs With Addresses * MOT WIT With Name ▼ Find Show DERCs With Addresses * WITH With Name ▼ Find Show DERCs With Addresses * Show DERCs With Addresses * WITH With Name ▼ Find Show DERCs With Addresses * WITH With Name ♥ Show DERCs With Addresses * WITH With Addresses * Show DERCs With Addresses	CE Routing Communities*:	Select
Export RT List:	Import RT List:	Select CE Routing Communities - Windows Internet Explorer
Import Route Map: Show CERCs with Name matching Find Export Route Map: Show CERCs with Name SRT Provider VPI Maxmum Routes 1 cerc_dat1009_new 28006-1010 28006-1010 SRT Provider VPI Threshold: Import Page 10 Import Page 10 Import Page 1 of 1 mm	Export RT List:	
Export Route Map: Showing 1 - 1 of 1 m Maxmum Routes I 0 SRT Provider VPU Maxmum Routes I 0 cerc_dat1009_new 28006-1010 28006-1010 28006-1010 28006-1010 Provider VPU RD*: Rows per page 10 IV IV <t< td=""><td>Import Route Map:</td><td>Show CERCs with Name 💌 matching *</td></t<>	Import Route Map:	Show CERCs with Name 💌 matching *
Maximum Routes UN Unover VPI Threshold 1. ⊙ cerc_dat1009_new 28006.1010 22006.10109 SP_NEW Threshold RD*: Rows per page 10 I// () Q o to page 1 or 1 () Select Incr Enable Muticast I Incr Incr Select Incr Enable Muticast Incr Incr Incr Incr Incr Incr Default MDT Addresses: Incr Incr Incr Incr Incr Incr Incr Data MDT Subret*: Incr I	Export Route Map:	Showing 1 - 1 of 1 record
Threshold: Rows per page: 10 v I() 0 to page 1 or 1 m I) RD*: Rows per page: 10 v I() 0 to page 1 or 1 m I) Enable Muticast I Enable Muticast I Enable Muticast I Default MDT Addresses: I Default MDT Addresses: I Data MDT Subnet*: (a.b.c.d) Data MDT Size: I Data MDT Size: I Default PIM Mode: SPARSE_DENSE_MODE v MDT MTU: (576 - 65535)	Maximum Routes: 🔍	1. O cerc dat1009 new 28006:1010 9 28006:10109 ISP NEW
RD*: Image: Discussion of the set of	Threshold: 🔍	David and another 10 and 10
Enable Muticast Enable Muticast Enable Muticast Enable Muticast Enable Muticast C Enable Muticast Enable Muticast Enable Muticast C Enable Muticast Enable	RD*:	Rows per page. 10
Enable Auto Pick MOT Addresses: Image: Comparison of the compa	Enable Multicast: 🔍	Select ancel
Default NDT Address*: (a.b.c.d) Data NDT Subnet*: (a.b.c.d) Data NDT Stat: (a.b.c.d) Data NDT Stat: (1.4294967 kilobta/sec) Data NDT Thresholt: (1.4294967 kilobta/sec) Default PM Mode: SPARSE_DENSE_MODE V MDT NTU: (576 - 66535)	Enable Auto Pick MDT Addresses:	
Data NDT Subnet : (a.b.c.d) Data NDT Size: (1 - 4254967 kilobtarisec) Data NDT Threshold: (1 - 4254967 kilobtarisec) Defauk PM Mode: SPARSE_DENSE_MODE (576 - 66535) MDT INTU- (4) (578 - 66535)	Default MDT Address*:	(a.b.c.d)
Data MDT Sce: I v Data MDT Threshod: (1 - 4294967 kitobts/sec) Default PM Mode: SPARSE_DENSE_MODE v MDT MTU: (576 - 65535)	Data MDT Subnet [*] :	(a.b.c.d)
Data MDT Threshold: (1 - 4294967 kilobita/sec) Default PM Mode: SPARSE_DENSE_MODE MDT MTU: (576 - 65535)	Data MDT Size:	
Default PIM Mode: SPARSE_DENSE_MODE MOD MTU: (576 - 65535)	Data MDT Threshold:	(1 - 4294967 kilobits/sec)
MDT INTU: (\$76 - 65535)	Default PIM Mode:	SPARSE_DENSE_MODE V
	мат мти: 🤍	(576 - 65535)
Enable PIM SSM: DEFAULT V	Enable PIM SSM:	T DEFAULT -

Figura 5.4.23: Parámetros de configuración de una VRF^[1]

Es importante mencionar lo siguiente:

- ✓ IMPORT RT: Es opcional cuando se crea una nueva VRF pero si ya existe una configurada previamente es necesario colocarlo.
- ✓ RD*: Colocar el mismo que se ingresó cuando se creó el CE correspondiente como se muestra en la figura 5.4.24:

Create VRF	
Name*:	dat1009
Provider [*] :	ISP_NEW Select
Description:	datos new
VRF Attributes	
CE Routing Communities [*] :	cerc_dat1009_new Select
Import RT List:	xxxxx (opcional)
Export RT List:	xxxxx (opcional)
Import Route Map:	
Export Route Map:	
Maximum Routes: 🔍	(1 - 4294967295)
Threshold: 🍳	(1 - 100)
RD*:	28006:101009
Enable Multicast: 🤍	
Enable Auto Pick MDT Addresses:	
Default MDT Address*:	(a.b.c.d)
Data MDT Subnet [*] :	(a.b.c.d)
Data MDT Size:	1 *
Data MDT Threshold:	(1 - 4294967 kilobits/sec)
Default PIM Mode:	SPARSE_DENSE_MODE
мот мти: 🤍	(576 - 65535)
Enable PIM SSM:	EFAULT -
SSM List Name*:	

Figura 5.4.24: Parámetros opcionales para la configuración de una VRF^[1]

5. Para crear la VRF escoger *Save* como se muestra en la figura 5.4.25:

CE Routing Communities*: cerc_dat1009_new Select Import RT List:
Import RT List:Export RT List:Import Route Map:Export Route Map:Maximum Routes:Maximum Routes:Import Route Map:Maximum Routes:Pashold:Import Route Map:Import Route Map:Import Route Map:Import Route Map:Import Route Map:Import Routes:Import Routes:Import Route Map:Import Route Multicast:Import
Export RT List: Import Route Map: Import Route Map: Import Route Map: Export Route Map: Import Route Map: Maximum Routes: Import Route Map: RD*: 28006:101009 RD*: 28006:101009 Enable Multicast: Import Route Rou
Import Route Map: Export Route Map: Maximum Routes: Maximum Routes: Import Route Map: Maximum Routes: Import Route Map: Import Route Map: Import Route Map: Import Routes: Import Route: Import Routes: Import Routes: <
Export Route Map: Maximum Routes: Maximum Routes: Threshold: Threshold: RD*: 28006:101009 Autopick RD Enable Multicast: P Enable Auto Pick MDT Addresses: Image: Point Point Addresses: Image: Point Point Addresses: Image: Point Po
Maximum Routes: (1 - 4294967295) Threshold: (1 - 100) RD*: 28006:101009 Autopick RD Enable Multicast: Enable Auto Pick MDT Addresses: Default MDT Address*: (a.b.c.d) Data MDT Subnet*: (a.b.c.d) Data MDT Size: (1 - 4294967 kilobits/sec) Default PIM Mode: SPARSE_DENSE_MODE
Threshold: (1 - 100) RD*: 28006:101009 Autopick RD Enable Mutticast: Enable Auto Pick MDT Addresses: Default MDT Address*: (a.b.c.d) Data MDT Subnet*: (a.b.c.d) Data MDT Size: 1 Data MDT Threshold: (1 - 4294967 kilobits/sec) Default PIM Mode: SPARSE_DENSE_MODE
RD*: 28006:101009 Autopick RD Enable Multicast: Image: Constraint of the system of the s
Enable Multicast: Image: Constraint of the set of the
Enable Auto Pick MDT Addresses: Image: Constraint of the set of
Default MDT Address*: (a.b.c.d) Data MDT Subnet*: (a.b.c.d) Data MDT Size: 1 Data MDT Threshold: (1 - 4294967 kilobits/sec) Default PIM Mode: SPARSE_DENSE_MODE
Data MDT Subnet*: (a.b.c.d) Data MDT Size: 1 Data MDT Threshold: (1 - 4294967 kilobits/sec) Default PIM Mode: SPARSE_DENSE_MODE
Data MDT Size: I Data MDT Threshold: (1 - 4294967 kilobits/sec) Default PIM Mode: SPARSE_DENSE_MODE
Data MDT Threshold: (1 - 4294967 kilobits/sec) Default PIM Mode: SPARSE_DENSE_MODE
Default PIM Mode: SPARSE_DENSE_MODE V
MDT MTU: 🤍 (576 - 65535)
Enable PIM SSM:
SSM List Name*:
Multicast Route Limit: (1 - 2147483647)
Enable Auto RP Listener:
Configure Static-RP:
My PIM Static-RPs*: Showing 0 of 0 records Edit
Static-RP Multicast-Group List Name Override
Rows per page: 10 💌 🛛 🗐 🖓 Go to page: 1 🖉 of 1 🗺 🕞 🕅
Save Cancel

Figura 5.4.25: Guardar las configuraciones de la VRF^[1]

6. Es importante verificar si el cliente se creó y se añadió satisfactoriamente como se muestra en la figura 5.4.26:

					Home Shortcuts Account	Index Help About Logout 🖹
11111111	IP Solution Center					
CISCO 🖌	Service Inventory Servi	ce Design Monitoring Dia	ignostics Administration			lines increates
	Connection Manager + Discour	un a Device Concela a				User: jparedes
• inventory and	connection manager v biscovi	ny • Device console •				
You Are Here: Service Inventory	Inventory and Connection Manager VF	Fo				Customer: None
	VRFs					
· Saprice Requests						
·· Traffic Engineering			Show VRF w	th VRF Name	Matching	Find
Management						Showing 1 - 5 of 5 records
Inventory Manager	*	VRF Name			Provider	
- Topology Tool	1. D bot		ONT			
· Devices	2 C dat1007		ONT			
- Device Groups			ETADA			
Customer Sites	2. I Datious		ETAPA			
·· CPE Devices	. dat1009		ISP_NEW			
Providera			CNT			
Provider Regions PE Devices Access Domains	Rows per page: 10 💌				∎<] <] Go to pa	ige:1 of 1 💷 ▷ ▷ I
Resource Pools CE Routing Communities					Create Edit	Copy Delete
• VRFs						
Named Physical Circuits						
·· NPC Rings						
Oneurdel Mitre Classe	-					
Status						
Operation: Save VRF						
Status: 🛒 Succeeded						

Figura 5.4.26: Verificación del cliente añadido satisfactoriamente [1]

5.4.4.7 VLANS

Para la creación de VLANS seguir con los pasos que se muestran a continuación:

1. Elegir la opción *Service Inventory* y dentro de ésta escoger la opción *Device Console* como se muestra en la figura 5.4.27:



Figura 5.4.27: Opción Device Console^[1]

2. Seleccionar la opción Next como se muestra en la figura 5.4.28:

				nome I Shortcuts I Account I	Index 1 Help 1 About 1 Logout
	IP Solution (Center			
CISCO	Service Inventor	Service Design Monitoring Diagnos	tics Administration		
4					User: jparedes
www.cory and t	connection Manager 👻 D	Discovery • Device Console • ,			
You Are Here: Service Inventory:	Device Console				Customer: None
	Device Console -	Choose Operation			
Mode: ADDING 1, Choose Operation 2	Operation:	Downlaad Commands Downlaad Template Downlaad Template Device Configuration Manager EXEC Commands Rebad			
	Select Operation Method:	Simplified Advanced (via wizard)			
	Sign 1 of 2				
	- Step 1 012 -			<back next=""></back>	Finish Cancel

Figura 5.4.28: Opción Next^[1]

3. La búsqueda se puede realizar ya sea por Dispositivos o por Grupos.

✓ BÚSQUEDA POR DISPOSITIVO

Para realizar una búsqueda por dispositivo ver la figura 5.4.29:

Device Console - Download Commands							
Devices:		Select/Deselect					
Groups:		🖉 Select Device(s) - Windows Internet Explorer					
Operation Commands:	Show Devices with Device Name Matching *LCL*			Find			
		#		Device Name	Management IP	Sho Type	Wing 1 - 1 of 1 record Parent Device
		1.		UIOLCLE01.andinatel.com	10.50.0.62	Cisco IOS Device	name
Options:	Upload Config After Dov Retrieve device attribute	Ro	ws per page:	10 💌		∎¶ ¶ Go to page: 1	of 1 🌀 🕨 🕅
						Se	elect Cancel
Note: * - Required Field							<u> </u>

Figura 5.4.29: Búsqueda por Dispositivo^[1]

✓ BÚSQUEDA POR GRUPO

Para realizar una búsqueda por grupo ver la figura 5.4.30:

ahaha	IP Solution Center	Home T	
CISCO	Service Inventory Serv	vice Design Monitoring Diagnostics Administration	
v Inventory and	Connection Manager 🔹 Discovery	🖉 Select Group(s) - Windows Internet Explorer	
You Are Here: • Service Inventory > Device Console Device Console - Downlo		http://10.8.33.9/8030/isc/device_console_collection.do	
		Show Device Groups with Device Group Name 👻 matching * Find	
	Devices:	Showing 1 - 9 of 9 records	
	Groups:	1. CNT-PE99	
	Operation Commands:	3. CNT-PE Region 1	
		4	
	Options:	C UT-PE Region 5	
		9. CIT-PE Region 7	
	Note: * - Required Field	Select Cancel	
1111		😜 Internet 🦓 + 🔍 100% - 🛒	

Figura 5.4.30: Búsqueda por Grupo^[1]

 Colocar los siguientes parámetros en el comando de operación como se muestra en el siguiente ejemplo y finalmente seleccionar Ok como se muestra en la figura 5.4.31:

Device Console - Download Commands				
Devices:	UIOLCLE01.andinatel.com	Select/Deselect		
Groups:		Select/Deselect		
Operation Commands:	exit interface vlan 999 no shut interface gigabitethernet5/1 switchport trunk allowed vlan 999	add		
Options:	Upload Config After Download Retrieve device attributes			
		OK Cancel		

Figura 5.4.31: Selección de parámetros en el comando de operación ^[1]

- ✓ Importante: no olvidar poner ADD en los comandos de operación.
- 2. Finalmente verificar si la vlan ya se encuentra creada como se muestra en la figura 5.4.32:

	Device Console Operation Result				
			Show Devices with Device Name matching * Find		
	Download Commands Results				
	# Device Name	Status	Results		
	1. UIOLCLE01.andinatel.com	Successful			
	Rows per page: 10 💌		N		
			Download Done		
Status Operation: Download Commands Status: Succeeded					

Figura 5.4.32: Verificación de la creación de la VLAN^[1]

5.4.4.8 MPLS VPN

Para la creación de MPLS VPN seguir los pasos que se muestra a continuación:

 En la opción Service Inventory escoger la opción Inventory and Connection Manager como se muestra en la figura 5.4.33:



Figura 5.4.33: Opción Inventory and Connection Manager^[1]

2. Para crear este servicio elegir la opción *Service Requests* como se muestra en la figura 5.4.34:



Figura 5.4.34: Opción Service Requests^[1]

3. En la barra desplegable en la opción *Create* seleccionar *MPLS VPN* como se muestra en la figura 5.4.35:
| abab | IP So | lutio | n Cei | iter | | | | | | Home Shor | tcuts Account Index | Help About Logout |
|---|--------------|----------|-------------|--------------------|------|---|------------|-----------------------|----------------------|-----------------|-------------------------|-----------------------------|
| CISCO | Service | e Inve | ntory | Service Desig | IN M | onitoring Di | agnostics | Administration | | | | User: jparedes |
| You Are Here: • Service Inventory > | Inventory an | id Conne | ction Manag | er> Service Reques | its | solo • ////////////////////////////////// | | | | | | Customer: None |
| Selection | Service | Requ | osts | | | | | | | | | |
| Service Requests Traffic Engineering | | | | | | | Show Servi | ces with Job ID | w matching | * | of Type All | Find |
| Management
·· Inventory Manager
·· Topology Tool | | Job ID | Data Files | State | | Type Operation | n Creator | Customer Name | Policy Name | Last Modified | Showing 141
Descript | - 148 of 148 records
Ion |
| ·· Devices | 141. 🗖 40 | 06 | | DEPLOYED | MPLS | ADD | jparedes | cu_vrf_etapa_internet | PL-VPN-VRF-
ETAPA | 4/14/09 6:16 PM | | |
| Device Groups Customers | 142. 🔲 40 | 07 | | DEPLOYED | VRF | MODIFY | jparedes | cu_vrf_etapa_internet | None | 4/15/09 6:02 PM | | |
| ·· Customer Sites | 143. 🔲 40 | 80 | | DEPLOYED | MPLS | ADD | aalmeida | cu_sip | PL-L3VPN-NoCE | 4/15/09 1:31 PM | | |
| Providers | 144. 🔲 40 | 09 | | DEPLOYED | MPLS | ADD | jparedes | cu_vrf_etapa_internet | PL-VPN-VRF-
ETAPA | 4/15/09 6:01 PM | | |
| Provider Regions PE Devices | 145. 🔲 41 | 10 | | DEPLOYED | VRF | MODIFY | jparedes | cu_vrf_etapa_internet | None | 4/15/09 6:01 PM | | |
| ·· Access Domains | 146. 🔲 41 | 14 | | CLOSED | MPLS | DELETE | jparedes | cu_vrf_etapa_internet | PL-VPN-VRF-
ETAPA | 4/16/09 3:31 PM | | |
| ·· CE Routing Communities | 147. 🔲 41 | 16 | | DEPLOYED | MPLS | ADD | jparedes | cu_vrf_etapa_internet | PL-VPN-VRF-
ETAPA | 4/16/09 3:47 PM | | |
| ·· VPNs | 148. 🔲 41 | 17 | | DEPLOYED | VRF | ADD | jparedes | cu_vrf_etapa_internet | None | 4/16/09 3:47 PM | | |
| Named Physical Circuits NPC Rings PseudoWireClass | Rowsp | per page | 10 💌 | | | | | | | | I 🗐 🗐 Go to page: 15 | of 15 💷 🕨 🕬 |
| | Auto Refn | esh: 🔽 |) | | | | | Create Details | Status y | Edit Deplo | y y Decommission | n Purge y |
| | | | | | | | _ | MPLS VPA | | | | |
| | | | | | | | | VPLS | | | | |
| | | | | | | | | VRF | | | | |
| | | | | | | | | TE | | | | |
| | | | | | | | | FlexUNI(EVC) | | | | |

Figura 5.4.35: Selección de la opción MPLS VPN^[1]

- 4. Siempre elegir la política (Policy) para todas las MPLS VPN que se vayan a crear como se muestra en la figura 5.4.36.
 - ✓ Se escoge esta política porque es una plantilla de configuraciones base para los servicios MPLS-VPN.

ababa	IP Solution Center	Home I Shortcuts I Account I Index I Help I About I Logout
CISCO	Service Inventory Service Design Monito	ring Diagnostics Administration User: Zackarias
You Are Here: + Service Inventory:	Inventory and Connection Manager > Service Requests	Customer: None
Selection	Select MPLS Policy	
Gervice Requests Traffic Engineering	Sho	v MPLS policies with Policy Name 💌 matching *
Inventory Manager Topology Tool	# Policy Hame	Showing 11 - 18 of 18 records Policy Owner
·· Devices	11. O PL-L3VPN-NoCE-Netpeer	Provider - CNT
Device Groups	12. O PL-L3VPN-NoCE-VolP	Provider - CNT Global
Customers Customer Sites	14. O PL-L3VPN-VRF_NETCNT_NO-CE-INT	Provider - CNT
Providers	15. O PL-VPN-NETCNT-NO-CE-INT	Provider - CNT
Provider Regions PE Devices	16 O DL VON VOE ETADA-NO-CE	Provider - ETAPA
Access Domains Besource Pools	17. O PL-VRF-NO-CE	Provider - CNI Provider - CNT-SIP
CE Routing Communities VRFs VPNs	Rows per page: 10 💌	⊲] ⊲] Go to page: 2 of 2
 Named Physical Circuits NPC Rings Result/MiscClass 		OK Cancel
·· PseudoVVireClass		

Figura 5.4.36: Selección de la opción Policy^[1]

5. Seleccionar el Customer anteriormente creado y escoger Select como se muestra en la figura 5.4.37:

MPLS Service	Request Editor			
			MPLS Service Request Editor	
Job ID:		SR ID:	SR State:	
Policy: PL	VPN_VRF_NEW_NO_C	E		
Customer: Se	lect Customer		🖉 Select Customer - Windows Internet Explorer	3
Description :			Show Customers with Customer Name matching	
#	Link ID	UNI device	Showing 1 - 10 of 17 records	Ink Attribute Logical Link
Rows per page:	10 💌			[I]] Go to page 1 of 1 🚾 ▷ ▷
			3. O cu_sip	Link Delete Link Save Cancel
			4. O cu_vrf_etapa_internet	
			5. O cu-datos	
			6. O cu-gestion	
			7. O cu-gesxdal	
			8. O cu-iptv	
			9. O cu-netandina	
			10. O cu-netcnt	
			Rows per page: 10 💌 🕅 🗟 Go to page 1 of 2 💷 🖗 🕅	
			Select Cancel	

Figura 5.4.37: Selección del Customer anteriormente creado^[1]

6. Añadir el enlace como se muestra en la figura 5.4.38:

						Home Shortcuts Account	t Index IHelp IAbout ILogo
ahaha	IP Solution Center						
CISCO	Service Inventory Servi	ce Design Monit	oring Diagnostics Adr	ninistra	ation		liser inared
Inventory and	Connection Manager + Discove	ry + Device Console					oser. jpurede
You Are Here: • Service Inventory>	Inventory and Connection Manager Se	rvice Requests					Customer: No
	MPLS Service Request Ed	tor					
Selection							
Service Requests Traffic Engineering			MPLS Servic	e Requ	uest Editor		
Management	Job ID:	SR ID:	SR State:				
 Inventory Manager 	Policy: PL_VPN_VRF_NEW	NO_CE					
·· Topology Tool	Customer; cu new						
·· Devices				_			
Device Groups	Description :						
Customers Customer Stee				<u> </u>			
·· CPE Devices							Showing 0 of 0 records
> Providers	# 🗌 Link ID	UNI device	UNI Interface	PE	PE Interface	Link Attribute	Logical Link
Provider Regions						14.4	
·· PE Devices	Rows per page: 10 💙						page: I OT I 🞯 🛛 🕅
Resource Pools						Add Link Delete Lin	k Save Cancel
·· CE Routing Communities						Add Link	- Dave Curreer
·· VRFs							
·· VPNs							
Named Physical Circuits NPC Dises							
. DeaudoWireClase							
- accountractors							

Figura 5.4.38: Adición de un enlace ^[1]

 Seleccionar el equipo del provider como se muestra en las figuras 5.4.39 y 5.4.40:

MPLS Se	ervic	e Request	Editor						
				MPLS Serv	/ice Request I	Editor			
Job ID:			SR ID:	SR State:					
Policy:		PL_VPN_VRF_N	IEW_NO_CE						
Customer:		cu_new							
Description	n :								
									Showing 1 - 1 of 1 reco
#		Link ID	UNI device	UNI Interface	PE	PE Interfac	e	Link Attribute	Logical Link
1.		0	Select UNI Device	~	Select PE		Add		N/A
Rowsp	ber pag	e: 10 💌						📢 🍕 Go to page	1 of 1 💷 🕅 🕅
							Add Lir	Delete Link	Save Cancel

Figura 5.4.39: Selección del equipo del proveedor^[1]

		MPLS Servi	ce Request Edit	tor		
Job ID:	SR ID:	SR State:				
Policy: PL_VPN_VRF	_NEW_NO_CE					
Customer: cu_new						
Description :			 X 			
						Showing 1 - 1 of 1 recr
# Link ID	UNI device	UNI Interface	PE	PE Interface	Link Attribute	Logical Link
1. 🔲 0	Select UNI Device	~	Select PE	~	Add	N/A
Rows per page: 10 💌	Select PE Device -	Windows Internet Explor	er		∎¶ ¶ Go t	opage: 1 of 1 💷 👂 🕽
	Show PEs with Dev	ice Name 💌 matching	*lci*	Find	Add Link Delete Li	ink Save Cancel
			Showing 1	1 - 1 of 1 record		
	# Device 1. () () UIOLCLE01.6	ndinatel.com CNT P	PE Region Name R-UIOLCL	N-PE		
	Rows per page: 10	✓ Id	Go to page: 1	of 1 💿 🕨 🕅		
			Select	Cancel		

Figura 5.4.40: Opción PE Device ^[1]

- 8. Elegir la interface que para este caso será la Vlan.
- 9. Revisar si la VLAN se encuentra configurada en el equipo correspondiente como se muestra en la figura 5.4.41:

IPLS Service I	Request Editor							
			MPLS Servic	e Request Edit	or			
Job ID:	SR ID:		SR State:					
Policy: PL_	_VPN_VRF_NEW_NO_CE							
Customer: cu_	_new							
Description :				4				
								Showing 1 - 1 of 1 record
# 🗌 Link I	D UNI device	UNI Interface	PE		PE Interface		Link Attribute	Logical Link
1. 🔲 0	Select UNI Device	~	UIOLCLE01	Select One	*	Add	l .	N/A
Rows per page:	10 💌			Loopback141 Loopback150 Loopback151		I	🕼 📢 Go to page:	of 1 💷 🖓 🕅
				Loopback155 Loopback200		Add Link	Delete Link	Save Cancel
				Tunnel0 Tunnel16218				
				Tunnel16222 Tunnel16226				
				Tunnel56260				
				Vlan1				
				Vlan116				
				Vlan200 Vlan201				
				Vlan202				
				Vlan203 Vlan204				
				Vlan2999				
				Vlan301				
				Vlan303				
				Vlan304				
				Vlan305 Vlan306				
				Vlan307	E			
				Vlan308				
				Vlan312 Vlan313		l l	Intranet local	100%
				Vlan999	~			- 100 %

Figura 5.4.41: Selección de la interface vlan^[1]

10. Añadir la Vlan creada como se muestra en la figura 5.4.42:

			MPLS Service	Request Editor				
Job ID:	SR ID:		SR State:					
Policy: PL_VF	N_VRF_NEW_NO_CE							
Customer: cu_ne	w							
Description :				<u>∼</u>				
							Sh	owing 1 - 1 of 1 reco
# Link D	UNI device	UNI Interface	PE		PE Interface	Link	Attribute	Logical Link
1. 🔲 0	Select UNI Device	~	UIOLCLE01	Vlan999	~	<u>Add</u>		N/A
Rows per page: 10	~					IQ Q	Go to page: 1	of 1 💿 👂 🕽
						Add Link Dele	te Link	Save Cancel

Figura 5.4.42: Adición de una vlan creada^[1]

- 11. En la opción *Interface Description* ingresar el nombre del administrador y número de servicio (NS) como se muestra en la figura 5.4.43.
 - NS: El número de servicio es un identificador numérico asignado para la identificación del circuito de un cliente.

MPLS Link Attribute Editor - Interface	
Attribute	Value
PE Information	
PE	UIOLCLE01
Interface Name:	Vian999. (1-4294967295)
Interface Description:	HEERAN_OSCAR_563
Shutdown Interface:	
- Step 1 of 3 -	<back liext=""> Finish Cancel</back>

Figura 5.4.43: Opción Interface Description^[1]

12. Colocar la IP WAN del equipo del cliente (CE^{50}) con su respectiva máscara es importante no dejar espacios como se muestra en la figura 5.4.44:

⁵⁰ Véase Acrónimos

MPLS Link Attribute Editor - IP Address Scheme	
Attribute	Value
PE-CE Interface Address/Mask	
IP Numbering Scheme:	IPv4 Numbered 🔹
Automatically Assign IP Addresses:	
PE Interface Address/Mask*:	192.168.1.1/30 a.b.c.d/e)
Note: * - Required Field	
- Step 2 of 3 -	<back itext=""> Finish Cancel</back>

Figura 5.4.44: Colocación de la IP WAN y máscara a un equipo^[1]

13. Colocar la IP LAN del equipo del cliente (CE) con su respectiva máscara es importante no dejar espacios además adicionar el tipo de prioridad como se muestra en la figura 5.4.45:

Attribute		Value						
CE Ipv4 Routing Information		🖉 🖉 Advertised Routes - Windows Internet Explorer 🛛 🗐						
outing Protocol	STATIC 💌							
sC Support:								
ive Only Default Routes to CE:		Advertised Routes						
edistribute Connected (BGP only):		Select IP Address/Mask (a.b.c.d/e) (1-255)						
efault Information Originate (BGP only):		✓ 172.16.1.0/29						
dvertised Routes for CE:	Edit							
ext Hop Option:	USE_OUTGOING_INTF_NAME	Add Delete OK Cancel						
* - Required Field								

Figura 5.4.45: Colocación de la IP LAN y máscara a un equipo^[1]

14. Escoger la opción *USE_NEXT_ HOP_IPADDR* la misma que permite cuál será el siguiente salto por donde se puede hallar la red LAN, como se muestra en la figura 5.4.46:

Attribute	Value
PE-CE Ipv4 Routing Information	
Routing Protocol	STATIC 💌
CsC Support:	
Give Only Default Routes to CE:	
Redistribute Connected (BGP only):	
Default Information Originate (BGP only):	
Advertised Routes for CE:	Edit
Next Hop Option:	USE_OUTGOING_INTF_NAME V
Note: * - Required Field	USE_NEXT_HOP_IPADDR

Figura 5.4.46: Opción USE_NEXT_ HOP_IPADDR ^[1]

15. Colocar la dirección IP WAN del siguiente salto del equipo del cliente como se muestra en la figura 5.4.47:

Attribute	Value
E Ipv4 Routing Information	
outing Protocol	STATIC 👱
sC Support:	
ive Only Default Routes to CE:	
edistribute Connected (BGP only):	
efault Information Originate (BGP only):	
dvertised Routes for CE:	Edit
ext Hop Option:	USE NEXT HOP IPADDR
ext Hop IP Address*:	192.168.1.2 a.b.c.d)
* - Required Field	

Figura 5.4.47: Colocación de la dirección IP WAN^[1]

Attribute	Value
RF Information	
Use VRF Object:	
VRF Object *:	dat1009 Select
BGP Multipath Load Sharing:	
BGP Multipath Load Sharing: te: * - Required Field	
BGP Multipath Load Sharing: te: * - Required Field	
BGP Multipath Load Sharing: e: * - Required Field	
BGP Mutpath Load Sharing: a: * - Required Field	
BGP Mutpath Load Sharing: e: * - Required Field	
BGP Mutpath Load Sharing: e: * - Required Field	
BGP Multipath Load Sharing e. * - Required Field	
BOP Muthpath Load Sharing:	

Figura 5.4.48: Opción Next^[1]

16. Escoger *Finish* como se muestra en la figura 5.4.49:

					Showing 1	- 1 of 1 recor
Device Nan	ne	Role Type		Template/Data File		
UIOLCLE01	N-PE		Add			
Rows per page: 40 💌				I ⊴ ⊲ Go	to page: 1	if 1 💿 🛛 🕅
* - Required Field						

Figura 5.4.49: Opción Finish^[1]

Es importante mencionar que cuando se olvida guardar la configuración aparece una advertencia y para ello se debe colocar la opción *Save* como se muestra en la figura 5.4.50:

ahaha	IP Solution Cent	er					Home Shi	ortcuts Account Inc	dex Help About Logou
CISCO	Service Inventory Se Connection Manager + Disc	rvice Design Mc	nitoring Diagn	ostics Admin	istration				User: jparede
You Are Here: • Service Inventory>	Inventory and Connection Manager>	Service Requests							Customer: Non
Selection	MPLS Service Request	Editor							
Service Requests				MPLS Service	Request Edito	r			
Management	Job ID:	SR ID:		SR State:					
Inventory Manager Topology Tool	Policy: PL_VPN_VRF_	NEW_NO_CE							
" Devices	Customer: cu_new								
Devices Device Groups Customers	Description :								
·· Customer Sites ·· CPE Devices					1				Showing 1 - 1 of 1 record
 Providers Provider Pegions 	# Link D	UNI device	UNI Interface	PE		PE Interface		Link Attribute	Logical Link
·· PE Devices	1. [] 0 Select (JNI Device	×	UIOLCLE01	Vlan999	~		Edited	N/A
Access Domains Resource Pools	Rows per page: 10 💌							∎∢] ∢] Go to page:	1 of 1 💷 🔉 🖓
VRFs VPNs							Add Link	Delete Link	Save Cancel
Named Physical Circuits NDC Direct									
PseudoWireClass									
Status Operation: Save Link Attribute									
Status: Failed More Info									

Figura 5.4.50: Advertencia para guardar cambios^[1]

5.4.4.9 CREACIÓN DE SERVICIO MPLS-VPN

Cuando se crea una MPLS-VPN automáticamente se crea una VRF pero si solo se desea añadir una VRF se debe seguir los siguientes pasos:

- 1. Crear la VRF
- 2. Adjuntar la VRF a la Interface como se muestra en la figura 5.4.51:

ILIIII CISCO	IP Solution Consection Manager	enter Service Des Discovery + Do	ign (Monitor vice Console 🔹	ring (E	liagnostics	Administratio	n	Home Shor	tcuts Account Index Help About User: j	l Logo
You Are Here: • Service Inventory:	Inventory and Connection Mar	lager> Service Requ	iests						Custor	ner: No
Selection	Service Requests									
Traffic Engineering					Show Ser	vices with Job ID	✓ matching		of Type All 👻 Find	
Management Inventory Manager Topology Tool	# 🔲 Job ID Data Files	State	Туре	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Showing 141 - 150 of 150 re Description	cords
· Devices	141. 🔲 406	DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/14/09 6:16 PM		_
Device Groups	142. 🔲 407	DEPLOYED	VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:02 PM		
Customers Customer Sites	143. 🔲 408	DEPLOYED	MPLS	ADD	aalmeida	cu_sip	PL-L3VPN-NoCE	4/15/09 1:31 PM		
·· CPE Devices	144. 🔲 409	DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/15/09 6:01 PM		
Providers Provider Regions	145. 🔲 410	DEPLOYED	VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:01 PM		
·· PE Devices	146. 🔲 414	CLOSED	MPLS	DELETE	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:31 PM		
Access Domains Resource Pools	147. 🔲 416	DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:47 PM		
· CE Routing Communities				and a	jparedes	cu_vrf_etapa_internet	None	4/16/09 3:47 PM		
VRFs VPNs	149. 🗹 418	REQUESTED	MPLS	4 0 0	jparedes	cu_new	PL_VPN_VRF_NEW_NO_CE	4/16/09 6:38 PM		
Named Physical Circuits	150. 🗹 419	REQUESTED	VRF	4 0 0	jparedes	cu_new	None	4/16/09 6:38 PM		
··· NPC Rings ·· PseudoWireClass	Rows per page: 10	~							【④ ④ Go to page: 15 of 15 Go	⊳⊳∎
	Auto Refresh: 🔽					Create 🔻 Do	tails Status 🔻	Edit Deplo	y v Decommission Purge	•

Figura 5.4.51: Adición de la VRF a la interface ^[1]

3. En la barra desplegable escoger la opción *Deploy* tanto para la VRF como para la interface como se muestra en la figura 5.4.52:

La opción *Deploy* sirve para que se ejecute la información de todos los formularios de configuración del servicio MPLS correspondiente.

ahaha	IP Solution C	enter						Home Shor	rtcuts Account Index He	lp About Logout
CISCO	Service Inventory	Service Des	ign Monito	ring	Diagnostics	Administration				User: jparedes
Inventory and	Connection Manager	Discovery • De	vice Console 🔹							
You Are Here: Service Inventory	Inventory and Connection Mar	nager Service Requ	iests							Customer: None
Selection	Service Requests									
Service Requests Traffic Engineering					Show Se	rvices with Job ID	✓ matching	*	of Type All	Find
Management									Showing 141 - 15	50 of 150 records
Inventory Manager Topology Tool	# 🔲 Job ID Data Files	State	Туре	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description	
·· Devices	141. 🔲 406	DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/14/09 6:16 PM		
Device Groups	142. 🔲 407	DEPLOYED	VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:02 PM		
Customers Customer Sites	143. 🔲 408	DEPLOYED	MPLS	ADD	aalmeida	cu_sip	PL-L3VPN-NoCE	4/15/09 1:31 PM		
·· CPE Devices	144. 🛄 409	DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/15/09 6:01 PM		
Provider Regions	145. 🛄 410	DEPLOYED	VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:01 PM		
·· PE Devices	146. 🔲 414	CLOSED	MPLS	DELETE	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:31 PM		
Access Domains Resource Pools	147. 🔲 416	DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:47 PM		
·· CE Routing Communities	148. 417	DEPLOYED	VRF	ADD	jparedes	cu_vrf_etapa_internet	None	4/16/09 3:47 PM		
·· VRFs	149. 🗹 418	REQUESTED	MPLS	ADD	jparedes	cu_new	PL_VPN_VRF_NEW_NO_CE	4/16/09 6:38 PM		
> Named Physical Circuits	150. 🖌 419	REQUESTED	VRF	ADD	jparedes	cu_new	None	4/16/09 6:38 PM		
·· NPC Rings ·· PseudoWireClass	Rows per paper	~							I⊲ ⊲ Go to page: 15	of 15 😡 🕅 🕅
	Auto Refresh: 🔽					Create v De	tails Status v	Edit Deplo	w Becommission	Purge 🔻
								De	ploy	
								Porce	Debioa	

Figura 5.4.52: Opción Deploy^[1]

4. Guardar los cambios efectuados como se muestra en la figura 5.4.53:

CISCO	IP Solutio	on Center
 Inventory and 	Connection Mar	nager 🗸 Discovery 🗸 Device Console 🔹
You Are Here: • Service Inventory •	Inventory and Conne Deploy Servic	ection Manager+ Service Requests Ce Requests
Service Requests Traffic Engineering	Task Name * :	Task Created 2009-04-16 18:41:11.528
Management	Task Type :	Deployment
Topology Tool Devices Device Groups	Task Description :	Created on Thu Apr 16 18:41:11
Customers Customer Sites CPE Devices	Single run: Operiodic Run: Operiodic Run: Operiodic Run: Operiodic Run	Now O Once Minute O Hourly O Daily O Weekly O Monthly
Providers Provider Regions PE Devices Access Domains	Periodic Run Attrib Run Interval: Run Limits:	butes
Resource Pools CE Routing Communities VRFs VPNs Named Physical Circuits	Start Date and Tim Date: April Time: 6	ne v 16 v 2009 v 41 v PM v
PseudoWireClass	End Date and Time Date: Month Time: Hour	e (Defaut is unlimited) v Day v Year v Min v AM v
	Service Requests	
		Showing 1 - 2 of 2 records
	# Job D 1. 418	iparedes cuinew
	2. 419	jparedes cu_new
	Rows per pa	age: 10 💌 🛛 📢 🔇 Go to page 1 of 1 💷 🕅 🕅
		Save Cancel

Figura 5.4.53: Guardar cambios efectuados ^[1]

5. Revisar el cambio de Estado y que se creó satisfactoriamente como se muestra en la figura 5.4.54:

abab	IP	s	oluti	ion Co	enter						Home Shor	tcuts Account Index	Help	About Logo
CISCO	Ser				Service Des	ign Moni	toring	liagnostics	Administratio					User: jpared
You Are Here: • Service Inventory	hyanti		and Con	nager v	agers Service Reau	uesta	* a							Customer: No
	Serv	ice	Req	uests	ager - serrice requ									
Service Requests Traffic Engineering								Show S	ervices with Job ID	watching	•	of Type All	~ [Find
Management Inventory Manager Topology Tool			Job ID	Data Files	State	Туре	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Showing 1 Descr	11 - 150 o Iption	f 150 recorda
- Devices	141.		406		DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/14/09 6:16 PM			
· Device Groups	142.		407		DEPLOYED	VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:02 PM			
Customera Customer Sites	143.		408		DEPLOYED	MPLS	ADD	aalmeida	cu_sip	PL-L3VPN-NoCE	4/15/09 1:31 PM			
·· CPE Devices	144.		409		DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/15/09 6:01 PM			
Providers Provider Regions	145.		410		DEPLOYED	VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:01 PM			
·· PE Devices	146.		414		CLOSED	MPLS	DELETE	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:31 PM			
·· Access Domains	147.		416		DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:47 PM			
·· CE Routing Communities	148		417		DEPLOYED	VRF	ADD	paredes	cu_vrf_etapa_internet	None	4/16/09 3:47 PM			
·· VRFs	149.		418		REQUESTED	MPLS	ADD	paredes	cu_new	PL_VPN_VRF_NEW_NO_CE	4/16/09 6:38 PM			
Named Physical Circuits	150.		419		REQUESTED	VRF	ADD	paredes	cu_new	None	4/16/09 6:38 PM			
NPC Rings PseudoWireClass	R	Rows	per pa	ge: 10	~							I⊲ ⊲ Go to page: 15	of 1	5 🚥 🕨 🕅
Status Deplay Service	Auto	o Ref	fresh:	V					Create y De	tails Status 👻	Edit Deplo	y y Decommissi	on	Purge 👻
Operation: Requests Status: Succeeded														

Figura 5.4.54: Revisión de los cambios efectuados ^[1]

6. Para finalizar verificar que ya se encuentran activas (Up) las interfaces como se muestra en la figura 5.4.55:

ahah	IP	Solut	ion Ce	enter						Home Shor	tcuts Account Index	Help About Logou
CISCO	Ser Conn	vice Invection M	ventory anager •	Service Des Discovery 🔶 De	ign Monitor vice Console 🔹	ing (I	Diagnostics	Administratio				User: jparede
ou Are Here: • Service Inventory •	Invent	ory and Cor	inection Man	ager > Service Requ	ests							Customer: Nor
Selection • Service Requests • Traffic Engineering	Serv	ice Rec	uests				Show Ser	vices with Job ID	watching 1		of Type All	Find
Management Inventory Manager Topology Tool	#	Job IE	Data Files	State	Туре	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Showing 141 Descript	150 of 150 records on
·· ·· Devices	141.	406		DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/14/09 6:16 PM		
Customers Customer Sites	142. 143.	407		DEPLOYED DEPLOYED	VRF MPLS	MODIFY ADD	jparedes aalmeida	cu_vrf_etapa_internet cu_sip	None PL-L3VPN-NoCE	4/15/09 6:02 PM 4/15/09 1:31 PM		
·· CPE Devices Providers	144.	409		DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/15/09 6:01 PM		
Provider Regions PE Devices	145.	410		CLOSED	MPLS	DELETE	jparedes jparedes	cu_vrf_etapa_internet	None PL-VPN-VRF-ETAPA	4/15/09 6:01 PM 4/16/09 3:31 PM		
Access Domains Resource Pools	147.	416		DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:47 PM		
CE Routing Communities VRFs VDNe	140.	417		DEPLOYED	MPLS	ADD	jparedes jparedes	cu_vrr_etapa_internet	NONE PL_VPN_VRF_NEW_NO_CE	4/16/09 5:47 PM		
Named Physical Circuits NPC Rings	150.	419		DEPLOYED	VRF	ADD	jparedes	cu_new	None	4/16/09 6:43 PM		
·· PseudoWireClass	R	lows per pa	ige: 10	*							Go to page: 15	of 15 🙆 🕨 🕅
	Auto	Refresh:	Z					Create V De	tails Status v	Edit Deplo	y v Decommission	Purge v

Figura 5.4.55: Verificación del estado de la interface ^[1]

5.4.4.10 BORRAR VRF'S

Para borrar una VRF realizar los pasos que se muestran a continuación:

1. Elegir una por una las interfaces para proceder a borrarlas y a continuación escoger la opción *Decommission* como se muestra en la figura 5.4.56:

ahaha	IP Solution Ce	nter						Home Shor	tcuts Account Index Help	About Logout
CISCO	Service Inventory Connection Manager •	Service Des Discovery • De	ign Monitor vice Console 🔹	ing Di	agnostics	Administration				User: Zackaria
You Are Here: • Service Inventory >	Inventory and Connection Man	ager> Service Requ	rests							Customer: None
	Service Requests									
Service Requests Traffic Engineering					Show Se	rvices with Job ID	💌 matching 1	,	of Type All	Find
Management ·· Inventory Manager ·· Topology Tool	# 🗍 Job ID Data Files	Stato	Туре	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Showing 141 - 15 Description	0 of 150 records
Devices	141. 🔲 406	DEPLOYED	MPLS	ADD	paredes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/14/09 6:16 PM		
·· Device Groups	142. 🔲 407	DEPLOYED	VRF	MODIFY	paredes	cu_vrf_etapa_internet	None	4/15/09 6:02 PM		
Customers Customer Sites	143. 🛄 408	DEPLOYED	MPLS	ADD	aalmeida	cu_sip	PL-L3VPN-NoCE	4/15/09 1:31 PM		
·· CPE Devices	144. 🔲 409	DEPLOYED	MPLS	ADD)	paredes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/15/09 6:01 PM		
Providers Provider Regions	145. 🛄 410	DEPLOYED	VRF	MODIFY	iparedes	cu_vrf_etapa_internet	None	4/15/09 6:01 PM		
·· PE Devices	146. 🛄 414	CLOSED	MPLS	DELETE	[paredes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:31 PM		
·· Access Domains	147. 🔲 416	DEPLOYED	MPLS	ADD j	paredes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:47 PM		
·· CE Routing Communities	140. 1 417	DEPLOYED	VRF	ADD)	iparedes .	cu_vrf_etapa_internet	None	4/16/09 3:47 PM		
·· VRFs	149. 🗹 418	DEPLOYED	MPLS	ADD)	paredes	cu_new	PL_VPN_VRF_NEW_NO_CE	4/17/09 10:30 AM		
 Named Physical Circuits 	160 171 410	DEPLOYED	VRF	ADD)	iparedes	cu_new	None	4/17/09 10:30 AM		
•• NPC Rings •• PseudoWireClass	Rows per page: 10	~							I⊲ ⊲ Go to page: 15	of 15 🐽 🗅 🖂
Status	Auto Refresh:					Create 🔻 Det	ails Status 🔻	Edit Deplo	y Decommission	Purge 🔻
Status:										

Figura 5.4.56: Opción Decommission^[1]

2. Para efectuar los cambios realizados seleccionar OK como se muestra en la figura 5.4.57:

r				
ahaha	IP Solution Cent	- T		Home Shortcuts Account Index Help About Logou
CISCO	Service Inventory Se	rvice Design Monitoring Diago	nostics Administration	
 Inventory and 	nd Connection Manager + Disc	overy + Device Console +		User: Zackana
You Are Here: • Service Inventor	ve Inventory and Connection Managere	Service Requests		Customer: No.
	Confirm Request			
Selection			onfirm Decommission Service Request(s)	
Traffic Engineering				Showing 1-1 of 1 records
Management	# Job ID	State	Operation Type	Customer Name
Inventory Manager Topplogy TopI	1.	419 DEPLOYED	ADD	cu_new
- Devices	Rows per page: 10 💙			🕼 🖉 Gotopage: 1 of 1 💷 🕅 🕅
Device Groups				
Customers Customer Sites				OK Cancel
·· CPE Devices				
Providers				
 Provider Regions 				
·· PE Devices				
·· Access Domains				
CE Routing Communities				
- VRFs				
- VPNs				
Named Physical Circuits				
•• NPC Rings				

Figura 5.4.57: Validación de cambios efectuados ^[1]

3. Escoger Deploy para eliminar las configuraciones anteriormente creadas como se muestra en la figura 5.4.58:

al. de	ID Solution Co							Home Short	cuts Account Index Help Abou	t i Logout
CISCO • Inventory and	Service Inventory Connection Manager +	Service Desi Discovery + De	ign Monit vice Console	oring [iagnostics	Administration	1		User:	Zackarias
You Are Here: • Service Inventory •	Inventory and Connection Man	ager> Service Requ	ests						Cust	omer: None
Selection	Service Requests									
Service Requests Traffic Engineering					Show Se	ervices with Job ID	🖌 matching	,	of Type 🛛 🖌 🔽 📕	nd
Management									Showing 141 - 150 of 150	records
Inventory Manager Topology Tool	# 🔲 Job ID Data Files	State	Туре	Operation Type	Creator	Customer Name	Policy Name	Last Modified	Description	
·· Devices	141. 🔲 406	DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/14/09 6:16 PM		
Device Groups	142. 🔲 407	DEPLOYED	VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:02 PM		
Customers Customer Sites	143. 🔲 408	DEPLOYED	MPLS	ADD	aalmeida	cu_sip	PL-L3VPN-NoCE	4/15/09 1:31 PM		
- CPE Devices	144. 🔲 409	DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/15/09 6:01 PM		
Providers Provider Regions	145. 🔲 410	DEPLOYED	VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:01 PM		
·· PE Devices	146. 🔲 414	CLOSED	MPLS	DELETE	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:31 PM		
Access Domains Resource Pools	147. 🔲 416	DEPLOYED	MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:47 PM		
• CE Routing Communities	148. 🗖 417	DEPLOYED	VRF	ADD	jparedes	cu_vrf_etapa_internet	None	4/16/09 3:47 PM		
VRFs VPNs	149. 🗹 418	REQUESTED	MPLS	DELETE	Zackarias	cu_new	PL_VPN_VRF_NEW_NO_CE	4/17/09 11:03 AM		
> Named Physical Circuits	150. 🗹 419	REQUESTED	VRF	DELETE	Zackarias		None	4/17/09 11:03 AM		
·· NPC Rings ·· PseudoWireClass	Rows per page: 10	~							I Go to page: 15 of 15 Go	I D D I
Status	Auto Refresh: 🔽					Create V De	tails Status v	Edit Deplo	y 🚽 Decommission Purg	c 🔻
Operation: Decommission Service Requests Status: Succeeded								Dep Force	Deploy	

Figura 5.4.58: Opción Deploy para eliminar configuraciones ^[1]

4. Guardar los nuevos cambios como se muestra en la figura 5.4.59:



Figura 5.4.59: Guardar nuevos cambios efectuados ^[1]

5. Revisar que la VRF y la interface estén inhabilitadas como se muestra en la figura 5.4.60:

ababa	IP Solutio	on Center						Home I Shor	tcuts Account inde	X I Help I About I Logou
CISCO	Service Inve	ntory Service	Design M	onitoring	iagnostics	Administratio				User: Zackaria
 Inventory and 	Connection Mar	ager • Discovery	 Device Cont 	sole •						
You Are Here: ● Service Inventory >	Inventory and Conne Service Requ	oction Manager> Servic	e Requests							Customer: Non
Selection Service Requests Traffic Engineering					Show S	ervices with Job ID	✓ matching	•	of Type All	Find
Management									Showing 1	141 - 150 of 150 records
·· Topology Tool	# 🔲 Job ID I	Data Files State	Тур	e Operation Type	Creator	Customer Name	Policy Name	Last Modified	Desc	ription
· Devices	141. 🔲 406	DEPL	OYED MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/14/09 6:16 PM		
· Device Groups	142. 🔲 407	DEPL	OYED VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:02 PM		
·· Customer Sites	143. 🔲 408	DEPL	OYED MPLS	ADD	aalmeida	cu_elp	PL-L3VPN-NoCE	4/15/09 1:31 PM		
·· CPE Devices	144. 🔲 409	DEPL	OYED MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/15/09 6:01 PM		
 Providers Provider Regions 	145. 🔲 410	DEPL	OYED VRF	MODIFY	jparedes	cu_vrf_etapa_internet	None	4/15/09 6:01 PM		
·· PE Devices		CLOSED	MPLS	DELETE	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:31 PM		
·· Access Domains	147. 🛄 416	DEPL	OYED MPLS	ADD	jparedes	cu_vrf_etapa_internet	PL-VPN-VRF-ETAPA	4/16/09 3:47 PM		
·· CE Routing Communities	148. 🔲 417	DEPL	OYED VRF	ADD	jparedes	cu_vrf_etapa_interner	None	4/16/09 3:47 PM		
·· VRFs		CLOSED	MPLS	DELETE	Zackarias	cu_new	PL_VPN_VRF_NEW_NO_CI	4/17/09 11:07 AM		
Named Physical Circuits	150. 🔲 419	CLOSED	VRF	DELETE	Zackarias		None	4/17/09 11:07 AM		
··· NPC Rings ··· PaeudoWireClass	Rowa per page	6 10 💌							I⊲ ⊲ Go to page: 15	of 15 🚥 🕞 🕞 🛙
	Auto Refresh:					Create y De	tails Status 👻	Edit Deplo	y y Decommise	ion Purge v

Figura 5.4.60: Verificación de la inactividad de la VRF y la Interface

5.4.5 OPCIÓN SERVICE DESING

La sección *Service Desing* contiene herramientas de administración para crear y administrar políticas y plantillas (Templates) como se muestra en la figura 5.4.61:



Figura 5.4.61: Opción Service Desing^[1]

- ✓ **Policies:** Crean y administran las políticas de servicios autorizados.
- ✓ **Templates:** Crean y administran templates y los datos asociados.

5.4.5.1 OPCIÓN POLICIES

Se muestran las diversas configuraciones previamente realizadas como el provider, nombre de la política y tipo de política como se muestra en la figura 5.4.62:

CISCO	IP Solution Center Service Inventory Templates - Protocole - Line was -	Home Shortouts Account Index Hep About Legour Disgnostics Administration User power
You Are Here: • Service Design	n> Policies	Customer: Non
	MPLS Policy Editor - Policy Type	
	Attribute	Value
	Policy Name*:	PL-VRF-HUB-NO-CE
Mode: EDITING of 1. Policy Type of 2. PE-CE Interface	Policy Owner:	Customer - Pravider - Global Piloty
Scheme	Provider*:	CNT Select
6	Policy Type:	Regular PE-CE INVRPCE: PE-CE
	CE Present:	
	Note. * - Required Field	
	- Step 1 of 4 -	< Back Next> Finish Cancel

Figura 5.4.62: Opción Policies^[1]

Para escoger el nombre de la política dar clic en la casilla que se muestra en la figura 5.4.62 y de la lista que se muestra escoger la opción PL-VRF-HUB-NO-CE como se muestra en la figura 5.4.63:

5.	L2VPN_EVC_PW_INTERNET	FLEXUNI	Provider - CNT
6. 🔲	L3VPN_FM	MPLS	Global
7. 🔲	PL_VPN_VRF_NEW_NO_CE	MPLS	Provider - ISP_NEW
8. 🔲	PL-L2VPN-NoCE-EoMPLS	FLEXUNI	Provider - CNT
9. 🗌	PL-L2VPN-NoCE-ERS	L2VPN	Provider - CNT
10. 🔲	PL-L2VPN-NoCE-EWS	L2VPN	Provider - CNT
11. 🗖	PL-L3VPN-NoCE	MPLS	Provider - CNT
12. 🔲	PL-L3VPN-NoCE-Gesxdsl	MPLS	Provider - CNT
13. 🗌	PL-L3VPN-NoCE-GesxdsI-Vlan	MPLS	Global
14. 🔲	PL-L3VPN-NoCE-IPTV	MPLS	Provider - CNT
15. 🔲	PL-L3VPN-NoCE-ISP-CNT	MPLS	Provider - CNT
16. 🔲	PL-L3VPN-NoCE-Netcht	MPLS	Provider - CNT
17. 🗌	PL-L3VPN-NoCE-Netdef	MPLS	Provider - CNT
18. 🔲	PL-L3VPN-NoCE-Netful	MPLS	Provider - CNT
19. 🗌	PL-L3VPN-NoCE-Netpeer	MPLS	Provider - CNT
20. 🔲	PL-L3VPN-NoCE-VolP	MPLS	Provider - CNT
21.	PL-L3VPN-NoCE-VoIP-VLAN	MPLS	Global
22. 🔲 (j	PL-L3VPN-VRF_NETCNT_NO-CE-INT	MPLS	Provider - CNT
23. 🔲	PL-TE	TE	TE Provider - CNT-TE-ISC
24. 🔲	PL-VPLS-GENERIC	VPLS	Provider - CNT
25.	PL-VPLS-NoCE-ERMS	VPLS	Provider - CNT
26.	PL-VPLS-NoCE-ERMS-PPPoE_CNT	VPLS	Provider - CNT
27.	PL-VPN-NETCNT-NO-CE-INT	MPLS	Provider - CNT
28. 🗌	PL-VPN-VRF-ETAPA-NO-CE	MPLS	Provider - ETAPA
29. 🗌	PL-VRF-HUB-NO-CE	MPLS	Provider - CNT
30. 🔲	PL-VRF-NO-GE	MPLS	Provider - CNT
Rows per page	r 30 💌		[4] € Go to page 1 of 2 @ [2]
		CI	reate V Edit Copy Delete

Figura 5.4.63: Selección del nombre de la política^[1]

5.4.5.2 OPCIÓN TEMPLATES

Escoger la plantilla que se requiere para la configuración como se muestra en la figura 5.4.64:

			Home Shortcuts Accoun	Index Help	About Logout
	IP Solution Center				
CISCO	Service Inventory Service Design Monit	toring Diagnostics A	dministration		User: pcueva
🔹 Policies 🔹	lemplates + Protocols + Link QoS +				
You Are Here: • Service Desi	n Templates				
Templates					
E ANA	Template: shutdownif				
Certificate					
E DIA-Channelization			Show Data Files Name Matching		Snow
🗄 🧰 Examples				Obauriaa	
🗄 🚞 Firewall-Psec				Showing	1-1 of Trecords
E 🗋 DS	Data File Name	Configlet	Description	In SR Use	In Policy Use
E 🚞 QoS	1. Data0	View		View	No
🗄 🧰 QoS L3					
🗄 🧰 interfaces	Rows per page, 10 💌		N 🖞 Go to pa	ge: 1 of 1 P	ages 🌆 🕅 🅅
			List All SRs List All Policies Create Template Creat	e Data File Ed	lit Delete

Figura 5.4.64: Opción Templates^[1]

5.4.6 OPCIÓN MONITORING

Contiene herramientas de monitoreo para administrar tareas, parámetros de ping, Service Level Agreement (SLA), informes de ingeniería de tráfico de rendimiento y otros informes, como se muestra en la figura 5.4.65:

cisco	IP Solution Center
🔸 Task Manage	er + Ping + SLA + TE Performance Report + Reports +
You Are Here: • Monitoring	
	Monitoring
	Tools to manage tasks, ping parameters, and generate Service Level Agreement (SLA) probes and reports.
	Task Manager Create and schedule tasks and monitor task run details.
	Ping Perform Ping connectivity tests.
	SLA Manage probes and view reports.
	TE Performance Report TE Performance Report.
	Reports Create and schedule reports.

Figura 5.4.65: Opción Monitoring^[1]

5.4.7 OPCIÓN DIAGNOSTICS

Esta opción contiene la solución de problemas y diagnóstico automatizado para VPNs MPLS, como se muestra en la figura 5.4.66:



Figura 5.4.66: Opción Diagnostics ^[1]

5.4.8 OPCIÓN ADMINISTRATION

Esta opción contiene herramientas que permiten realizar configuraciones para:

- ✓ La gestión de usuarios
- ✓ La configuración del ISC
- ✓ Servidores y licencias
- \checkmark Ver los usuarios y el registro de acceso de los usuarios
- ✓ Especificar los atributos de algunos mensajes como se muestra en la figura 5.4.67:



Figura 5.4.67: Opción Administration^[1]

Este manual es muy útil para las diferentes configuraciones de usuario porque presenta diversas aplicaciones para la mejor administración de servicios.

5.5 MANUAL NAGIOS

5.5.1 OBJETIVO

Conocer el manejo de la plataforma Nagios, así como la creación de equipos, servicios y alarmas

5.5.2 INSTALACIÓN DEL SERVIDOR NAGIOS

Para poder instalar el servidor Nagios se debe digitar el siguiente comando:

sudo aptitude install -y nagios3

Adicional con Nagios se instalarán otros paquetes necesarios para el funcionamiento eficiente del mismo. En el proceso de instalación se pedirá el ingreso de una contraseña para Nagios, es necesario fijarla, para poder ingresar a la interfaz web.

Una vez que se concluya la instalación se reiniciará el servidor *apache2*, el cual está encargado de subir el sitio web de consulta de Nagios. Para poder acceder a la interfaz web de Nagios se debe digitar:

✓ http://ip-del-servidor/nagios3/

El directorio donde se ejecuta Nagios es: */etc/nagios3/*. Dentro de la carpeta nagios3 se encuentra un directorio llamado *conf.d*, aquí se alojan los archivos de configuraciones de host, grupos de host y servicios.

Se debe cambiar los permisos del directorio /etc/nagios3/conf.d/, así:

sudo chmod 777 /etc/nagios3/conf.d/

Aquí se va a crear los equipos, servicios y demás definiciones que van a ser utilizados por el servidor Nagios.

A continuación se presenta una pequeña guía de creación de equipos.

5.5.3 CREACIÓN DE EQUIPOS PARA NAGIOS

Para la creación de equipos seguir los pasos que se indican a continuación:

1. Se debe crear un archivo con extensión .cfg en el directorio /etc/nagios3/conf.d/

Ejemplo: A continuación se presenta un ejemplo del archivo a crear

sudo nano /etc/nagios3/conf.d/equipos.cfg

2. Se copia la siguiente plantilla al archivo creado:

define host { use generic-host host_name "NOMBRE" alias "NOMBRE" addresss 1.1.1.1

- 3. Se modifican los campos *host_name*, *alias*, *address* como se requiera.
- Para guardar los cambios se debe presionar en el teclado CRTL+O y dar Enter para confirmar la grabación del archivo.

Ejemplo:

define host{	
use	generic-host ; Inherit default values from a template
host_name	WAN INTERNET - PRESIDENCIA DE LA REPUBLICA ; The name we're giving to this switch
allas	WAN INTERNET - PRESIDENCIA DE LA REPUBLICA ; A longer name associated with the switch
address	
<pre>lcon_image }</pre>	clsco-logo.glt ; IP address of the switch
define host{	
use	generic-host ; Inherit default values from a template
host_name	WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES ; The name we're giving to this switch
alias	WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES ; A longer name associated with the switch
address	201,219.62.90
icon_image }	cisco-logo.gif ; IP address of the switch
define host{	
use	generic-host ; Inherit default values from a template
host_name	WAN INTERNET - MINISTERIO DE AGRICULTURA ; The name we're giving to this switch
alias	WAN INTERNET - MINISTERIO DE AGRICULTURA ; A longer name associated with the switch
address	201,219.63.226
icon_image }	cisco-logo.gif ; IP address of the switch
define host{	
use	generic-host ; Inherit default values from a template
host_name	WAN INTERNET - MINISTERIO DE INCLUSION ECON. Y SOCIAL ; The name we're giving to this switch
alias	WAN INTERNET - MINISTERIO DE INCLUSION ECON. Y SOCIAL ; A longer name associated with the swi
address	190.152.88.234
icon_image }	cisco-logo.gif ; IP address of the switch

Figura 5.5.1: Creación de equipos^[1]

5.5.4 CREACIÓN DE SERVICIOS PARA NAGIOS

Para crear un servicio se debe tener al menos un equipo registrado que pueda ser señalado en algún archivo de configuración, cuando ya se cuenta con el o los equipos se debe seguir el siguiente proceso:

1. Crear un archivo con extensión .cfg en el directorio /etc/nagios3/conf.d/

sudo nano /etc/nagios3/conf.d/servicios.cfg

2. Copiar la siguiente plantilla al archivo creado

define service {	
use generic-service	
host_name "NOMBRE HOST"	
service_description "NOMBRE SERVICIO"	
check_command check_(servicio)! (parámetros)	

Ejemplo: A continuación se presenta un ejemplo del archivo a crear

```
define service{
                                          generic-service ; Inherit values from a template
WAN INTERNET - PRESIDENCIA DE LA REPUBLICA
          use
host_name
          service_description
check_command
                                          Upti
                                          check_snmp! -C public -o sysUpTime.0
define service{
                                       generic-service ; Inherit values from a template
WAN INTERNET - PRESIDENCIA DE LA REPUBLICA
       use
host_name
       service_description
                                       WAN INTERNET
                                       check_snmp! -C public -o ifOperStatus.6 -r 1 -m RFC1213-MIB
       check_command
define service{
                                          generic-service ; Inherit values from a template
WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES
          use
host name
          service_description
check_command
                                          Uptime
                                          check_snmp! -C public -o sysUpTime.0
define service{
                                       generic-service ; Inherit values from a template
WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES
WAN INTERNET
       use
host name
       service description
       check_command
                                       check_snmp! -C public -o ifOperStatus.14 -r 1 -m RFC1213-MIB
define service{
         use
host_name
service_description
check_command
                                          generic-service ; Inherit values from a template
WAN INTERNET - MINISTERIO DE AGRICULTURA
                                          Uptime
                                          check_snmp! -C public -o sysUpTime.0
```

Figura 5.5.2: Creación se servicios^[1]

Es recomendable que se revise la documentación o ejemplos de las definiciones de los *check_command* ya que dependiendo de los servicios los parámetros pueden cambiar o la misma definición de llamada del servicio. Esta documentación se puede encontrar en Internet o buscando los archivos *check_*, para esto se puede buscar con el comando *locate check_** en un Terminal.

Los tipos de servicios pueden ser SNMP⁵¹, PING⁵², FTP⁵³ entre otros dependiendo de las necesidades de monitoreo.

No se incluyen estas definiciones por que se refieren como a 35 diferentes tipos de checks.

1. Cambiar los parámetros *host_name*, *service_description* y *check_command* acorde a las necesidades.

⁵¹ Véase Acrónimos

⁵² Véase Acrónimos

⁵³ Véase Acrónimos

 Para guardar los cambios se debe presionar en el teclado CRTL+O y dar Enter para confirmar la grabación del archivo.

5.5.5 CREACIÓN DE ALERTAS POR EMAIL DE NAGIOS

Para que las alertas se puedan enviar de forma adecuada, se deben configurar algunos paquetes extras.

- 1. Instalar un paquete denominado *postfix*, que es una herramienta de gestión de correo muy reducida.
- 2. Para instalar el paquete se debe digitar el siguiente comando:

sudo aptitude install –y postfix

- Una vez que este paquete se haya instalado, se debe configurar/crear un archivo denominado *main.cf* que debe encontrase en el directorio /*etc/postfix/main.cf*/
- 4. Añadir las siguientes definiciones al main.cf:

biff=no
append_dot_mydomain=no
myhostname= NOMBRE-SERVIDOR-DNS
alias_maps= hash:/etc/aliases
alias_database= hash:/etc/aliases
mydestination= DOMINIO1, DOMINIO2, DOMINION, localhost
relavhost= IP-SERV-SMTP:PUERTO

Todos los valores en color azul deben ser cambiados según se requiera.

 Para guardar los cambios se debe presionar en el teclado CRTL+O y dar Enter para confirmar la grabación del archivo

- Abrir el archivo *commands.cfg* en la carpeta /*etc/nagios3*/ y verificar que existan las definiciones '*notify-host-by-email*' y '*notify-service-by-email*'. Por defecto suelen estar habilitadas.
- Finalmente en la carpeta /etc/nagios3/conf.d/ se encuentra el archivo contactnagios2.cfg, en donde se debe abrir y modificar la dirección de correo electrónico del root por una cuenta de correo real.

5.5.6 INSTALACIÓN DE HERRAMIENTAS DE NAGIOS - NDOUTILS

La herramienta *ndoutils* es un complemento desarrollado para que la información manejada de Nagios, pueda ser guardada en una base de datos *mysql*, esta herramienta debe ser instalada luego de que Nagios haya sido instalado completamente.

1. Para instalar este complemento se debe digitar el siguiente comando:

sudo aptitude install—*y ndoutils*

2. Junto a estos cambios se deben digitar los siguientes comandos

sudo nano /etc/nagios3/nagios.cfg

Es un *plugin* que permite que los datos de Nagios se correlacionen en una base de datos.

5.5.7 CONFIGURACIÓN DE DISPOSITIVOS

define hosti	
use	generic-host ; Inherit default values from a template
host_name	WAN INTERNET - PRESIDENCIA DE LA REPUBLICA ; The name ve're giving to this switch
alias	WAN INTERNET - PRESIDENCIA DE LA REPUBLICA : A longer name associated with the switch
address	201.219.63.130
1con_image	cisco-logo.gif : IP address of the switch
)	
define host{	
use	generic-host : Inherit default values from a template
host name	WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES ; The name we're giving to this switch
alias	WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES ; A longer name associated with the switch
address	201.219.62.90
icon image	cisco-logo.gif : IP address of the switch
}	
define host(
use	generic-host : Inherit default values from a template
host name	WAN INTERNET - MINISTERIO DE AGRICULTURA : The name we're giving to this switch
alias	WAN INTERNET - MINISTERIO DE AGRICULTURA ; A longer name associated with the switch
address	201.219.63.226
icon image	cisco-loop.oif : IP address of the switch
}	
define host{	
use	generic-host ; Inherit default values from a template
host name	WAN INTERNET - MINISTERIO DE INCLUSION ECON. Y SOCIAL ; The name we're giving to this switch
alias	WAN INTERNET - MINISTERIO DE INCLUSION ECON. Y SOCIAL : A longer name associated with the s
address	190,152,88,234
icon image	cisco-loop.gif : IP address of the switch
3	

Figura 5.5.3: Configuración de dispositivos ^[1]

5.5.8 CONFIGURACIÓN DE SERVICIOS

*********	# SNMP UPTIME & CHECK
define service{ use host_name service_description check_command }	generic-service ; Inherit values from a template WAN INTERNET - PRESIDENCIA DE LA REPUBLICA Untime check_snmp! -C public -o sysUpTime.0
<pre>define service{ use host_name service_description check_command }</pre>	generic-service ; Inherit values from a template WAN INTERNET - PRESIDENCIA DE LA REPUBLICA WAN INTERNET check_snmp! -C public -o ifOperStatus.6 -r 1 -m RFC1213-MIB
<pre>define service{ use host_name service_description check_command }</pre>	generic-service ; Inherit values from a template WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES Uptime check_snmp! -C public -o sysUpTime.0
define service{ use host_name service_description check_command }	generic-service ; Inherit values from a template WAN INTERNET - MINISTERIO DE RELACIONES EXTERIORES WAN INTERNET check_snmp! -C public -o ifOperStatus.14 -r 1 -m RFC1213-MIB
define service{ use host_name service_description check_command }	generic-service ; Inherit values from a template WAN INTERNET - MINISTERIO DE AGRICULTURA Uptime check_snmp! -C public -o sysUpTime.0

Figura 5.5.4: Configuración de servicios [1]

5.6.1 OBJETIVOS

- Conocer las herramientas de la plataforma ACS para mejorar le seguridad en cuanto al control de acceso de la administración de los equipos de la red IP/MPLS.
- Investigar cómo se realiza la asignación de privilegios a determinados usuarios.

5.6.2 INTRODUCCIÓN

La plataforma ACS^{54} es utilizada para proporcionar una aplicación centralizada de accesos, privilegios y políticas. Proporciona autenticación y autorización de punto de control entre dispositivos de red que utilizan TACACS + RADIUS, y un grupo de bases de datos que residen en los servidores.

5.6.3 INGRESO A LA PLATAFORMA

Para poder ingresar a esta plataforma de autentificación y seguridad seguir los pasos que se muestran a continuación:

- 1. Colocar la dirección IP del servidor correspondiente en el browser.
- 2. A continuación aparecerá la pantalla de inicio de la plataforma.
- 3. Colocar el nombre de usuario y la contraseña respectivamente como se muestra en la figura 5.6.1:

⁵⁴ **ACS (ACCESS CONTROL SERVER):** Permite controlar el acceso del usuario a la red, autorizar los diferentes tipos de servicios de red para los usuarios o grupos de usuarios, y llevar un registro de todas las acciones de la red del usuario.



Figura 5.6.1: Pantalla de ingreso a la plataforma^[1]

5.6.4 PANTALLA PRINCIPAL

En esta pantalla se encuentran todas las herramientas para la administración del ACS.

En el Panel de Navegación se encuentran diversas opciones usadas para la configuración de usuarios, grupo de usuarios, perfiles, dispositivos, protocolos, bases de datos externos y logs como se muestra en la figura 5.6.2:



Figura 5.6.2: Pantalla principal^[1]

Para la correcta administración de los ACS's se debe seguir la siguiente secuencia de configuración:

- 1. Perfiles de autorización
- 2. Dispositivos de red
- 3. Grupos de usuarios
- 4. Usuarios dentro de un grupo

A continuación se mostrará las opciones más utilizadas para la asignación de privilegios a los administradores así como también el establecimiento de seguridades:

5.6.5 TAB USER SETUP

Esta opción permite configurar la información de cada usuario, añadir uno nuevo o eliminarlo de la base de datos como se muestra en la figura 5.6.3:

CISCO SYSTEMS	User Setup	
antillinaantillinaa	Select	
User Setup		
Group Setup		User:
Shared Profile Components		Find Add/Edit
Network Configuration		
System Configuration		List users beginning with letter/number:
Interface Configuration		N O P Q R S T U V W X X Z O 1 2 3 4 5 6 7 8 9
Administration Control		List All Users
Databases		
Reports and Activity		Back to Help
Online Documentation		

Figura 5.6.3: Tab user setup^[1]

5.6.5.1 CONFIGURACIÓN DE USUARIOS EN UNA BASE DE DATOS EXTERNA

El servidor ACS puede autenticar a los usuarios en una base de datos externa para ello se debe tomar en cuenta que se debe realizar las configuraciones previas en dicha base de datos. Es importante mencionar que en el tab *User Setup* no se puede añadir o eliminar nombres de usuario de la base de datos externa.

5.6.5.2 ENCONTRAR UN USUARIO ESPECÍFICO EN LA BASE DE DATOS

Para buscar un usuario que ya se encuentra en la base de datos realizar los siguientes pasos:

- 1. Colocar la primera letra del nombre en el campo de usuario.
- A continuación agregar un asterisco (*) como comodín para realizar la búsqueda correspondiente.
- 3. Finalmente dar un clic en Buscar.
- 4. Posteriormente aparecerá la lista de nombres de usuario en la parte derecha de la pantalla, haga clic en el nombre de usuario cuya información desea ver o cambiar como se muestra en la figura 5.6.4:

Cisco Systems	User Setup			Ε
User Setup Setup Setup	User	User List		Next
B Shared Profile Components	Find Add/Edit	User	Status	Group
Network Configuration		ralmeida	Enabled	INGENIERIA (6 users)
Sutan.	List ware baginning with latteringshar	icastro	Enabled	GESTION RED (25 users)
Configuration	A B C D E I O H I Z K L M	bsanchez	Enabled	MPLS NIVEL 1 (13 users)
Interface Configuration	NOPORSIUVNXXI	Itorres	Enabled	MPLS NIVEL 1 (13 users)
-90 Latropistration		icamacho	Enabled	INGENIERIA (6 users)
Control	List All Users	ivillagran	Enabled	MPLS NIVEL 2 (6 users)
Diternal User		aalmeida	Enabled	MPLS ADMINISTRADORES (7 users)
C L Report Ford	😵 Back to Help	iparedes	Enabled	MPLS ADMINISTRADORES (7 users)
Activity		sarias	Enabled	MPLS ADMINISTRADORES (7 users)
Documentation		arevelo	Enabled	INGENIERIA (6 users)
		ocorrea	Expired	INGENIERIA (6 users)
		gsarango	Enabled	CALL CENTER (62 users)
		pguapulema	Enabled	CALL CENTER (62 users)
		papolo	Enabled	GESTION RED (25 users)
		rrumipamba	Enabled	CALL CENTER (62 users)
		iguato	Enabled	CALL CENTER (62 users)
		kmoncavo	Enabled	GESTION RED (25 users)
		vgutierrez	Enabled	CALL CENTER (62 users)
		gbonilla	Enabled	O&M SOLUCIONES DATOS INTERNET TV (21 users)
		acarrera	Enabled	NOC (14 users)
				Hext

Figura 5.6.4: Ubicación de usuarios en la base de datos^[1]

5.6.5.3 LISTADO DE NOMBRES QUE EMPIEZAN CON UN CARACTER PARTICULAR

Para mostrar una lista de los nombres de usuario que comienzan con una letra o un número específico realizar los siguientes pasos:

- Dar clic en la letra que se encuentra en la lista alfanumérica, o escriba el caracter en el campo de usuario seguido de un asterisco (*).
- Dar clic en *Find*, posteriormente aparecerá una lista de usuarios en la parte derecha de la pantalla con los nombres que comienzan con la letra o número escogido anteriormente.
- 3. A continuación haga clic en el nombre del usuario cuya información desea ver o cambiar como se muestra en la figura 5.6.5:



Figura 5.6.5: Listado de los nombres de usuario que empiezan con un carácter en particular.^[1]

5.6.5.4 CAMBIO DE UN NOMBRE DE USUARIO EN LA BASE DE DATOS

Los nombres de usuario no pueden ser cambiados o modificados en la base de datos es preferible eliminar el nombre de usuario y agregar uno nuevo.

5.6.5.5 CONFIGURACIÓN DE UN USUARIO

Para realizar la configuración de un usuario específico es necesario en primer lugar seleccionar el nombre de usuario que se desea configurar en la lista correspondiente

y posteriormente aparecerá una ventana en donde se deberá colocar los parámetros necesarios como se muestra en la figura 5.6.6:

Cinco Sverens	User Setup		
Ab. Ab.	Edit		
User Setup	User: damos		
Den and Server	Contrain Cost		
Compared Profile	C Account Disabled		
Ref work Configuration	Supplementary User Info	1	
System Configuration	Real Name David Nelson Arcos		
beterface	Description Gestion ATM	2	
-90 (Administration			
Control	Free Seture 9		
DG Databases	Deserved betweender		
C Reports and Activity	Pasiword Autoestication: CiscoSecure Database		
Decramentation	CiscoSecure PAP (Also used for CHAP/MS+CHAP/ARAP, if the	3	
	Separate field is not checked.)		
	Confirm Password		
	Separate (CHAP/MS-CHAP/ARAP)		
	Password •••••		
	Confirm Password		
	When a token server is used for authentication, usephysing a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.		
	Group to which the user is assigned.		
	Calback	4	
	Submit Delete Cancel		
		5	

Figura 5.6.6: Configuración de un usuario^[1]

1. ACCOUNT DISABLED STATUS

Coloque un visto en esta casilla para deshabilitar esta cuenta o desactive la casilla para activar la cuenta nuevamente.

2. SUPPLEMENTARY USER INFO

Escribir la información correspondiente en los cuadros que aparecen en esta opción. Para agregar o cambiar los campos, haga clic en la opción *Interface Configuration*, y luego dar clic en la opción *User Data Configuration*. Se puede realizar la configuración de hasta cinco campos.

3. PASSWORD AUTHENTICATION

Colocar una contraseña de autenticación de acuerdo a una base de datos para proceder a su validación y colocar las confirmaciones de dichas contraseñas como se indica en la figura 5.6.6.

4. GRUPO AL CUAL EL USUARIO ES ASIGNADO (GROUP TO WHICH THE USER IS ASSIGNED)

En la lista, seleccione el grupo al que pertenece el usuario para definir el tipo de servicios que le estarán permitidos usar. Para configurar la información del grupo, haga clic en la opción *Group Setup*.

5. ELIMINACIÓN DE UN USUARIO

El botón *Delete* sólo aparece cuando se está editando una cuenta de usuario, o cuando se va a agregar uno nuevo.

Para eliminar la cuenta de usuario actual de la base de datos haga clic en la opción *Delete*, cuando se le pregunte que confirme la acción dar clic en Aceptar como se muestra en la figura 5.6.6.

Cisco Systems	User Setup	CALLBACK			
-dbdb-	 Use group set 	tting			
User Setup	 No callback 	allowed			6
and Group	O Callback usin	ng this number			
E Setup	 Diatup chent Use Window 	specifies caliback in a Database caliback	mber settings		
Components		a providence compositor	, scould's	- 1 1	
Retwork Configuration		Client IP Address	Assignment		
Suntern Configuration	 Use group set 	tings			
Interface	 No IP address 	s assignment			1
_ I Administration	 Assigned by d 	ialup client			
Control	Assign static I	P address			
Databases	Assigned by A	UAA CBEER DOOL		_	
Reports and Activity					
Carl Dollar					
		Advanced S	iettings		
	Netw	ork Access Restri	ctions (NAR)	?	8
	Per User Defined Netwo	ork Access Restricti	ons		•
		Define IP-based acc	est restrictions		
	Table Define	III: Permitted Calling/P	Lidrees		
		10 1020	Autor		
		remove.			
	AAA CSett Pod	All AAA Clients	<u></u>		
	Aldress				
		Submit Delet	te Cancel	×	

Figura 5.6.7: Eliminación de un usuario^[1]

6. CALLBACK

Es una cadena de comandos que son pasados al servidor de acceso. Se puede utilizar una cadena de callbacks para inicializar un módem y realizar llamadas al usuario mediante un número específico. Esta opción se encuentra conformada por varios campos para lo cual se recomienda colocar los parámetros apropiados de acuerdo a los privilegios que se les vaya a dar a cada uno de los usuarios.

7. CLIENT IP ADDRESS ASSIGNMENT

Ubicar la dirección IP que ha sido asignada para el usuario, esta opción se encuentra conformada por varios campos para lo cual se recomienda colocar los parámetros apropiados de acuerdo a los privilegios que se les vaya a dar a cada uno de los usuarios.

8. ADVANCED SETTINGS

Permite realizar configuraciones avanzadas tales como permitir o denegar el acceso a un usuario utilizando un filtro de acceso etc., estas opciones deben ser marcadas de acuerdo a los requerimientos de cada uno de los usuarios como se muestra en la figura 5.6.7

Case States	User Setup	
Shared Profile Components Market work Configuration	Max Sessions	
Betreen Configuration Configuration Configuration Administration	Sessions available to user O Unlimited O 1 @ Use group setting	9
Def Deternal User	Account Disable	
Contraction and Contraction	Never Disable account if: Date exceed: Failed attempts exceed: Failed attempts since last successful login: 0 Reset current failed attempts count on submit	10

Figura 5.6.8: Opción Advanced Settings^[1]

9. MAX SESSIONS

Establece el número máximo de conexiones simultáneas para este usuario. Existen tres opciones para establecer las sesiones de usuario tales como:

- Unlimited: Seleccionar esta opción para permitir que un usuario tenga un número ilimitado de sesiones simultáneas.
- r: Escriba el número máximo de sesiones simultáneas permitidas para este usuario.
- ✓ Use group setting: Seleccionar esta opción si se desea utilizar el valor máximo de sesiones para el grupo.

10. ACCOUNT DISABLE

Define las circunstancias en que esta cuenta de usuario se desactivará. Se encuentra conformado por varias opciones las cuales deben ser seleccionadas de acuerdo a los requerimientos como se muestra en la figura 5.6.8.

- ✓ **Disable account if:** Seleccionar esta opción para deshabilitar la cuenta.
- ✓ Date exceeds: Para desactivar una cuenta después de una fecha determinada, seleccione la casilla de verificación y especifique la fecha.
- ✓ Failed attempts exceed: Permite desactivar una cuenta después de un cierto número de intentos fallidos de conexión, para ello seleccione la casilla de verificación y escriba el número de intentos fallidos que deshabilitarán la cuenta.
- ✓ Failed attempts since last successful login: Este contador muestra el número de intentos fallidos de ingreso desde la última vez que el usuario fue registrado con éxito.
- Reset current failed attempts count on submit: Si una cuenta está deshabilitada porque el número de intentos fallidos se ha superado, seleccione la casilla de verificación y seleccione *Submit* para reiniciar el contador de intentos fallidos para este usuario y así restablecer la cuenta.

5.6.6 TAB GROUP SETUP

La configuración de grupo se utiliza para activar y configurar las autorizaciones específicas asignadas a todo un grupo de usuarios. El grupo se le asigna a un usuario y este se configura en la sección *User Setup*.

5.6.6.1 CREACIÓN DE UN GRUPO DE USUARIO

Para la creación de un grupo de usuarios seguir los pasos que se muestras a continuación:

- 1. Seleccionar del panel de navegación la opción Group Setup.
- 2. Seleccionar un número libre en la barra desplegable como se muestra en la figura 5.6.9:

CISCO SYSTEMS	Group Setup
.adlillinaadlillina -	Select
User Setup	
Group Setup	Group : 35: Group 35
Shared Profile Components	Users in Group Edit Settings Rename Group
Network Configuration	
System Configuration	
Interface Configuration	Pack to Help
Administration Control	
External User Databases	
Reports and Activity	
0nline Documentation	

Figura 5.6.9: Creación de un grupo de usuario^[1]

3. Dar clic en *User in Group* para observar la lista de todos los usuarios asignados al grupo seleccionado como se muestra en la figura 5.6.10:

Cisco Systems	Group Setup			
-utililite-	Select	User List		
User Setup		User	Status	Group
Group Setup	Group : 0: MPLS NIVEL 2 (6 users)	jvillagran	Enabled	MPLS NIVEL 2 (6 users)
(Ba Shared Profile	Users in Group Edit Settings Rename Group	ilopez	Enabled	MPLS NIVEL 2 (6 users)
"We Components		oherran	Enabled	MPLS NIVEL 2 (6 users)
Configuration		ifonte	Enabled	MPLS NIVEL 2 (6 users)
Fibel Sustem		acueva	Enabled	MPLS NIVEL 2 (6 users)
Configuration		evepez	Enabled	MPLS NIVEL 2 (6 users)
Configuration	💡 Back to Help			
Administration Control				

Figura 5.6.10: Opción User in Group^[1]

4. Dar clic en *Edit Settings* para modificar los privilegios de autorización del grupo seleccionado como se muestra en la figura 5.6.11:

CISCO SYSTEMS	Group Setup			
tillitutillitu	Select	User List		
User Setup		User	Status	Group
Setup	Group : 0: MPLS NIVEL 2 (6 users)	ivillagran	Enabled	MPLS NIVEL 2 (6 users)
Shared Profile	Users in Group Edit Settings Rename Group	ilopez	Enabled	MPLS NIVEL 2 (6 users)
152 Components		oherran	Enabled	MPLS NIVEL 2 (6 users)
Network Configuration		ifonte	Enabled	MPLS NIVEL 2 (6 users)
System		acueva	Enabled	MPLS NIVEL 2 (6 users)
Configuration		eyepez	Enabled	MPLS NIVEL 2 (6 users)
Configuration	💡 Back to Help			
Administration Control				

Figura 5.6.11: Opción Edit Settings^[1]

5.6.6.2 RENOMBRAR UN GRUPO

Elegir la opción *Renaming Group* para escribir un nuevo nombre de grupo y haga clic en Submit para asignar un nombre más descriptivo para el perfil de grupo. Haga clic en Cancelar para volver a la ventana de configuración de grupo sin guardar un nombre de grupo como se muestra en la figura 5.6.12:

CISCO SYSTEMS	Group Setup	
IIIItotIIIto	Select	
User Setup	Renaming Group: MPLS NIVEL 2	
Group Setup		
Shared Profile Components	Group MPLS NIVEL 2	
Network Configuration	Submit Cancel	
System Configuration		
Interface Configuration	Back to Help	
Administration Control		
Databases		
Reports and Activity		
Online Documentation		

Figura 5.6.12: Renombrar un grupo^[1]

5.6.7 TAB SHARE PROFILE COMPONENTS

Esta opción permite realizar configuraciones para añadir a los grupos creados, para ello realizar los siguientes pasos:

 Seleccionar la opción *Shell Command Authorization Sets* que permite utilizar múltiples tipos de comandos de autorización como se muestra en la figura 5.6.13:

CISCO SYSTEMS	Shared Profile Components
User Setup	Select
Group Setup	PIX Command Authorization Sets
Shared Profile Components	💡 Back to Help
Network Configuration	
Configuration	
Administration Control	
External User Databases	
Reports and Activity	
Online Documentation	

Figura 5.6.13: Opción Shell Command Authorization^[1]

2. Posteriormente aparecerá el siguiente recuadro que muestra todos los grupos que se encuentran previamente configurados con sus respectivas descripciones como se muestra en la figura 5.6.14:
| User
Setup | | |
|------------------------------|-----------------------|--|
| Group | | Shell Command Authorization Sets |
| Setup | Name | Description |
| Shared Profile
Components | Administracion | Permite todos los comandos exclusivos para el o los
encargados de la red MPLS |
| Configuration (| Configuracion | Permite comandos para visualizacion, throubleshooting y
configuracion MPLS. |
| Configuration | Visualizacion | Permite comandos exclusivos para visualización y pruebas de
conectividad. |
| Administration
Control | Visualización
Plus | Adiciona al perfil de Visualización los comandos necesarios
para monitoreo y configuracion basica |
| External User
Databases | | |
| Reports and | | |
| Online | | |
| Documentation | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Figura 5.6.14: Grupos configurados previamente^[1]

5.6.7.1 CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Es un conjunto de configuraciones de reglas de autorización emitidas durante el uso de una aplicación de administración de dispositivos.

5.6.7.2 AÑADIR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Para agregar un conjunto de comandos de autorización dar haga clic en la opción *Add* y seguidamente aparecerá una ventana en donde se permiten o se deniegan dichos comandos.

5.6.7.3 EDITAR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Para editar un conjunto de comandos de autorización existente realizar los siguientes pasos:

- 1. En la columna *Name* dar haga clic en el nombre del grupo que se desee configurar.
- En la página que aparece, se puede agregar o quitar los comandos de acuerdo a los requerimientos de cada uno de los usuarios como se muestra en la figura 5.6.15:

CISCO SYSTEMS	Shared Profile Components
User Setup Setup Setup Shared Profile Components Shared Profile Components Network Configuration System Configuration System Configuration External User Databases Seturnal Seturnal Seturnal Configuration Control	Sidied Frome Command Edit Edit Shell Command Authorization Set Name: Description: Unmatched Commands: Substitution Subst
	Submit Delete Cancel

Figura 5.6.15: Edición de un conjunto de comandos de autorización ^[1]

5.6.7.4 AÑADIR Y EDITAR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Para agregar o editar un comando de autorización, completar las siguientes pasos y posteriormente dar clic en *Submit*.

- 1. Name: Escribir el nombre del conjunto de comandos de autorización.
- Description: Colocar una descripción del conjunto de comandos de autorización.
- Unmatched Commands: Niega o permite comandos de autorización en este caso se da de la siguiente manera:
 - ✓ Seleccionar la opción Permit cuando se desee denegar el uso de un comando.
 - ✓ Seleccionar la opción Deny cuando se desee permitir el uso de un comando.
- 4. **Permit Unmatched Args:** Permite o deniega argumentos que no están seleccionados en la lista de argumentos.
- 5. Add Command: Permite añadir nuevos comandos en la lista.
- 6. **Remove Command:** En la lista de comandos, seleccione el comando que se desee eliminar y finalmente dar clic en la opción *Remove Command*.

5.6.7.5 ELIMINAR UN CONJUNTO DE COMANDOS DE AUTORIZACIÓN

Para eliminar un conjunto de comandos de autorización realizar los siguientes pasos:

- 1. En la columna Name dar clic en el nombre del grupo que se desee eliminar.
- Posteriormente en la ventana que aparece se procede a eliminar los comandos de acuerdo a las necesidades del usuario.
- 3. Finalmente confirmar la eliminación del comando dando clic en OK.

5.6.8 TAB NETWORK CONFIGURATION

Esta opción permite realizar configuraciones a los grupos de dispositivos que se encuentran en la red.

5.6.8.1 CONFIGURACIÓN DE DISPOSITIVOS

Para configurar un dispositivo seguir los pasos que se indican a continuación:

- 1. Seleccionar del panel de navegación la opción Network Configuration.
- 2. Antes de iniciar la configuración cabe destacar que los equipos se encuentran divididos en MPLS e INTERNET los mismos que se encuentran en la lista de *Network Device Group*.

En MPLS se encuentran los equipos, IP (Core), PE ⁵⁵(Border), L2(Acceso)

En INTERNET se encuentran Core, Borde, Acceso, Route Reflector, BRAS (autentificación).También se encuentran configurados los equipos de gestión ISC, ANA, CACTI, NAGIOS, etc.

3. Para agregar un nuevo grupo seleccionar la opción *Add/Entry* como se muestra en la figura 5.6.16:

Cisco Systems	Network Configuration						
IIII maatiii ma	Select						
User Setup							
Group Setup	Network Device Groups						
Shared Profile Components	Network Device Group	AAA Clients	AA	A Servers			
Network	Internet Core	4		0			
Configuration	Internet Borde y Acceso	10		0			
System Configuration	Route Reflector	3		0			
	BRAS	2		0			
Configuration	Equipos Frontera E99	4		0			
Administration	Equipos P	11		0			
- LEvternalliger	Equipos L2	267		0			
Databases	Equipos PE	93		0			
Reports and Activity	Equipos Gestion	5		0			
	(Not Assigned)	0		1			
Documentation	Add Entry Search						
	Proxy Dist	tribution Table		?			
	Character String	AAA Servers	Strip	Account			
	(Default) andir	ate-vroqah	No	Local			
	Add Entr	y Sort Entries					

Figura 5.6.16: Configuración de dispositivos^[1]

⁵⁵ Véase Acrónimos

4. Colocar el nombre del grupo y dar clic en *Submit* como se muestra en la figura 5.6.17:

CISCO SYSTEMS	Network Configuration
IllinIllin	Select
User Setup	New Network Device Group
Group Setup	
Shared Profile Components	Network Device Group Name
Network Configuration	Submit Cancel

Figura 5.6.17: Opción Submit^[1]

5. Una vez creado el grupo se procede a configurar cada uno de los equipos que van a estar dentro de dicho grupo, para ello elegir la opción *Add Entry* como se muestra en la figura 5.6.18:

CISCO SYSTEMS	Network Configurati	on						
tilltutilltu	Select							
User Setup								
Group Setup	% Q	Internet Core AAA Clie	ents 🤶					
Components	AAA Client Hostname	AAA Client IP Address	Authenticate Using					
Network Configuration	GYEBLLC01	190.152.253.2	TACACS+ (Cisco IOS)					
System Configuration	GYECNTC01	190.152.253.1	TACACS+ (Cisco IOS)					
, i interface	UIOINQC01	190.152.252.1	TACACS+ (Cisco IOS)					
Configuration	UIOMSCC01	190.152.252.2	TACACS+ (Cisco IOS)					
Administration Control		Add Entry Search						
Activity	% Q	Internet Core AAA Ser	vers 🤶					
Documentation	AAA Server Name	AAA Server IP Address	AAA Server Type					
		None Defined						
		Add Entry Search						

Figura 5.6.18: Opción Add Entry^[1]

6. A continuación aparecerá una ventana en la cual se debe colocar los parámetros correspondientes al equipo como se muestra en la figura 5.6.19:

CISCO SYSTEMS	Network Configuration
.additio.additio	Edit
User Setup	Add AAA Client
Shared Profile Components	AAA Client Hostname
Network Configuration	AAA Client IP Address
Interface Configuration	Key BRAS
Administration Administration External User Databases Reports and Activity Online Documentation	Authenticate Using TACACS+ (Cisco IOS) Single Connect TACACS+ AAA Client (Record stop in accounting on failure). Log Update/Watchdog Packets from this AAA Client Log RADIUS Tunneling Packets from this AAA Client Replace RADIUS Port info with Username from this AAA Client
	Submit Submit + Restart Cancel

Figura 5.6.19: Configuración de los parámetros del equipo^[1]

- 7. Colocar el nombre del equipo
- 8. Colocar la dirección IP
- 9. Clave de autenticación con el ACS
- 10. En la lista, haga clic en el nombre del grupo de dispositivos de red a la que pertenece el cliente AAA.
- Colocar el protocolo para la autenticación, en el caso de dispositivos Cisco elegir el protocolo TACACS-CISCO IOS y en el caso de dispositivos Huawei elegir el protocolo RADIUS
- 12. Para que los cambios efectuados se guarden correctamente elegir la opción Submit+Restart.

5.6.9 TAB SYSTEM CONFIGURATION

Este tab se encuentra conformado por un conjunto de opciones como se muestra en la figura 5.6.20, los mismos que permiten la correcta configuración del sistema.



Figura 5.6.20: Tab System Configuration^[1]

La única opción usada en este tab es *Service Control* ya que las demás opciones no se encuentran implementadas.

5.6.9.1 Service Control

Seleccionar esta opción para realizar configuraciones para el control de servicios como se muestra en la figura 5.6.21:

CISCO SYSTEMS	System Configuration
Image: Stared Profile Image: Stared Profile <td< th=""><th>Select Select CiscoSecure ACS on andinate-vroqah Ci</th></td<>	Select Select CiscoSecure ACS on andinate-vroqah Ci
	Restart Stop Cancel

Figura 5.6.21: Opción Service Control^[1]

5.6.9.1.1 Services Log File Configuration

Las opciones de esta sección de control establecen los parámetros de registro del servicio y el directorio.

- Level of detail: Dar clic en una de las opciones siguientes para determinar el nivel de detalle que aparecerá en el archivo de registro.
 - ✓ **None:** Cuando no hay archivo de registro generado.
 - ✓ Low: Inicia y detiene las acciones en el sistema.
 - ✓ **Full:** Todas las acciones de los servicios se registran.
- Generate New File: Si ha seleccionado la opción Low o Full para el nivel de detalle proceder a dar clic en una de las opciones que se muestran en la ventana para configurar el nuevo archivo de registro. Para este caso

seleccionar la opción *When size is greater than X KB* que tiene un valor por defecto de 2048 KB.

- Manage Directory: Para configurar los parámetros del directorio de los archivos de registro, seleccione la casilla *Manage Directory* y chequee las siguientes opciones:
 - \checkmark Keep only the last X files: El valor predeterminado es 7 ficheros.
 - ✓ **Delete files older than** *X* **days:** El valor predeterminado es 7 días.

5.6.10 TAB INTERFACE CONFIGURATION

Esta opción permite configurar las opciones de protocolos de Autenticación, en este caso se usa TACACS+ (Cisco IOS) para equipos cisco y Radius(Alcatel) para equipos Alcatel como se muestra en la figura 5.6.22:

CISCO SYSTEMS	Interface Configuration
adiiilinaadiiilina -	Select
User Setup	Et User Data Configuration
Group Setup	TACACS+ (Cisco IOS)
Shared Profile	RADIUS (Alcatel)
Sar Components	RADIUS (IETF)
Network Configuration	Advanced Options
System Configuration	😵 Back to Help
Interface Configuration	

Figura 5.6.22: Tab Interface Configuration^[1]

5.6.10.1 CONFIGURACION DEL PROTOCOLO TACAS+ (CiscoIOS)

Para su configuración seguir los pasos que se muestran a continuación:

- 1. Seleccionar la opción TACACS+ (Cisco IOS)
- 2. Seleccione la casilla de verificación, ya sea para usuarios y / o de grupo para cada TACACS + Services que desea que aparezca como una opción

configurable en la configuración del usuario y / o en la ventana de configuración de grupo, en consecuencia.

- 3. Cuando haya terminado de seleccionar las opciones, haga clic en *Submit*, en este caso se considera el servicio *Shell*.
- En Advanced Configuration Options elegir la opción que permite visualizar una ventana por cada servicio seleccionado en el momento que ingresan a TACAS+Attributes.
- 5. Dar clic en *Submit* para guardar los cambios efectuados como se muestra en la figura 5.6.23:

CISCO SYSTEMS	Interfa	ce Confi	iguration TA	CACS+	(Cisco)		
User Setup			TAC	ACS+ S	ervices		<u> ?</u>
Setup		~					
Shared Profile Components	User	Group					
Network			PPP IP				
Configuration			DDD Makikat				
System Configuration			DDD Assile 7	C 1-11-			
			PPP Apple 1	auk			
Configuration			PPP VPDN				
- Administration			ADAD				
Control			ARAP Shall (anal)				
Databases			Shell (exec)	1.10			
Reports and			ST ID	xsneii)			
Activity			SLIP				
Documentation	New S	ervices					
			Service		Pro	otocol	
			Advanced	onfigur	tion Ontion		2
			Auvanceuv	Joingui	tion Option	15	
	🗌 Ađ	vanced TA	CACS+ Feature	es			
	Dis ove	play a Time rride the de	e-of-Day access efault Time-of-D	grid for e ay setting	very TACA(s	CS+ service v	where you can
	🗹 Dis	play a wind	low for each ser	vice selec	ted in which	you can enter	customized
	TA	CACS+ at	tributes			-	
	🔲 Dis	play enable	default (Undefi	ned) servi	ce configurat	ion	
				💡 Back t	o Help		
			ſ	Submit	Cancel		

Figura 5.6.23: Configuración del protocolo tacas+ (Cisco IOS)^[1]

5.6.10.2 CONFIGURACIÓN DEL PROTOCOLO RADIUS (Alcatel)

Cabe mencionar que se colocó un parche para que el servidor ACS reconozca equipos Alcatel. Para la configuración de este protocolo seguir los pasos se muestran a continuación:

- 1. Seleccionar la opción RADIUS(Alcatel)
- 2. Habilite los atributos específicos del protocolo RADIUS para los equipos Alcatel RADIUS ya sea en la configuración de usuario y / o en la ventana de configuración de grupo.
- 3. Cuando haya terminado, haga clic en *Submit* para guardar los cambios como se muestra en la figura 5.6.24:

CISCO SYSTEMS	Interface Configuration
User Setup Setup Setup Setup	RADIUS (Alcatel)
Network Configuration Suptem Configuration Configuration Administration Detabases Detabases Reports and Activity Dolline Documentation	User Group [026/800/001] Alcatel-Auth-Group [026/800/002] Alcatel-Slot-Port [026/800/003] Alcatel-Time-of-Day [026/800/003] Alcatel-Client-IP-Addr [026/800/003] Alcatel-Group-Desc [026/800/006] Alcatel-Port-Desc [026/800/006] Alcatel-Port-Desc [026/800/006] Alcatel-Auth-Group-Protocol [026/800/006] Alcatel-Auth-Group-Protocol [026/800/006] Alcatel-Asa-Access [026/800/009] Alcatel-Asa-Access [026/800/009] Alcatel-Acce-Priv-F-R1 [V] [026/800/004] Alcatel-Acce-Priv-F-R1 [V] [026/800/004] Alcatel-Acce-Priv-F-R2
	Cancel Concel Conce

Figura 5.6.24: Configuración del protocolo Radius (Alcatel)^[1]

5.6.11 TAB ADMINISTRATION CONTROL

Este tab presenta opciones que permiten agregar o editar las cuentas administrativas y editar o establecer acceso, sesión y políticas de auditoría.

Para visualizar esta ventana dar clic en la opción *Administration Control* como se muestra en la figura 5.6.25:

CISCO SYSTEMS	Administration Control
IIII in	Select
User Setup Group Setup	Administration Control
Shared Profile Components	Administrators
Network Configuration	aalmeida
Surtan	Irodriguez
Configuration	logs
Interface Configuration	jsuntaxi
	jparedes
Control	ilopez
External User	ffalconi
	erodriguez
Activity Online Documentation	Add Administrator
	Access Policy Audit Policy

Figura 5.6.25: Opción Administration Control^[1]

En la ventana del *Administration Control* se puede visualizar una serie de opciones para las respectivas configuraciones, las mismas que se describen a continuación:

5.6.11.1 Add Administrator

Dar clic en esta opción para agregar un nuevo administrador, a continuación aparecerá la ventana que se muestra en la figura 5.6.26, aquí se deberán realizar las configuraciones respectivas.

CISCO SYSTEMS	Administration Control				
	Add Administrator	^			
User Setup	Administrator Details 2				
Group Setup					
Shared Profile	Administrator Name				
- I Network	Password				
Configuration	Confirm Password				
System Configuration		=			
Configuration	Administrator Privileges				
Administration Control	Grant All Revoke All				
External User Databases	User & Group Setup				
Reports and	Add/Edit users in these groups				
Activity	Setup of these groups				
Doilee Documentation	A variable groups				
	Shared Profile Components				
	Network Access Kestriction Sets				
	Downloadable ACLs				
	Shell Command Authorization Sets				
	PIX Command Authorization Sets	~			
	Submit Cancel				

Figura 5.6.26: Opciones Administration Control^[1]

- Administrator Details: Utilice esta tabla para configurar el nombre y la contraseña del administrador que está agregando.
- Administrator Privileges: Seleccione cualquiera o todos los siguientes privilegios que desea permitir para este administrador.
- Shared Profile Components: En esta opción se puede escoger los parámetros que se indican en la figura 5.6.26, pero para este caso no se habilita esta opción.

5.6.11.2 Access Policy

Dar clic en esta opción para configurar las políticas de acceso que permiten a los administradores del servidor ACS limitar el acceso de un intervalo de direcciones IP. En la pantalla que aparece seleccionar las opciones adecuadas como se muestra en la figura 5.6.27:

CISCO SYSTEMS	Administration Co	ntrol						
	Edit		<u>^</u>					
User Setup		Access Policy Setu						
Group Setup		, i	-					
Shared Profile Components		IP Address Filtering	?					
Network Configuration	Allow all IP addres	ses to connect						
System Configuration	 Allow only listed IP Reject connections 	addresses to connect from listed IP addresses						
Interface Configuration								
Administration		IP Address Ranges	?					
- L Evternalliser	Start IP Addres	s End IP	Address					
Databases	1 172.16.19.129	172.16.1	9.158					
Reports and Activity	2 172.16.23.67	172.16.2	3.67					
📑 🖹 Online	3 172.17.1.23	172.17.1	23					
Documentation	4							
	5							
	6							
	7							
	8							
	9							
	10							
		HTTP Configuration	<u>?</u>					
	HTTP Port Allocation	1						
	 Allow any TCP por 	rts to be used for Administratio	m HTTP Access					
	Restrict Administration Sessions to the following port range From Port							
	1024 to Port 6	5535	~					
		Submit Cancel						

Figura 5.6.27: Opción Access Policy^[1]

- IP Address Filtering: De las opciones que se muestran en la figura dar clic en la opción Allow all IP addresses to connect que es por defecto, esta opción indica cuando no hay filtrado en cualquier dirección IP por lo tanto se efectúa cuando el administrador tiene acceso al servidor ACS de forma remota.
- IP Address Ranges: En esta opción especificar el rango de direcciones IP para permitir o denegar el acceso.
- HTTP Configuration: Se recomienda escoger la opción Allow any TCP ⁵⁶ports to be used for Administration HTTP⁵⁷ Access para permitir que los puertos TCP sean usados para sesiones de administración remotas. La opción Restrict Administration Sessions to the following port range From Port X to Port Y, permite restringir los puertos TCP utilizados para las sesiones de administración remotas a un rango específico, para ello dar clic en esta opción y completar los siguientes campos:

⁵⁶ Véase Acrónimos

⁵⁷ Véase Acrónimos

- ✓ X: Número de puerto del extremo inferior del rango de puertos TCP
- ✓ Y: Número de puerto del extremo superior del rango de puertos TCP

5.6.11.3 Session Policy

Dar clic en esta opción para establecer el tiempo de espera de la sesión para permitir una sesión local automática y habilitar o deshabilitar respuestas de acceso remoto de las direcciones IP no válidas como se muestra en la figura 5.6.28:

CISCO SYSTEMS	Administration Control
antillitum tillitum •	Select
User Setup	Session Policy Setup
Shared Profile Components	Session Configuration ?
Network Configuration	Session idle timeout (minutes) 120
Sustem Configuration	Allow automatic local login
Interface Configuration	✓ Respond to invalid IP address connections
External User Databases	Lock out Administrator after successive failed attempts
Dournertakon	🔮 Back to Help
	[Submit] [Cancel]

Figura 5.6.28: Opción Session Policy^[1]

A continuación se muestran las respectivas configuraciones de las políticas de sesión como se indican en la figura 5.6.28.

- Session idle timeout (minutes): Colocar el número de minutos de inactividad, después del cual el navegador finaliza la conexión de administración remota. El valor por defecto es de 60 minutos.
- Allow automatic local login: Dar clic en esta opción para desactivar esta casilla con el fin de forzar a los administradores iniciar sesión en la interfaz de usuario en el servidor ACS. Esta opción está seleccionada por defecto.

- Respond to invalid IP address connections: Si esta casilla de verificación está activada, el servidor ACS responde con un mensaje de error en el administrador remoto cuando la estación está en un intervalo no válido. Si esta casilla está desactivada, ningún mensaje de error se generará. Los administradores pueden deshabilitar esta opción para evitar la identificación no autorizada del servidor ACS. Esta opción está seleccionada por defecto.
- Lock out Administrator after x successive failed attempts: Permite bloquear a un administrador después de una serie de intentos de conexión fallidos, para ello seleccionar esta opción y luego, en el cuadro X, escriba un número de intentos fallidos para el ingreso, después de lo cual el administrador será bloqueado.

5.6.12 TAB EXTERNAL USER DATABASE

Esta opción por el momento no se maneja pero permite tener una base de datos de las distintas configuraciones y cargarlas en los equipos de manera automática y de esta manera ahorra tiempo como se muestra en la figura 5.6.29:



Figura 5.6.29: Opción External User Database^[1]

Unknown User Policy

Permite realizar un proceso de autenticación de usuarios desconocidos que no se encuentran configurados en la base de datos.

Database Group Mappings

Permite configurar privilegios de autorización a un grupo de usuarios en una base de datos externa.

> Database Configuration

Permite configurar un tipo particular de base de datos externa para que los usuarios puedan autenticarse.

5.6.13 TAB REPORT AND ACTIVITY

Esta opción permite visualizar los informes que genera ACS.

 ✓ Seleccione el informe que desee dando clic en la opción correspondiente en la parte derecha de la ventana.

Los informes están disponibles para TACACS + y / o RADIUS si un cliente de la AAA se ha configurado para utilizar el protocolo como se muestra en la figura 5.6.30:



Figura 5.6.30: Opción Report and Activity^[1]

Estos informes se pueden importar a hojas de cálculo y base de datos con la extensión .csv, así como también se los puede descargar eligiendo el archivo que requiera.

A continuación se presenta una descripción de los informes actualmente manejados por el área:

5.6.13.1 TACACS+ Accounting

Contiene un registro de todas las autenticaciones que se han realizado con éxito. La información capturada incluye fecha / hora, nombre de usuario, tipo de conexión, la cantidad de tiempo conectado, y bytes transferidos como se muestra en la figura 5.6.31:

Γ	Cisco Systems	Re	ports and Activit	y												[
		Se	lect	Select												
	User Setup	D.	norts	C Refresh	Down	iload										
Γ	Group Setup	Inc.	ports		TACACS+ Accounting 2011-06-27(08-47-48).csv											
ľ	ob. Shared Profile	B.	TACACS+									,				
	TSP Components		Accounting TACACS+	Date 🗣	Time	User- Name	<u>Group-Name</u>	Caller-Id	Acct- Flags	elapsed time	<u>service</u>	<u>bytes</u> in	bytes out	paks in	paks out	<u>task</u>
	Configuration	~	Administration	07/01/2011	22:34:17	anauser		10.8.33.6	start		shell					46998
	Configuration		RADIUS Accounting	07/01/2011	22:34:17	jarmendariz	MULTISERVICIOS R2	172.16.24.179	start		shell					22706
	Configuration	D	Passed Authentications	07/01/2011	22:34:14	jarmendariz	MULTISERVICIOS		NAS Port	3623						22705
	Deternal User		Failed Attempts				R2		used							
l ř	Con L Reports and		Logged-in Users	07/01/2011	22:34:08	anauser		10.8.33.6	stop	30	shell					46998
	Activity	144 1013	ACS Backup And	07/01/2011	22:33:51	jarmendariz	MULTISERVICIOS R2	172.16.24.179	stop	2890	shell					3975
Ľ	Documentation		Restore	07/01/2011	22:33:38	anauser		10.8.33.6	start		shell					46998
		143	Replication	07/01/2011	22:33:28	anauser		10.8.33.6	stop	30	shell					46998
		80	Administration	07/01/2011	22:32:58	anauser		10.8.33.6	start		shell					46998
			Audit	07/01/2011	22:32:47	anauser		10.8.33.6	stop	30	shell					46998
		0a	User Password	07/01/2011	22:32:17	anauser		10.8.33.6	start		shell					46998
			Changes ACE Survivo	07/01/2011	22:32:07	anauser		10.8.33.6	stop	30	shell					46998
		₽.	ACS Service Monitoring	07/01/2011	22:31:37	anauser		10.8.33.6	start		shell					46998
				07/01/2011	22:31:28	anauser		10.8.33.6	stop	30	shell					46998
				07/01/2011	22:30:58	anauser		10.8.33.6	start		shell					46998
				07/01/2011	22:30:47	anauser		10.8.33.6	stop	30	shell					46998
			Back to Help	07/01/2011	22:30:17	anauser		10.8.33.6	start		shell					46998
				07/01/2011	22:30:11	tdurazno	CALL CENTER	10.50.87.1	stop	27611	shell					372
				07/01/2011	22:30:11	tdurazno	CALL CENTER	172.16.7.141	stop	28066	shell					38462
Γ				07/01/2011	22:30:07	anauser		10.8.33.6	stop	30	shell					46998
				07/01/2011	22:29:37	anauser		10.8.33.6	start		shell					46998

Figura 5.6.31: Opción TACACS+ Accounting^[1]

5.6.13.2 TACAS+ ADMINISTRATION

Registra todos los comandos que el usuario ha ejecutado en los equipos. Esto se suele utilizar cuando Cisco Secure ACS se está utilizando para gestionar el acceso a los routers como se muestra en la figura 5.6.32:

CISCO SYSTEMS	Re	ports and Activit	у											
	Se	elect	Select											
User			🗈 <u>Refresh</u>	Down	load									
A L Group	Re	ports			_									
Setup					Ta	cacs+	Administration 201	1-07	-04((08-39	0-27).cs	V		
Shared Profile Components	Ľ	Accounting				Crown		and	main		NAS		NAS ID	
Network Configuration	B	TACACS+	Date 🖊	Time	User-Name	Name	cmd	arg	<u>lvl</u>	<u>service</u>	Portname	<u>task id</u>	Address	reason
Sustem Configuration	B	Administration RADIUS Accounting	07/04/2011	10:50:16	iecheverria	DESCA	show interfaces interfaces MgmtEth0/8/CPU0/2 include Description: <cr></cr>		0	shell	/dev/vty1	263546	10.4.1.100	
Configuration		VoIP Accounting Passed	07/04/2011	10:50:15	anauser		show running-config interface GigabitEthernet 1/27 <cr></cr>		15	shell	tty7	274811	10.5.10.100	
External User Databases		<u>Authentications</u> <u>Failed Attempts</u> <u>Logged-in Users</u> Disabled	07/04/2011	10:50:15	iecheverria	DESCA	show interfaces MgmtEth0/8/CPU0/0 include "packets input packets output" <cr></cr>		0	shell	/dev/vty1	263545	10.4.1.100	
Online Documentation	l 🛰 Ba	Accounts ACS Backup And	07/04/2011	10:50:14	iecheverria	DESCA	show mpls traffic-eng tunnels 1001 detail <cr></cr>		0	shell	/dev/vty0	8403713	10.3.1.100	
		<u>Restore</u> <u>Database</u>	07/04/2011	10:50:14	anauser		show running-config interface Port-channel 2 <cr></cr>		15	shell	tty7	274806	10.5.10.100	
	_	Replication	07/04/2011	10:50:13	iecheverria	DESCA	xml <cr></cr>		0	shell	/dev/vty1	263544	10.4.1.100	
	}	Administration Audit	07/04/2011	10:50:13	iecheverria	DESCA	show processes cpu include CPU utilization <cr></cr>		0	shell	/dev/vty0	8403712	10.3.1.100	
		Changes	07/04/2011	10:50:12	anauser		show running-config interface GigabitEthernet 1/29 <cr></cr>		15	shell	tty1	2119996	10.20.100.19	
	₽	<u>ACS Service</u> <u>Monitoring</u>	07/04/2011	10:50:11	anauser		show ethernet service instance detail <cr></cr>		15	shell	tty1	8233	10.3.11.194	
		Back to Help	07/04/2011	10:50:11	iecheverria	DESCA	show interfaces GigabitEthernet0/5/0/8 include line protocol <cr></cr>		0	shell	/dev/vty1	263543	10.4.1.100	
	-	2	07/04/2011	10:50:11	SANDRANGO	NOC	ping vrf dat1342 10.1.0.61 <cr></cr>		15	shell	tty2	2853	10.6.10.100	
			07/04/2011	10:50:11	iecheverria	DESCA	show route ipv4 static <cr></cr>		0	shell	/dev/vty1	263542	10.4.1.100	
			07/04/2011	10.60.10	la de consta	DECCA	show interfaces interfaces MgmtEth0/8/CPU0/2 include		0	-111		262641	10 1 1 100	

Figura 5.6.32: Opción TACAS+ ADMINISTRATION^[1]

5.6.13.3 LOGGED IN USERS

Registra todos los usuarios AAA que se han logueado⁵⁸ en los equipos, no genera ningún archivo .csv pero este reporte puede ser impreso como se muestra en la figura 5.6.33:

CISCO SYSTEMS	Reports and Activity				X
tillter	Select	Select			^
User Setup	Reports	Select	a AAA Cl	ient	-
Shared Profile Components	TACACS+ Accounting	Name	IP Address	Logged in Users	
Network	TACACS+	AMBCENM01	10.50.76.3	3	
Configuration	Administration	AMBCNTP01	10.3.2.100	3	
System Configuration	RADIUS Accounting	AMBCNTP01	10.80.2.98	1	
Interface	VoIP Accounting	AMBPJLM01	10.50.76.17	1	
Configuration	Passed Authentications	AMBSURE01	10.8.0.76	7	
Administration Control	Lograd in Usar	AMBSURM01	10.50.76.1	4	
External User	Disabled Accounts	AMBSURM02	10.50.76.2	1	
J Databases	ACS Backup And	AMBSURP01	10.3.1.100	4	
Reports and Activity	Restore	AZGCNTE01	10.6.20.100	2	
m Online	Database Replication	BBHQVDE01	10.5.60.100	1	
Documentation	Administration Audit	CCACNTE01	10.6.10.100	1	
	User Password	CCACNTP01	10.6.1.100	4	
	Changes	CCAGLZM01	10.6.10.199	1	
	Monitoring	CCANNRM01	10.6.10.221	1	
	Monatoring	CCASPNM01	10.6.10.220	3	
		ECCCENE01	10.8.0.84	16	
		EL CARMEN SW296	0 10.70.34.21	1	
	Pack to Help	ESMPALE01	10.1.10.100	1	
		ESMPALE02	10.8.0.87	11	
		ESMPALM01	10.50.87.2	2	
		ESMPALP01	10.1.1.100	2	
		ESMREFM02	10.50.87.3	1	
		External RADIUS Prox	10.50.26.6	1	
		GESTION IP ATM 2	10.50.10.10	2	
		GRDCNTE01	10.5.40.100	1	



⁵⁸ **Loguearse**: Identificarse para ingresar a un sitio restringido

5.6.13.4 ADMINISTRATION AUDIT

Este reporte contiene una lista de los administradores que han accedido a Cisco Secure ACS en la fecha que corresponda, las acciones que hizo o intentó hacer, y el tiempo de la acción. Ejemplos de acciones registradas incluyen iniciar y detener la sesión de administración, edición de datos de usuarios y grupos, y cambiar la configuración de la red como se muestra en la figura 5.6.34:

Select <u> Refresh</u>	🗗 <u>Dowr</u>	<u>load</u>		
			Adn	ninistration Audit.csv
Date 🕈	Time	Name	Browser IP	Message
06/07/2011	16:46:14	lrodriguez	127.0.0.1	Viewed "Reports & Activity - Passed Authentications" report 'Passed Authentications active.csv'
06/07/2011	16:44:38	lrodriguez	127.0.0.1	Viewed "Reports & Activity - TACACS+ Administration" report 'Tacacs+ Administration active.csv'
06/07/2011	16:43:55	lrodriguez	127.0.0.1	Viewed "Reports & Activity - TACACS+ Administration" report 'Tacacs- Administration active.csv'
06/07/2011	16:42:38	lrodriguez	127.0.0.1	Viewed "Reports & Activity - TACACS+ Accounting" report 'TACACS- Accounting active.csv'
06/07/2011	16:42:27	lrodriguez	127.0.0.1	Viewed "Reports & Activity - TACACS+ Accounting" report 'TACACS- Accounting active.csv'
06/07/2011	16:35:17	jlopez	172.16.19.148	Administration session finished
06/07/2011	16:25:45	jlopez	172.16.19.148	Viewed "Reports & Activity - TACACS+ Administration" report 'Tacacs- Administration 2011-06-07(11-14-30).csv'
06/07/2011	16:24:47	jlopez	172.16.19.148	Viewed "Reports & Activity - TACACS+ Administration" report 'Tacacs- Administration 2011-06-07(07-29-10).csv'
06/07/2011	16:24:33	jlopez	172.16.19.148	Administration session started
06/07/2011	16:03:28	lrodriguez	127.0.0.1	Administration session started

Figura 5.6.34: Opción Administration Audit^[1]

5.6.13.5 ACS SERVICE MONITORING

Este reporte contiene un registro de los eventos producidos en Cisco Secure ACS cuando trata de controlar los servicios, tales como CSAdmin. Este reporte está activado por defecto como se muestra en la figura 5.6.35:

CISCO SYSTEMS	Reports and Activity	/										I
	Select	Select										
User Setup	-	🗈 <u>Refresh</u>	Down	lload								
Group Setup	Reports				CS	MonL	og.csv					
Shared Profile Components	TACACS+ Accounting											
Network Configuration	Administration	Date 🕈	Time	Description_of_Event	<u>CSAdmin</u> HandleCount	CSAdmin Memory Usage	CSAdmin CPU	<u>CSAdmin</u> ThreadCount	<u>CSAuth</u> HandleCount	CSAuth Memory Usage	CSAuth CPU	<u>CSAuth</u> ThreadCou
Configuration	Accounting					(<u>KB</u>)	Usage			<u>(KB)</u>	Usage	
Administration	VoIP Accounting Passed Authentications Failed Attemnts	07/04/2011	12:20:22	User system has attempted to log into 10.20.100.19 from 202.10.67.204 after the account has been disabled.	679	12432	0	14	1414	18668	0	40
Databases Image: Constraint of the second	Logged-in Users Disabled Accounts ACS Backup And	07/04/2011	11:57:40	User jsuarez has attempted to log into 10.20.100.19 from 202.10.67.204 after the Account Lockout.	679	12400	0	14	1414	18620	0	40
Documentation	Database Replication Administration	07/04/2011	11:43:18	User sflores has attempted to log into 10.20.100.19 from 202.10.67.204 after the Account Lockout.	675	12260	0	14	1412	18600	0	40
	Audit User Password Changes ACS Service Monitoring	07/04/2011	11:33:16	Service CSRadius has been restarted so monitoring will now continue. Service CSTacacs has been restarted so monitoring will now continue.	675	12260	0	14	1420	18632	0	40
	💡 Back to Help	07/04/2011	10:19:24	Service CSRadius has been restarted so monitoring will now continue. Service CSTacacs has been restarted so monitoring will now continue.	670	12140	0	15	1409	18628	2	40
			00.01.12	Service CSAuth has been suspended for a configured	612	11764	0	14	953	14704	24	21

Figura 5.6.35: Opción Acs Service Monitoring^[1]

5.7 PROCESOS O&M/MPLS

Los manuales de usuario personalizados de las plataformas de gestión y monitoreo anteriormente descritos son necesarios y complementarios para el siguiente diagrama general que abarca los procedimientos correspondientes para los cuatro incidentes(Pérdidas de paquetes por intermitencias de enlace, fallos en equipos de acceso, conectividad limitada o nula, problemas en configuración de plataformas) más comunes en la red, para reducir los tiempos de respuesta y resolver de manera más eficiente los problemas y dar mayor satisfacción al cliente.

5.7.1 DIAGRAMA GENERAL DE LOS PROCESOS Y USO DE LAS PLATAFORMAS.

En este diagrama se podrá observar las secciones en las cuales se encuentran los procedimientos de las plataformas correspondiente a cada ítem de verificación en caso de incidentes.



5.7.2 PÉRDIDAS DE PAQUETES POR INTERMITENCIAS DE ENLACES

Para escalar un problema de intermitencias al MPLS previamente se debe disponer de al menos los siguientes datos:

- ✓ NODO IP: Ejemplo. UIOMSCE01, PVJCALM01, etc.
- ✓ INTERFAZ: Ejemplo. Interface vlan xx, interfaces gi13/43, etc.

Para verificar pérdidas de paquetes por intermitencias siga las siguientes instrucciones:

- 1. Verificar mediante las herramientas SNMP (CACTI) que no exista saturación en dicha interfaz.
- 2. Verificar la ingeniería del enlace que tiene problemas para identificar si pasa por fibra oscura o por una red de transmisión.
- Revisar si se obtiene alguna información útil en el log del equipo mediante el comando UIOINQE01#show logging.

PARA IDENTIFICAR SI ES UN PROBLEMA A NIVEL FÍSICO SIGA LAS SIGUIENTES INSTRUCCIONES:

- 1. Verificar mediante el comando *show interface* si existe intermitencia (up, down, up, down) y repetir este procedimiento varias veces para observar si se presentan problemas en la transmisión.
- 2. Verificar los parámetros de la interface
 - a. Verificar que el estado de la interfaz y del protocolo estén activos.

- b. Verificar que exista flujo de tráfico de datos.
- c. Verificar que no se presenten errores en las interfaces (CRC).
- d. Verificar la velocidad y negociación del puerto.

IVLO	INTEO1#show interface Gig 1/20
siga	abitEthernet 20 is up, line protocol is up (connected)
Ĥ.	ardware is ×40 <u>G 1Gb 802.3. address is 0027.0</u> dca.2e40 (bia 0027.0dca.2e40)
De	escription: ### MPLS – LINK TO UIOOCNE01 – Giga 13/6 ###
II	nternet address is 10.80.14.38/30
M	ru 2000 bytes, BW 1000000 Kbit, DLY 10 usec,
	reliability 255/255, txload 1/255, rxload 1/255
E	ncapsulation ARPA, loopback not set
K	eepalive set (10 sec)
6	ill-duplex, 1000Mb/s, media type is LX
11	put flow-control is off, output flow-control is on
C.	lock mode is auto
AF	RP type: ARPA, ARP Timeout 04:00:00
Lá	ast liput 00:00:00, output 00:00:00, output hang never
Lá	ast clearing of "show interface" counters 42w0d
II	nput queue: 0/500/0/0 (size/max/drops/flushes); Total output drops: 0
Q	ueueing strategy: fifo
01	utput queue: 0/40 (size/max)
30) second input rate 24000 bits/sec, 44 packets/sec
30) second output rate 25000 bits/sec, 48 packets/sec
L	2 Switched: ucast: 685739201 pkt, 55371056562 bytes – mcast: 10155581 pkt, 5117460186 byte:
L.3	3 in Switched: ucast: 141610230630 pkt, 110924710870688 bytes - mcast: 0 pkt, 0 bytes mcas1
L3	3 out switched: ucast: 12 <u>1786918884 pkt,</u> 28855909541818 bytes mcast: 0 pkt, 0 bytes
	142311582359 packets Input, 110985788340946 bytes, 0 no buffer
	Received 15528030 broadcasts (O IP multicasts)
	0 runts, 0 giants, 0 throttles
	Tinput errors, O CRC, O frame, O overrun, O ignored
	0 watchdog, 0 multicast, 0 pause input
	0 input packets with dribble condition detected
	122657459210 packets output, 29033327343435 bytes, 0 underruns
	0 output errors, 0 collisions, 59 interface resets
	u pappies, u late collision, u deterred
	U lost carrier, U no carrier, U pause output
	u output burrer rallures, u output burrers swapped out

Figura 5.7.1: Show Interface^[1]

- En caso de que exista problemas de transmisión como por ejemplo CRC. Escalar a transmisiones y seguir el Check list de Transmisión.
- 4. Una vez realizados los pasos anteriores y la interfaz continúe flapeando (cambiando de estado de UP a DOWN), y que no se presenten inconvenientes de CRC además que TRANSMISIONES (RTFO, Radio, etc) haya descartado un problema físico procedemos a verificar el estado de las interfaces a nivel lógico.

Para la verificación a nivel lógico en enlaces capa 2 siga las siguientes instrucciones:

 Verificar Spanning Tree mediante el comando *show spanning-tree mst 1*. En MPLS en su mayoría el tipo de STP usado es el de MSTP (Multiple STP) y todas las vlans se mapean sobre la instancia 1.

COLEMPED	1 tob coopping tree part 1
GTEPINSEU	T#20 ShauuuR-nice 0020 T
##### MS	11 <u>vlans</u> mapped: 1-4094
Bridge	address 0021.559e.f200 priority 1 (0 sysid 1)
Root	this switch for MST1
Interface	Role Sts Cost Prio Nbr Type
Gi12/1	Desg FWD 20000 128.2817 P2p
Gi12/2	Desg FWD 20000 128.2818 P2p
Gi12/8	Desg FWD 20000 128.2824 P2p
Gi12/11	Desg FWD 20000 128.2827 P2p
Gi12/12	Desg FWD 20000 128.2828 P2p
Gi12/15	Desg FWD 20000 128.2831 P2p
Gi12/16	Desg FWD 20000 128.2832 P2p
Gi12/18	Desg FWD 20000 128.2834 P2p Bound(PVS
Gi13/1	Desg FWD 20000 128.3073 P2p

Figura 5.7.2: Spanning Tree

- 2. Revisar que el estado del STP se mantenga en FWD, en el caso de que este estado cambie de FWD a BLK varias veces escalar a MPLS debido a que es un problema de intermitencia.
- 3. Es posible que se presente un flaping a nivel de macs para verificar dicha incidencia usar el comando *show mac-address-table address <dir mac>*.

UIOINQE01#sh mac-address-table address 001c.c096.291f
Legend: * - primary entry
age - seconds since last seen
n/a - not available
vlan mac address type learn age ports
++++++
Module 9:
* 343 001c.c096.291f dynamic Yes 15 10.4.30.100, 343

Figura 5.7.3: Mac Address

Se recomienda repetir este comando varias veces; si realmente existe flapeo se observa que la entrada de la mac desaparece o cambia de puerto como se observa en el siguiente ejemplo.

UIOINQE01#sh mac-address-table address 0024.13e1.7c19 Legend: * - primary entry age - seconds since last seen n/a - not available
vlan mac address type learn age ports
++++++
Module 13:
* 343 0024.13e1.7c19 dynamic Yes 0 Gi13/39
UIOINQE01#sh mac-address-table address 0024.13e1.7c19 Legend: * - primary entry age - seconds since last seen
n/a - not available
vlan mac address type learn age ports
++++++
Module 9:
* 343 0024.13e1.7c19 dynamic Yes 0 10.4.30.100, 343

Figura 5.7.4: Ejemplo de flapeo por Mac

En este caso procedemos a escalar a MPLS.

Si no se observa cambio en el estado del STP, ni flapeo de macs se procede a verificar conectividad con una interfaz vlan (SVI).

 Verificar conexión hacia la WAN (Si es enlace capa 3) o hacia una interfaz vlan (SVI) (si es enlace capa 2) con las diferentes variaciones del comando como por ejemplo con carga (size→MTU), sin carga, sin desfragmentación (df-bit), con muchas repeticiones, etc. Ejemplo de un ping extendido.



Figura 5.7.5: Ping Extendido

Lo ideal es que se observe el mismo comportamiento con todos estos parámetros; por ejemplo pase un MTU de 1900 sin desfragmentar.

Este procedimiento es válido para revisión de clientes, lo única que cambia es los escalamientos y que algunos de los comandos deben ser cambiados con la opción vrf como se muestra en los siguientes ejemplos.

4.1 Para verificar la conexión WAN del MPLS realizarlo mediante el siguiente comando: *ping vrf <nombre de la vrf ><ip wan>*.

```
NVLCNTE01#ping vrf netcnt 186.42.165.185
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 186.42.165.185, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avq/max = 1/1/1 ms
```

Figura 5.7.6: Conexión WAN MPLS

En el caso de que existan problemas con la conexión de esta interfaz ESCALAR AL MPLS.

4.2 Verificar conexión hacia la WAN del cliente *ping vrf <nombre de la vrf> <ip wan>*.

NVLCNTE01#ping vrf netcnt 186.42.165.186
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 186.42.165.186, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms NVLCNTE01#

Figura 5.7.7: Conexión WAN del cliente

En el caso de no tener respuesta de la interfaz, el problema es de última milla.

4.3 Verificar la ruta del cliente show ip route vrf <nombre de la vrf ><ip wan>.

NvLCNTE01#show ip route vrf netdef 190.152.88.90
Routing Table: netdef Routing entry for 190.152.88.88/30 Known via "connected", distance 0, metric 0 (connected, via interface) Redistributing via bgp 28006 Advertised by bgp 28006 Routing Descriptor Blocks:
* directly connected, via Vlan42/
Route metric is 0, trainic share count is 1

Figura 5.7.8: Ruta- Cliente

En este punto se debe verificar si existe duplicación de rutas ya que esto puede presentar intermitencias.

4.4 Verificar conexión hacia la LAN del cliente *ping vrf <nombre de la vrf > <ip LAN>*.

NVLCNTE01#PING vrf netdef 201.219.33.1
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 201.219.33.1, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

Figura 5.7.9: Conexión LAN

En caso de no tener respuesta de la interfaz el problema pasa a ser de última milla.

4.5 Verificar la conexión a la LAN y WAN desde otro equipo PE.

UIOQCNE01#PING vrf netdef 201.219.33.1
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 201.219.33.1, timeout is 2 seconds:
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms UIOQCNE01#PING vrf netdef 190.152.88.90
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 190.152.88.90, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

Figura 5.7.10: Conexión LAN – WAN

Después de tener respuestas satisfactorias en los pasos 7.3 - 9 y no tener respuesta desde otro equipo PE proceder a ESCALAR AL MPLS.

5. En caso de que las intermitencias sean aleatorias revisar el procesamiento del equipo mediante el comando show processes cpu history.



Figura 5.7.11: Procesamiento del Equipo

Si en el grafico histórico se observa picos mayores a 89% significa que existe alto procesamiento del equipo

6. Si detecta que el 100% de CPU se dispara por el proceso ARP Input y IP Input mediante el comando en el show processes cpu sorted significa que hay un ataque desde la LAN hacia el router, ocasionando que haya pérdida de paquetes, por ende intermitencias con ICMP (ping).

MBSI	JREO1 # sh pro⊝	cesses cpu	sorted					
ΈΡΟ ι	utilization 1	for five se	econds: 4%/1	.%; one	minute:	8%; fi	ive r	minutes: 11%
PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TΤΥ	Process
489	345681560	532034553	649	1.03%	0.65%	0.54%	0	PDU DISPATCHER
490	9487887762	2379843942	0	0.39%	1.21%	1.28%	0	SNMP ENGINE
202	4265576884	4262272056	0	0.31%	0.52%	0.62%	0	IP Input
98	188	826	227	0.31%	0.03%	0.00%	2	Virtual Exec
94	135914584	150239626	904	0.31%	1.42%	3.88%	6	SSH Process
76	70404460	92753892	759	0.31%	0.14%	0.17%	0	IPC LC Message H
83	132203188	15500125	8529	0.23%	0.23%	0.23%	0	Compute load avg
10	501538924	568200034	882	0.23%	0.66%	0.71%	0	ARP Input
488	94467004	983185136	96	0.07%	0.16%	0.15%	0	IP SNMP
142	732	16197	45	0.07%	0.00%	0.00%	4	Virtual Exec
436	1590100	1573149	1010	0.07%	0.10%	0.09%	0	RPC pm-mp
11	205432	39420714	5	0.00%	0.00%	0.00%	0	ARP Background
12	0	3	0	0.00%	0.00%	0.00%	0	ATM Idle Timer
9	0	2	0	0.00%	0.00%	0.00%	0	Timers
15	0	1	0	0.00%	0.00%	0.00%	0	Policy Manager
13	0	1	0	0.00%	0.00%	0.00%	0	ATM ASYNC PROC
14	0	161	0	0.00%	0.00%	0.00%	0	AAA_SERVER_DEADT
16	1456	2524	576	0.00%	0.00%	0.00%	0	Entity MIB API
19	116	627030	0	0.00%	0.00%	0.00%	0	IPC Dynamic Cach
20	21072	7519972	2	0.00%	0.00%	0.00%	0	IPC Service NonC
21	0	3	0	0.00%	0.00%	0.00%	0	VTEMPLATE Backgr
22	36244	37544550	0	0.00%	0.00%	0.00%	0	IPC Periodic Tim
17	88256	4210825	20	0.00%	0.00%	0.00%	0	EEM ED Syslog
18	0	1	0	0.00%	0.00%	0.00%	0	IFS Agent Manage
25	7606840	47085013	161	0.00%	0.01%	0.00%	0	IPC Seat Manager
23	214624	163862266	1	0.00%	0.00%	0.00%	0	IPC Managed Time
27	119096	7535854	15	0.00%	0.00%	0.00%	0	IPC Loadometer
28	8	58	137	0.00%	0.00%	0.00%	0	RO Notity Timers
29	0	1	0	0.00%	0.00%	0.00%	0	RMI RM Notifv Wa

Figura 5.7.12: Procesamiento del cpu

7. En caso de que las intermitencias sean periódicas escalar a MPLS, puede deberse a afinamiento del control plane (arquitectura interna de routers) o afinamiento en las políticas de QoS; debido a que el ping (ICMP) no tiene preferencia.

NOTA: El ping no es una buena referencia para verificar la disponibilidad de un servicio.

5.7.3 FALLO DE EQUIPOS DE ACCESO

Estos fallos se pueden dar por las siguientes causas:

- ✓ Cuando una vlan no esté creada.
- ✓ Cuando la vlan no pasa por una interfaz
- ✓ Cuando un puerto está mal configurado
- ✓ Cuando la vlan no está aprendiendo la dirección Mac
- ✓ Por problemas de Spanning Tree
- ✓ En ciertos casos problemas con la MTU

PARA VERIFICAR EL FALLO EN EQUIPOS DE ACCESO SIGA LAS SIGUIENTES INTRUCCIONES:

1. Verificar que se encuentre creada la vlan mediante el comando show vlan id <vlan>.

	NTEO1#	show vlan i	d 201							
VLAN	Name				Stat	tus Por	rts			
201	VLAN02	201			act	ive Gil	L/3 e1	fp_id 201	>	
VLAN 201	туре enet	SAID 100201	MTU 1500	Parent -	RingNo 	BridgeNo 	stp -	BrdgMode 	Trans1 0	Trans2 0
Remot Disak	e SPAN	N VLAN								
Prima	ary se	condary Type	e 		Ports					

Figura 5.7.13: Parámetros de Vlan

En el caso que la vlan no se encuentre pasada por algún puerto solicitar dicha operación al área O&M.

 Revisar la interfaz usando el comando *show interface <interface>* y verificar los siguiente parámetros:

- a. Verificar que el estado de la interfaz y del protocolo estén activos.
- b. Verificar que exista flujo de tráfico de datos.
- c. Verificar que no se presenten errores en las interfaces (CRC).
- d. Verificar la velocidad y negociación del puerto.



Figura 5.7.14: Verificación de la Interfaz

 Verificar que la vlans están aprendiendo direcciones mac, mediante comando show mac address-table vlan<vlan>.

AMBCNT Legend	E01#show mac-addr 1: * - primary ent age - seconds s n/a - not avail	ess-table ry ince last able	vlan 30 seen	7		
vlar	n mac address	type	learn	age	ports	
10dule * 307	2: 000d.281b.e161	dynamic	Yes	0	10.8.0.62, 307	

Figura 5.7.15: Recepción de Mac

 En el caso que se tenga el dato de la dirección mac del equipo se puede verificar la interfaz usando el comando show mac address-table address <dir mac>.

AMBCNTEC Legend:	1#show mac-addre * – primary entr age – seconds si n/a – not availa	ess-table Y ince last ible	address seen	000d.281).elől
vlan	mac address	type	learn	age	ports
Module 2 * 307	: 000d.281b.e161	dynamic	Yes	0	10.8.0.62, 307

Figura 5.7.16: Verificación con la dirección Mac

En clientes corporativos por lo general se presentan problemas de Spanning Tree para verificarlos seguimos los siguientes pasos:

1. Ingresamos el comando show spanning-tree interface < interface>.

UIOQCNE01#show spann	ning-tree	interface	fa6/5	
Mst Instance	Role Sts	Cost	Prio.Nbr	туре
MSTO MST1 UIOQCNE01#	Desg FWD Desg FWD	200000 200000	128.1285 128.1285	P2p P2p P2p

Figura 5.7.17: Spanning Tree

- 2. Verificar que el estado de la interface se encuentre en FWD (Forwarding) que es el más óptimo. En el caso de que el estado sea BLK (Bloqueado) ocasiona que el e protocolo pase a un estado de Error Disable, se produce bloqueo de la vlan y como consecuencia de ello presentarse un fallo en el acceso a los equipos.
- 3. Verificar que los puertos estén configurados correctamente ya sea como modo troncal o acceso mediante el comando: *show run interface <interface>*.

UIOQCNE01#show run interface fa6/5 Building configuration	
Current configuration : 238 bytes interface FastEthernet6/5 description *** Link DSLAM ASCAZUBI *** świtchport switchport trunk encapsulation dot1q switchport trunk allowed vlan 200,201,300-331,333-342,344,34 switchport nonegotiate end	45,704

Figura 5.7.18: Verificación de puertos

En ciertas ocasiones se pueden presentar problemas con la mtu ya sea porque se encuentra configurado con un menor valor del requerido lo cual también produce un fallo en los equipos de acceso.

4. Verificar las mtu configuradas para las interfaces mediante el comando *show interface mtu*.

UIOQCNE	01#show interfaces mtu
Port	Name MTU
Fa6/1	### link to UIONNG 1500
Fa6/2	1500
Fa6/3	1500
Fa6/4	*** IAD SAN JOSE D 1500
Fa6/5	*** Link DSLAM ASC 1500
Fa6/0 Fa6/7 Fa6/8	*** Link IPDSLAM N 1500 #### DSLAM ZTE EL C 1500
Fa6/9	FERROCARRILES_DEL_ 1500
Fa6/10	*** Link SERVER DW 1900
Fa6/11	INTEGRACISN_M2000_ 1500
Fa6/12	*** IAD_ECORUTA_AL 1500
Fa6/13	FUNDACION CRISFE 1500

Figura 5.7.19: MTU de la interfaces

5.7.4 CONECTIVIDAD LIMITADA O NULA

Estas incidencias se pueden presentar a nivel de Corporativos y Masivos

PARA VERIFICAR CONECTIVIDAD EN CORPORATIVOS SIGA LAS SIGUIENTES INTRUCCIONES:

1. Verificar la vlan del cliente mediante el comando show vlan.



Figura 5.7.20: Comprobación de la VLAN

2. Verificar la vrf asignada al cliente mediante el comando show run vrf <vrf>.



Figura 5.7.21: Comprobación de la VRF
3. Revisar si la interface se encuentra activa mediante el comando *show interface* <*interface*>.



Figura 5.7.22: Verificación de Interfaz

4. Realizar un ping a la vrf

```
AMBSURE01#ping vrf netcnt 10.14.0.76
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.14.0.76, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
AMBSURE01#
```

Figura 5.7.23: Ping a la vrf

Si después de haber realizado este procedimiento verificando que la interfaz, la vlan y la vrf se encuentran en un estado óptimo y la conectividad aun es limitada se procede a:

5. Verificar el enrutamiento mediante el comando *show ip route <vrf>* para determinar si el router está activo para enrutamiento.

BBHCNTE01#show ip route vrf dat1062
Routing Table: dat1062 Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - ISS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 i a IS-IS, inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 10.8.0.22 to network 0.0.0.0
<pre>B* 0.0.0.0/0 [200/0] via 10.8.0.22, 4w3d 10.0.0.0/8 is variably subnetted, 145 subnets, 6 masks 10.3.0.0/28 [200/0] via 10.20.100.10, 4w2d 8 10.5.5.0/29 [200/0] via 10.8.0.22, 4w3d 8 10.7.0.0/28 [200/0] via 10.8.0.95, 1w3d 8 10.10.5.0/30 [200/0] via 10.8.0.95, 1w3d 8 10.10.10.16/30 [200/0] via 10.8.0.95, 1w3d 8 10.10.10.16/30 [200/0] via 10.8.0.14, 4w3d 8 10.10.10.236/30 [200/0] via 10.8.0.14, 4w3d 8 10.10.11.24/30 [200/0] via 10.8.0.14, 4w3d 8 10.10.11.24/30 [200/0] via 10.7.10.100, 2w3d 8 10.10.11.36/30 [200/0] via 10.7.20.100, 34, 4w3d 8 10.10.11.36/30 [200/0] via 10.7.20.100, 2w3d 8 10.10.11.36/30 [200/0] via 10.7.20.100, 1w5d 8 10.10.11.40/30 [200/0] via 10.7.20.100, 1w5d 8 10.10.11.72/30 [200/0] via 10.4.20.100, 1w5d 9 10.10.11.72/30 [200/0] via 10.4.20.100, 100.34, 4w3d</pre>

Figura 5.7.24: Enrutamiento VRF

- Identificar los puertos troncales y de acceso mediante el comando *show run interface <interface>*.
- 7. Realizar un ping al router de siguiente salto.

```
NVLCNTE01#ping vrf netcnt 186.42.165.186
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 186.42.165.186, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms
NVLCNTE01#
```

Figura 5.7.25: Ping al siguiente salto

En caso de no tener respuesta satisfactoria el problema se debe a las siguientes causas

- ✓ Vlan no configurada en el dslam
- \checkmark Vlan no forma parte de una interfaz
- El puerto asignado para la vlan se encuentre mal configurado ya sea como modo troncal o de acceso.
- 8. Verificar que el puerto configurado en el switch tenga una ruta estática.

5.7.5 PROBLEMAS DE CONFIGURACIÓN EN PLATAFORMAS

Estos fallos se pueden dar por las siguientes causas:

- ✓ Cambio de velocidad en la vlan
- ✓ Cambio de la vrf de un cliente
- ✓ Cambios de clientes a otra troncal por problemas de transmisión

PARA VERIFICAR PROBLEMAS DE CONFIGURACION EN PLATAFORMAS SIGA LAS SIGUIENTES INTRUCCIONES:

- 1. Verificar el estado actual de la vlan mediante el comando show run in vlan.
- 2. Revisar la velocidad configurada en la vlan.
- 3. Verificar que las Políticas de Servicio estén correctamente configuradas.

```
LOJCNTE01#sh run int vlan 1914
Building configuration...
Current configuration : 182 bytes
!
interface Vlan1914
description 515610_INNFA_LOJA
ip vrf forwarding netcnt
ip address 192.168.75.57 255.255.255.252
service-policy input 3Mbps
service-policy output 3Mbps
end
```

Figura 5.7.26: Verificación de Políticas

En el caso de que la velocidad configurada no sea la requerida solicitar al área O&M el cambio de velocidad

En el caso de un problema de configuración en la vrf e ip de un cliente siga las siguientes instrucciones:

 Verificar el estado actual de la vrf configurada mediante el comando *show run* vrf<vrf>.



Figura 5.7.27: Estado actual VRF

 Verificar la ip de la LAN de la vrf usando el dato de la ip de la WAN del Router del cliente.

> BBHQVDE02#sh run vrf dat1094 |i 10.0.1.222 ip route vrf dat1094 192.168.120.0 255.255.255.0 10.0.1.222

Figura 5.7.28: Verificación de la LAN

En el caso que la vrf y la ip no coincidan con lo requerido se solicita un cambio de vrf y de la ip de la LAN.

3. Verificar el camino por la cual está saliendo la vrf configurada mediante el comando *show ip route vrf <vrf>*.



Figura 5.7.29: Ruta VRF

4. En ocasiones se puede presentar que un enlace de la troncal tuvo problemas de transmisión, es necesario verificar el estado de la interfaz que presenta incidencias mediante el siguiente comando *show int Gi2/28 | i line | rate | errors*.



Figura 5.7.30: Estado de la interfaz

Como se puede observar existe problemas en la transmisión de datos por esta razón es preciso cambiar el enlace para que todo el tráfico se envié por el nuevo enlace.

5. Verificar que la interfaz con incidencias ha sido bloqueado por spinning tree lo hacemos mediante el comando *show spanning tree mts*.

AMBSURE01#show	√ spanning-tree mst	
##### MSTO Bridge Root Regional Root	vlans mapped: none address 001f.9ed2.7880 priority address 0022.56cf.8c8c priority port G12/18 path cost	28672 (28672 sysid 0) 4096 (4096 sysid 0) 20000
Operational Configured	hello time 2 , forward delay 15, max hello time 2 , forward delay 15, max	age 20, txholdcount 6 age 20, max hops 20
Interface	Role Sts Cost	Prio.Nbr Type
Gi1/3 Gi1/4 Gi1/4 Gi1/7 Gi1/10 Gi1/10 Gi1/10 Gi1/13 Gi1/16 Gi1/16 Gi1/16 Gi1/17 Gi1/22 Gi1/22 Gi1/23 Gi1/24 Gi2/5 Gi2/18 Gi2/18 Gi2/28 Fa3/7 Fa3/7	Desg FwD 20000 Desg FwD 20000 Desg FwD 1 Desg FwD 20000 Desg FwD 20000	128.3 P2p 128.4 P2p 128.5 P2p 128.7 P2p 128.10 P2p 128.11 P2p 128.12 P2p 128.13 P2p 128.14 P2p 128.22 P2p 128.23 P2p 128.24 P2p 128.263 P2p 128.263 P2p 128.279 P2p 128.279 P2p 128.279 P2p 128.279 P2p 128.517 P2p

Figura 5.7.31: Spanning Tree

Si en el estado STP cambia de FWD a BLK varias veces escalar a MPLS.

A continuación se presentan los diagramas de flujo de los procesos anteriormente descritos.











CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- MPLS es una tecnología orientada a paquetes con etiquetas IP muy flexible que proporciona la ventaja de poder usar las características de los protocolos de las capas enlace y de red sin ningún tipo de restricción, además permite la implementación de una serie de aplicaciones como Ingeniera de tráfico, QoS, VPNs para de esta manera optimizar el proceso de routing y forwarding dentro de una red.
- Las medidas de seguridad que presta la plataforma ACS son de gran utilidad con lo que respecta al control de acceso de los equipos de la red IP/MPLS así como también para establecer privilegios a cada uno de los administradores de acuerdo a sus requerimientos. El presente manual será de gran ayuda para los administradores ya que les permitirá manejar las herramientas de la plataforma de forma fácil y rápida.
- Las Plataformas de Gestión y Monitoreo son de gran utilidad para organizaciones que poseen una estructura de red bien definida y que requieren establecer comunicación entre usuarios de diferentes sedes ya que por medio de ésta utilidad el administrador de red podrá tener un control sobre todos los dispositivos y servicios que la integran; así como también mantener información actual acerca de diversos sucesos o eventos que se ejecuten dentro de la red y fallas de algún componente de hardware.
- IPsolutionC es una herramienta que permite realizar diversas configuraciones de equipos y usuarios, este manual es de gran utilidad para los administradores ya que proporciona toda la información necesaria para realizar dichas configuraciones de forma fácil y rápida

336

- Nagios brinda ayuda a los administradores para que puedan tener siempre el control de qué está pasando en la red y conocer los problemas que ocurren en la infraestructura que administran antes de que los usuarios de la misma los perciban, vigila los equipos y servicios que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.
- La información contenida en ITIL son esenciales para una eficiente administración de las TI, debido a que proveen a los profesionales de la informática los conocimientos y recursos necesarios para dirigir y mantener una infraestructura tecnológica de forma efectiva, con el objetivo fundamental de cubrir las necesidades de los clientes, mediante la mejor utilización de los recursos disponibles.
- ITIL define las mejores prácticas en la gestión de servicios TI mediante la aplicación de procesos los mismos que tienen que ser implementados, esto implican tiempo, cambio en la cultura de trabajo y requiere soporte, compromiso y disciplina para su adopción, además el personal debe entender, saber y usar la herramienta que los soporta
- La generación de los manuales de usurario de las plataformas de gestión y monitoreo son esenciales para el personal que trabajan en las áreas O&M, Gestión y NOC ya que contienen la información detallada de cada una de estas herramientas para su correcto uso y de esta manera solucionar los problemas de forma eficiente y rápida para dar mayor satisfacción al usuario.

6.2 RECOMENDACIONES

Es importante que el personal del área de O&M, NOC y GESTIÓN de la Corporación Nacional de Telecomunicaciones actualice de manera periódica cada uno de los manuales de las plataformas de gestión y monitoreo, para que en caso de presentarse algún inconveniente se pueda solucionar de forma rápida y eficaz. El área NOC debe realizar correctamente el check list que se ha elaborado en conjunto con el área O&M, el mismo que reúne una serie de procesos para resolver problemas comunes que se presentan a diario en los equipos que conforman la red CNT y como efecto ofrecer una mayor disponibilidad a los usuarios.

REFERENCIAS BIBLIOGRÁFICAS

BIBLIOGRAFÍA CAPITULO UNO

[1] http://www.cnt.gob.ec/

[2] Autores Tesis

BIBLIOGRAFIA CAPITULO DOS

[1]RUBIANO, Gina y URBANO, Humberto, *Investigación de la arquitectura mpls ventajas y servicios*, Tesis Universidad de Los Andes Facultad de Ingeniería Eléctrica y Electrónica, Bogota – Colombia, 2006.

 [2] HINOJOSA, Mayra y HERRERA, Fabricio, Diseño de una red mpls utilizando el protocolo ipv6 para proveedores de servicios de telecomunicaciones, Tesis EPN
 Facultad de Ingeniería Eléctrica y Electrónica, Quito, julio 2009

[3] BARBERÁ, J., "Una arquitectura de backbone para la Internet del siglo XXI", Boletín de RedIRIS, Nº 52. Septiembre 2.000.

[4] CANALIS, María Sol, *MPLS MULTI PROTOCOL LABEL SWITCHING Una Arquitectura de Backbone para la Internet del Siglo XXI*, Trabajo Final de Aplicación, Universidad Nacional del Nordeste Facultad de Ciencias Exactas, Naturales y Agrimensura, Argentina, 2003

[5] BALLESTEROS, Alex y otros, Diseño e Implementación Mediante el Simulador Dynamips de una Red MPLS para la Conexión WAN de una Empresa Mediana con sus Sucursales, ESPOL Facultad de Ingeniería en Electricidad y Computación, Guayaquil – Ecuador, 2007.

[6] http://jedicerocool.blogspot.com/2009/08/mpls.html]

[7] MORALES, Luis, *Investigación de Redes VPN con Tecnología MPLS*, Universidad de las Américas Puebla Escuela de Ingeniería y Ciencias Departamento de Computación, Electrónica, Física e Innovación, Cholula, Puebla- México a 16 de mayo de 2006.

[8] http://dspace.ups.edu.ec/bitstream/123456789/209/3/Capitulo%202.pdf, p. 5.

[9] http://sx-de-tx.wikispaces.com/MPLS-FDDI (grafico cabecera)

[10] JAMOUSSI, B., Otros, "*Constraint-Based LSP Setup using LDP*", RCF 3212. Enero 2.002.

[11] GONZÁLEZ, Agustín, *Multi-Protocol Label Switching*, University of Maryland Dept. of Computer Science.

[12] http://www.slideshare.net/ing.adolfo/gestion-de-redes

[13] DOMINGUEZ, José, Infraestructura de Gestión de Red, Universidad de Oregón

[14] CASARES, Diana, Gestión de Red, Octubre, 2001, p 18

[15]http://www.gleijah.com/archivos/9_Admon%20de%20redes.pdf

[16] GARCÍA, Adolfo, *Gestión TMN Telecomunications Management Network*, version 1.0, www.ccapitalia.net/netica

BIBLIOGRAFÍA CAPÍTULO TRES

[1]http://es.scribd.com/doc/53123700/GESTION-Y-MONITOREO PLATAFORMAS- LINUX-WINDOWS-38110

[2] http://www.slideshare.net/magicdrums/presentacion-de-nagios

[3] http://nagios.sourceforge.net/download/contrib/documentation/misc/

Nagios_spanish.pdf

[4]http://www.desarrolloweb.com/de_interes/nagios-completo-servicio-monitoreoweb-4085.html

[5] http://rm-rf.es/cacti-monitorizacion-grafica-de-redes-y-servidores/

[6] http://ws.edu.isoc.org/data/2009/16360680324ac60486606cb/cacti.pdf

[7] http://www.cacti.net

[8] http://forums.cacti.net/

[9] http://ciscosystems.com/

[10] http://www.cisco.com/en/US/products/ps6776/index.html

[11] Cisco 2011, Advanced Services' Cisco Active Network Abstraction (ANA-Operations Training Version 3.7

[12] Cisco 2009, IP Solution Center 5.2 Product Training

[13] http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

BIBLIOGRAFÍA CAPITULO CUATRO

[1] http://www.osiatis.es/

[2] http://www.ieee.org.ar/downloads/2006-hrabinsky-itil.pdf

[3]_http://www.cybertesis.cl/tesis/uchile/2006/donoso_f/sources/donoso_f.pdf

[4] http://1180.wikispaces.com/file/view/ITIL+para+FCA+Informatica.pdf

[5] http://www.manageengine.com/products/service-desk/spanish-libro-v2.pdf-

BIBLIOGRAFÍA CAPITULO CINCO

[1] Autores Tesis

ANEXOS

	PERDIDA DE	PAQUETES PO	R INTERMITENC	CIA DE ENLACES		
	ORIGEN	ENLACE	DESTINO			
]]		
	RUTA			INODOS INTERME	סוח	
INTEREAZ EÍSICA					DIOS	
INTERFAZ LÓGICA		L		J		
REVISION DE HERRAMIENTAS DE MONITO	REO:					
CACTI BACKBONE (172.16.19.152)	Novedades				1	
	Novedades					
					-	
REVISIÓN A NIVEL FÍSICO MEDIANTE COM	ANDOS DE LINEA:					COMANDO
Ingresar al equipo revisar estado de la	interface	Status	UP	Protocol	UP	show interface
			DOWN		DOWN	
		Autonegotati	on			
		Full Duplex				
		Control de Flu	JO			
		CKC		-		
Medir niveles de potencia		Pin		Pout		sh int giga1/1 transceiver
Extraer el log del equipo						show logging
Comprobar Conectividad L2						cdp neighbors
REVISIÓN A NIVEL LÓGICO:						
Verificar status del spannig tree		Status	FWD			show spannig-tree mst1
Bevisar flaning a nivel mac			BLK			show mac-address table
Verificar conexión			Ping WAN			
			Ping VRF			
			-	ł		

		FNLACE	,				
	ORIGEN		DESTINO	-			
NOMBRE DEL CLIENTE CORPORATIVO PETICIÓN/# SERVICIO AB CONTRATADO		_J 	L	Se dispone	de Ingenie	ría del Cliente	SI NO
JODO EQUIPO DE UK NTERFAZ FÍSICA NTERFAZ LÓGICA	RUTA TRANSMISIÓN			NODOS INTERM	IEDIOS		
EVISION DE HERRAMIENTAS DE MONITO	REO:						
CACTI BACKBONE (172.16.19.152) CACTI DE ACCESO (10.10.30.14/cacti)	Novedades Novedades						
REVISIÓN A NIVEL FÍSICO MEDIANTE COM	ANDOS DE LINEA: interface	Status Autonegotatio Full Duplex Control de Flu CRC	UP DOWN on ijo	Protocol	UP DOWN	COMANDO	
Medir niveles de potencia Extraer el log del equipo Comprobar Conectividad L2		Pin		Pout		sh int giga1/1 t show logging cdp neighbors	ransceiver
REVISIÓN A NIVEL LÓGICO: Verificar status del spannig tree		Status	FWD BLK			show spannig-	tree mst1
Verificar conexión			Ping WAN Ping VRF	\square		Show mac-add	

FALLA DE EQUIPOS DE ACCESO							
PROBLEMA:			-				
			NODOS IN	NTERME	DIOS		
			-				
INTERFAZ LÓGICA			1				1
REVISION DE HERRAMIENTAS DE MONITOREO:							
CACTI BACKBONE (172.16.19.152) Novedades							
CACTI DE ACCESO (10.10.30.14/cacti) Novedades							
REVISIÓN A NIVEL FÍSICO MEDIANTE COMANDOS DE LINEA:							COMANDO
Ingresar al equipo revisar estado de la interface	Status	UP	Prote	ocol	UP		show interface
	Autopogotati	DOWN			DOWN]
	Full Duplex	UII					
	Control de Fl	uio					
	CRC		_				
	Dia		Davit				
Extraer el log del equipo	PIN		_ Pout			_	sh int giga1/1 transceiver
Comprobar Conectividad L2							cdp neighbors
REVISIÓN A NIVEL LÓGICO:							
Verificar status del spannig tree	Status	FWD					show spannig-tree mst1
Revisar fallos a nivel mac		BLK					show mac-address table
Verificar conexión		Ping DSLAM					
Revisión VLAN y MTU							show vlan id
			-				
Configuración de Puerto		Acceso					show running-interface
		Troncal					

		PROBLE	MAS DE CONFI	GURACIÓN DI	E PLATAFORMAS		
			ENLACE				
		ORIGEN		DESTINO			
		-			_		
NODO		RUTA			NODOS INTERMI	EDIOS	
EQUIPO DE UK					_		
		TRANSMISION					
INTERFAZ LOGICA							
REVISION DE HERRAM	1IENTAS DE MONITORE	EO:					
	(172.16.19.152)	Novedades]	
CACTI DE ACCESO) (10.10.30.14/cacti)	Novedades					
	CACTI	Novedades					
SALIDAS INTERNA	CIONALES	Novedades					
REVISIÓN A NIVEL FÍS	ICO MEDIANTE COMAN	NDOS DE LINEA:					COMANDO
Ingresar al equipo	o revisar estado de la ir	nterface	Status	UP	Protocol	UP	show interface
				DOWN		DOWN	
			Autonegotati	ion			
			Full Duplex				
			Control de Fl	ujo			
			CRC				
Medir niveles de	notencia		Pin		Pout		sh int giga1/1 transceiver
Extraer el log del	equipo						
Comprobar Cone	ctividad L2						cdp neighbors
REVISIÓN A NIVEL LÓ	GICO:						
Verificar status de	el spannig tree		Status	FWD			show spannig-tree mst1
				BLK			
Revisar flaping a r	nivel mac						show mac-address table
Verificar conexiór	1			Ping WAN			
				Ping VRF			
Revisión VLAN 20	1 Fast Boy Normal						show vlan id
Revisión VLAN 20	2 Fast Boy ip fija						show vlan id