

ESCUELA SUPERIOR POLITECNICA DEL LITORAL



TOPICO DE GRADUACION

PREVIO A LA OBTENCION DEL TITULO DE:

**Análisis de Soporte de
Microcomputadores**

TEMA:

Administración y Seguridades de Redes LAN y
WAN en el Centro de Estudios
Espíritu Santo

Manual de Usuario

AUTORES:

Holanda Virginia Carló Laínez
Wendy Elizabeth Fernández Ortiz

DIRECTOR:

Ing. Rocky Barboza Gilces

Año 2010

ESCUELA SUPERIOR POLITECNICA DEL LITORAL



TÓPICO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DE TÍTULO DE
ANÁLISIS DE SOPORTE DE
MICROCOMPUTADORES

TEMA

ADMINISTRACIÓN Y SEGURIDADES DE REDES
LAN Y WAN EN EL CENTRO DE ESTUDIOS
ESPIRITU SANTO

MANUAL DE USUARIO

AUTORES:

HOLANDA VIRGINIA CARLÓ LAÍNEZ

WENDY ELIZABETH FERNÁNDEZ ORTIZ

DIRECTOR

ING. ROCKY BARBOZA GILCES

AÑO

2010



AGRADECIMIENTO

Agradezco este importante logro en mi vida primeramente al Creador de todo, Dios que ha estado en cada segundo de mi existencia dándome las fuerzas necesarias para continuar.

Agradezco a mi padre Jorge Daniel Fernández Trejo por haber estado apoyándome y aconsejándome en cada momento decisivo de mi vida, a mi madre Norma Esther Ortiz Vera quien con su comprensión y amor de madre ha estado en los momentos más difíciles dándome aliento para continuar.

A mi profesor de Tópico el Ing. Rocky Fabián Barboza quien sin duda es un ejemplo a seguir y que a lo largo de la carrera, siempre ha estado preparándonos y aportando con sus valiosos conocimientos, gracias a él y a todas las personas que en algún momento formaron parte de este gran éxito.

Srta. Wendy Elizabeth Fernández Ortiz

AGRADECIMIENTO

Primeramente agradezco a Dios por la fortaleza que me da, de inspiración en este Manual, por la fuerza y vigor que les da a mis padres ya que por ellos estoy en este nivel como estudiante y la confianza que me inspira seguir.

A mi Maestro de Tópico Ing. Fabian Barboza ya que se convierte para mí en espejo de ejemplo en superación y experiencia vivida en la Institución como docente.

Srta. Holanda Virginia Carló Láinez



DEDICATORIA

Dedico este manual a Dios, ya que sin él esto no sería posible. A mis padres Jorge Fernández y Norma Ortiz, quienes han sabido comprenderme y apoyarme a lo largo de mi vida. A mis familiares quienes me decían que la firmeza de carácter se alcanza con la práctica.

A mis profesores que son un pilar fundamental en mi vida, que siempre estuvieron dispuestos a enseñar de la manera correcta, a mis amistades por estar allí cuando más los necesite, y a todas aquellas personas, compañeros que conocí y aprendí a lo largo de mi carrera.

Srta. Wendy Elizabeth Fernández Ortiz



DEDICATORIA

Primeramente dedico este manual a mis padres Luz Holanda Láinez Yagual y Víctor Joaquin Carló Soriano ya que por ellos he llegado a esta etapa como hija y ahora profesional ya que han sido mi fuerza y mi apoyo incondicional en los momentos más difíciles de mi vida.

A mis hermanos ya que de una u otra manera son mi inspiración para seguir adelante. Ya que voy dejando huellas en el camino para que ellos puedan seguir y alcanzar una meta en la vida.

A mis amigas y amigos que han estado ahí animándome a seguir aun en los momentos más duros para nosotros de la carrera.

Y aquellas personas que contribuyeron con lo más mínimo de apoyo Moral y Espiritual para mi vida.

Srta. Holanda Virginia Carló Láinez



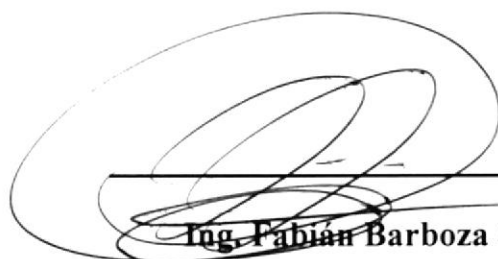
DECLARACIÓN EXPRESA

La Responsabilidad por los hechos; datos y doctrinas expuestas en este tópico de graduación nos corresponde exclusivamente y patrimonio intelectual de la misma al EDCOM (Escuela De Diseño y Comunicación Visual).

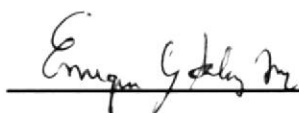
(Reglamento de Exámenes y títulos profesionales de la ESPOL).



FIRMA DE LOS MIEMBROS DEL TRIBUNAL DE GRADO



Ing. Fabián Barboza Gilces



Delegado

FIRMA DE LAS AUTORAS DEL TOPICO

A handwritten signature in black ink, appearing to read "Wendy Elizabeth Fernández Ortiz", written over a solid horizontal line.

Srta. Wendy Elizabeth Fernández Ortiz

A handwritten signature in black ink, appearing to read "Holanda Virginia Carló Láinez", written over a solid horizontal line.

Srta. Holanda Virginia Carló Láinez

INDICE GENERAL

CAPITULO 1	1
1.- SITUACIÓN ACTUAL	1
1.1- ANTECEDENTES.....	1
1.1.1.- HISTORIA	2
1.1.2.- MISIÓN	2
1.1.3.-VISIÓN	2
1.2.- INFRAESTRUCTURA DE RED LAN	3
1.2.1.- ESTACIONES DE TRABAJO	3
1.2.2.- IMPRESORA	5
1.3.- DISPOSITIVOS DE COMUNICACIÓN	6
1.3.1.- SWITCH	6
1.3.2.- CARACTERÍSTICAS DEL SWITCH	7
1.3.3.- CARACTERÍSTICAS FÍSICAS.....	7
1.3.- MEDIOS DE COMUNICACIÓN.....	10
1.3.1.- INALÁMBRICOS:	10
1.3.1.1- WIRELESS	10
1.3.1.2- ROUTERS.....	10
1.3.2.- ACCESS POINT	11
1.3.2.1.- CARACTERÍSTICAS TÉCNICAS	11
1.3.2.2- FUNCIONAMIENTO DEL ACCESS POINT	11
1.4.- RED WAN	12
1.4.1- MEDIOS DE COMUNICACIÓN.....	12
1.4.1.1- FIBRA ÓPTICA.....	12
1.4.2.- DISPOSITIVOS DE COMUNICACIÓN	12
1.4.2.1.- ROUTER CISCO 2600 SERIES.....	12
1.4.2.2.- ROUTER MICROTIK	13
1.5.- SERVIDORES	16
1.6.- SEGURIDADES	19
1.7.- INTERNET	19
1.8.- PROBLEMAS ENCONTRADOS	19



CAPITULO 2	20
2.- SOLUCIÓN PROPUESTA.....	20
2.1.- PROBLEMAS ENCONTRADOS	20
2.2.- SOLUCIÓN PROPUESTA.....	21
2.3.- ESTUDIO DE LA FACTIBILIDAD	22
2.3.1.- ALTERNATIVA “A”	22
2.3.1.1.- FACTIBILIDAD TÉCNICA HARDWARE	22
2.3.1.2.-FACTIBILIDAD TÉCNICA DE DISPOSITIVOS DE COMUNICACIÓN.....	23
2.3.1.3.- FACTIBILIDAD ECONÓMICA.....	23
2.3.1.3.1.- COSTO HARDWARE.....	23
2.3.1.3.2.- COSTO DE SOFTWARE.....	24
2.3.1.3.2.1- CARACTERISTICAS PRINCIPALES DEL NOD 32	24
2.3.1.3.3.-COSTO DEL DISPOSITIVO	25
2.3.1.3.4.- COSTOS OPERATIVOS.....	26
2.3.1.3.5.- FACTIBILIDAD OPERATIVA	27
2.3.1.3.6.- Cuadro de Costos Totales de la Alternativa “A”.....	28
2.4.- VENTAJAS Y BENEFICIOS DE LA ALTERNATIVA “A”	28
2.4.1- VENTAJAS	28
2.4.1.1.- BENEFICIOS.....	28
2.4.2.- FORMA DE PAGO Y LAPSO A DESARROLLARSE	29
2.4.3.- GARANTÍA.....	29
2.5.-CRONOGRAMA DE TRABAJO.....	30
2.6.- ESTUDIO DE LA FACTIBILIDAD	31
2.6.1.- ALTERNATIVA “B”	31
2.6.1.1.- FACTIBILIDAD TÉCNICA HARDWARE	31
2.6.1.2.-FACTIBILIDAD TÉCNICA DE DISPOSITIVOS DE COMUNICACIÓN.....	32
2.6.2.- FACTIBILIDAD ECONÓMICA.....	32
2.6.2.1.- COSTO HARDWARE.....	32
2.6.2.2.- COSTO DE SOFTWARE.....	33
2.6.2.3.-COSTO DEL DISPOSITIVO	34
2.6.2.4.-COSTOS OPERATIVOS DE LA ALTERNATIVA “B”.....	35
2.6.2.5.- FACTIBILIDAD OPERATIVA ALTERNATIVA “B”	36
2.6.2.6.- CUADRO DE COSTOS TOTALES DE LA ALTERNATIVA “B”.....	37
2.7.- VENTAJAS Y BENEFICIOS DE LA ALTERNATIVA “B”.....	37



2.7.1.- VENTAJAS.....	37
2.7.1.1.- BENEFICIOS.....	37
2.7.2.- FORMA DE PAGO Y LAPSO A DESARROLLARSE	38
2.7.3.- GARANTÍA	38
2.8.- CRONOGRAMA DE TRABAJO.....	39
3.1.- INTRODUCCIÓN A LOS ROUTERS.....	41
3.1.1. PARTES INTERNAS DEL ROUTER.....	41
3.1.2. PARTES EXTERNAS DEL ROUTER.....	43
3.1.3.- CONEXIONES INTERNAS DEL ROUTER.....	44
3.2. MEDIOS DE COMUNICACIÓN QUE UTILIZA UN ROUTER	45
3.2.1. CABLE DCE (DATA CIRCUIT EQUIPMENT)	45
3.3. MODOS DEL ROUTER.....	46
3.4.- COMANDOS DEL ROUTER EN EL MODO EXEC USUARIO.....	47
3.5.- COMANDOS EN EL MODO EXEC PRIVILEGIADO	49
3.6.- COMANDOS DE CONFIGURACIÓN GLOBAL	51
3.7.- COMANDOS DE EDICIÓN	54
3.8.- CONFIGURACIONES EN EL ROUTER.....	55
3.9.- ASIGNACIÓN DE NOMBRES A LOS ROUTERS DEL TECNOLÓGICO ESPIRITU SANTO.....	55
3.10.- ASIGNACIÓN DE NOMBRES A LOS ROUTERS DE LA UEES	56
3.11.- ASIGNACIÓN DE NOMBRES A LOS ROUTERS DEL ECOTEC	56
3.12.- ASIGNACIÓN DE NOMBRE AL ROUTER ISP	57
3.13.- ASIGNACIÓN DE IP Y MÁSCARAS A LAS SERIALES DEL ROUTER PRINCIPAL TES.....	57
3.14.- ASIGNACIÓN DE DIRECCIÓN IP Y MASCARA A LAS SERIALES DEL ROUTER TES-1.....	59
3.15.- ASIGNACIÓN DE IP Y MÁSCARAS A LAS SERIALES DEL ROUTER PRINCIPAL UEES	59
3.16.- ASIGNACIÓN DE IP Y MÁSCARAS A LAS SERIALES DEL ROUTER UEES-1 ..60	60
3.17.- ASIGNACIÓN DE IP Y MÁSCARAS A LAS SERIALES DEL ROUTER UEES-2 ..61	61
3.18.- ASIGNACIÓN DE DIRECCIÓN IP Y MÁSCARA A LAS SERIALES DEL ROUTER PRINCIPAL ECOTEC.....	61
3.19.- ASIGNACIÓN DE DIRECCIÓN IP Y MÁSCARA A LAS SERIALES DEL ROUTER ECOTEC-1	62
3.20.- ASIGNACIÓN DE DIRECCIÓN IP Y MÁSCARA A LAS SERIALES DEL ROUTER ECOTEC-2	63

3.21.- PROTOCOLOS DE ENRUTAMIENTOS	63
3.21.1 ENRUTAMIENTO ESTÁTICO	64
3.21.2.- ENRUTAMIENTO PREDETERMINADO	64
3.21.3.- ENRUTAMIENTO DINÁMICO.....	64
3.22.- TIPOS DE DIRECCIONAMIENTO	65
3.22.1.- DIRECCIONAMIENTO CON CLASE.....	65
3.23.- ALGORITMOS DE ENRUTAMIENTO POR VECTOR DE DISTANCIA	65
3.24.- BUCLES DE ENRUTAMIENTO EN ALGORITMOS POR VECTOR DE DISTANCIA	66
3.25.- ALGORITMOS DE ENRUTAMIENTO DE ESTADO DE ENLACE	67
3.26.- PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (RIP)	69
3.26.1.- CARACTERÍSTICAS PRINCIPALES DE RIP.....	70
3.26.2.- FUNCIONAMIENTO RIP	70
3.26.3.- VENTAJAS	70
3.26.4.- INCONVENIENTES	71
3.26.5.- LIMITACIONES RIP	71
3.26.6.- MENSAJES RIP	71
3.26.6.1.- TIPOS DE MENSAJES RIP	71
3.26.7.- FORMATO DE LOS MENSAJES RIP	72
3.26.8.- DIAGNÓSTICO DE FALLAS RIP.....	72
3.27.- PROTOCOLO “PRIMERO LA RUTA MÁS CORTA” (OSPF).....	73
3.27.1.- FUNCIÓN DE OSPF	74
3.27.2.- CARACTERÍSTICAS DE OSPF	74
3.27.3.- VENTAJAS DE OSPF.....	74
3.27.4.- TIPOS DE AREA QUE DISTINGUE OSPF	75
3.27.4.1.- ÁREA BACKBONE.....	75
3.27.4.2.- ÁREA STUB.....	75
3.27.4.3.- ESTADO DE LAS INTERFACES	75
3.27.4.4.- ESTADO DESACTIVADO (DOWN).....	76
3.27.4.5.- ESTADO DE INICIALIZACIÓN (INIT).....	76
3.27.4.6.- ESTADO BIDIRECCIONAL (TWO-WAY)	76
3.27.4.7.- ESTADO DE INTERCAMBIO (EXCHANGE)	76
3.27.4.8.- ESTADO CARGANDO (LOADING).....	77
3.28.- TABLA DE PROTOCOLOS DE ENRUTAMIENTO.....	77



3.29.-REDISTRIBUCIÓN DE RUTAS	78
3.29.1.- PARA QUÉ SE UTILIZA LA REDISTRIBUCIÓN DE RUTAS.....	78
3.29.2.- LAS MÉTRICAS	79
3.29.3.- REDISTRIBUCIÓN EN RIP	79
3.29.4.- REDISTRIBUCIÓN EN OSPF.....	79
3.30.- CONFIGURACIÓN DE OSPF EN LOS ROUTERS TES Y TES-1	80
3.31.- CONFIGURACIÓN DE RIP V2 Y OSPF EN EL ROUTER UEES.....	81
3.32.- CONFIGURACIÓN DE RIP V2 EN LOS ROUTERS	81
UEES-1 Y UEES-2	81
3.33.- CONFIGURACIÓN DE RIP V2 Y OSPF EN EL ROUTER ECOTEC	82
3.34.- CONFIGURACIÓN DE RIP V2 EN LOS ROUTERS ECOTEC-1	82
3.35.- COMANDO SHOW IP ROUTE EN EL ROUTER TES	83
3.36.- COMANDO SHOW IP ROUTE EN EL ROUTER TES-1	85
3.37.- COMANDO SHOW IP ROUTE EN EL ROUTER UEES	86
3.38.- COMANDO SHOW IP ROUTE EN EL ROUTER UEES-1	87
3.39.- COMANDO SHOW IP ROUTE EN EL ROUTER UEES-2	88
3.40.- COMANDO SHOW IP ROUTE EN EL ROUTER ECOTEC.....	89
3.41.-COMANDO SHOW IP ROUTE EN EL ROUTER	91
ECOTEC-1	91
3.42.- COMANDO SHOW IP ROUTE EN EL ROUTER	92
ECOTEC-2	92
3.43.- DEFINICIÓN Y FUNCIÓN DEL SWITCH	93
3.43.1.- LED SISTEMAS – SWITCHES.....	94
3.43.2.-CONFIGURACIÓN ACTIVA POR DEFECTO.....	94
3.44.- LAN VIRTUALES O VLAN	95
3.44.1.- VENTAJAS	95
3.44.2.- TIPOS DE VLAN	95
3.45.- CONFIGURACIÓN DE VLAN EN LOS SWITCHES	96
3.45.1.-CREACIÓN DE VLANS EN EL SW-TES	96
3.45.2.- ENLACES TRONCALES (VTP).....	97
3.46.- CREACIÓN DE VLANS EN EL SW-TES-1.....	98
3.47.- CREACIÓN DE VLANS EN EL SW-UEES	99
3.48.- CREACIÓN DE VLANS EN EL SW-UEES-1.....	99
3.49.- CREACIÓN DE VLANS EN EL SW-UEES-2.....	100



3.50.- CREACIÓN DE VLANS EN EL SW-ECOTEC.....	101
3.51.- CREACIÓN DE VLANS EN EL SW-ECOTEC-1	102
3.52.- CREACIÓN DE VLANS EN EL SW-ECOTEC-2	103
3.53.- COMANDO SHOW VLAN EN EL SWITCH TES.....	104
3.54.- COMANDO SHOW VLAN EN EL SWITCH TES-1	105
3.55.- COMANDO SHOW VLAN EN EL SWITCH UEES.....	106
3.56.- COMANDO SHOW VLAN EN EL SWITCH UEES-1.....	107
3.57.- COMANDO SHOW VLAN EN EL SWITCH UEES-2.....	108
3.58.- COMANDO SHOW VLAN EN EL SWITCH ECOTEC	109
3.59.- COMANDO SHOW VLAN EN EL SWITCH ECOTEC-1	110
3.60.- COMANDO SHOW VLAN EN EL SWITCH ECOTEC-2	111
3.61.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER TES.....	112
3.62.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER TES-1	113
3.63.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER UEES.....	113
3.64.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER UEES-1	114
3.65.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER UEES-2	114
3.66.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER ECOTEC	115
3.67.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER ECOTEC-1	115
3.68.- CONFIGURACION DE LAS SUBINTERFACES EN EL ROUTER ECOTEC-2	116
3.69.- COMANDO SHOW INTERFACES EN EL ROUTER TES.....	116
3.70.- COMANDO SHOW INTERFACES EN EL ROUTER	119
TES-1.....	119
3.71.- COMANDO SHOW INTERFACES EN EL ROUTER UEES.....	120
3.72.- COMANDO SHOW INTERFACES EN EL ROUTER UEES-1	121
3.73.- COMANDO SHOW INTERFACES EN EL ROUTER UEES-2.....	122
3.74.- COMANDO SHOW INTERFACES EN EL ROUTER ECOTEC.....	123
3.75.- COMANDO SHOW INTERFACES EN EL ROUTER ECOTEC-1	125
3.76.- COMANDO SHOW INTERFACES EN EL ROUTER ECOTEC-2	127
3.77.- COMANDO SHOW INTERFACES EN EL ROUTER ISP	128
3.78.- COMANDO SHOW PROTOCOLS EN EL ROUTER TES.....	130
3.79.- COMANDO SHOW PROTOCOLS EN EL ROUTER TES-1.....	131
3.80.- COMANDO SHOW PROTOCOLS EN EL ROUTER UEES	131
3.81.- COMANDO SHOW PROTOCOLS EN EL ROUTER	132
UEES-1.....	132



3.82.- COMANDO SHOW PROTOCOLS EN EL ROUTER.....	132
UEES-2.....	132
3.83.- COMANDO SHOW PROTOCOLS EN EL ROUTER ECOTEC	133
3.84.- COMANDO SHOW PROTOCOLS EN EL ROUTER ECOTEC-1	133
3.85.- COMANDO SHOW PROTOCOLS EN EL ROUTER ECOTEC-2	134
3.86.- COMANDO SHOW PROTOCOLS EN EL ROUTER ISP	134
3.87. ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER PRINCIPAL TES	135
3.87.1.- PROTEGER EL ACCESO AL MODO PRIVILEGIADO.....	135
3.87.2.- ACTIVAR EL MODO DE ADMINISTRACIÓN REMOTA	136
3.88.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER TES-1.....	136
3.89.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER UEES	137
3.90 .- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER UEES-1.....	137
3.91.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER UEES-2.....	138
3.92.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER ECOTEC	138
3.93.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER ECOTEC-1	139
3.94.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER ECOTEC-2	139
3.95.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER ISP	140
3.96.- LISTAS DE CONTROL DE ACCESO	141
3.96.1.-Estructura Básica.....	141
3.96.2.-MÁSCARA DE WILDCARD	142
3.96.3.-TIPO DE ACL: ESTÁNDAR	142
3.96.3.1.- COMO SE CONFIGURAN ACL ESTÁNDAR.....	143
3.96.4.-TIPO DE ACL: EXTENDIDA	144
3.96.5.- LISTA DE ACCESO ENTRANTE	144
3.96.6. -LISTA DE ACCESO SALIENTE	144
3.96.7. FUNCIONAMIENTO DE LAS ACL	145
3.96.8.-QUE CONSIDERACIONES HAY QUE TENER PARA INSTALAR ACLS	145
3.96.8.1.-DENEGACIÓN POR DEFECTO Y LOG.....	145

3.97.- REGLAS ESPECIFICAS Y GENERALES	145
3.98.-TELNET.....	146
3.99.-PING (ICMP).....	147
3.100.-FTP.....	147
3.101.-SSH	148
3.101.1.-Características de SSH.....	149
3.102.-FIREWALL	150
3.103.-PUERTOS.....	151
3.104.-UBICACIÓN DE UNA ACL.....	152
3.105.-CREACIÓN DE LAS ACL	152
3.106.-CREACIÓN DE ACCESS LIST EN EL ROUTER TES	153
3.107.-CREACIÓN DE ACCESS LIST EN EL ROUTER TES-1	156
3.108.-CREACIÓN DE ACCESS LIST EN EL ROUTER UEES	158
3.109.-CREACIÓN DE ACCESS LIST EN EL ROUTER UEES-1	159
3.110.-CREACIÓN DE ACCESS LIST EN EL ROUTER UEES-2	160
3.111.-CREACIÓN DE ACCESS LIST EN EL ROUTER ECOTEC.....	161
3.112.-CREACIÓN DE ACCESS LIST EN EL ROUTER	162
ECOTEC-1	162
3.113.-CREACIÓN DE ACCESS LIST EN EL ROUTER	164
ECOTEC-2	164
3.114.-CREACIÓN DE ACCESS LIST EN EL ROUTER ISP.....	165
3.115.- SHOW ACCESS-LISTS EN EL ROUTER TES.....	166
3.116.-SHOW ACCESS-LISTS EN EL ROUTER TES-1	169
3.117.-SHOW ACCESS-LISTS EN EL ROUTER UEES.....	171
3.118.-SHOW ACCESS-LISTS EN EL ROUTER UEES-1	171
3.119.-SHOW ACCESS-LISTS EN EL ROUTER UEES-2	172
3.120.-SHOW ACCESS-LISTS EN EL ROUTER ECOTEC	173
3.121.-SHOW ACCESS-LISTS EN EL ROUTER ECOTEC-1	174
3.122.-SHOW ACCESS-LISTS EN EL ROUTER ECOTEC-2.....	175
3.123.-SHOW ACCESS-LISTS EN EL ROUTER ISP.....	176
3.124.-SHOW RUNNING-CONFIG EN EL ROUTER PRINCIPAL TES.....	176
3.125.-SHOW RUNNING-CONFIG EN EL ROUTER TES-1.....	181
3.126.-SHOW RUNNING-CONFIG EN EL ROUTER UEES	184
3.127.-SHOW RUNNING-CONFIG EN EL ROUTER UEES-1	186



3.128.-SHOW RUNNING-CONFIG EN EL ROUTER	189
UEES-2.....	189
3.129.-SHOW RUNNING-CONFIG EN EL ROUTER ECOTEC.....	191
3.130.-SHOW RUNNING-CONFIG EN EL ROUTER ECOTEC-1	194
3.131.-SHOW RUNNING-CONFIG EN EL ROUTER ECOTEC-2	196
GLOSARIO.....	200



INDICE DE FIGURA

Figura 1 - 1: Pc Usuario	3
Figura 1 - 2: Pc de Laboratorio	4
Figura 1 - 3: Equipo Mac	5
Figura 1 - 4: Impresora hp	5
Figura 1 - 5: Impresora Lexmark	6
Figura 1 - 6: Switch D-Link.....	6
Figura 1 - 7: Comunicación de Switch	8
Figura 1 - 8: Diseño de red Lan	9
Figura 1 - 9: Router Linksys	10
Figura 1 - 10: Access Point.....	11
Figura 1 - 11: Router Mikrotik.....	13
Figura 1 - 12: Diseño de red Wan.....	15
Figura 1 - 13: Gráfico de conexión a Internet.....	19
Figura 2 - 1: Diagrama de Gantt	30
Figura 2 - 2: Gráfico Motor integrado de antivirus	33
Figura 2 - 3: Diagrama de Gantt Alternativa "B"	39
Figura 3 - 1: Gráfico de RED LAN y WAN.....	40
Figura 3 - 2: Partes Internas del Router	41
Figura 3 - 3: Interfaces del Router	43
Figura 3 - 4: Interfaces del Router	44
Figura 3 - 5: Cable DCE	45
Figura 3 - 6: Cable DTE	45
Figura 3 - 7: Enrutamiento Vector Distancia.....	66
Figura 3 - 8: Protocolo Rip	69
Figura 3 - 9: Primero la ruta mas corta	73
Figura 3 - 10: Switch	93
Figura 3 - 11: ACL.....	141
Figura 3 - 12: SSH	147
Figura 3 - 13: SSH	148
Figura 3 - 14 : Firewall en las ACL	150
Figura 3 - 15:Clases de Puerto Usados en las ACL.....	151
Figura 3 - 16: Ejemplo de Ubicación de una ACL	152

ÍNDICE DE TABLAS

Tabla 1 - 1: Características de la PC Usuario	3
Tabla 1 - 2: Características de la Pc de Lab.....	4
Tabla 1 - 3: Características de Pc Mac	5
Tabla 1 - 4: Características de Impresora HP	5
Tabla 1 - 5: Características de la Impresora Lexmark	6
Tabla 1 - 6: Características de router Linksys	10
Tabla 1 - 7: Características del Router Cisco 2600 Series.....	13
Tabla 1 - 8: Características de los servidores	17
Tabla 1 - 9: Características de los Srv. BD y Aplicación	17
Tabla 1 - 10: Características de Srv. Antivirus y otros.....	18
Tabla 2 - 1: Problemas Encontrados	20
Tabla 2 - 2: Solución Propuesta.....	21
Tabla 2 - 3: Factibilidad Técnica hardware	22
Tabla 2 - 4: Factibilidad Técnica de Dispositivos	23
Tabla 2 - 5: Costo Hardware.....	23
Tabla 2 - 6: Costo de Software	24
Tabla 2 - 7: Costo de Dispositivo	25
Tabla 2 - 8: Costos Operativos	26
Tabla 2 - 9: Factibilidad Operativa.....	27
Tabla 2 - 10: Costos Totales de la Alternativa "A"	28
Tabla 2 - 11: Factibilidad Técnica hardware "B"	31
Tabla 2 - 12: Factibilidad Técnica de Dispositivos	32
Tabla 2 - 13: Costo Hardware "B"	32
Tabla 2 - 14: Costo de Software "B"	33
Tabla 2 - 15: Costo de Dispositivos.....	34
Tabla 2 - 16: Costos operativos Alternativa "B"	35
Tabla 2 - 17: Factibilidad Operativa Alternativa "B"	36
Tabla 2 - 18: Costos Totales Alternativa "B"	37
Tabla 3 - 1: Detalle Interfaces Router.....	43
Tabla 3 - 2: Comandos del Router- modo usuario.....	48
Tabla 3 - 3: Comandos del Router-modo Privilegiado	50
Tabla 3 - 4: Comandos de configuración Global.....	53
Tabla 3 - 5: Comandos de Edición del Router.....	54
Tabla 3 - 6: Protocolo de Enrutamiento.....	77
Tabla 3 - 7: Tipos de Vlan	95
Tabla 3 - 8 : Numeración de las Listas de Accesos	142

INTRODUCCIÓN

Este manual se lo ha desarrollado en base a la infraestructura de red del CEES “Centro De Estudios Espiritu Santo”.

Objetivos de este manual

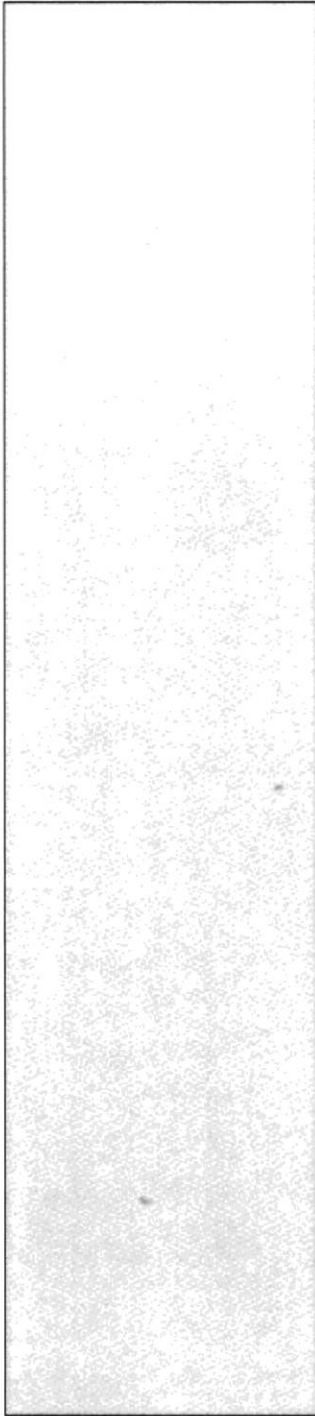
El Objetivo de este manual es poder llenar las expectativas de las personas a quienes les ayude este manual de Infraestructura de redes del Centro De Estudios Espiritu Santo y así poder compartir nuestros conocimientos con quienes los necesitan y se dejan enseñar. Poder ser parte de sus sueños que quieran realizar, que no hay obstáculo para vencer y poder ser alguien en la vida.

Lo que se debe conocer

Los conocimientos mínimos que deben tener las personas que utilizan este manual deben ser:

- ✓ Conocimientos básicos de Windows.
- ✓ Conceptos básicos de redes y sistemas operativos.
- ✓ Conceptos básicos de informática e Internet.





CAPITULO 1
SITUACIÓN ACTUAL

CAPITULO 1

1.- SITUACIÓN ACTUAL

1.1- ANTECEDENTES

El INSTITUTO SUPERIOR TECNOLÓGICO ESPÍRITU SANTO, es una entidad educativa de nivel superior, que forma profesionales de mandos medios, con una metodología activa, para que al egresar como Tecnólogo, pueda insertarse en el ámbito laboral, con competencias sólidas y conocimientos empresariales actualizados.

El Centro De Estudios cuenta con 16 departamentos:

- 1.- Sistemas
- 2.- Ces-Escuela
- 3.- Ces-Colegio
- 4.- Rectorado
- 5.- RRHH
- 6.- Caja
- 7.- Contabilidad
- 8.- Biblioteca
- 9.- Bar
- 10.- Tes-Escuelas
- 11.- Tes-Bienestar
- 12.- Capacites
- 13.- Marketing
- 14.- Fes-Escuela
- 15.- Fes-Colegio
- 16.- SPIRIT-GYM



1.1.1.- HISTORIA

Fue creada el 18 de enero de 1988, mediante acuerdo No. 681 otorgado por la Dirección Provincial de Educación del Guayas, como nivel post bachillerato del Centro de Estudios Espíritu Santo, CEES.

El 12 de junio de mismo año, con acuerdo No. 2582 el Ministerio de Educación y Cultura, le concede al TECNOLÓGICO ESPÍRITU SANTO, la calidad de EXPERIMENTAL.

El 23 de diciembre de 1992, mediante acuerdo No. 1838 el Ministerio de Educación y Cultura, le confiere al TECNOLÓGICO ESPÍRITU SANTO, la calidad de AUTÓNOMO.

En 1992 los Institutos Superiores fueron integrados al Sistema Nacional de Educación Superior, junto a las Universidades y Escuelas Politécnicas, regidos por el CONESUP, organismo que de conformidad a lo dispuesto en el artículo No. 21 de la Ley Orgánica de Educación Superior, acogió al INSTITUTO SUPERIOR TECNOLÓGICO ESPÍRITU SANTO, con el Registro Institucional No. 09-004, por lo tanto somos una entidad legítimamente reconocidas.

1.1.2.- MISIÓN

Somos una institución de educación superior que forma profesionales con visión gerencial, emprendedores, generadores de cambio, y conducta ética, dispuestos y preparados para enfrentar exitosamente los desafíos del mundo globalizado aportando al desarrollo económico, político, social y cultural de su entorno.

1.1.3.-VISIÓN

El Tecnológico Espíritu Santo, será la institución educativa más reconocida en el país por generar empresarios con capacidad gerencial, preparados por un staff de docentes altamente calificados, utilizando tecnología de punta e instalaciones de primer nivel, colaborando estrechamente en el desarrollo sostenible del entorno.



1.2.- INFRAESTRUCTURA DE RED LAN

1.2.1.- ESTACIONES DE TRABAJO

El Centro de Estudios Espíritu Santo posee:

117 equipos para Usuarios Administrativos

En la siguiente tabla se muestran las características de los equipos pertenecientes a cada usuario los cuales están distribuidos en las siguientes áreas: RR.HH,



Figura 1 - 1: Pc Usuario



Cantidad	S.O.	Procesador	Disco Duro	Memoria	Nic/ Velocidad
177	Windows XP	desde 1.6 Hasta 3.0 Ghz	Desde 40 hasta 320 GB	Desde 256 Hasta 4.0MB	D-Link/ 10/100 Kbps

Tabla 1 - 1: Características de la PC Usuario

266 Equipos en 12 Laboratorios de computación los cuales están ubicados para el aérea del CES(masculino) 5 laboratorios A,B,C,D y Mac para el FES (femenino) 4 laboratorios D,E,F, G.



Figura 1 -2: Pc de Laboratorio

En las siguientes tablas se muestran las características generales de los equipos pertenecientes a los Laboratorios.

Cantidad	S.O.	Procesador	Disco Duro	Memoria	Nic/ Velocidad
151	Windows XP	3.0 Ghz		512 MB	D-Link/ 10/100 Kbps
73		Dual Core	80 GB	1 GB	
26		1.80 Ghz		256 MB	

Tabla 1 -2: Características de la Pc de Lab.





Figura 1 -3: Equipo Mac

Cantidad	S.O.	Procesador	Disco Duro	Memoria	Nic/Velocidad
16	MAC	2.6 Ghz	160 GB	1 GB	10/100 Kbps

Tabla 1 -3: Características de Pc Mac

1.2.2.- IMPRESORA

En la siguiente tabla se muestra las características de las impresoras que se encuentran en cada departamento:



Figura 1 - 4: Impresora hp

Cantidad	Marca	Modelo
80	Hp	Deskjet 3550

Tabla 1 -4: Características de Impresora HP

En la siguiente tabla se muestra las características de las impresoras pertenecientes a los Laboratorios tanto del Ces como Fes cabe recalcar que en cada laboratorio hay una sola impresora:



Figura 1 -5: Impresora Lexmark

Cantidad	Marca	Modelo
12	Lexmark	E220

Tabla 1 -5: Características de la Impresora Lexmark

También cuenta con equipos eléctricos de los cuales se destacan los siguientes:

- ✓ 2 APS de 3 KVA
- ✓ 2 UPS de 3
- ✓ 2 UPS de 2.2 KVA



1.3.- DISPOSITIVOS DE COMUNICACIÓN

1.3.1.- SWITCH

El switch que usa es D-Link y pertenece a la capa 1 del modelo OSI cabe recalcar que no es administrable, y hay 28 dispositivos en el Centro de Estudios.



Figura 1 -6: Switch D-Link

1.3.2.- CARACTERÍSTICAS DEL SWITCH

A continuación se detallan las características generales de Switch modelo DES -1024R

- ✓ Marca y Modelo: D-Link DES-1024R+
- ✓ 24 Fast ethernet
- ✓ 2 Fibra Óptica (Modulo Disponible)
- ✓ Transmisión: 10/100 Kbps
- ✓ Estándares: IEEE 802.3 10Base-T Ethernet , IEEE 802.3u 100-BaseTX, 100Base-FX Fast Ethernet
- ✓ Flow Control: IEEE 802.3x (Flow control) en modo Full duplex Back - Pressure en Half Duplex
- ✓ Tasa Transferencia de Datos: Ethernet: 10Mbps (half-duplex), 20Mbps (full-duplex)Fast - Ethernet: 100Mbps (half-uplex), 200Mbps (full-duplex)
- ✓ Cables de Red: 10BASE-T: 2 pair UTP Cat.3 (100 m), 4 pair UTP Cat.4,5 (100 m)EIA/TIA-568 100-ohm STP (100 m)100BASE-TX: 2-pair UTP Cat.5 (100 m)EIA/TIA-568 100-ohm Screened Twisted Pair (STP) (100 m)100BASE-FX:Multi-modo (62.5/125µm or 50/125µm fiber cabling with SC Connector)
- ✓ Método de Transmisión: Store-and-Forward
- ✓ Topología: Estrella
- ✓ RAM Buffer: 256KB por ocho Puertas
- ✓ Direcciones MAC: 4K por switch

1.3.3.- CARACTERÍSTICAS FÍSICAS

- ✓ Tamaño: Montable en rack estándar de 19"
- ✓ Temperatura de Operación: 32 ° ~ 122 °F (0 ° ~ 50 °C)
- ✓ Temperatura de Almacenaje: 13 ° ~ 131 °F (-25 ° ~ 55 °C)
- ✓ Seguridad: L (UL 1950), CSA (CSA950), TUV/GS (EN60950)
- ✓ Dimensión: 441 x 207 x 44 mm (IU),
- ✓ Peso: 2.7 Kg

La tecnología que utiliza es TRUNHING PORT (PUERTO TRUNCADO) Permite Reducir el nivel de congestión entre 2 Switch. Mejora el Perfomato de la Red.



En el siguiente grafico se muestra el Switch como reparte la transmisión por los puertos a los servidores, a las diferentes estaciones de trabajo y a los laboratorios.

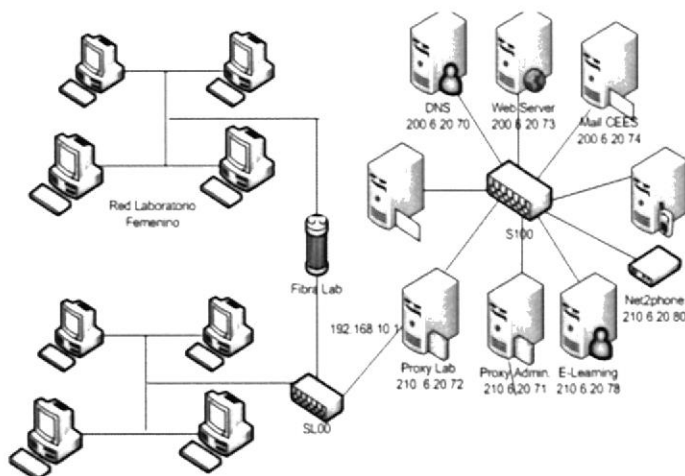


Figura 1 -7: Comunicación de Switch

Diseño de Red Lan Administrativa

Switch de Red

- SA00 Master
- SA01 Sistemas
- SA02 CES-Escuela
- SA03 CES-Colegio
- SA04 Rectorado
- SA05 RRHH
- SA06 Caja
- SA07 Contabilidad
- SA08 Biblioteca
- SA09 Bar
- SA10 Tes-Escuelas
- SA11 Tes-Bienestar
- SA12 CAPACITES
- SA13 Marketing
- SA14 FES-Piso1
- SA15 FES-Piso3
- SA16 SPIRIT-GYM
- TFA1:Fibra-Sistemas
- TFA2:Fibra-FES

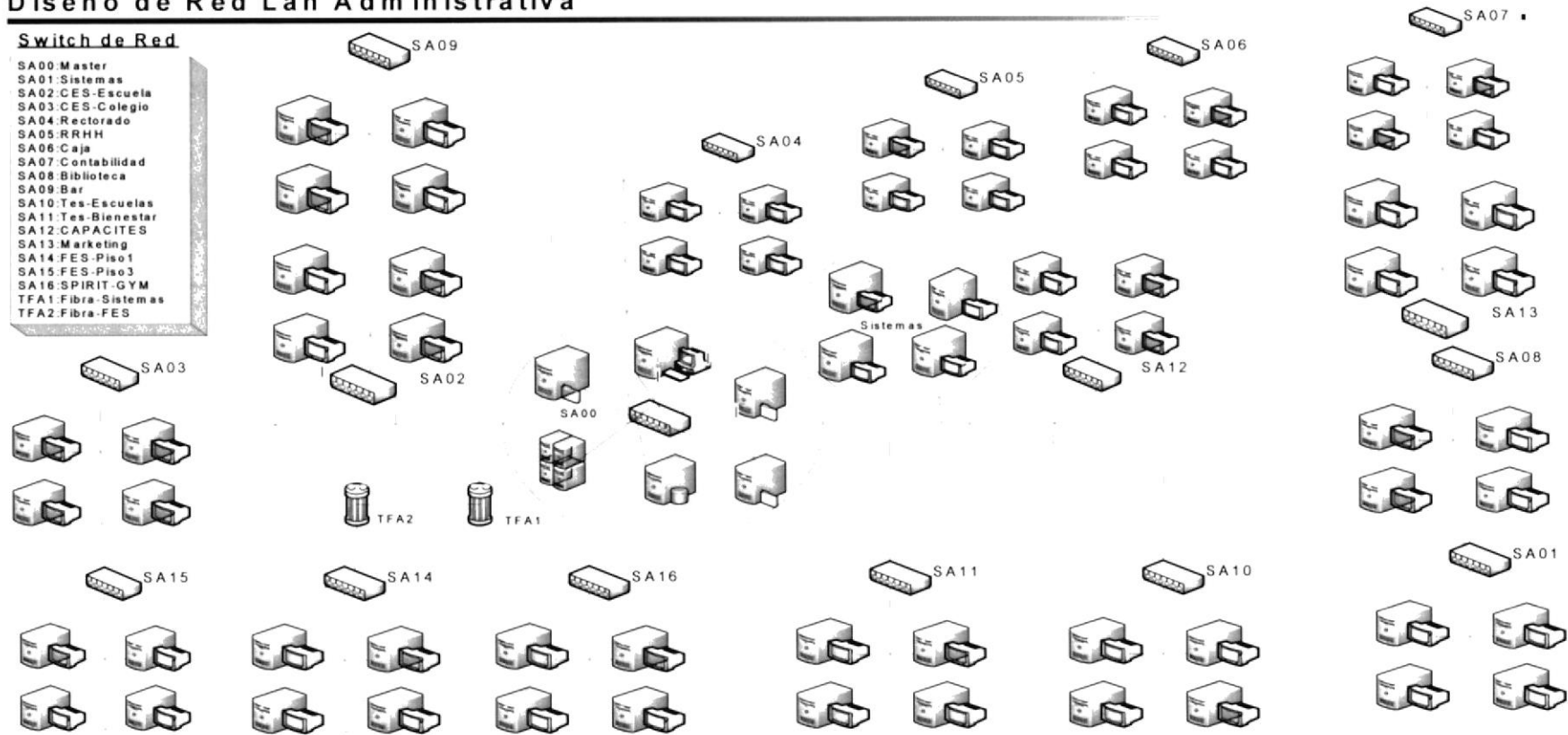


Figura 1 -8: Diseño de red Lan

Leyenda:

Switch d-link des-1024r+



Pc – Usuario



Transmisor de fibra



Servidor



1.3.- MEDIOS DE COMUNICACIÓN

1.3.1.- INALÁMBRICOS:

1.3.1.1- WIRELESS

Cuentan con esta tecnología y su ancho de banda es de 512 Kbps.

1.3.1.2- ROUTERS

El Router Linksys, permite la comunicación entre diferentes segmentos de Red. Trabaja basado en el Protocolo IP.



Figura 1 -9: Router Linksys

Hay 5 medios en total en los departamentos de Biblioteca, Dpto. de Sistemas, Fes (femenino), Spirit, Dirección Ejecutiva.

A continuación se detallan las características:

Marca	Modelo	Tipo de puertos	Velocidad	Frecuencia	Dimensiones	Peso
Linksys	Wrt54G Versión 5	4 LAN RJ45, 1 WAN RJ45	54 Mbps	2.4GHz	18,6 x 17,5 x 4,8 cm	482 g

Tabla 1 - 6: Características de router Linksys

Asimismo, dispone de dos antenas externas conectadas a través de conectores de polaridad inversa TNC.

Se comunican a través:

- Vía UTP Categoría 5E

En el siguiente grafico se muestra como los usuarios se conectan desde sus portátiles o móvil a la red inalámbrica.

1.3.2.- ACCESS POINT

Access Point es un punto de acceso inalámbrico privado, para conectar sus computadoras a Internet sin necesidad de cables, permitiendo compartir recursos de red.

1.3.2.1.- CARACTERÍSTICAS TÉCNICAS

- ✓ Marca: Alvarion
- ✓ Modelo: N6-4D1W
- ✓ Opera en el estándar inalámbrico IEEE 802.11g.
- ✓ Velocidad de transferencia máxima de 11 Mbps y se ajusta automáticamente en función de la cobertura y calidad de la transmisión.
- ✓ Facilidad de auto instalación y fácil configuración.
- ✓ Capacidad de encriptación de las comunicaciones.
- ✓ Alcance de 50 m en interiores y 200 en exteriores, aunque estas mediciones son simples referencias ya que el alcance real vendrá determinado por el entorno físico en el que se instale.
- ✓ Puede soportar hasta 6 equipos inalámbricos para una navegación óptima constituidos como una red local (LAN) inalámbrica.

Hay 3 puntos de Acceso (ACCESS POINT), ubicados en el Fes(femenino), Ces(masculino), bar.

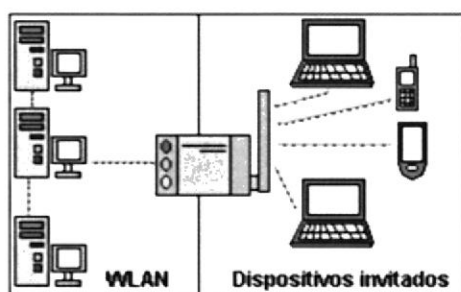


Figura 1 -10: Access Point



1.3.2.2- FUNCIONAMIENTO DEL ACCESS POINT

- ✓ El Access Point se encuentra conectado en una red local inalámbrica (WLAN).
- ✓ Los dispositivos inalámbricos externos le envían la petición de acceso a los recursos de la red (Internet, E-mail, impresión, Chat, etc.).
- ✓ El Access Point se encarga de determinar en base a su configuración, que dispositivos están autorizados a acceder a la red y cuáles no.

1.4.- RED WAN

1.4.1- MEDIOS DE COMUNICACIÓN

1.4.1.1- FIBRA ÓPTICA

La fibra es de tipo Multimodo y tiene una Longitud de 310 M. Cuenta con 2 Segmentos de Fibra. Se comunica vía UTP de Categoría 5E.

La Fibra se conecta al Router a través de:

- ✓ 4 Transciver, Marca ALLIED – TELESYN.

Aparte cuenta con 2 Transciver de Contingencia.

El centro cuenta con redes privadas.

1.4.2.- DISPOSITIVOS DE COMUNICACIÓN

1.4.2.1.- ROUTER CISCO 2600 SERIES

La serie 2600 de Cisco de arquitectura modular ofrece a los administradores de red y proveedores de servicios una solución de sucursal que ofrece la versatilidad necesaria para adaptarse a los cambios en la tecnología de red.

El Centro cuenta con 2 Router Cisco ubicadas en el área Fes y Ces.



1.4.2.1.1.-CARACTERÍSTICAS:


Marca	Modelo	Características	Tipo de puertos	Dimensiones
Cisco 	2600 Series	Procesador CPU Power PC RISC Memoria Flash, 8 MB, ampliable a SIMM de 16 MB Memoria DRAM del sistema 24 MB de DRAM, ampliables a DIMM de 64 MB de DRAM	1 x RJ45 Ethernet 0/0 1 x RJ45 Aux 1 x RJ45 Consola	(Al x An x Pr) 1,69 x 17,5 x 11,8 pulgadas

Tabla 1 -7: Características del Router Cisco 2600 Series

1.4.2.2.- ROUTER MICROTIK

El Centro de Estudios tiene 2 routers microtik modelo RouterBOARD 450

El Router Microtik hace de firewall luego de recibir del cisco la conexión con el proveedor.

El segundo Router recibe vía transceiver la señal y la redistribuye para otro punto de acceso wireless para el FES el cual lleva Internet y red administrativa para el FES



Figura 1 -11: Router Microtik

1.4.2.2.1.- CARACTERÍSTICAS DEL ROUTER

- ✓ RouterOS Wireless AP/Firewall/Routing (nivel 4)
- ✓ CPU Atheros 680MHz
- ✓ 5 Puertos Ethernet 10/100/1000 Auto MDI-X
- ✓ 256MB Ram
- ✓ 512 MB NAND
- ✓ Altavoz en placa
- ✓ 1 puerto serie DB9 RS232C
- ✓ Alimentación por Jack o PoE 9..28V DC
- ✓ Consumo de energía a plena carga: 3-4W
- ✓ 115mm x 90mm (4.53in x 3.54in)



Diseño de Red Wan – Centro de Estudios Espiritu Santo

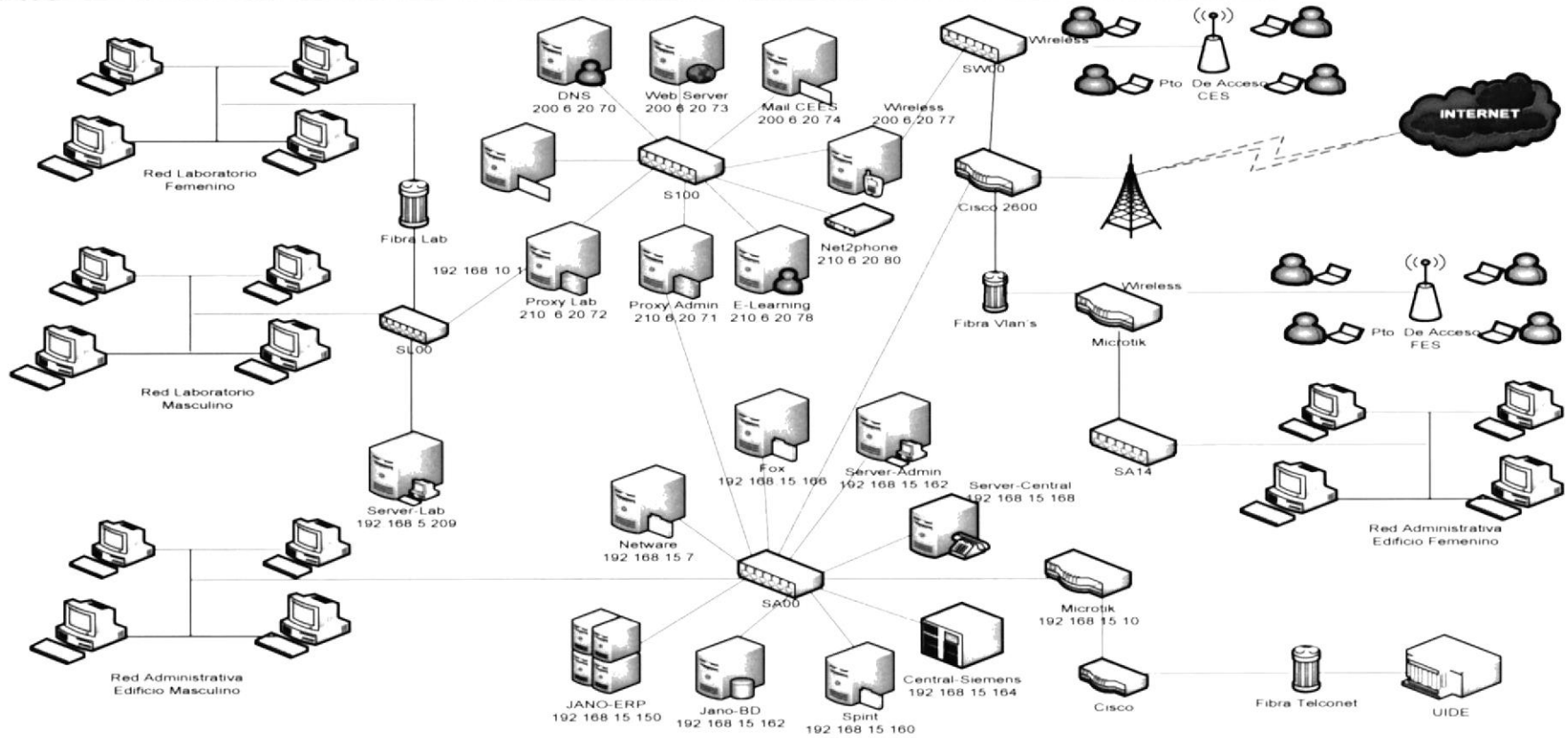


Figura 1-12: Diseño de red Wan

Leyenda:

Pc Usuario	Transmisión de fibra	Switch	d-link des-1024r+	Servidor	Router	Pto. De Acceso	Proveedor de Internet	Enlace

1.5.- SERVIDORES



Tiene 18 servidores los cuales están ubicados en el Dpto. de Sistemas. A continuación se los menciona:

- 1.- DNS
- 2.- Mail TES
- 3.- Web-Server
- 4.- Mail CEES
- 5.- Wireless
- 6.- e-Learning
- 7.- Proxy- Admin
- 8.- Proxy-Lab
- 9.- Fox
- 10.- Netware
- 11.- Server-Admin
- 12.- Server-Central
- 13.- SPIRIT
- 14.- Jano-DB
- 15.- Jano-ERP
- 16.- Desarrollo
- 17.- Server-Lab
- 18.- Sistema Antivirus



En la siguiente tabla detallamos las características de cada uno de los servidores:

Cantidad	S.O	Procesador	Disco Duro	Memoria	Nic/ Velocidad	Observación
9	Fedora Core Windows 2003	Pentium IV 2.0 Ghz	80GB	1GB	D-Link 10/100 Kbps	Sata

Tabla 1 -8: Características de los servidores

En la siguiente tabla se muestran las características del servidor de la base de datos:

Cantida d	Rol	S.O	Proces -ador	Disco Duro	Memori a	Nic/ Velocida d	Observació n
1	B.D	Postgre s	Xeon	2 H.D De 140 c/u	2GB	D-Link 10/100 Kbps	Los discos trabajan en espejo
2	Aplica -ción	Novel 31. Fedora Core		80G B			

Tabla 1 -9: Características de los Srv. BD y Aplicación

En la siguiente tabla se detallan las características de los siguientes servidores:

Cantidad	Rol	S.O	Proce- sador	Disco Duro	Memoria	Nic/ Veloci- dad	Observa- ción
1	Srv. Antivirus lab.	W i n d o w s X P	P e n t i u m I V 2 0 G h z	80 GB	1GB	D-Link 10/100 Kbps	
1	Antivirus Admin						
1	Central Telefonic						
1	Correo Electro- nico						

Tabla 1 -10: Características de Srv. Antivirus y otros

1.6.- SEGURIDADES

El Centro de Estudios Espíritu Santo maneja su seguridad a través del Servidor Proxy en la cual tienen configurado el Firewall. No utiliza firewall físico; sino un software que está configurado bajo la plataforma Linux para ser utilizado juntamente con el servidor proxy.

1.7.- INTERNET

Su proveedor es ESPOLTEL y su ancho de banda es de 3MB de velocidad. Además el proveedor tiene el software de firewall que lo maneja a través de reglas de iptables.

En el siguiente grafico vemos como el proveedor de internet EspolTEL se conecta a la torre de transmisión, la cual está conectada a un router cisco y este se conecta al Switch quien se encargara de conectarse y repartir internet a las estaciones de trabajo.

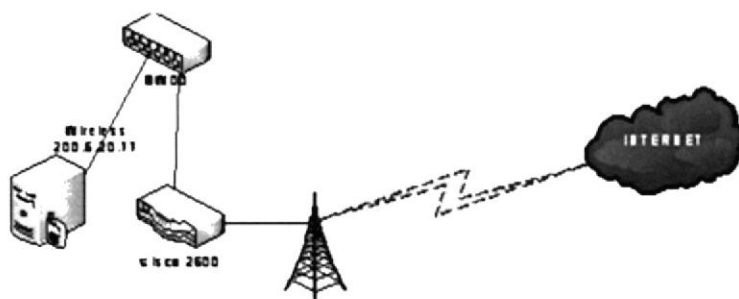
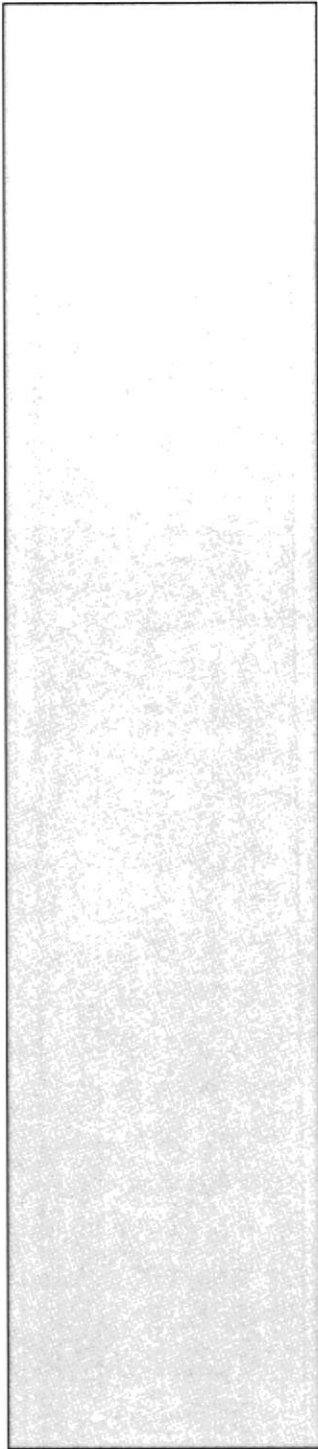


Figura 1 -13: Grafico de conexión a Internet

1.8.- PROBLEMAS ENCONTRADOS

- ✓ Exceso de Broadcast en la red Lan del Fes.
- ✓ Hardware no adecuado en los servidores para los sistemas que utiliza.
- ✓ No Cuentan con políticas de actualización del Antivirus dentro de la institución.
- ✓ No cuentan con una arquitectura Cliente – Servidor para el Antivirus.



CAPITULO 2
SOLUCIÓN PROPUESTA

CAPITULO 2

2.- SOLUCIÓN PROPUESTA

2.1.- PROBLEMAS ENCONTRADOS

PROBLEMAS	CAUSA	EFEECTO
Exceso de Broadcast en la red Lan del Fes.	La red Lan en el Fes no esta segmentada por departamentos.	Congestionamiento en la red Lan del Fes.
Hardware no adecuado en los servidores para los sistemas que utiliza.	Falta de presupuesto y Despreocupación del Administrador de Sistemas.	Lentitud en los Servidores.
No Cuentan con políticas de actualización del Antivirus dentro de la institución	Despreocupación del Administrador de Sistemas.	Posible pérdida de información por infecciones de los PCs en la Red Lan.
No cuentan con una arquitectura Cliente – Servidor para el Antivirus	El Antivirus es obsoleto ya que no ofrece una actualización centralizada para la red LAN	Pérdida de Tiempo y lentitud del Internet por las actualizaciones individuales del Antivirus

Tabla 2 -1: Problemas Encontrados



2.2.- SOLUCIÓN PROPUESTA

PROBLEMAS	SOLUCIÓN	ALCANCE
Exceso de Broadcast en la red Lan del Fes.	Creación de vlan departamentales en la red Lan del Fes.	Mejorar los tiempos de respuesta de la red LAN
Hardware no adecuado en los servidores para los sistemas que utiliza.	Implementar nuevos servidores con mejores tecnologías	Mejorar el rendimiento de los Servidores.
No cuentan con políticas de actualización del Antivirus dentro de la institución	Establecer e Implementar las políticas de actualizaciones de Antivirus.	Disminuir el riesgo de posibles infecciones la red Lan.
No cuentan con una arquitectura Cliente – Servidor para el Antivirus	Implementar un Antivirus que permita realizar de manera centralizada y automática las actualizaciones del Antivirus	Mejorar el tiempo de respuesta en las redes Lan Cliente Servidor.

Tabla 2 -2: Solución Propuesta

2.3.- ESTUDIO DE LA FACTIBILIDAD

2.3.1.- ALTERNATIVA “A”

El objetivo de esta alternativa es la implementación de una red Lan en el Fes con vlan para reducir el dominio de Broadcast. El Centro De Estudios realizara la compra de licencias de un buen antivirus impidiendo así la propagación de virus y archivos infectados. En cuanto a los servidores se realizara la implementación de nuevos equipos, los cuales agilizaran los procesos y actividades programadas en los mismos.

2.3.1.1.- FACTIBILIDAD TÉCNICA HARDWARE


Cantidad	Descripción	Ubicación
3 Servidores HP Servidor ML110 G5 Dual Core 	*DualCore Intel Xeon X3065 (2.33GHZ) *(2GB RAM) *1disco 160GB SATA * Red Gigabit * DVD-Rom/tower	Cuarto de Servidores

Tabla 2 -3: Factibilidad Técnica hardware



2.3.1.2.-FACTIBILIDAD TÉCNICA DE DISPOSITIVOS DE COMUNICACIÓN

En el siguiente cuadro se detallan los dispositivos a utilizar, los cuales no se van a comprar; ya que se hará uso de los mismos que tiene el Centro de Estudios.



Cantidad	Descripción	Ubicación
8 switch 	Marca y Modelo: D-Link DES-1024R+ 24 Fast ethernet 2 Fibra Óptica (Modulo Disponible) Transmisión: 10/100 Kbps	Lab. Fes
1 Router 	Serie Cisco 2600 Procesador CPU Power PC RISC Memoria Flash, 8 MB, ampliables a SIMM de 16 MB Memoria DRAM del sistema 24 MB de DRAM, ampliables a DIMM de 64 MB de DRAM	

Tabla 2 - 4: Factibilidad Técnica de Dispositivos

2.3.1.3.- FACTIBILIDAD ECONÓMICA

2.3.1.3.1.- COSTO HARDWARE

Cantidad	Precio	Total
3 Servidores	\$1.200.00	\$3.600.00
Costo Total de Adquisición de Hardware :		\$3.600.00

Tabla 2 -5: Costo Hardware



2.3.1.3.2.- COSTO DE SOFTWARE


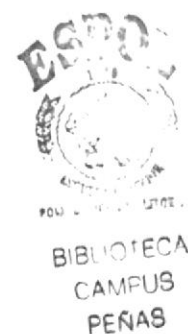
Cantidad	Descripción	Precio	Total
9 paquetes y cada uno contienen 35 licencias. 	Licencia Nod 32 4.0	\$500	\$4.500
Costo Total de Adquisición de Software: \$4.500			

Tabla 2-6: Costo de Software

2.3.1.3.2.1- CARACTERISTICAS PRINCIPALES DEL NOD 32

ESET NOD32 tiene cuatro características únicas que lo destacan del resto de los antivirus del mercado, y que según fuentes especializadas lo convierten en uno de los más eficientes y eficaces.

- ✓ Detección de Códigos Maliciosos
- ✓ Velocidad de Exploración
- ✓ Bajo consumo de recursos del Sistema
- ✓ Tecnología ThreatSense®



2.3.1.3.3.-COSTO DEL DISPOSITIVO

Cantidad	Precio	Total
8 Switch	\$0.00	\$0.00
1 Router	\$0.00	\$0.00
Costo Total de Adquisición de Hardware :		\$0.00

Tabla 2 -7: Costo de Dispositivo



2.3.1.3.4.- COSTOS OPERATIVOS

N° Semanas	Persona o grupo implicada	Costo Semanal	Costo Total	Total Fase
Fase de Análisis				
7 días	1 Analista de Soporte	\$250	\$250	\$250
Fase de Diseño				
1	1 Analista de Soporte	\$200	\$200	\$200
Fase de Implementación				
1	2 Analista de Soporte	\$300	\$600	\$600
Fase de Prueba LAN				
1	1 Analista de Soporte	\$100	\$100	\$175
	1 Asistente de redes	\$75	\$75	
Fase de Documentación				
1 día	1 Analista de Soporte	\$200	\$200	\$200
Costo Total Operativo:				\$1.425.00

Tabla 2 -8: Costos Operativos

2.3.1.3.5.- FACTIBILIDAD OPERATIVA

N°	Persona o grupo implicada	Descripción	Tiempo
Fase de Análisis LAN			
1	Analista de Soporte	Análisis de Falencias halladas en las redes	7 días
Fase de Diseño LAN			
1	Analista de Soporte	Segmentar las redes en vlan.	1 semana
Fase de Implementación LAN			
1	Analista de Soporte	Configuración de redes del Fes.	1 semana
	Analista de Soporte	Instalación y configuración de servidores	
Fase de Prueba LAN			
1	Analista de Soporte Y Asistente en redes	Prueba de transmisión de paquetes de datos y tiempos de respuestas en las red Lan del Fes. Prueba de procesos y aplicaciones en los servidores. Pruebas de manejo de actualización de Antivirus.	1 semana
Fase de Documentación LAN			
1	Analista de Soporte	Entrega de manual sobre red con diagramas y tablas de ip para los equipos	1 día

Tabla 2 -9: Factibilidad Operativa

2.3.1.3.6.- Cuadro de Costos Totales de la Alternativa “A”

Detalle	Precio
Costo Total de Adquisición de Hardware	\$3.600.00
Costo Total de Adquisición de Software	\$4.500.00
Costo Total de Factibilidad “A”	\$8.100.00
IVA 12%	\$ 972.00
Costo Total	\$9.072.00

Tabla 2 -10 : Costos Totales de la Alternativa “A”

2.4.- VENTAJAS Y BENEFICIOS DE LA ALTERNATIVA “A”**2.4.1- VENTAJAS**

- ✓ Disminuye el tráfico de la red.
- ✓ Mayor disponibilidad de las direcciones Ip.
- ✓ Mejora la transmisión de datos en cliente servidor.
- ✓ Mejora y la seguridad en las estaciones de trabajo.
- ✓ Mejora el tiempo de respuesta de los servidores a los equipos de trabajo.

2.4.1.1.- BENEFICIOS

- ✓ Mayor confiabilidad en la transmisión de la información.
- ✓ Mejor distribución de la comunicación e información en el Establecimiento, que facilitara el crecimiento de la misma.
- ✓ Mejor tiempo de respuesta en la comunicación entre los usuarios departamentales.

2.4.2.- FORMA DE PAGO Y LAPSO A DESARROLLARSE

Para la aplicación de este proyecto en el Centro de Estudios se lo hará en 3 pagos:

El 50% corresponderá al costo de validez de la propuesta la cual incluye la etapa de Fase de Análisis.

El 30% corresponderá a la etapa de Fase de Diseño Lan y De La Fase De Implementación donde se va adquirir todo el hardware y software.

El 20% corresponderá a la terminación de la etapa de prueba y documentación Lan.

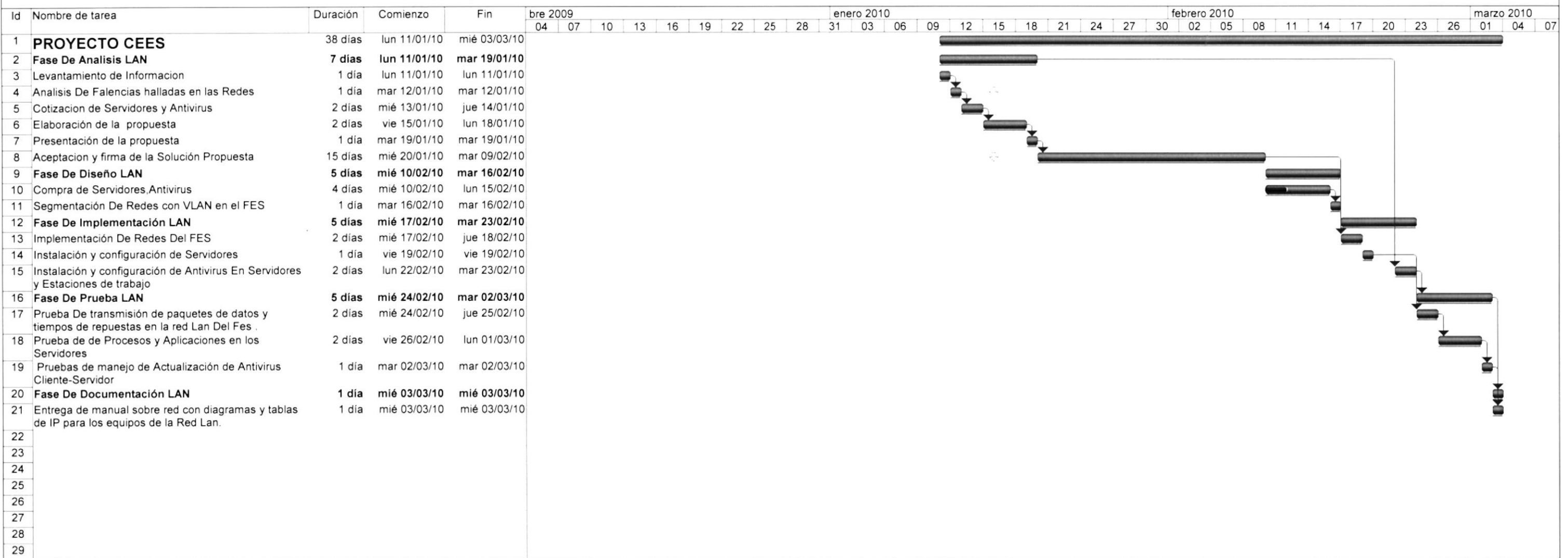
2.4.3.- GARANTÍA

Cuando el cliente este conforme y haya aceptado la nueva propuesta se procederá con la firma del representante del Dpto. de Sistemas el Ing. Jesús Uriña y la empresa contratada para la aplicación del proyecto aquí aplicado.

Las garantías correspondientes las nombraremos a continuación:

- ✓ Todos los equipos que se implementen en esta solución propuesta, contaran con 1 año de garantía.
- ✓ El servicio técnico de lo que se implemente en el establecimiento tendrá una garantía de 6 meses gratis, después de este período el servicio técnico tendrá un costo adicional.

2.5.-CRONOGRAMA DE TRABAJO ALTERNATIVA "A"



Proyecto: Alternativa "A"

Tarea Progreso Resumen Tareas externas Fecha límite

División Hito Resumen del proyecto Hito externo

2.6.- ESTUDIO DE LA FACTIBILIDAD

2.6.1.- ALTERNATIVA “B”

El objetivo de esta alternativa es la implementación de una red Lan en el Fes con vlan para reducir el dominio de Broadcast. El Centro De Estudios realizara la contratación de licencias del antivirus Fore Front impidiendo así la propagación de virus y archivos infectados. En cuanto a los servidores se realizara la implementación de nuevos equipos, los cuales agilizaran los procesos y actividades programadas en los mismos.

2.6.1.1.- FACTIBILIDAD TÉCNICA HARDWARE

Cantidad	Descripción	Ubicación
3 Servidores PowerEdge T300 	Intel® Celeron® Processor 445 at 1.86GHz, 512K Cache, 1066MHz FSB Memoria 2GB DDR2,667MHz Primera Unidad de Disco Duro 160GB serial ATA	Cuarto De Servidores

Tabla 2 -11: Factibilidad Técnica hardware “B”



2.6.1.2.-FACTIBILIDAD TÉCNICA DE DISPOSITIVOS DE COMUNICACIÓN

En el siguiente cuadro se detallan los dispositivos a utilizar, los cuales no se van a comprar; ya que se hará uso de los mismos que tiene el Centro de Estudios.


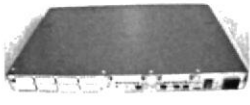
Cantidad	Descripción	Ubicación
8 switch 	Marca y Modelo: D-Link DES-1024R+ 24 Fast ethernet 2 Fibra Óptica (Modulo Disponible) Transmisión: 10/100 Kbps	Lab. Fes
1 Router 	Serie Cisco 2600 Procesador CPU Power PC RISC Memoria Flash, 8 MB, Ampliables a SIMM de 16 MB Memoria DRAM del sistema 24 MB de DRAM, ampliables a DIMM de 64 MB de DRAM	

Tabla 2 -12: Factibilidad Técnica de Dispositivos

2.6.2.- FACTIBILIDAD ECONÓMICA

2.6.2.1.- COSTO HARDWARE

Cantidad	Precio	Total
3 Servidores	\$900.00	\$2.700.00
Costo Total de Adquisición de Hardware : \$2.700.00		

Tabla 2 -13: Costo Hardware "B"

2.6.2.2.- COSTO DE SOFTWARE

Cantidad	Descripción	Precio	Total
300	Licencia Microsoft Forefront Client Security	\$6 anual	\$1.800.00
Costo Total de Adquisición de Software: \$1.800.00			

Tabla 2 -14: Costo de Software "B"

Características de Forefront Client Security

Motor integrado de antivirus y anti software espía, que brinda una protección en tiempo real y un escaneo programado para virus, software espía y otras amenazas.

Sistema de administración central, que genera informes y alertas sobre el estado de seguridad de su entorno.

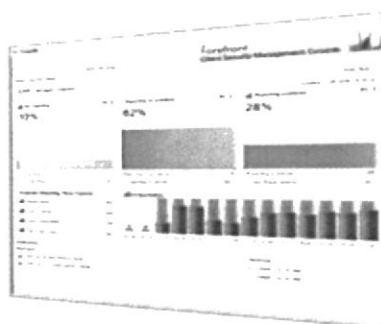


Figura 2 -2: Grafico Motor integrado de antivirus

Evaluación del estado, o escaneos para determinar qué computadoras administradas necesitan parches o están inseguramente configuradas.

2.6.2.3.-COSTO DEL DISPOSITIVO

Cantidad	Precio	Total
8 Switch	\$0.00	\$0.00
1 Router	\$0.00	\$0.00
Costo Total de Adquisición de Hardware :		\$0.00

Tabla 2 -15: Costo de Dispositivos



2.6.2.4.-COSTOS OPERATIVOS DE LA ALTERNATIVA "B"

Nº Semanas	Persona o grupo implicada	Costo Semanal	Costo Total	Total Fase
Fase de Análisis				
7 días	1 Analista de Soporte	\$250	\$250	\$250
Fase de Diseño				
1	1 Analista de Soporte	\$200	\$200	\$200
Fase de Implementación				
1	2 Analista de Soporte	\$300	\$600	\$600
Fase de Prueba LAN				
1	1 Analista de Soporte	\$100	\$100	\$175
	1 Asistente en redes	\$75	\$75	
Fase de Documentación				
1 día	1 Analista de Soporte	\$200	\$200	\$200
Costo Total Operativo:				\$1.425.00

Tabla 2 -16: Costos operativos Alternativa "B"

2.6.2.5.- FACTIBILIDAD OPERATIVA ALTERNATIVA "B"

N°	Persona o grupo implicada	Descripción	Tiempo
Fase de Análisis LAN			
1	Analista de Soporte	Análisis de Falencias halladas en las redes	7 días
Fase de Diseño LAN			
1	Analista de Soporte	Segmentar las redes en vlan.	1 semana
Fase de Implementación LAN			
1	Analista de Soporte	Configuración de redes del Fes	1 semana
	Analista de Soporte	Instalación y configuración de servidores	
Fase de Prueba LAN			
1	Analista de Soporte Y Asistente en redes	Prueba de transmisión de paquetes de datos y tiempos de respuestas en las red Lan del Fes. Prueba de procesos y aplicaciones en los servidores. Pruebas de manejo de actualización de Antivirus.	1 semana
Fase de Documentación LAN			
1	Analista de Soporte	Entrega de manual sobre red con diagramas y tablas de ip para los equipos	1 día

Tabla 2 -17: Factibilidad Operativa Alternativa "B"

**2.6.2.6.- CUADRO DE COSTOS TOTALES DE LA ALTERNATIVA
“B”**

Detalle	Precio
Costo Total de Adquisición de Hardware	\$2.700.00
Costo Total de Adquisición de Software	\$1.800.00
Costo Total de Factibilidad “B”	\$4.500.00
IVA 12%	\$ 540.00
Costo Total	\$5040.00

Tabla 2 -18: Costos Totales Alternativa "B"

**2.7.- VENTAJAS Y BENEFICIOS DE LA ALTERNATIVA
“B”****2.7.1.- VENTAJAS**

- ✓ Disminuye el tráfico de la red.
- ✓ Mayor disponibilidad de las direcciones Ip.
- ✓ Mejora la transmisión de datos en cliente servidor.
- ✓ Mejora y la seguridad en las estaciones de trabajo.
- ✓ Mejora el tiempo de respuesta de los servidores a los equipos de trabajo.

2.7.1.1.- BENEFICIOS

- ✓ Mayor confiabilidad en la transmisión de la información.
- ✓ Mejor distribución de la comunicación e información en el Establecimiento, que facilitará el crecimiento de la misma.
- ✓ Mejor tiempo de respuesta en la comunicación entre los usuarios departamentales.

2.7.2.- FORMA DE PAGO Y LAPSO A DESARROLLARSE

Para la aplicación de este proyecto en el Centro de Estudios se lo hará en 3 pagos:

El 50% corresponderá al costo de validez de la propuesta la cual incluye la etapa de Fase de Análisis.

El 30% corresponderá a la etapa de Fase de Diseño Lan y De La Fase De Implementación donde se va adquirir todo el hardware y software.

El 20% corresponderá a la terminación de la etapa de prueba y documentación Lan .

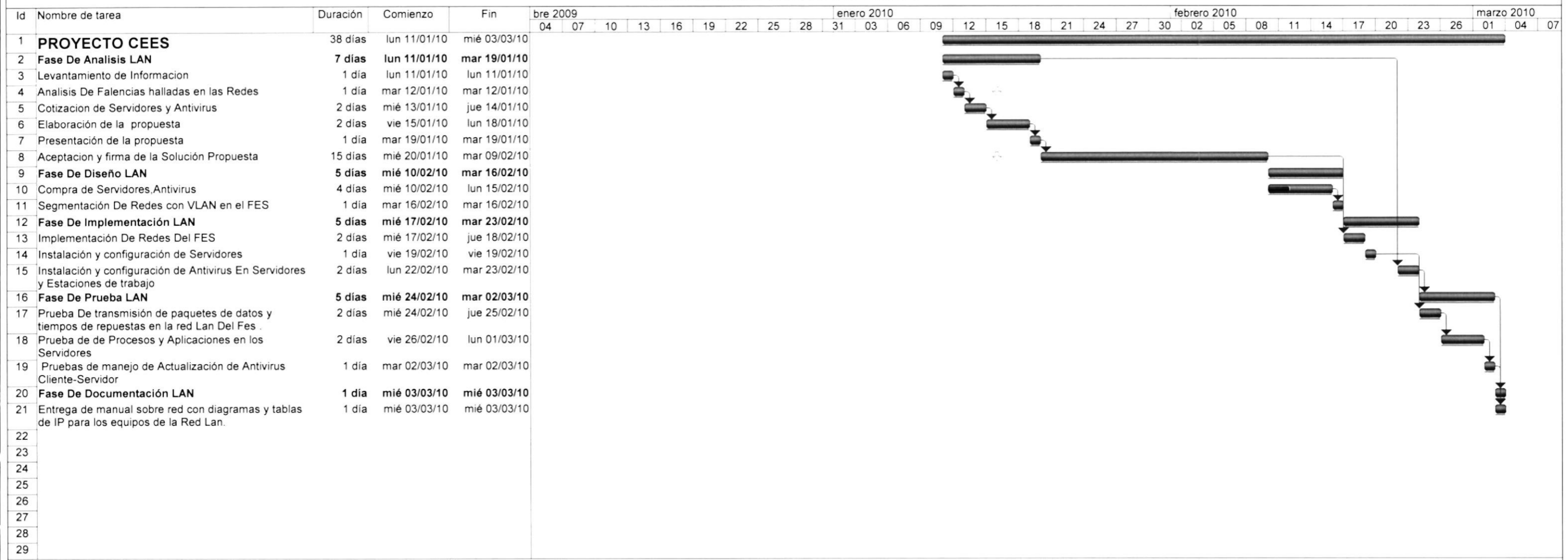
2.7.3.- GARANTÍA

Cuando el cliente este conforme y haya aceptado la nueva propuesta se procederá con la firma del representante del Dpto. de Sistemas el Ing. Jesús Uriña y la empresa contratada para la aplicación del proyecto aquí aplicado.

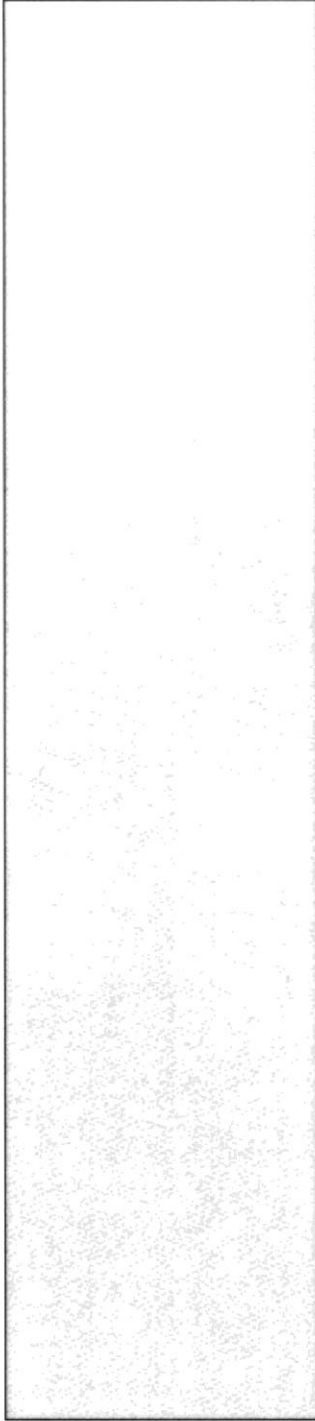
Las garantías correspondientes las nombraremos a continuación:

- ✓ Todos los equipos que se implementen en esta solución propuesta, contarán con 1 año de garantía.
- ✓ El servicio técnico de lo que se implemente en el establecimiento tendrá una garantía de 6 meses gratis, después de este período el servicio técnico tendrá un costo adicional.

2.8.-CRONOGRAMA DE TRABAJO ALTERNATIVA "B"



Proyecto: Alternativa "B"	Tarea		Progreso		Resumen		Tareas externas		Fecha limite	
	División		Hito		Resumen del proyecto		Hito externo			



CAPITULO 3
CONFIGURACIÓN DE DISPOSITIVOS
ROUTERS Y SWICTH

3.- GRÁFICO DE RED LAN Y WAN DEL CENTRO DE ESTUDIOS ESPIRITU SANTO

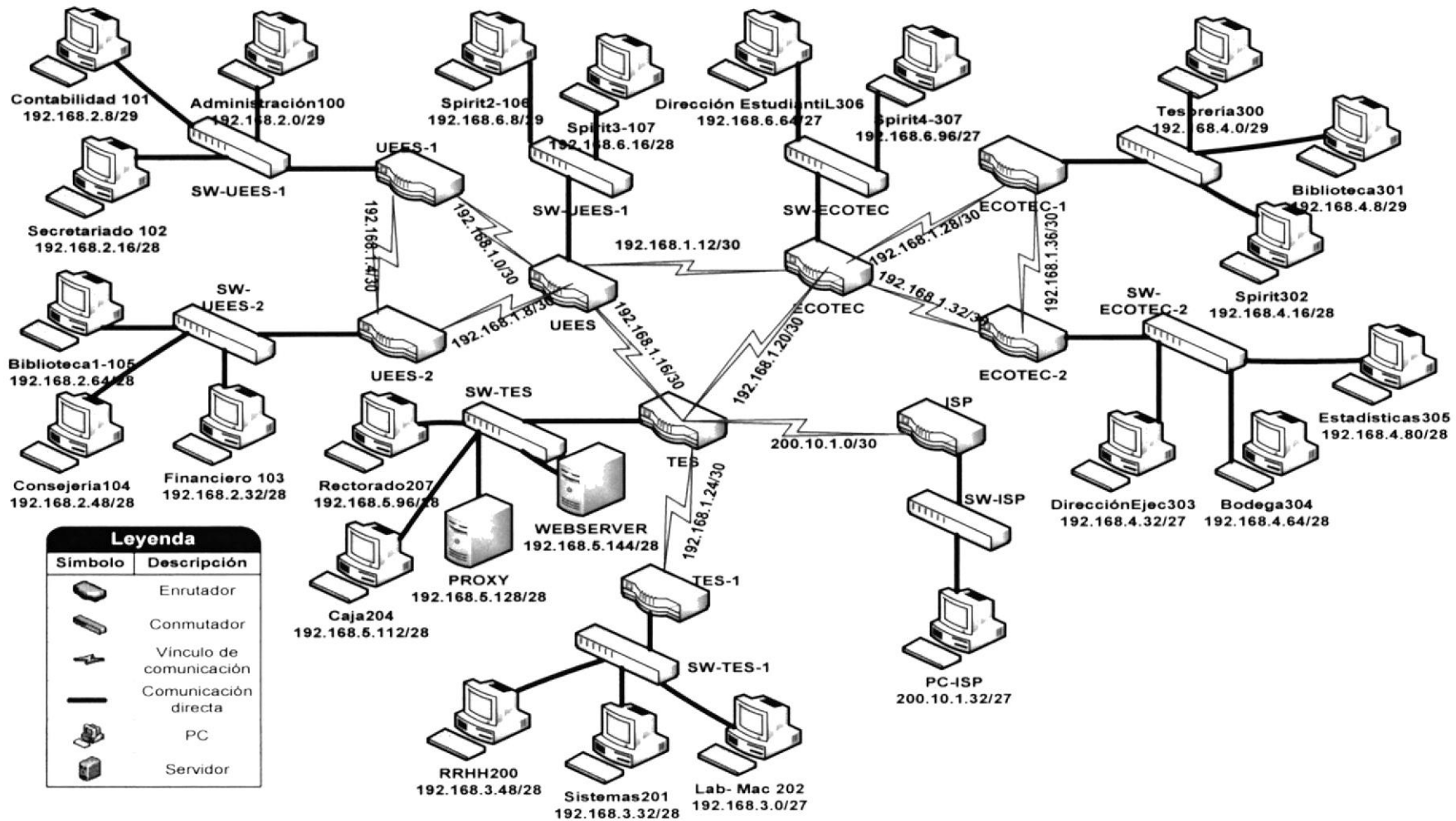


Figura 3 -1: Grafico de RED LAN y WAN

3.1.- INTRODUCCIÓN A LOS ROUTERS

Un router (en español: enrutador o encaminador) es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo IP esta sería la dirección IP). Otras decisiones son la carga de tráfico de red en las distintas interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.

3.1.1. PARTES INTERNAS DEL ROUTER

Los principales componentes internos del router son:

- Memoria de acceso aleatorio (RAM)
- Memoria de acceso aleatorio no volátil (NVRAM)
- Memoria flash
- Memoria de sólo lectura (ROM)
- Interfaces.

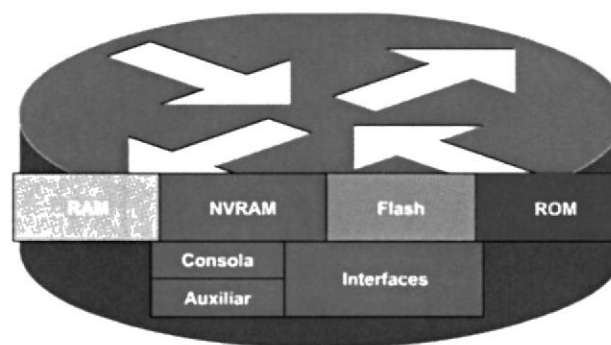


Figura 3 -2: Partes Internas del Router



BIBLIOTECA
CAMPUS
PENAS

CPU: Ejecuta las instrucciones del sistema operativo. Estas funciones incluyen la inicialización del sistema, las funciones de enrutamiento y el control de la interfaz de red. La CPU es un microprocesador. Los grandes routers pueden tener varias CPU.

RAM: Se usa para la información de las tablas de enrutamiento, el caché ARP, el caché de conmutación rápida, la configuración actual y las colas de paquetes. Brinda una memoria temporal para el archivo de configuración del router mientras está encendido. Pierde el contenido cuando se apaga o reinicia el router.

NVRAM: La memoria de acceso aleatorio no volátil (NVRAM) se utiliza para almacenar el archivo de configuración inicial. Retiene el contenido cuando se apaga o reinicia el router.

MEMORIA FLASH: Se utiliza para almacenar una imagen completa del software IOS (Sistema operativo del internetworking) de Cisco. Puede almacenar varias versiones del software IOS. Es un tipo de ROM programable, que se puede borrar electrónicamente (EEPROM).

ROM: Se utiliza para almacenar las instrucciones para el diagnóstico de la prueba de inicio (POST). Guarda el programa bootstrap y el software del sistema operativo. Requiere del reemplazo de chips que se pueden conectar en el motherboard para las actualizaciones del software.

BUSES: La mayoría de los routers contienen un bus de sistema y un bus de CPU. El bus de sistema se usa para la comunicación entre la CPU y las interfaces y/o ranuras de expansión. Este bus transfiere los paquetes hacia y desde las interfaces.

3.1.2. PARTES EXTERNAS DEL ROUTER

Un router básicamente tiene tres tipos de interfaces o conexiones:
de consola/Aux.

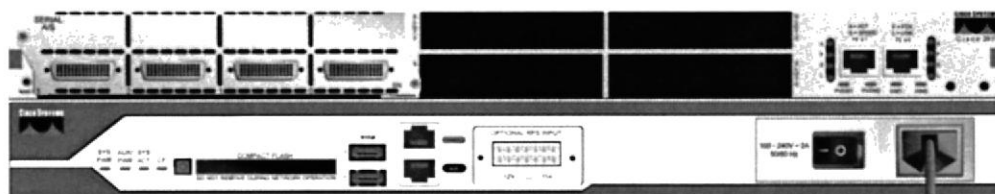


Figura 3 -3: Interfaces del Router

Conexiones LAN	Por lo general son tecnología Ethernet.
Conexiones WAN	Pueden ser seriales por lo general vienen dos por cada Router.
Conexiones RDSI	Los puertos de consola/Aux, son puertos para la administración o configuración de la máquina.

Tabla 3 - 1: Detalle Interfaces Router

3.1.3.- CONEXIONES INTERNAS DEL ROUTER

La función de los puertos de administración es diferente a la de las otras conexiones. Las conexiones LAN y WAN proporcionan conexiones de red por donde se transmiten los paquetes. El puerto de administración proporciona una conexión basada en texto para la configuración y diagnóstico de fallas del router. Los puertos auxiliares y de consola Constituyen la interfaces de administración comunes. Estos son paquetes seriales asincrónicos EIA – 232. Están conectados a un puerto de comunicaciones de un computador.

El computador debe ejecutarse un programa de comunicación de terminal para iniciar la sesión basada en el texto con el router.

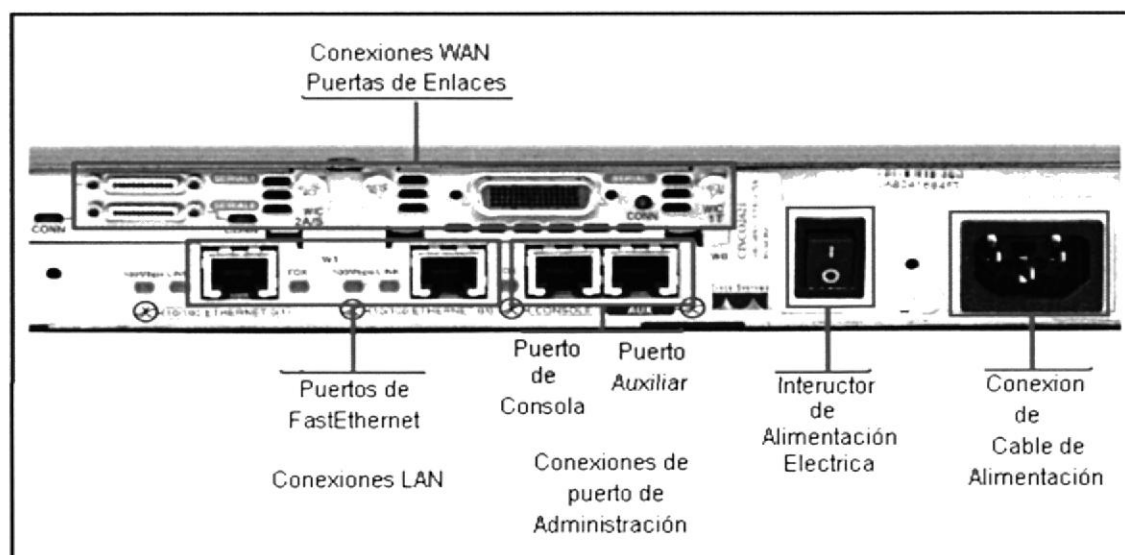


Figura 3 -4: Interfaces del Router



3.2. MEDIOS DE COMUNICACIÓN QUE UTILIZA UN ROUTER

3.2.1. CABLE DCE (DATA CIRCUIT EQUIPMENT)

Es el cable que se conectará al equipo que realiza la función de DCE. Para simular la conexión serie con otro router, se utilizan dos cables uno DCE-DTE. Siendo el DCE el que marcará el clock rate. Es un conector hembra distinguible por tener el conector smartnet más pequeño.



Figura 3 -5: Cable DCE

3.2.2. CABLE DTE (DATA TERMINAL EQUIPMENT)

Es el cable que se conectará al equipo que realiza la función de DTE. Generalmente será el cable que unirá un router a un modem CSU/DSU. Es un conector macho distinguible por tener el conector smartnet más grande.



Figura 3 -6: Cable DTE



3.3. MODOS DEL ROUTER

Modo usuario: Permite consultar toda la información relacionada al router sin poder modificarla. El ejemplo es el siguiente:

```
Router >
```

Usuario privilegiado: Permite visualizar el estado del router e importar o exportar imágenes de IOS. El ejemplo es el siguiente:

```
Router #
```

Modo de configuración global: Permite utilizar los comandos de configuración generales del router. El ejemplo es el siguiente:

```
Router (config) #
```

Modo de configuración de interfaces: Permite utilizar comandos de configuración de interfaces (Direcciones IP, mascarar, etc.). El ejemplo es el siguiente:

```
Router (config-if) #
```

Modo de configuración de línea: Permite configurar una línea (ejemplo: acceso al router por Telnet). El ejemplo es el siguiente:

```
Router (config-line) #
```

Modo espacial: RXBoot Modo de mantenimiento que puede servir, especialmente, para reinicializar las contraseñas del router. El ejemplo es el siguiente:

```
rommon >
```



3.4.- COMANDOS DEL ROUTER EN EL MODO EXEC USUARIO

MODO EXEC USUARIO	
COMANDO	DESCRIPCIÓN
connect {dirección_ip nombre}	Permite conectarse remotamente a un host
disconnect conexión	Desconecta una sesión telnet establecida desde el router.
Enable	Ingresa al modo EXEC Privilegiado.
Logout	Sale del modo EXEC.
ping {dirección_ip nombre}	Envía una petición de eco para diagnosticar la conectividad básica de red.
Resume conexión	Resume una sesión telnet interrumpida con la secuencia CTRL+SHIFT+6 y X.
show cdp	Muestra el intervalo entre publicaciones CDP, tiempo de validez y versión de la publicación.
show cdp entry [* nombre_dispositivo] [protocol version]}	Muestra información acerca de un dispositivo vecino registrado en una tabla CDP.
show cdp interfaces [tipo número]	Muestra información acerca de las interfaces en las que CDP está habilitado.
show cdp neighbors [tipo número] [detail]	Muestra los resultados del proceso de descubrimiento de CDP.
show clock	Muestra la hora y fecha del router.
show history	Muestra el historial de comandos ingresados.
show hosts	Muestra una lista en caché de los nombres de host y direcciones.



COMANDO	DESCRIPCIÓN
show ip rip database	Muestra el contenido de la base de datos privada de RIP
show ip route [dirección protocolo]	Muestra el contenido de la tabla de enrutamiento IP. El parámetro dirección permite acotar la información que se desea visualizar, exclusivamente a la dirección ingresada. El parámetro protocolo permite indicar la fuente de aprendizaje de las rutas que se desean visualizar, como por ejemplo rip, igrp, static y connected
show sessions	Muestra las conexiones Telnet establecidas en el router
show versión	Muestra información sobre el Cisco IOS y la plataforma
telnet {dirección_ip nombre}	Permite conectarse remotamente a un host.
terminal editing	Reactiva las funciones de edición avanzada.
terminal history size numero_líneas	Establece el tamaño del buffer del historial de comandos.
terminal no editing	Deshabilita las funciones de edición avanzada.
traceroute dirección_ip	Muestra la ruta tomada por los paquetes hacia un destino

Tabla 3 -2: Comandos del Router- modo usuario



3.5.- COMANDOS EN EL MODO EXEC PRIVILEGIADO

MODO EXEC PRIVILEGIADO	
COMANDO	DESCRIPCIÓN
configure terminal	Configura la terminal manualmente desde la terminal de consola.
copy flash tftp	Copia la imagen del sistema desde la memoria Flash a un servidor TFTP
copy running-config startup-config	Guarda la configuración activa en la NVRAM
erase flash	Borra el contenido de la memoria Flash
erase startup-config	Borra el contenido de la NVRAM
no debug all	Desactiva todas las depuraciones activadas en el dispositivo
Reload	Reinicia el router
Setup	Entra a la facilidad de Diálogo de configuración inicial
show access-lists [Nro_ACL Nom-bre_ACL]	Muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número de ACL como opción a este comando
show arp	Muestra la asignación de direcciones IP a MAC a Interfaz del router
show cdp traffic	Muestra los contadores CDP, incluyendo el número de paquetes enviados y recibidos, y los errores de checksum
show controllers serial [número]	Muestra información importante como que tipo de cable se encuentra conectado



BIBLIOTECA
CAMPUS
PEÑAS

COMANDO	DESCRIPCIÓN
show flash	Muestra la disposición y contenido de la memoria Flash
show interfaces [tipo número]	Muestra estadísticas para la/las interfaces indicadas
show ip interface [tipo número]	Muestra los parámetros de estado y globales asociados con una interfaz
show ip protocols [summary]	Muestra los parámetros y estado actual del proceso de protocolo de enrutamiento activo
show memory	Muestra estadísticas acerca de la memoria del router, incluyendo estadísticas de memoria disponible
show processes	Muestra información acerca de los procesos activos
show protocols	Muestra los protocolos de capa 3 configurados
show running-config	Muestra la configuración actual en la RAM
show sessions	Muestra las conexiones Telnet establecidas en el router
show stacks	Controla el uso de la pila de procesos y rutinas de interrupción y muestra la causa del último re arranque del sistema
show startup-config	Muestra la configuración que se ha guardado, que es el contenido de la NVRAM
terminal monitor	Si se utiliza una sesión por telnet para examinar el router, entonces, permite redirigir el resultado y los mensajes del sistema hacia a terminal remota

Tabla 3 -3: Comandos del Router-modo Privilegiado



BIBLIOTECA
CAMPUS
PEÑAS

3.6.- COMANDOS DE CONFIGURACIÓN GLOBAL

MODO DE CONFIGURACIÓN GLOBAL	
COMANDO	DESCRIPCIÓN
access-list Nro_ACL {permit deny} Origen	Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes que llegan desde un Origen. Este último parámetro puede ser una dirección IP más una máscara wildcard, la palabra host más una dirección IP o el wildcard any
access-list Nro_ACL {permit deny} Proto Origen Destino [Operador Nro_puerto] [established][echo echo-reply]	Crea o agrega una sentencia de condición a la ACL que permitirá o denegará los paquetes que lleguen desde un Origen y vayan hacia un Destino. Proto identifica el protocolo a verificar. Origen y Destino pueden ser una dirección IP más una máscara wildcard, la palabra host más una dirección IP o el wildcard any. Operador puede ser lt (menor que), gt (mayor que), eq (igual a) o neq (distinto a). Nro_puerto indica el puerto TCP o UDP. El parámetro established permite el paso de tráfico cuando hay una sesión establecida. En el caso del protocolo ICMP se puede utilizar echo o echo-reply.
Banner motd #mensaje del día#	Configura un cartel con un mensaje del día. Ej: banner motd #Bienvenido#
boot system flash [nombre_imagen_IOS]	Especifica que el router cargue el IOS desde la Flash Ej: boot system flash c2500-IOS
boot system rom	Especifica que el router cargue el IOS desde la ROM



COMANDO	DESCRIPCIÓN
boot system tftp nombre_imagen_IOS dir_IP_server_tftp	Especifica que el router cargue el IOS desde un servidor TFTP. Ej: boot system tftp c2500-IOS 24.232.150.1
cdp run	Habilita CDP globalmente en el router
clock set hh : mm : ss mes día año	Modificar la fecha y hora del router. Ej: clock set 12:31:00 July 12 2004
config-register valor_registro_configuración	Cambia los valores del registro de configuración. Ej: config-register 0x2142
enable password contraseña	Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio. Ej: enable password class
enable secret contraseña	Especifica una capa de seguridad adicional mediante el comando enable password. Ej: enable secret class
hostname nombre	Modifica el nombre del router. Ej: hostname Lab_A
interface tipo número	Configura un tipo de interfaz y entra al modo de configuración de interfaz. Ej: interface ethernet 0
ip access-list {tandard extended} Nombre	Permite crear una ACL nombrada. Se debe indicar el tipo. Este comando ingresa al router al submodo de configuración que puede reconocerse por el prompt.



COMANDO	DESCRIPCIÓN
ip classless	Permite que el router no tome en cuenta los límites con definición de clases de las redes en su tabla de enrutamiento y simplemente transmita hacia la ruta por defecto
ip default-network dirección_red	Establece una ruta por defecto. Ej: ip default-network 210.32.45.0
Ip route dirección_red máscara dir_ip_salto [distancia administrativa]	Establece rutas estáticas. Ej: ip route 210.42.3.0 255.255.255.0 211.1.2.1
line tipo número	Identifica una línea específica para la configuración e inicia el modo de reunión de comandos de configuración. Ej: line console 0 ó line vty 0 4
router protocolo_de_enrutamiento [nro_AS]	Inicia un proceso de enrutamiento definiendo en primer lugar un protocolo de enrutamiento IP. Ej: router rip ó router igrp 120
service password-encryption	Habilita la función de cifrado de la contraseña

Tabla 3 -4: Comandos de configuración Global

BIBLIOTECA
CAMPUS
PEÑAS

3.7.- COMANDOS DE EDICIÓN

COMANDOS DE EDICIÓN Y OTROS	
TECLAS / COMANDO	DESCRIPCIÓN
Ctrl+A	Permite desplazarse al principio de la línea de comandos
Esc+B	Permite desplazarse una palabra hacia atrás
Ctrl+B (o Flecha Izquierda)	Permite desplazarse un carácter hacia atrás
Ctrl+E	Permite desplazarse hasta el final de la línea de comandos
Ctrl+F (o Flecha Derecha)	Permite desplazarse un carácter hacia delante
Ctrl+P (o Flecha Arriba)	Muestra el último comando ingresado
Ctrl+N (o Flecha Abajo)	Muestra el comando más reciente
(tecla Tabulador)	Completa el comando ingresado parcialmente
Ctrl+Z (o end)	Estando en cualquier modo de configuración regresa al modo EXEC Privilegiado
Ctrl+C	Cancela la ejecución del Dialogo de configuración inicial o Setup
Ctrl+Shift+6	Permite interrumpir intentos de ping, traceroute y traducciones de nombres
Exit	Estando en el modo de configuración global o cualquiera de sus submodos regresa al modo anterior. Estando en los modos EXEC Usuario o EXEC Privilegiado, cierra la sesión.

Tabla 3 -5: Comandos de Edición del Router



3.8.- CONFIGURACIONES EN EL ROUTER

En los siguientes pasos o puntos, procederemos a la configuración:

- Asignar nombre a los routers.
- Asignar dirección ip y mascarar a los routers.
- Configuración del protocolo RIP V2 en los routers.
- Configuración del protocolo OSPF en los routers.
- Creación de vlans en los switches.
- Creación de subinterfaces en los routers.
- Creación de Access List.
- Asignación de contraseñas en los routers.

3.9.- ASIGNACIÓN DE NOMBRES A LOS ROUTERS DEL TECNOLÓGICO ESPIRITU SANTO

Doble clic en el router principal TES

```
Router>-----→ Privilegio de usuario no de Administrador
Router>enable: -----→Comando que cambia de usuario normal a Administrador
Router#-----→ Modo privilegiado
Router# configure terminal: -----→ Comando para entrar a la configuración global
Router (config)# hostname TES: ----→ Asigna un nombre al router en nuestro caso:
TES
TES (config)# exit: ----→ Salir de la configuración
TES#wr: -----→Guarda los cambios realizados en el router
Building configuration..
```

Doble clic en el router TES-1

```
Router>enable
Router#configure terminal
Router(config)#hostname TES-1
TES-1(config)#exit
TES-1#wr
```



3.10.- ASIGNACIÓN DE NOMBRES A LOS ROUTERS DE LA UEES

```
Router>enable  
Router#configure terminal  
Router(config)#hostname UEES  
UEES(config)#exit  
UEES#wr
```

```
Router>enable  
Router#configure terminal  
Router(config)#hostname UEES-1  
UEES-1(config)#exit  
UEES-1#wr
```

```
Router>enable  
Router#configure terminal  
Router(config)#hostname UEES-2  
UEES-2(config)#exit  
UEES-2#wr
```

3.11.- ASIGNACIÓN DE NOMBRES A LOS ROUTERS DEL ECOTEC

```
Router>enable  
Router#configure terminal  
Router(config)#hostname ECOTEC  
ECOTEC(config)#exit  
ECOTEC#wr
```

```
Router>enable  
Router#configure terminal  
Router(config)#hostname ECOTEC-1  
ECOTEC-1(config)#exit  
ECOTEC-1#wr
```

```
Router>enable  
Router#configure terminal  
Router(config)#hostname ECOTEC-2  
ECOTEC-2(config)#exit  
ECOTEC-2#wr
```



3.12.- ASIGNACIÓN DE NOMBRE AL ROUTER ISP

```
Router>enable
Router#configure terminal
Router(config)#hostname ISP
ISP(config)#exit
ISP#wr
```

3.13.- ASIGNACIÓN DE IP Y MÁSCARAS A LAS SERIALES DEL ROUTER PRINCIPAL TES

Es uno de los pasos primordiales junto con la asignación de los protocolos para establecer comunicación.

La forma de asignar las IP es la misma tanto en routers como en switches, se aplica el comando `interface serial /interface fastethernet(A)`, en donde A es el número de la interfaz, entra a la interface y con el comando `ip address (ip) (mask)` asigna la dirección donde ip es la dirección IP y mask es la máscara de subred.

Después de asignar la IP se asigna un clock rate (DCE) para después ejecutar el comando `no shutdown` para que la interfaz se levante.

TES(config)#interface serial 1/2

↓
Número del puerto

↓
Este es el dispositivo 1

Entra al modo de configuración de interfaz del serial

TES(config-if)#ip address 192.168.1. 25 255.255.255.252

↓
Dirección del serial de salida

↓
Mascara de subred

Asigna una dirección IP y máscara de subred para las rutas.



TES(config-if)#clock rate 64000

Velocidad del reloj

Permite asignar sincronización de reloj en interfaz DCE

TES(config-if)#no shutdown

Activa una interfaz desactivada

%LINK-5-CHANGED: Interface Serial1/2, changed state to down

TES(config-if)#exit

Regresa al modo anterior

TES(config)#interface fastethernet 0 /0

Número del puerto

Este es el dispositivo 0

Entra al modo de configuración de interfaz de la ethernet

TES(config-if)#ip address 192.168.5.65 255.255.255.224

Máscara de subred

Dirección ip de la puerta de enlace

TES(config-if)#no shutdown
TES(config-if)#exit

TES(config)#interface serial 1/3
TES(config-if)#ip address 192.168.1.1 255.255.255.252
TES(config-if)#clock rate 64000
TES(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/3, changed state to down
TES(config-if)#exit

TES(config)#interface serial 1/0
TES(config-if)#ip address 192.168.1.18 255.255.255.252
TES(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0, changed state to down
TES(config-if)#exit



```
TES(config)#interface serial 1/1
TES(config-if)#ip address 192.168.1.22 255.255.255.252
TES(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/1, changed state to down
TES(config-if)#exit
```

3.14.- ASIGNACIÓN DE DIRECCIÓN IP Y MASCARA A LAS SERIALES DEL ROUTER TES-1

```
TES-1(config)#interface serial 1/0
TES-1(config-if)#ip address 192.168.1.26 255.255.255.252
TES-1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0, changed state to down
TES-1(config-if)#exit
```

3.15.- ASIGNACIÓN DE IP Y MÁSCARAS A LAS SERIALES DEL ROUTER PRINCIPAL UEES

```
UEES(config)#interface serial 1/0
UEES(config-if)#ip address 192.168.1.2 255.255.255.252
UEES(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0, changed state to down
UEES(config-if)#exit
```

```
UEES(config)#interface serial 1/1
UEES(config-if)#ip address 192.168.1.10 255.255.255.252
UEES(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/1, changed state to down
UEES(config-if)#exit
```

```
UEES(config)#interface serial 1/2
UEES(config-if)#ip address 192.168.1.13 255.255.255.252
UEES(config-if)#clock rate 64000
UEES(config-if)#no shutdown
UEES(config-if)#exit
```



```
UEES(config)#interface serial 1/3
UEES(config-if)#ip address 192.168.1.17 255.255.255.252
UEES(config-if)#clock rate 64000
UEES(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/3, changed state to down
UEES(config-if)#exit
```

```
UEES(config)#interface fastethernet 0/0
UEES(config-if)#ip address 192.168.6.1 255.255.255.224
UEES(config-if)#no shutdown
UEES(config-if)#exit
```

3.16.- ASIGNACIÓN DE IP Y MÁSCARAS A LAS SERIALES DEL ROUTER UEES-1

```
UEES-1(config)#interface serial 1/1
UEES-1(config-if)#ip address 192.168.1.1 255.255.255.252
UEES-1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/1, changed state to down
UEES-1(config-if)#exit
```

```
UEES-1(config)#interface serial 1/0
UEES-1(config-if)#ip address 192.168.1.5 255.255.255.252
UEES-1(config-if)#clock rate 64000
UEES-1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0, changed state to down
UEES-1(config-if)#exit
```

```
UEES-1(config)#interface fastethernet 0/0
UEES-1(config-if)#ip address 192.168.1.65 255.255.255.224
UEES-1(config-if)#no shutdown
UEES-1(config-if)#exit
```



3.17.- ASIGNACIÓN DE IP Y MÁSCARAS A LAS SERIALES DEL ROUTER UEES-2

```
UEES-2(config)#interface serial 1/0
UEES-2(config-if)#ip address 192.168.1.9 255.255.255.252
UEES-2(config-if)#clock rate 64000
UEES-2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0, changed state to down
UEES-2(config-if)#exit
```

```
UEES-2(config)#interface serial 1/1
UEES-2(config-if)#ip address 192.168.1.6 255.255.255.252
UEES-2(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/1, changed state to down
UEES-2(config-if)#exit
```

```
UEES-2(config)#interface fastethernet 0/0
UEES-2(config-if)#ip address 192.168.1.97 255.255.255.224
UEES-2(config-if)#no shutdown
```

3.18.- ASIGNACIÓN DE DIRECCIÓN IP Y MÁSCARA A LAS SERIALES DEL ROUTER PRINCIPAL ECOTEC

```
ECOTEC(config)#interface serial 1/0
ECOTEC(config-if)#ip address 192.168.1.14 255.255.255.252
ECOTEC(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0 changed state to down
ECOTEC(config-if)#exit
```

```
ECOTEC(config)#interface serial 1/1
ECOTEC(config-if)#ip address 192.168.1.29 255.255.255.252
ECOTEC(config-if)#clock rate 64000
ECOTEC(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/1 changed state to down
ECOTEC(config-if)#exit
```

```
ECOTEC(config)#interface serial 1/2
ECOTEC(config-if)#ip address 192.168.1.33 255.255.255.252
ECOTEC(config-if)#clock rate 64000
ECOTEC(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/2 changed state to down
ECOTEC(config-if)#exit
```

```
ECOTEC(config)#interface serial 1/3
ECOTEC(config-if)#ip address 192.168.1.21 255.255.255.252
ECOTEC(config-if)#clock rate 64000
ECOTEC(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/3changed state to down
ECOTEC(config-if)#exit
```

```
ECOTEC(config)#interface fastethernet 0/0
ECOTEC(config-if)#ip address 192.168.6.33 255.255.255.224
ECOTEC(config-if)#no shutdown
ECOTEC(config-if)#exit
```

3.19.- ASIGNACIÓN DE DIRECCIÓN IP Y MÁSCARA A LAS SERIALES DEL ROUTER ECOTEC-1

```
ECOTEC-1(config)#interface serial 1/0
ECOTEC-1(config-if)#ip address 192.168.1.30 255.255.255.252
ECOTEC-1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/0changed state to down
ECOTEC-1(config-if)#exit
```

```
ECOTEC-1(config)#interface serial 1/1
ECOTEC-1(config-if)#ip address 192.168.1.38 255.255.255.252
ECOTEC-1(config-if)#clock rate 64000
ECOTEC-1(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial1/1changed state to down
ECOTEC-1(config-if)#exit
```

```
ECOTEC-1(config)#interface fastethernet 0/0
ECOTEC-1(config-if)#ip address 192.168.1.161 255.255.255.224
ECOTEC-1(config-if)#no shutdown
ECOTEC-1(config-if)#exit
```



3.20.- ASIGNACIÓN DE DIRECCIÓN IP Y MÁSCARA A LAS SERIALES DEL ROUTER ECOTEC-2

```
ECOTEC-2(config)#interface serial 1/0  
ECOTEC-2(config-if)#ip address 192.168.1.34 255.255.255.252  
ECOTEC-2(config-if)#no shutdown  
%LINK-5-CHANGED: Interface Serial1/0changed state to down  
ECOTEC-2(config-if)#exit
```

```
ECOTEC-2(config)#interface serial 1/2  
ECOTEC-2(config-if)#ip address 192.168.1.37 255.255.255.252  
ECOTEC-2(config-if)#no shutdown  
%LINK-5-CHANGED: Interface Serial1/2changed state to down  
ECOTEC-2(config-if)#exit
```

```
ECOTEC-2(config)#interface fastethernet 0/0  
ECOTEC-2(config-if)#ip address 192.168.1.193 255.255.255.252  
ECOTEC-2(config-if)#no shutdown  
ECOTEC-2(config-if)#exit
```



3.21.- PROTOCOLOS DE ENRUTAMIENTOS

Los protocolos de enrutamiento proporcionan mecanismos distintos para elaborar y mantener las tablas de enrutamiento de los diferentes routers de la red, así como determinar la mejor ruta para llegar a cualquier host remoto. En un mismo router pueden ejecutarse protocolos de enrutamiento independientes, construyendo y actualizando tablas de enrutamiento para distintos protocolos encaminados.

Ejemplos de protocolos de enrutamiento:

- Protocolo de información de enrutamiento (RIP).
- Protocolo de enrutamiento de gateway interior (IGRP).
- Protocolo de enrutamiento de gateway interior mejorado (EIGRP).
- Protocolo “Primero la ruta más corta” (OSPF).

3.21.1 ENRUTAMIENTO ESTÁTICO

Las rutas estáticas se configuran manualmente, el administrador debe configurarla en el router, mediante el comando ip route. La distancia administrativa es un parámetro opcional que da una medida del nivel de confiabilidad de la ruta. La distancia administrativa por defecto cuando se usa una ruta estática es 1.

Este método de enrutamiento resulta ventajoso en las siguientes situaciones:

- Un circuito poco fiable que deja de funcionar constantemente. Un protocolo de enrutamiento dinámico podría producir demasiada inestabilidad, mientras que las rutas estáticas no cambian.
- Se puede acceder a una red a través de una conexión de acceso telefónico. Dicha red no puede proporcionar las actualizaciones constantes que requiere un protocolo de enrutamiento dinámico.
- Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.
- Un cliente no desea intercambiar información de enrutamiento dinámico.

Las operaciones con rutas estáticas pueden dividirse en tres partes:

- El administrador de red configura la ruta.
- El router instala la ruta en la tabla de enrutamiento.
- Los paquetes se enrutan de acuerdo a la ruta estática.



3.21.2.- ENRUTAMIENTO PREDETERMINADO

Es una ruta estática que se refiere a una conexión de salida o Gateway de “último recurso”. El tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida. Esta ruta se indica como la red de destino **0.0.0.0/0.0.0.0**.

3.21.3.- ENRUTAMIENTO DINÁMICO

Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero.

Permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers.

3.22.- TIPOS DE DIRECCIONAMIENTO

Para el diseño de arquitectura de cualquier red, es también muy importante conocer y utilizar los siguientes conceptos, con el fin de optimizar y simplificar el direccionamiento y el tamaño de las tablas de enrutamiento. Gracias a la utilización de estas técnicas, los datos reales a principios de 2000 mostraban que el tamaño de la tabla de enrutamiento era aproximadamente de 76000 rutas.

3.22.1.- DIRECCIONAMIENTO CON CLASE

Es también conocido como Direccionamiento IP básico. Siguiendo este modelo de direccionamiento, a una dirección IP únicamente se le puede asignar su máscara predeterminada o máscara natural. Esto supone muy poca flexibilidad, y no es recomendable salvo para redes locales muy pequeñas.

3.23.- ALGORITMOS DE ENRUTAMIENTO POR VECTOR DE DISTANCIA

El término vector de distancia se deriva del hecho de que el protocolo incluye un vector (lista) de distancias (número de saltos u otras métricas) asociado con cada destino, requiriendo que cada nodo calcule por separado la mejor ruta para cada destino. Los envían mensajes actualizados a intervalos establecidos de tiempo, pasando toda su tabla de enrutamiento al router vecino más próximo (routers a los que está directamente conectado), los cuales repetirán este proceso hasta que todos los routers de la red están actualizados.

Si un enlace o una ruta se vuelve inaccesible justo después de una actualización, la propagación del fallo en la ruta se iniciará en la próxima propagación, ralentizándose la convergencia. Los protocolos de vector de distancia más nuevos, como EIGRP y RIP-2, introducen el concepto de actualizaciones desencadenadas. Éstas propagan los fallos tan pronto ocurran, acelerando la convergencia considerablemente.

Los protocolos por vector de distancia tradicionales trabajan sobre la base de actualizaciones periódicas y contadores de espera: si no se recibe una ruta en un cierto periodo de tiempo, la ruta entra en un estado de espera, envejece y desaparece, volviéndose inalcanzable.

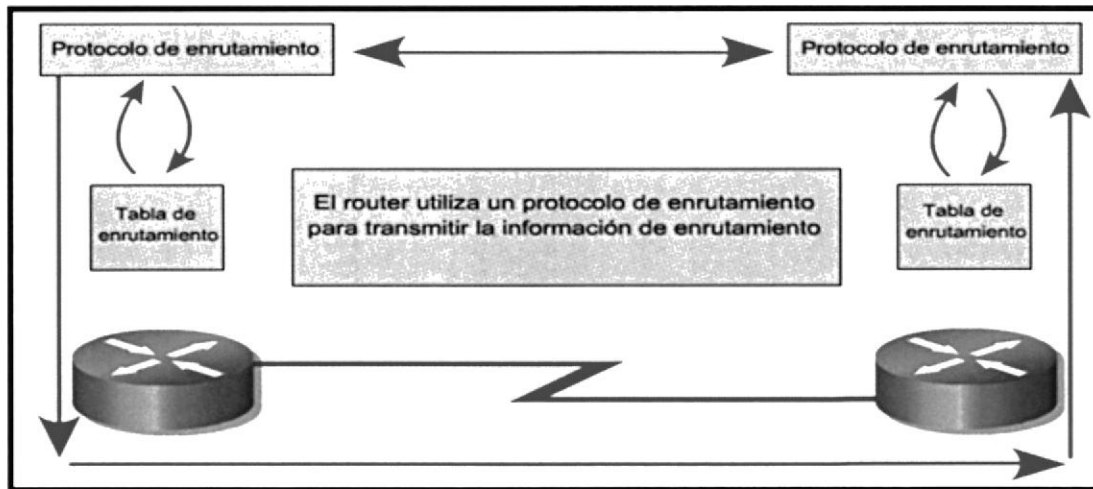


Figura 3 -7: Enrutamiento Vector Distancia

3.24.- BUCLES DE ENRUTAMIENTO EN ALGORITMOS POR VECTOR DE DISTANCIA

Los bucles de enrutamiento producen entradas de enrutamiento incoherentes, debido generalmente a un cambio en la topología. Si un enlace de un router A se vuelve inaccesible, los routers vecinos no se dan cuenta inmediatamente, por lo que se corre el riesgo de que el router A crea que puede llegar a la red perdida a través de sus vecinos que mantienen entradas antiguas. Así, añade una nueva entrada a su tabla de enrutamiento con un coste superior. A su vez, este proceso se repetiría una y otra vez, incrementándose el coste de las rutas, hasta que de alguna forma se parase dicho proceso.

Los métodos utilizados para evitar este caso son los que siguientes:

Horizonte Dividido.

La regla del horizonte dividido es que nunca resulta útil volver a enviar información acerca de una ruta a la dirección de dónde ha venido la actualización original.

Actualización Inversa.

Cuando una red de un router falla, este envenena su enlace creando una entrada para dicho enlace con coste infinito. Así deja de ser vulnerable a actualizaciones incorrectas proveniente de routers vecinos, donde esté involucrada dicha red. Cuando los routers

vecinos ven que la red ha pasado a un coste infinito, envían una actualización inversa indicando que la ruta no está accesible.

Definición de Máximo.

Con este sistema, el protocolo de enrutamiento permite la repetición del bucle hasta que la métrica exceda el valor máximo permitido. Una vez que la red alcanza ese máximo, se considera inalcanzable.

Actualización desencadenada.

Normalmente, las nuevas tablas de enrutamiento se envían a los routers vecinos a intervalos regulares. Una actualización desencadenada es una nueva tabla de enrutamiento que se envía de forma inmediata, en respuesta a un cambio. El router que detecta el cambio envía inmediatamente un mensaje de actualización a los routers adyacentes que, a su vez, generan actualizaciones desencadenadas para notificar el cambio a todos sus vecinos.

Sin embargo surgen dos problemas:

- Los paquetes que contienen el mensaje de actualización podrían ser descartados o dañados por algún enlace de la red.
- Las actualizaciones desencadenadas no suceden de forma instantánea. Es posible que un router que no haya recibido aún la actualización desencadenada genere una actualización regular que cause que la ruta defectuosa sea insertada en un vecino que hubiese recibido ya la actualización.

Combinando las actualizaciones desencadenadas con los temporizadores se obtiene un esquema que permite evitar estos problemas

3.25.- ALGORITMOS DE ENRUTAMIENTO DE ESTADO DE ENLACE

Utiliza un modelo de base de datos distribuida y replicada. Los routers intercambian paquetes de estado de enlace que informa a todos los routers de la red sobre el estado de sus distintos interfaces. Esto significa que sólo se envía información acerca de las conexiones directas de un determinado router, y no toda la tabla de enrutamiento como ocurre en el enrutamiento por vector de distancia. Aplicando el algoritmo SPF (primero la ruta más corta), más conocido como algoritmo Dijkstra, cada router calcula un árbol de las ruta más cortas hacia cada destino, situándose a sí mismo en la raíz.

Los protocolos de estado de enlace no pueden proporcionar una solución de conectividad global, como la que se requiere en grandes redes como Internet, pero si son utilizados por muchos proveedores como protocolo de enrutamiento en el interior de un SA. Los protocolos más conocidos son OSPF e IS-IS.

Algunos de los beneficios de estos protocolos son:

- No hay límite en el número de saltos de una ruta. Los protocolos del estado de enlace trabajan sobre la base de las métricas de enlace en lugar de hacerlo en función del número de saltos.
- El ancho de banda del enlace y los retrasos puede ser factorizados cuando se calcule la ruta más corta hacia un destino determinado.
- Los cambios de enlace y nodo son inmediatamente introducidos en el dominio mediante actualizaciones del estado de enlace.
- Soporte para VLSM y CIDR, ya que intercambian información de máscara en las actualizaciones.

3.26.- PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO (RIP)

RIP son las siglas de Routing Information Protocol. (PROTOCOLO DE INFORMACIÓN DE ENRUTAMIENTO)

RIP evita que los bucles de enrutamiento se prolonguen de forma indefinida, mediante la fijación de un límite en el número de saltos permitidos en una ruta, desde su origen hasta su destino.

Si existen dos rutas posibles para alcanzar el mismo destino, RIP elegirá la ruta que presente un menor número de saltos. RIP no tiene en cuenta la velocidad ni la fiabilidad de las líneas a la hora de seleccionar la mejor ruta. RIP envía un mensaje de actualización del enrutamiento cada 30 segundos (tiempo predeterminado en routers Cisco), en el que se incluye toda la tabla de enrutamiento del router, utilizando el protocolo UDP para el envío de los avisos.

RIP-1 está limitado a un número máximo de saltos de 15, no soporta VLSM y CIDR, y no soporta actualizaciones desencadenadas. RIP-1 puede realizar equilibrado de la carga en un máximo de seis rutas de igual coste.

RIP-2 es un protocolo sin clase que admite CIDR, VLSM, resumen de rutas y seguridad mediante texto simple y autenticación MD5. RIP publica sus rutas sólo a los routers vecinos.

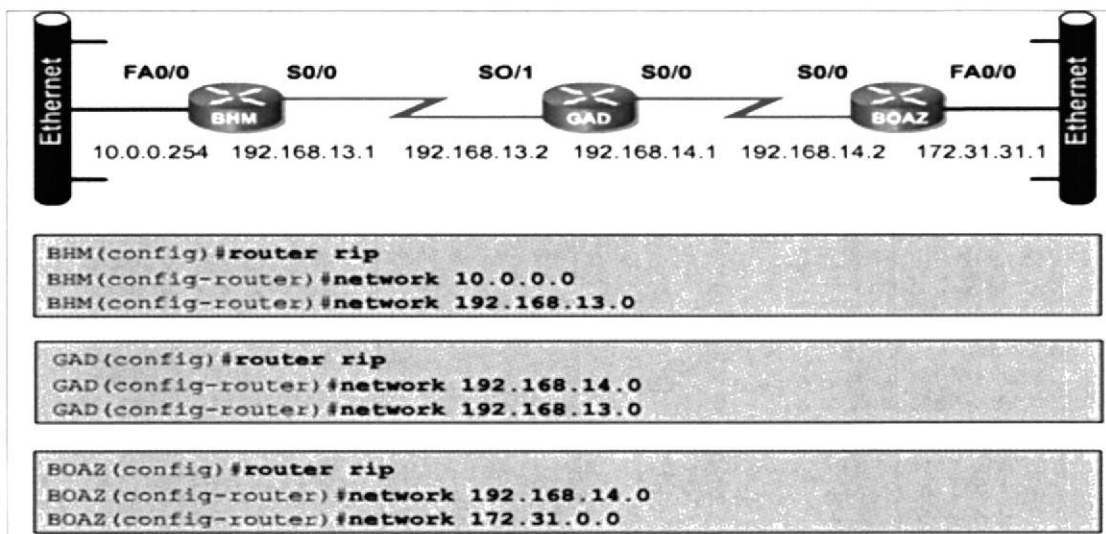


Figura 3 -8: Protocolo Rip

3.26.1.- CARACTERÍSTICAS PRINCIPALES DE RIP

- Es un protocolo de enrutamiento por vector-distancia.
- Utiliza el número de saltos como métrica para la selección de rutas.
- Si el número de saltos es superior a 15, el paquete es desechado.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.
- Protocolo tipo Broadcast.
- Máximo número de rutas 6, por defecto son 4.
- Temporizador de espera 180 sg.



3.26.2.- FUNCIONAMIENTO RIP

RIP V1 utiliza el puerto UDP 520 para enviar sus mensajes por difusión Broadcast. RIP V2 utiliza propagación multicast 224.0.0.9.

RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancia. La distancia o métrica está determinada por el número de saltos del router hasta alcanzar la red de destino.

RIP no es capaz de detectar bucles, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como inalcanzable.

La métrica de un destino se calcula como el número de saltos comunicado por un vecino más la distancia en alcanzar a ése vecino. La tabla de rutas hacia ese destino se actualiza sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la de la ruta almacenada. Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta.

3.26.3.- VENTAJAS

- En comparación con otros protocolos de enrutamiento, RIP es más fácil de configurar.
- Es un protocolo abierto, soportado por muchos fabricantes.

3.26.4.- INCONVENIENTES

- Tiene la desventaja que, para determinar la mejor métrica, únicamente toma en cuenta el número de saltos (por cuántos routers o equipos similares pasa la información); no toma en cuenta otros criterios importantes, como por ejemplo ancho de banda de los enlaces.

Por ejemplo, si tenemos una métrica de 2 saltos hasta el destino con un enlace de 64 kbps y una métrica de 3 saltos, pero con un enlace de 2 Mbps, lamentablemente RIP tomara el enlace de menor número de saltos aunque sea el más lento. Protocolo usado pero con limitaciones.

3.26.5.- LIMITACIONES RIP

- No envía actualización de máscara de subred en sus actualizaciones.
- Envía las actualizaciones en Broadcast a 255.255.255.255.
- No admite la autenticación.
- No puede admitir enrutamiento entre dominios de VLSM o sin clase (CIDR).

3.26.6.- MENSAJES RIP

3.26.6.1.- TIPOS DE MENSAJES RIP

Los mensajes RIP pueden ser de dos tipos.

Petición: Enviados por algún enrutador recientemente iniciado que solicita información de los enrutadores vecinos.

Respuesta: mensajes con la actualización de las tablas de enrutamiento.

Existen tres tipos:

Mensajes ordinarios: Se envían cada 30 segundos. Para indicar que el enlace y la ruta siguen activos. Se envía la tabla de ruteo completa.

Mensajes enviados como respuesta a mensajes de petición.

Mensajes enviados cuando cambia algún coste. Se envía toda la tabla de ruteo.

3.26.7.- FORMATO DE LOS MENSAJES RIP

Los mensajes tienen una cabecera que incluye el tipo de mensaje y la versión del protocolo RIP, y un máximo de 25 entradas RIP de 20 bytes.

Las entradas en RIPv1 contienen la dirección IP de la red de destino y la métrica.

Las entradas en RIPv2 contienen la dirección IP de la red de destino, su máscara, el siguiente enrutador y la métrica. La autenticación utiliza la primera entrada RIP.

3.26.8.- DIAGNÓSTICO DE FALLAS RIP

Un comando muy efectivo para detectar problemas de actualización es el debug Ip rip. El comando debug ip rip muestra las actualizaciones de enrutamiento RIP a medida que se las envía y recibe. Para desactivar la depuración se escribe: no debug al



3.27.- PROTOCOLO “PRIMERO LA RUTA MÁS CORTA” (OSPF)

OSPF es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos. Se describe en diversos estándares de la Fuerza de Tareas de Ingeniería de Internet (IETF). OSPF se puede usar y configurar en una sola área en las redes pequeñas. También se puede utilizar en las redes grandes. Las redes OSPF grandes utilizan un diseño jerárquico. Varias áreas se conectan a un área de distribución o a un área 0 que también se denomina backbone. El enfoque del diseño permite el control extenso de las actualizaciones de enrutamiento. La definición de área reduce el gasto de procesamiento, acelera la convergencia, limita la inestabilidad de la red a un área y mejora el rendimiento. OSPF reúne la información de los routers vecinos acerca del estado de enlace de cada router OSPF.

El término “libre” en “Primero la ruta libre mas corta” significa que está abierto al público y no es propiedad de ninguna empresa.

OSPF soporta VLSM, ofrece convergencia rápida, autenticación de origen de ruta, y publicación de ruta mediante multidifusión. OSPF publica sus rutas a todos los routers del mismo área. En la RFC 2328 se describe el concepto y operatividad del estado de enlace en OSPF, mientras que la implementación de OSPF versión 2 se muestra en la RFC 1583. OSPF toma las decisiones en función del corte de la ruta, disponiendo de una métrica máxima de 65535.

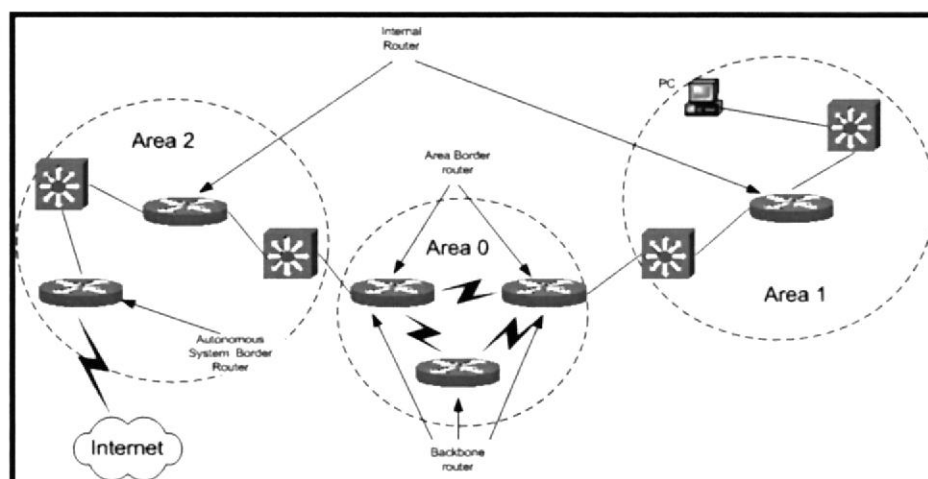


Figura 3- 9: Primero la ruta mas corta



3.27.1.- FUNCIÓN DE OSPF

La función del OSPF es encontrar la trayectoria mas corta de un dispositivo de encaminamiento a todos los demás. Cada dispositivo de encaminamiento tiene almacenada en una base de datos la topología de la red de la que forma parte. La representación de esta topología se expresa como un grafo dirigido.

Al arrancar un dispositivo de almacenamiento, este protocolo envía paquetes HELLO por todas sus líneas punto a punto y los retransmite a todos los demás dispositivos de encaminamiento. Gracias a las respuestas que recibe sabe cuales son sus dispositivos de encaminamiento vecinos. El OSPF se basa en el intercambio de información entre los dispositivos de encaminamiento adyacentes, que no es lo mismo que vecinos. Para que no todos los dispositivos tengan que hablar con los demás, se designa uno como adyacente a todos los demás y es este el que intercambia información con los restantes.

Para la configuración de OSPF se requiere un número de proceso, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. Los administradores acostumbran usar un número de SA como número de proceso.

OSPF tiene los siguientes beneficios:

- Velocidad de convergencia.
- Admite máscara de subred de longitud variable (VLSM).
- Tamaño de la red.
- Selección de ruta.
- Agrupación de miembros.

3.27.2.- CARACTERÍSTICAS DE OSPF

- Es un protocolo público conocido como “PRIMERO LA RUTA MAS CORTA”
- Es un protocolo de enrutamiento de estado — enlace
- Es un protocolo de enrutamiento público (open Standard)
- Usa el algoritmo SPF para calcular el costo más bajo hasta un destino
- Las actualizaciones de enrutamiento producen un gran volumen de tráfico al ocurrir cambios en la topología.

3.27.3.- VENTAJAS DE OSPF

- Las rutas calculadas mediante OSPF nunca presentan bucles.
- OSPF puede escalar a interconexiones de redes mayores o mucho mayores.
- La reconfiguración correspondiente a los cambios de topología de la red es más rápida

3.27.4.- TIPOS DE AREA QUE DISTINGUE OSPF

3.27.4.1.- ÁREA BACKBONE

El backbone, también denominado área cero, forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red.

La conexión entre un área y el backbone se realiza mediante los ABR, que son responsables de la gestión de las rutas no-internas del área (esto es, de las rutas entre el área y el resto de la red).

3.27.4.2.- ÁREA STUB

Un área stub es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de enrutamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.

Los nodos de una red basada en OSPF se conectan a ella a través de una o varias interfaces con las que se conectan a otros nodos de la red. El tipo de enlace (link) define la configuración que asume la interfase correspondiente. OSPF soporta las siguientes tipos de enlace, y provee para cada uno de ellos una configuración de interfaz:

- Punto a punto (point-to-point, abreviadamente ptp).
- Punto a multipunto (point-to-multipoint, abreviadamente ptmp).
- Broadcast.
- Enlace virtual (virtual link).
- Enlace de múltiple acceso no-broadcast (Non-broadcast Multiple Access, NBMA).

3.27.4.3.- ESTADO DE LAS INTERFACES

- Down (sin actividad).
- Waiting (estado de espera).
- Loopback.
- Point-to-point (interface punto a punto)
- DR, abreviatura de Designated Router (interface de enrutador designado).

- Backup, por Backup Designated Router (interface de enrutador designado auxiliar, BDR).
- DROther (interface en una red broadcast o NBMA sin estatus DR ni BDR).

3.27.4.4.- ESTADO DESACTIVADO (DOWN)

En el estado desactivado, el proceso OSPF no ha intercambiado información con ningún vecino. OSPF se encuentra a la espera de pasar al siguiente estado (Estado de Inicialización)

3.27.4.5.- ESTADO DE INICIALIZACIÓN (INIT)

Los routers (enrutadores) OSPF envían paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los Routers vecinos. Cuando una interfaz recibe su primer paquete Hello, el router entra al estado de Inicialización.

Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa.

Los dos tipos de relaciones son Bidireccional y Adyacencia. Un router debe recibir un paquete Hello (Hola) desde un vecino antes de establecer algún tipo de relación.

3.27.4.6.- ESTADO BIDIRECCIONAL (TWO-WAY)

(encaminador = enrutador)

Empleando paquetes Hello, cada enrutador OSPF intenta establecer el estado de comunicación bidireccional (dos-vías) con cada enrutador vecino en la misma red IP. Entre otras cosas, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen. Un enrutador ingresa al estado Bidireccional cuando se ve a sí mismo en un paquete Hello proveniente de un vecino.

3.27.4.7.- ESTADO DE INTERCAMBIO (EXCHANGE)

En el estado de intercambio, los encaminadores vecinos emplean paquetes DBD tipo 2 para enviarse entre ellos su información de estado de enlace. En otras palabras, los encaminadores se describen sus bases de datos de estado de enlace entre ellos. Los encaminadores comparan lo que han aprendido con lo que ya tenían en su base de datos de estado de enlace.

Si alguno de los encaminadores recibe información acerca de un enlace que no se encuentra en su base de datos, este envía una solicitud de actualización completa a su vecino. Información completa de encaminamiento es intercambiada en el estado Cargando.

3.27.4.8.- ESTADO CARGANDO (LOADING)

Después de que las bases de datos han sido completamente descritas entre vecinos, estos pueden requerir información más completa empleando paquetes tipo 3, requerimientos de estado de enlace (LSR). Cuando un enrutador recibe un LSR este responde empleando un paquete de actualización de estado de enlace tipo 4 (LSU). Estos paquetes tipo 4 contienen las publicaciones de estado de enlace (LSA) que son el corazón de los protocolos de estado de enlace. Los LSU tipo 4 son confirmados empleando paquetes tipo 5 conocidos como confirmaciones de estado de enlace (LSAcks).

3.28.- TABLA DE PROTOCOLOS DE ENRUTAMIENTO

	RIP-1	RIP-2	IGRP	EIGRP	OSPF
¿Soporta VLSM?	NO	SI	NO	SI	SI
Velocidad Convergencia	Lenta	Media	Media	Rápida	Rápida
Tecnología	Vector	Vector	Vector	Mixto	Enlace
Número max. Saltos	15	15	255	255	65535
Seguridad		MD5		MD5	MD5
Selección de Ruta	Saltos	Saltos	Varias Métricas	Varias Métricas	Ancho Banda
Compatibilidad	Universal	Universal	Cisco	Cisco	Universal
Tipo	IGP	IGP	IGP	IGP	IGP
¿Proceso / ASN?	NO	NO	PROCESO	PROCESO	PROCESO
¿Depende de Topología?	NO	NO	NO	NO	SI

Tabla 3- 6: Protocolo de Enrutamiento

3.29.-REDISTRIBUCIÓN DE RUTAS

Es posible tener zonas que usan protocolos de encaminamiento distintos. Por ejemplo OSPF y RIPv2. Hay que inyectar las rutas que se aprenden de un protocolo a otro. A este proceso se la llama “**redistribución de rutas**”

Para que dos dispositivos (routers o switches capa 3) intercambien información de enrutamiento es preciso, en principio, que ambos dispositivos utilicen el mismo protocolo, sea RIP, EIGRP, OSPF, BGP, etc. Diferentes protocolos de enrutamiento, o protocolos configurados de diferente forma (p.e. diferente sistema autónomo en EIGRP) no intercambian información.

Sin embargo, cuando un dispositivo aprende información de enrutamiento a partir de diferentes fuentes (p.e. rutas estáticas o a través de diferentes protocolos) Cisco IOS permite que la información aprendida por una fuente sea publicada hacia otros dispositivos utilizando un protocolo diferente. Por ejemplo, que una ruta aprendida a través de RIP sea publicada hacia otros dispositivos utilizando OSPF. Esto es lo que se denomina “**Redistribución**” de rutas. Utilizar un protocolo de enrutamiento para publicar rutas que son aprendidas a través de otro medio (otro protocolo, rutas estáticas o directamente conectadas).

El mecanismo de redistribución es propietario de Cisco IOS. Este mecanismo establece algunas reglas:

- La ruta a redistribuir debe estar presente en la tabla de enrutamiento.
- No se redistribuyen rutas que están presentes en tablas topológicas de los protocolos pero no en la tabla de enrutamiento.
- La ruta redistribuida será recibida por el dispositivo vecino con la métrica raíz del protocolo en el que se redistribuye.

3.29.1.- PARA QUÉ SE UTILIZA LA REDISTRIBUCIÓN DE RUTAS

En principio es deseable que una red utilice un único protocolo de enrutamiento. Sin embargo, en algunos casos puede requerirse el uso de redistribución: fusiones de empresas, diferentes departamentos de una misma empresa administrados por diferentes equipos de personal, entornos multi-vendor, migraciones, etc. Al momento de abordar una redistribución de rutas se deben tener presentes algunos aspectos particulares del enrutamiento:

Las diferentes métricas, las distancias administrativas de cada protocolo, las capacidades de enrutamiento classful y classless, y la topología de la red.

3.29.2.- LAS MÉTRICAS

Cada protocolo de enrutamiento utiliza una métrica diferente. Esto hace que al redistribuir rutas se pierda la métrica original del protocolo y sea redefinida en los términos del nuevo protocolo. Por ejemplo, si se redistribuye una ruta OSPF con una métrica de 1642 en RIP, RIP le asignará una métrica en cantidad de saltos (entre 1 y 15).

La métrica con la que un protocolo recibe las rutas aprendidas por otro, se denomina **métrica raíz**.

Cada protocolo utiliza una métrica raíz por defecto:

- RIP - métrica raíz por defecto: infinito.
- EIGRP - métrica raíz por defecto: infinito.
- OSPF - métrica raíz por defecto: 20.

Esta métrica raíz por defecto también puede ser modificada utilizando el comando default metric.

3.29.3.- REDISTRIBUCIÓN EN RIP

Como en EIGRP, al redistribuir en RIP el protocolo utiliza una métrica por defecto de infinito, con lo que es necesario especificar una métrica diferente para que el router vecino incorpore la información de enrutamiento en su tabla.

3.29.4.- REDISTRIBUCIÓN EN OSPF

La métrica por defecto que utiliza OSPF es de 20, por lo que no exige que especifiquemos una métrica para que la ruta sea aprendida por los dispositivos adyacentes. Sin embargo, cuando hay múltiples subredes de una misma red y se desea publicar rutas para cada subred, es preciso indicarlo pues de lo contrario OSPF sumará todas las subredes al límite de la clase y publicará una sola ruta.



3.30.- CONFIGURACIÓN DE OSPF EN LOS ROUTERS TES Y TES-1

TES(config)#router ospf 1 → ID del proceso

Comando para asignar el tipo de Protocolo de enrutamiento

TES(config-router)#network 192.168.5.64 0.0.0.31 area 0

Máscara de Longitud inversa

Dirección de red

La información se envía a todos los routers de esa área

Asigna una dirección de red a la cual el router se encuentra directamente conectado

```
TES(config-router)#network 192.168.1.16 0.0.0.3 area 0
TES(config-router)#network 192.168.1.20 0.0.0.3 area 0
TES(config-router)#network 192.168.1.24 0.0.0.3 area 0
TES(config-router)#network 200.10.1.0 0.0.0.3 area 0
TES(config-router)#exit
```

ROUTER TES-1

```
TES-1(config)#router ospf 1
TES-1(config-router)#network 192.168.1.128 0.0.0.31 area 0
TES-1(config-router)#network 192.168.1.24 0.0.0.3 area 0
```



3.31.- CONFIGURACIÓN DE RIP V2 Y OSPF EN EL ROUTER UEES

```
UEES(config)#router rip
```

Comando para asignar enrutamiento dinámico Rip

```
UEES(config)#version 2
```

Versión del protocolo de Rip

```
UEES(config-router)#network 192.168.6.0
```

```
UEES(config-router)#network 192.168.1.0
```

```
UEES(config-router)#network 192.168.1.8
```

```
UEES(config-router)#redistribute ospf 1 metric 1
```

Distancia Administrativa a la que se encuentran los Routers

Protocolo e ID del proceso cual se va a redistribuir

Redistribuye a través de los enlaces de comunicación

```
UEES(config-router)#exit
```

```
UEES(config)#router ospf 1
```

```
UEES(config-router)#network 192.168.1.12 0.0.0.3 area 0
```

```
UEES(config-router)#network 192.168.1.16 0.0.0.3 area 0
```

```
UEES(config-router)#redistribute rip subnets
```

Redistribuir a rip la subred



3.32.- CONFIGURACIÓN DE RIP V2 EN LOS ROUTERS UEES-1 Y UEES-2

```
UEES-1(config)#router rip
```

```
UEES-1(config)#version 2
```

```
UEES-1(config-router)#network 192.168.1.64
```

```
UEES-1(config-router)#network 192.168.1.0
```

```
UEES-1(config-router)#network 192.168.1.4
```

```
UEES-1(config)#exit
```

```
UEES-2(config)#router rip
UEES-2(config)#version2
UEES-2(config-router)#network 192.168.1.96
UEES-2(config-router)#network 192.168.1.4
UEES-2(config-router)#network 192.168.1.8
UEES-2(config)#exit
```

3.33.- CONFIGURACIÓN DE RIP V2 Y OSPF EN EL ROUTER ECOTEC

```
ECOTEC(config)#router rip
ECOTEC(config)#version2
ECOTEC(config-router)#network 192.168.6.32
ECOTEC(config-router)#network 192.168.1.28
ECOTEC(config-router)#network 192.168.1.32
ECOTEC(config-router)#redistribute ospf 1 metric 1
ECOTEC(config-router)#exit
```

```
ECOTEC(config)#router ospf 1
ECOTEC(config-router)#network 192.168.1.12
ECOTEC(config-router)#network 192.168.1.20
ECOTEC(config-router)#redistribute rip subnets
```

3.34- CONFIGURACIÓN DE RIP V2 EN LOS ROUTERS ECOTEC-1

```
ECOTEC-1(config)#router rip
ECOTEC-1(config)#version2
ECOTEC-1(config-router)#network 192.168.1.160
ECOTEC-1(config-router)#network 192.168.1.28
ECOTEC-1(config-router)#network 192.168.1.36
ECOTEC-1(config-router)#exit
```

```
ECOTEC-2(config)#router rip
ECOTEC-2(config)#version2
ECOTEC-2(config-router)#network 192.168.1.192
ECOTEC-2(config-router)#network 192.168.1.32
ECOTEC-2(config-router)#network 192.168.1.36
ECOTEC-2(config-router)#exit
```

3.35.- COMANDO SHOW IP ROUTE EN EL ROUTER TES

Muestra, un resumen de la tabla de enrutamiento o la vía de información para determinadas direcciones IP, máscaras de red o protocolos.

TES>enable

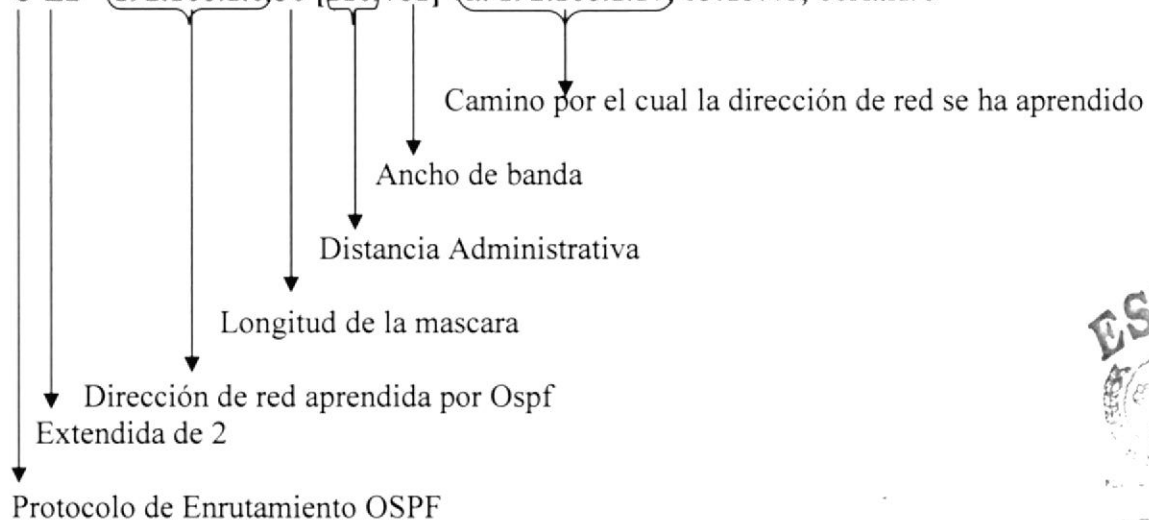
TES#SHOW IP ROUTE

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 15 subnets, 2 masks

O E2 192.168.1.0/30 [110/781] via 192.168.1.17, 03:15:48, Serial1/0



O E2 192.168.1.4/30 [110/781] via 192.168.1.17, 03:14:40, Serial1/0

Interfaz de Sallida

Tiempo transcurrido desde la última actualización, RIP se actualiza cada 30 segundos.



O E2 192.168.1.8/30 [110/781] via 192.168.1.17, 03:15:48, Serial1/0
 O E2 192.168.1.12/30 [110/781] via 192.168.1.17, 03:15:48, Serial1/0
 C 192.168.1.16/30 is directly connected, Serial1/0
 C 192.168.1.20/30 is directly connected, Serial1/1

C 192.168.1.24/30 is directly connected, Serial1/2

Dirección de red

Longitud de mascara de red

Conexión Directa

O E2 192.168.1.28/30 [110/781] via 192.168.1.21, 03:15:48, Serial1/1
 O E2 192.168.1.32/30 [110/781] via 192.168.1.21, 03:15:48, Serial1/1
 O E2 192.168.1.36/30 [110/781] via 192.168.1.21, 03:15:14, Serial1/1
 O E2 192.168.1.64/27 [110/781] via 192.168.1.17, 03:15:48, Serial1/0
 O E2 192.168.1.96/27 [110/781] via 192.168.1.17, 02:32:58, Serial1/0
 O 192.168.1.128/27 [110/782] via 192.168.1.26, 03:15:48, Serial1/2
 O E2 192.168.1.160/27 [110/781] via 192.168.1.21, 03:15:04, Serial1/1
 O E2 192.168.1.192/27 [110/781] via 192.168.1.21, 03:15:14, Serial1/1
 O E2 192.168.2.0/24 [110/781] via 192.168.1.17, 02:33:26, Serial1/0
 192.168.3.0/24 is variably subnetted, 3 subnets, 2 masks
 O 192.168.3.0/27 [110/782] via 192.168.1.26, 03:15:48, Serial1/2
 O 192.168.3.32/28 [110/782] via 192.168.1.26, 03:15:48, Serial1/2
 O 192.168.3.48/28 [110/782] via 192.168.1.26, 03:15:48, Serial1/2
 O E2 192.168.4.0/24 [110/781] via 192.168.1.17, 03:15:04, Serial1/0
 192.168.5.0/24 is variably subnetted, 6 subnets, 3 masks
 O E2 192.168.5.0/24 [110/781] via 192.168.1.21, 03:15:04, Serial1/1
 C 192.168.5.64/27 is directly connected, FastEthernet0/0
 C 192.168.5.96/28 is directly connected, FastEthernet0/0.2
 C 192.168.5.112/28 is directly connected, FastEthernet0/0.3
 C 192.168.5.128/28 is directly connected, FastEthernet0/0.4
 C 192.168.5.144/28 is directly connected, FastEthernet0/0.5
 192.168.6.0/24 is variably subnetted, 6 subnets, 3 masks
 O E2 192.168.6.0/29 [110/781] via 192.168.1.17, 01:10:51, Serial1/0
 O E2 192.168.6.8/29 [110/781] via 192.168.1.17, 03:15:48, Serial1/0
 O E2 192.168.6.16/28 [110/781] via 192.168.1.17, 03:15:48, Serial1/0
 O E2 192.168.6.32/27 [110/781] via 192.168.1.21, 03:15:48, Serial1/1
 O E2 192.168.6.64/27 [110/781] via 192.168.1.21, 03:15:48, Serial1/1
 O E2 192.168.6.96/27 [110/781] via 192.168.1.21, 03:15:48, Serial1/1
 200.10.1.0/24 is variably subnetted, 2 subnets, 2 masks
 C 200.10.1.0/30 is directly connected, Serial1/3
 O E2 200.10.1.32/27 [110/781] via 200.10.1.2, 03:15:48, Serial1/3



3.36.- COMANDO SHOW IP ROUTE EN EL ROUTER

TES-1

TES-1#show ip route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 15 subnets, 2 masks
O E2 192.168.1.0/30 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O E2 192.168.1.4/30 [110/1562] via 192.168.1.25, 00:07:56, Serial1/0
O E2 192.168.1.8/30 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O E2 192.168.1.12/30 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O 192.168.1.16/30 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O 192.168.1.20/30 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
C 192.168.1.24/30 is directly connected, Serial1/0
O E2 192.168.1.28/30 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O E2 192.168.1.32/30 [110/1562] via 192.168.1.25, 00:03:46, Serial1/0
O E2 192.168.1.36/30 [110/1562] via 192.168.1.25, 00:07:26, Serial1/0
O E2 192.168.1.64/27 [110/1562] via 192.168.1.25, 00:08:51, Serial1/0
O E2 192.168.1.96/27 [110/1562] via 192.168.1.25, 00:07:56, Serial1/0
C 192.168.1.128/27 is directly connected, FastEthernet0/0
O E2 192.168.1.160/27 [110/1562] via 192.168.1.25, 00:07:26, Serial1/0
O E2 192.168.1.192/27 [110/1562] via 192.168.1.25, 00:08:23, Serial1/0
O E2 192.168.2.0/24 [110/1562] via 192.168.1.25, 00:07:36, Serial1/0
192.168.3.0/24 is variably subnetted, 3 subnets, 2 masks
C 192.168.3.0/27 is directly connected, FastEthernet0/0.2
C 192.168.3.32/28 is directly connected, FastEthernet0/0.3
C 192.168.3.48/28 is directly connected, FastEthernet0/0.4
O E2 192.168.4.0/24 [110/1562] via 192.168.1.25, 00:07:26, Serial1/0
192.168.5.0/24 is variably subnetted, 6 subnets, 3 masks
O E2 192.168.5.0/24 [110/1562] via 192.168.1.25, 00:03:36, Serial1/0
O 192.168.5.64/27 [110/782] via 192.168.1.25, 00:10:54, Serial1/0
O 192.168.5.96/28 [110/782] via 192.168.1.25, 00:10:54, Serial1/0
O 192.168.5.112/28 [110/782] via 192.168.1.25, 00:10:54, Serial1/0
O 192.168.5.128/28 [110/782] via 192.168.1.25, 00:10:54, Serial1/0
O 192.168.5.144/28 [110/782] via 192.168.1.25, 00:10:54, Serial1/0
192.168.6.0/24 is variably subnetted, 6 subnets, 4 masks
O E2 192.168.6.0/24 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O E2 192.168.6.8/29 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O E2 192.168.6.16/28 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O E2 192.168.6.32/27 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0



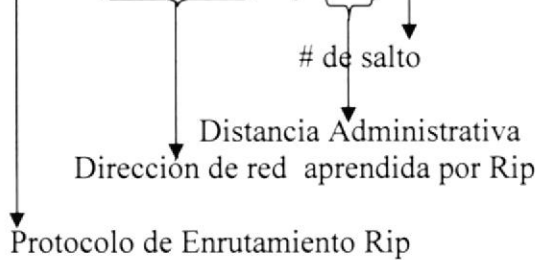
O E2 192.168.6.64/27 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O E2 192.168.6.96/27 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
200.10.1.0/24 is variably subnetted, 2 subnets, 2 masks
O 200.10.1.0/30 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
O E2 200.10.1.32/27 [110/1562] via 192.168.1.25, 00:10:54, Serial1/0
TES-1#

3.37.- COMANDO SHOW IP ROUTE EN EL ROUTER UEES

UEES#show ip route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set
192.168.1.0/24 is variably subnetted, 15 subnets, 2 masks
C 192.168.1.0/30 is directly connected, Serial1/0
R 192.168.1.4/30 [120/1] via 192.168.1.1, 00:00:01, Serial1/0



[120/1] via 192.168.1.9, 00:00:12, Serial1/1
[120/1] via 192.168.1.14, 00:00:06, Serial1/2
C 192.168.1.8/30 is directly connected, Serial1/1
C 192.168.1.12/30 is directly connected, Serial1/2
C 192.168.1.16/30 is directly connected, Serial1/3
O 192.168.1.20/30 [110/1562] via 192.168.1.18, 00:13:46, Serial1/3
O 192.168.1.24/30 [110/1562] via 192.168.1.18, 00:13:46, Serial1/3
O E2 192.168.1.28/30 [110/1562] via 192.168.1.18, 00:13:46, Serial1/3
R 192.168.1.32/30 [120/3] via 192.168.1.14, 00:00:06, Serial1/2
O E2 192.168.1.36/30 [110/1562] via 192.168.1.18, 00:10:21, Serial1/3
R 192.168.1.64/27 [120/1] via 192.168.1.1, 00:00:01, Serial1/0
[120/1] via 192.168.1.14, 00:00:06, Serial1/2
R 192.168.1.96/27 [120/1] via 192.168.1.9, 00:00:12, Serial1/1
[120/1] via 192.168.1.14, 00:00:06, Serial1/2
O 192.168.1.128/27 [110/1563] via 192.168.1.18, 00:13:46, Serial1/3



```

O E2 192.168.1.160/27 [110/1562] via 192.168.1.18, 00:10:21, Serial1/3
O E2 192.168.1.192/27 [110/1562] via 192.168.1.18, 00:11:15, Serial1/3
R 192.168.2.0/24 [120/1] via 192.168.1.1, 00:00:01, Serial1/0
    [120/1] via 192.168.1.9, 00:00:12, Serial1/1
    [120/1] via 192.168.1.14, 00:00:06, Serial1/2
192.168.3.0/24 is variably subnetted, 4 subnets, 3 masks
R 192.168.3.0/24 [120/1] via 192.168.1.14, 00:00:06, Serial1/2
O 192.168.3.0/27 [110/1563] via 192.168.1.18, 00:13:46, Serial1/3
O 192.168.3.32/28 [110/1563] via 192.168.1.18, 00:13:46, Serial1/3
O 192.168.3.48/28 [110/1563] via 192.168.1.18, 00:13:46, Serial1/3
O E2 192.168.4.0/24 [110/1562] via 192.168.1.18, 00:10:21, Serial1/3
    192.168.5.0/24 is variably subnetted, 6 subnets, 3 masks
R 192.168.5.0/24 [120/1] via 192.168.1.14, 00:00:06, Serial1/2
O 192.168.5.64/27 [110/782] via 192.168.1.18, 00:13:46, Serial1/3
O 192.168.5.96/28 [110/782] via 192.168.1.18, 00:13:46, Serial1/3
O 192.168.5.112/28 [110/782] via 192.168.1.18, 00:13:46, Serial1/3
O 192.168.5.128/28 [110/782] via 192.168.1.18, 00:13:46, Serial1/3
O 192.168.5.144/28 [110/782] via 192.168.1.18, 00:13:46, Serial1/3
    192.168.6.0/24 is variably subnetted, 7 subnets, 4 masks
O E2 192.168.6.0/24 [110/1562] via 192.168.1.18, 00:13:46, Serial1/3
C 192.168.6.0/29 is directly connected, FastEthernet0/0
C 192.168.6.8/29 is directly connected, FastEthernet0/0.2
C 192.168.6.16/28 is directly connected, FastEthernet0/0.3
O E2 192.168.6.32/27 [110/1562] via 192.168.1.18, 00:13:46, Serial1/3
O E2 192.168.6.64/27 [110/1562] via 192.168.1.18, 00:13:46, Serial1/3
O E2 192.168.6.96/27 [110/1562] via 192.168.1.18, 00:13:46, Serial1/3
    200.10.1.0/24 is variably subnetted, 3 subnets, 3 masks
R 200.10.1.0/24 [120/1] via 192.168.1.14, 00:00:07, Serial1/2
O 200.10.1.0/30 [110/1562] via 192.168.1.18, 00:13:46, Serial1/3
O E2 200.10.1.32/27 [110/1562] via 192.168.1.18, 00:13:46, Serial1/3
UEES#

```



3.38.- COMANDO SHOW IP ROUTE EN EL ROUTER

UEES-1

UEES-1#show ip route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 15 subnets, 2 masks

```

C    192.168.1.0/30 is directly connected, Serial1/1
C    192.168.1.4/30 is directly connected, Serial1/0
R    192.168.1.8/30 [120/1] via 192.168.1.6, 00:00:07, Serial1/0
R    192.168.1.12/30 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.1.16/30 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.1.20/30 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.1.24/30 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.1.28/30 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.1.32/30 [120/4] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.1.36/30 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
C    192.168.1.64/27 is directly connected, FastEthernet0/0
R    192.168.1.96/27 [120/1] via 192.168.1.6, 00:00:07, Serial1/0
R    192.168.1.128/27 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.1.160/27 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.1.192/27 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
192.168.2.0/24 is variably subnetted, 4 subnets, 3 masks
R    192.168.2.0/24 [120/1] via 192.168.1.6, 00:00:07, Serial1/0
C    192.168.2.0/29 is directly connected, FastEthernet0/0.2
C    192.168.2.8/29 is directly connected, FastEthernet0/0.3
C    192.168.2.16/28 is directly connected, FastEthernet0/0.4
R    192.168.3.0/24 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.4.0/24 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.5.0/24 [120/2] via 192.168.1.2, 00:00:22, Serial1/1
R    192.168.6.0/24 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
R    200.10.1.0/24 [120/1] via 192.168.1.2, 00:00:22, Serial1/1
UEES-1#

```

3.39.- COMANDO SHOW IP ROUTE EN EL ROUTER UEES-2

UEES-2#show ip route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

```

192.168.1.0/24 is variably subnetted, 15 subnets, 2 masks
R    192.168.1.0/30 [120/1] via 192.168.1.5, 00:00:25, Serial1/1
C    192.168.1.4/30 is directly connected, Serial1/1
C    192.168.1.8/30 is directly connected, Serial1/0
R    192.168.1.12/30 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R    192.168.1.16/30 [120/1] via 192.168.1.10, 00:00:15, Serial1/0

```

```

R 192.168.1.20/30 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.1.24/30 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.1.28/30 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.1.32/30 [120/4] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.1.36/30 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.1.64/27 [120/1] via 192.168.1.5, 00:00:25, Serial1/1
C 192.168.1.96/27 is directly connected, FastEthernet0/0
R 192.168.1.128/27 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.1.160/27 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.1.192/27 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
192.168.2.0/24 is variably subnetted, 4 subnets, 2 masks
R 192.168.2.0/24 [120/1] via 192.168.1.5, 00:00:25, Serial1/1
C 192.168.2.32/28 is directly connected, FastEthernet0/0.2
C 192.168.2.48/28 is directly connected, FastEthernet0/0.3
C 192.168.2.64/28 is directly connected, FastEthernet0/0.4
R 192.168.3.0/24 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.4.0/24 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.5.0/24 [120/2] via 192.168.1.10, 00:00:15, Serial1/0
R 192.168.6.0/24 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
R 200.10.1.0/24 [120/1] via 192.168.1.10, 00:00:15, Serial1/0
UEES-2#

```

3.40.- COMANDO SHOW IP ROUTE EN EL ROUTER ECOTEC

ECOTEC#show ip route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is not set

```

192.168.1.0/24 is variably subnetted, 15 subnets, 2 masks
O E2 192.168.1.0/30 [110/1562] via 192.168.1.22, 00:31:30, Serial1/3
O E2 192.168.1.4/30 [110/1562] via 192.168.1.22, 00:28:59, Serial1/3
O E2 192.168.1.8/30 [110/1562] via 192.168.1.22, 00:31:30, Serial1/3
C 192.168.1.12/30 is directly connected, Serial1/0
O 192.168.1.16/30 [110/1562] via 192.168.1.22, 00:31:30, Serial1/3
C 192.168.1.20/30 is directly connected, Serial1/3
O 192.168.1.24/30 [110/1562] via 192.168.1.22, 00:31:30, Serial1/3
C 192.168.1.28/30 is directly connected, Serial1/1
C 192.168.1.32/30 is directly connected, Serial1/2
R 192.168.1.36/30 [120/1] via 192.168.1.34, 00:00:03, Serial1/2

```



[120/1] via 192.168.1.30, 00:00:27, Serial1/1
[120/1] via 192.168.1.13, 00:00:08, Serial1/0
O E2 192.168.1.64/27 [110/1562] via 192.168.1.22, 00:28:59, Serial1/3
O E2 192.168.1.96/27 [110/1562] via 192.168.1.22, 00:28:32, Serial1/3
O 192.168.1.128/27 [110/1563] via 192.168.1.22, 00:31:30, Serial1/3
R 192.168.1.160/27 [120/1] via 192.168.1.30, 00:00:27, Serial1/1
[120/1] via 192.168.1.13, 00:00:08, Serial1/0
R 192.168.1.192/27 [120/1] via 192.168.1.34, 00:00:03, Serial1/2
[120/1] via 192.168.1.13, 00:00:08, Serial1/0
O E2 192.168.2.0/24 [110/1562] via 192.168.1.22, 00:28:05, Serial1/3
192.168.3.0/24 is variably subnetted, 4 subnets, 3 masks
R 192.168.3.0/24 [120/1] via 192.168.1.13, 00:00:08, Serial1/0
O 192.168.3.0/27 [110/1563] via 192.168.1.22, 00:31:30, Serial1/3
O 192.168.3.32/28 [110/1563] via 192.168.1.22, 00:31:30, Serial1/3
O 192.168.3.48/28 [110/1563] via 192.168.1.22, 00:31:30, Serial1/3
R 192.168.4.0/24 [120/1] via 192.168.1.34, 00:00:03, Serial1/2
[120/1] via 192.168.1.30, 00:00:27, Serial1/1
[120/1] via 192.168.1.13, 00:00:08, Serial1/0
192.168.5.0/24 is variably subnetted, 6 subnets, 3 masks
O E2 192.168.5.0/24 [110/1562] via 192.168.1.22, 00:24:11, Serial1/3
O 192.168.5.64/27 [110/782] via 192.168.1.22, 00:31:30, Serial1/3
O 192.168.5.96/28 [110/782] via 192.168.1.22, 00:31:30, Serial1/3
O 192.168.5.112/28 [110/782] via 192.168.1.22, 00:31:30, Serial1/3
O 192.168.5.128/28 [110/782] via 192.168.1.22, 00:31:30, Serial1/3
O 192.168.5.144/28 [110/782] via 192.168.1.22, 00:31:30, Serial1/3
192.168.6.0/24 is variably subnetted, 7 subnets, 4 masks
R 192.168.6.0/24 [120/1] via 192.168.1.13, 00:00:08, Serial1/0
O E2 192.168.6.0/29 [110/1562] via 192.168.1.22, 00:31:30, Serial1/3
O E2 192.168.6.8/29 [110/1562] via 192.168.1.22, 00:31:30, Serial1/3
O E2 192.168.6.16/28 [110/1562] via 192.168.1.22, 00:31:30, Serial1/3
C 192.168.6.32/27 is directly connected, FastEthernet0/0
C 192.168.6.64/27 is directly connected, FastEthernet0/0.2
C 192.168.6.96/27 is directly connected, FastEthernet0/0.3
200.10.1.0/24 is variably subnetted, 3 subnets, 3 masks
R 200.10.1.0/24 [120/1] via 192.168.1.13, 00:00:08, Serial1/0
O 200.10.1.0/30 [110/1562] via 192.168.1.22, 00:31:30, Serial1/3
O E2 200.10.1.32/27 [110/1562] via 192.168.1.22, 00:31:30, Serial1/3
ECOTEC#



3.41.-COMANDO SHOW IP ROUTE EN EL ROUTER ECOTEC-1

ECOTEC-1#show ip route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

```

192.168.1.0/24 is variably subnetted, 15 subnets, 2 masks
R   192.168.1.0/30 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.1.4/30 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.1.8/30 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.1.12/30 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.1.16/30 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.1.20/30 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.1.24/30 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
C   192.168.1.28/30 is directly connected, Serial1/0
R   192.168.1.32/30 [120/1] via 192.168.1.37, 00:00:16, Serial1/1
C   192.168.1.36/30 is directly connected, Serial1/1
R   192.168.1.64/27 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.1.96/27 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.1.128/27 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
C   192.168.1.160/27 is directly connected, FastEthernet0/0
R   192.168.1.192/27 [120/1] via 192.168.1.37, 00:00:16, Serial1/1
R   192.168.2.0/24 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.3.0/24 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
192.168.4.0/24 is variably subnetted, 4 subnets, 3 masks
R   192.168.4.0/24 [120/1] via 192.168.1.37, 00:00:16, Serial1/1
C   192.168.4.0/29 is directly connected, FastEthernet0/0.2
C   192.168.4.8/29 is directly connected, FastEthernet0/0.3
C   192.168.4.16/28 is directly connected, FastEthernet0/0.4
R   192.168.5.0/24 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   192.168.6.0/24 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
R   200.10.1.0/24 [120/1] via 192.168.1.29, 00:00:28, Serial1/0
ECOTEC-1#

```



3.42.- COMANDO SHOW IP ROUTE EN EL ROUTER ECOTEC-2

ECOTEC-2#show ip route

Codes: C - connected, S - static, I - IGRP, 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, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

```

192.168.1.0/24 is variably subnetted, 15 subnets, 2 masks
R   192.168.1.0/30 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.4/30 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.8/30 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.12/30 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.16/30 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.20/30 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.24/30 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.28/30 [120/1] via 192.168.1.38, 00:00:11, Serial1/2
C   192.168.1.32/30 is directly connected, Serial1/0
C   192.168.1.36/30 is directly connected, Serial1/2
R   192.168.1.64/27 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.96/27 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.128/27 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.1.160/27 [120/1] via 192.168.1.38, 00:00:11, Serial1/2
C   192.168.1.192/27 is directly connected, FastEthernet0/0
R   192.168.2.0/24 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.3.0/24 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
192.168.4.0/24 is variably subnetted, 4 subnets, 3 masks
R   192.168.4.0/24 [120/1] via 192.168.1.38, 00:00:11, Serial1/2
C   192.168.4.32/27 is directly connected, FastEthernet0/0.2
C   192.168.4.64/28 is directly connected, FastEthernet0/0.3
C   192.168.4.80/28 is directly connected, FastEthernet0/0.4
R   192.168.5.0/24 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   192.168.6.0/24 [120/1] via 192.168.1.33, 00:00:05, Serial1/0
R   200.10.1.0/24 [120/1] via 192.168.1.33, 00:00:05, Serial1/0

```

3.43.- DEFINICIÓN Y FUNCIÓN DEL SWITCH

El switch (palabra que significa “conmutador”) es un dispositivo que permite la interconexión de redes sólo cuando esta conexión es necesaria. Para entender mejor que es lo que realiza, pensemos que la red está dividida en segmentos por lo que, cuando alguien envía un mensaje desde un segmento hacia otro segmento determinado, el switch se encargará de hacer que ese mensaje llegue única y exclusivamente al segmento requerido.

El switch opera en la capa 2 del modelo OSI, que es el nivel de enlace de datos, y tienen la particularidad de aprender y almacenar las direcciones (los caminos) de dicho nivel, por lo que siempre irán desde el puerto de origen directamente al de llegada, para evitar los bucles (habilitar más de un camino para llegar a un mismo destino). Asimismo, tiene la capacidad de poder realizar las conexiones con velocidades diferentes en sus ramas, variando entre 10 Mbps y 100 Mbps.

De esta manera los Switches reciben tramas en una interfaz, seleccionan el puerto correcto por el cual enviar las tramas, y entonces envían la trama de acuerdo a la selección de ruta. Los switches elaboran y mantienen las tablas de envío, además también elaboran y mantienen una topología sin bucles en toda la LAN. Los switches LAN o de la Capa 2 envían tramas en base a la información de la dirección MAC. La diferencia entre la conmutación de Capa 2 y Capa 3 es el tipo de información que se encuentra dentro de la trama.

La latencia de switch es el período transcurrido desde el momento que una trama entra a un switch hasta que la trama sale del switch. La latencia se mide en fracciones de segundo.

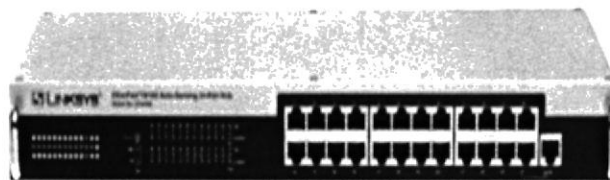


Figura 3- 10: Switch

3.43.1.- LED SISTEMAS – SWITCHES

Una vez que se conecta el cable de energía eléctrica, el switch inicia una serie de pruebas denominadas Autocomprobación de Encendido (POST).

POST se ejecuta automáticamente para verificar que el switch funcione correctamente.

El LED del sistema indica el éxito o falla de la POST. Si el LED del sistema está apagado pero el switch está enchufado, entonces POST está funcionando.

Si el LED del sistema está verde, entonces la POST fue exitosa.

Pero si el LED del sistema está ámbar, entonces la POST falló. La falla de la POST se considera como un error fatal. No se puede esperar que el switch funcione de forma confiable si la POST falla.

3.43.2.-CONFIGURACIÓN ACTIVA POR DEFECTO

El nombre de host por defecto es Switch.

No se establece ninguna contraseña en las líneas del terminal de consola o virtual (vty).

Se le puede otorgar al switch una dirección IP para fines de administración. Esto se configura en la interfaz virtual, VLAN 1. Por defecto, el switch no tiene dirección IP.

Los puertos o interfaces del switch se establecen en modo automático y todos los

Puerto de switch están en VLAN 1. VLAN 1 se conoce como la VLAN de administración por defecto.

El directorio flash por defecto tiene un archivo que contiene la imagen IOS, un archivo llamado env_vars y un subdirectorio llamado html. Una vez que se configura el switch, el directorio flash contiene un archivo con el nombre config.text así como una base de datos de VLAN.

3.44.- LAN VIRTUALES O VLAN

Es un agrupamiento lógico de estaciones y dispositivos de red, sin importar la ubicación física de los usuarios. Los switches y puentes envían tráfico unicast, multicast y broadcast sólo en segmentos de LAN que atienden a la VLAN a la que pertenece el tráfico. Los dispositivos en la VLAN sólo se comunican con los dispositivos que están en la misma VLAN. Los routers suministran conectividad entre diferentes VLAN.

3.44.1.- VENTAJAS

- Controlan los broadcast de capa 3.
- Trasladar fácilmente las estaciones de trabajo en la LAN.
- Agregar fácilmente estaciones de trabajo a la LAN.
- Cambiar fácilmente la configuración de la LAN.
- Controlar fácilmente el tráfico de red.
- Mejorar la seguridad.



3.44.2.- TIPOS DE VLAN

Existen tres tipos de vlan:

TIPOS DE VLAN	DESCRIPCIÓN
Basada en Puertos	Los puertos se asignan individualmente, en grupos o filas. Se implementa con DHCP
Basada en Max	Escasa frecuencia de uso. Es necesario introducir y configurar cada dirección de forma individual.
Basada en Protocolo	Se configuran como las direcciones MAC; pero usan una dirección lógica (IP)

Tabla 3- 7: Tipos de Vlan

3.45.- CONFIGURACIÓN DE VLAN EN LOS SWITCHES

Son puertos en un switch que se asignan manualmente a una VLAN. Estos puertos mantienen su configuración de VLAN asignada hasta que se cambien manualmente. La cantidad máxima de VLAN depende del switch. La VLAN Ethernet por defecto es VLAN 1.

Se envían publicaciones del Protocolo de Descubrimiento de Cisco (CDP) y Protocolo de Enlace Troncal de VLAN (VTP) en la VLAN 1. La dirección IP del switch se encuentra por defecto en el dominio de broadcast de la VLAN 1. El switch debe estar en el modo de servidor VTP para crear, agregar o borrar VLAN.

3.45.1.-CREACIÓN DE VLANS EN EL SW-TES

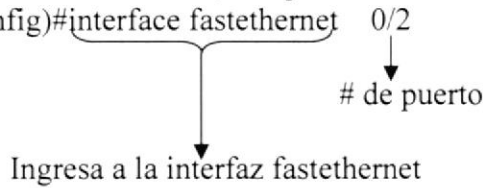
Switch>enable → Instrucción para entrar en modo privilegiado
Switch#vlan database
↓ Ingresar en el modo base de datos de VLAN
Comando para configurar una VLAN

% Warning: It is recommended to configure VLAN from config mode, as VLAN database mode is being deprecated. Please consult user documentation for configuring VTP/VLAN in config mode.

SW-TES (vlan)#vlan, {203} name Rectorado
↓ # de Vlan ↓ Palabra clave a la que sigue el nombre de la VLAN
Configurar una VLAN Nombre de la Vlan

VLAN 203 added:
Name: Rectorado
SW-TES(vlan)#vlan 204 name Caja
VLAN 204 added:
Name: Caja
SW-TES (vlan)#vlan 205 nameProxy
VLAN 205 added:
Name: Proxy
SW-TES (vlan)#vlan 206 nameWeb Server
VLAN 206 added:
Name: Web Server

```
SW-TEs (vlan)#exit  
APPLY completed.  
Exiting....  
SW-TEs #configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
SW-TEs (config)#interface fastethernet 0/2
```



```
SW-TEs (config-if)#switchport access vlan 203
```

Asigna un puerto a la vlan

```
SW-TEs (config-if)#exit  
SW-TEs (config)#interface fastethernet 0/3  
SW-TEs (config-if)#switchport access vlan 204  
SW-TEs (config-if)#exit  
SW-TEs (config)#interface fastethernet 0/4  
SW-TEs (config-if)#switchport access vlan 205  
SW-TEs (config-if)#exit  
SW-TEs (config)#interface fastethernet 0/5  
SW-TEs (config-if)#switchport access vlan 206  
SW-TEs (config-if)#exit
```



3.45.2.- ENLACES TRONCALES (VTP)

Es una conexión física y lógica entre dos switches a través de la cual se transmite el tráfico de red. Es un único canal de transmisión entre dos puntos. En una red conmutada, un enlace troncal es un enlace punto a punto que admite varias VLAN. El propósito de un enlace troncal es conservar los puertos cuando se crea un enlace entre dos dispositivos que implementan las VLAN. No se puede establecer un enlace troncal entre un router y un switch.

```
SW-TEs (config)#interface fastethernet 0/1  
SW-TEs (config-if)#switchport mode trunk
```

Especifica un puerto como punto extremo para un tronco VLAN

Configura el modo de pertenencia VLAN para un puerto

Tronco.- Un tronco es un enlace directo entre dos conmutadores, de manera que el puerto transmite y recibe cuadros etiquetados que identifican la fuente VLAN.

```
SW-TES (config)#exit
%SYS-5-CONFIG_I: Configured from console by console
SW-TES #
```

3.46.- CREACIÓN DE VLANS EN EL SW-TES-1

```
SW-TES-1>enable
SW-TES-1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.
```

```
SW-TES-1(vlan)#vlan 200 name RRHH
VLAN 200 added:
  Name: RRHH
SW-TES-1(vlan)#vlan 201name Sistemas
VLAN 201 added:
  Name: Sistemas
SW-TES-1 (vlan)#vlan 202 name Lac-Mac
VLAN 202 added:
  Name: Lac-Mac
SW-TES-1 (vlan)#ex
APPLY completed.
Exiting....
SW-TES-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW-TES-1 (config)#interface fastethernet 0/2
SW-TES-1 (config-if)#switchport access vlan 200
SW-TES-1 (config-if)#exit
SW-TES-1 (config)#interface fastethernet 0/3
SW-TES-1 (config-if)#switchport access vlan 201
SW-TES-1 (config-if)#exit
SW-TES-1 (config)#interface fastethernet 0/4
SW-TES-1 (config-if)#switchport access vlan 202
SW-TES-1 (config-if)#exit
SW-TES-1 (config)#interface fastethernet 0/1
SW-TES-1 (config-if)#switchport mode trunk
SW-TES-1 (config-if)#exit
SW-TES-1 (config)#exit
%SYS-5-CONFIG_I: Configured from console by console
SW-TES-1#
```

3.47.- CREACIÓN DE VLANS EN EL SW-UEES

```
SW-UEES>enable
SW-UEES#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

SW-UEES (vlan)#vlan 106 name SPIRIT2
VLAN 106 added:
  Name: SPIRIT2
SW-UEES (vlan)#vlan 107name SPIRIT3
VLAN 107 added:
  Name: SPIRIT3
SW- UEES (vlan)#exit
APPLY completed.
Exiting....
SW- UEES #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW- UEES (config)#interface fastethernet 0/2
SW-UEES (config-if)#switchport access vlan 106
SW- UEES (config-if)#exit
SW- UEES (config)#interface fastethernet 0/3
SW- UEES (config-if)#switchport access vlan 107
SW- UEES (config-if)#exit
SW- UEES (config)#interface fastethernet 0/1
SW- UEES (config-if)#switchport mode trunk
SW- UEES (config-if)#exit
SW- UEES 1 (config)#exit
%SYS-5-CONFIG_I: Configured from console by console
SW- UEES #
```



3.48.- CREACIÓN DE VLANS EN EL SW-UEES-1

```
SW-UEES-1>enable
SW-UEES-1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

SW-UEES-1 (vlan)#vlan 100 name Administración
VLAN 100 added:
  Name: Administración
SW-UEES-1 (vlan)#vlan 101name Contabilidad
VLAN 101 added:
  Name: Contabilidad
```

```
SW-UEES-1 (vlan)#vlan 102 name Secretariado
VLAN 102 added:
  Name: Secretariado

SW- UEES-1 (vlan)#exit
APPLY completed.
Exiting....
SW- UEES-1 #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW- UEES-1 (config)#interface fastethernet 0/2
SW-UEES-1 (config-if)#switchport access vlan 100
SW- UEES-1 (config-if)#exit
SW- UEES-1 (config)#interface fastethernet 0/3
SW- UEES-1 (config-if)#switchport access vlan 101
SW- UEES-1 (config-if)#exit
SW- UEES-1 (config)#interface fastethernet 0/4
SW-UEES-1 (config-if)#switchport access vlan 102
SW- UEES-1 (config-if)#exit
SW- UEES-1 (config)#interface fastethernet 0/1
SW- UEES-1 (config-if)#switchport mode trunk
SW- UEES-1 (config-if)#exit
SW- UEES 1 (config)#exit
%SYS-5-CONFIG_I: Configured from console by console
SW- UEES-1 #
```

3.49.- CREACIÓN DE VLANS EN EL SW-UEES-2

```
SW-UEES-2>enable
SW-UEES-2#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

SW-UEES-2 (vlan)#vlan 103 name Financiero
VLAN 103 added:
  Name:Financiero
SW-UEES-2 (vlan)#vlan 104name Consejería
VLAN 104 added:
  Name: Consejería
SW-UEES-2 (vlan)#vlan 105 name Bibliotecal
VLAN 105 added:
  Name: Bibliotecal

SW- UEES-2 (vlan)#exit
APPLY completed.
Exiting....
SW- UEES-2 #configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
SW- UEES-2 (config)#interface fastethernet 0/2
SW-UEES-2 (config-if)#switchport access vlan 103
SW- UEES-2 (config-if)#exit
SW- UEES-2 (config)#interface fastethernet 0/3
SW- UEES-2 (config-if)#switchport access vlan 104
SW- UEES-2 (config-if)#exit
SW- UEES-2 (config)#interface fastethernet 0/4
SW-UEES-2 (config-if)#switchport access vlan 105
SW- UEES-2 (config-if)#exit
SW- UEES-2 (config)#interface fastethernet 0/1
SW- UEES-2 (config-if)#switchport mode trunk
SW- UEES-2 (config-if)#exit
SW- UEES 2 (config)#exit
%SYS-5-CONFIG_I: Configured from console by console
SW- UEES-2 #
```

3.50.- CREACIÓN DE VLANS EN EL SW-ECOTEC

```
SW-ECOTEC>enable
SW-ECOTEC#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

SW-ECOTEC (vlan)#vlan 306 name Dirección Estudiantil
VLAN 306 added:
  Name: Dirección Estudiantil

SW-ECOTEC (vlan)#vlan 307name Spirit4
VLAN 307 added:
  Name: Spirit4
SW-ECOTEC (vlan)#exit
APPLY completed.
Exiting....
SW- ECOTEC #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW- ECOTEC (config)#interface fastethernet 0/2
SW- ECOTEC (config-if)#switchport access vlan 306
SW- ECOTEC (config-if)#exit
SW- ECOTEC (config)#interface fast ethernet0/3
SW- ECOTEC (config-if)#switchport access vlan 307
SW- ECOTEC (config-if)#exit
SW -ECOTEC (config)#interface fastethernet 0/1
SW- ECOTEC (config-if)#switchport mode trunk
SW- ECOTEC (config-if)#exit
SW- ECOTEC (config)#exit
```

```
%SYS-5-CONFIG_I: Configured from console by console  
SW- ECOTEC #
```

3.51.- CREACIÓN DE VLANS EN EL SW-ECOTEC-1

```
SW-ECOTEC-1>enable  
SW-ECOTEC-1#vlan database  
% Warning: It is recommended to configure VLAN from config mode,  
as VLAN database mode is being deprecated. Please consult user  
documentation for configuring VTP/VLAN in config mode.  
  
SW-ECOTEC-1 (vlan)#vlan 300 name Tesoreria  
VLAN 300 added:  
Name: Tesoreria  
SW-ECOTEC-1 (vlan)#vlan 301name Biblioteca  
VLAN 301 added:  
Name: Biblioteca  
SW-ECOTEC-1 (vlan)#vlan 302name Spirit  
VLAN 302 added:  
Name: Spirit  
SW-ECOTEC-1 (vlan)#exit  
APPLY completed.  
Exiting....  
SW- ECOTEC-1 #configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
SW- ECOTEC-1 (config)#interface fastethernet 0/2  
SW- ECOTEC-1 (config-if)#switchport access vlan 300  
SW- ECOTEC-1 (config-if)#exit  
SW- ECOTEC-1 (config)#interface fastethernet 0/3  
SW- ECOTEC-1 (config-if)#switchport access vlan 301  
SW- ECOTEC-1 (config-if)#exit  
SW- ECOTEC-1 (config)#interface fastethernet 0/4  
SW- ECOTEC-1 (config-if)#switchport access vlan 302  
SW- ECOTEC-1 (config-if)#exit  
SW -ECOTEC-1 (config)#interface fastethernet 0/1  
SW- ECOTEC-1 (config-if)#switchport mode trunk  
SW- ECOTEC-1 (config-if)#exit  
SW- ECOTEC-1 (config)#exit  
%SYS-5-CONFIG_I: Configured from console by console  
SW- ECOTEC-1 #
```

3.52.- CREACIÓN DE VLANS EN EL SW-ECOTEC-2

```

SW-ECOTEC-2>enable
SW-ECOTEC-2#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.
SW-ECOTEC-2 (vlan)#vlan 303 name Dirección Ejecutiva
VLAN 303 added:
  Name: Dirección Ejecutiva
SW-ECOTEC-2 (vlan)#vlan 304name Bodega
VLAN 304 added:
  Name: Bodega
SW-ECOTEC-2 (vlan)#vlan 305name Estadísticas
VLAN 305 added:
  Name: Estadísticas
SW-ECOTEC-1 (vlan)#exit
APPLY completed.
Exiting....
SW- ECOTEC-2 #configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW- ECOTEC-2 (config)#interface fastethernet 0/2
SW- ECOTEC-2 (config-if)#switchport access vlan 303
SW- ECOTEC-2 (config-if)#exit
SW- ECOTEC-2 (config)#interface fastethernet 0/3
SW- ECOTEC-2 (config-if)#switchport access vlan 304
SW- ECOTEC-2 (config-if)#exit
SW- ECOTEC-2 (config)#interface fastethernet 0/4
SW- ECOTEC-2 (config-if)#switchport access vlan 305
SW- ECOTEC-2 (config-if)#exit
SW -ECOTEC-2 (config)#inter fast 0/1
SW- ECOTEC-2(config-if)#switchport mode trunk
SW- ECOTEC-2 (config-if)#exit
SW- ECOTEC-2 (config)#exit
%SYS-5-CONFIG_I: Configured from console by console
SW- ECOTEC-2 #

```



3.53.- COMANDO SHOW VLAN EN EL SWITCH TES

Muestra la información de las vlan.

SW-TES#SHOW VLAN

VLAN Name	Status	Ports
1 default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig1/1 Gig1/2

# de vlan	Nombre de la vlan	Estado	#Puerto
203	Rectorado	active	Fa0/2

204	Caja	active	Fa0/3
205	Proxy	active	Fa0/4
206	WebServer	active	Fa0/5
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
303	enet	100303	1500	-	-	-	-	-	0	0
304	enet	100304	1500	-	-	-	-	-	0	0
305	enet	100305	1500	-	-	-	-	-	0	0
1002	enet	101002	1500	-	-	-	-	-	0	0
1003	enet	101003	1500	-	-	-	-	-	0	0
1004	enet	101004	1500	-	-	-	-	-	0	0
1005	enet	101005	1500	-	-	-	-	-	0	0



3.54.- COMANDO SHOW VLAN EN EL SWITCH TES-1

SW-TES-1#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
200 RRHH	active	Fa0/4
201 Sistemas	active	Fa0/3
202 Lab-Mac	active	Fa0/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	



VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	No Stp	BrdgMode	Trans1	Trans2
1 enet	100001	1500	-	-	-	-	-	0	0
303 enet	100303	1500	-	-	-	-	-	0	0
304 enet	100304	1500	-	-	-	-	-	0	0
305 enet	100305	1500	-	-	-	-	-	0	0
1002 enet	101002	1500	-	-	-	-	-	0	0
1003 enet	101003	1500	-	-	-	-	-	0	0
1004 enet	101004	1500	-	-	-	-	-	0	0
1005 enet	101005	1500	-	-	-	-	-	0	0

3.55.- COMANDO SHOW VLAN EN EL SWITCH UEES

SW-UEES#SHOW VLAN

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig1/1, Gig1/2
106 Spirit2	active	Fa0/2
107 Spirit3	active	Fa0/3
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1 enet	100001	1500	-	-	-	-	-	0	0
303 enet	100303	1500	-	-	-	-	-	0	0
304 enet	100304	1500	-	-	-	-	-	0	0
305 enet	100305	1500	-	-	-	-	-	0	0
1002 enet	101002	1500	-	-	-	-	-	0	0
1003 enet	101003	1500	-	-	-	-	-	0	0
1004 enet	101004	1500	-	-	-	-	-	0	0
1005 enet	101005	1500	-	-	-	-	-	0	0

3.56.- COMANDO SHOW VLAN EN EL SWITCH UEES-1

SW-UEES-1#SHOW VLAN

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
100 Administración	active	Fa0/2
101 Contabilidad	active	Fa0/3
102 Secretariado	active	Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	



VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
303	enet	100303	1500	-	-	-	-	-	0	0
304	enet	100304	1500	-	-	-	-	-	0	0
305	enet	100305	1500	-	-	-	-	-	0	0
1002	enet	101002	1500	-	-	-	-	-	0	0
1003	enet	101003	1500	-	-	-	-	-	0	0
1004	enet	101004	1500	-	-	-	-	-	0	0
1005	enet	101005	1500	-	-	-	-	-	0	0

3.57.- COMANDO SHOW VLAN EN EL SWITCH UEES-2

SW-UEES-2#show vlan

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
103 Financiero	active	Fa0/2
104 Consejería	active	Fa0/3
105 Biblioteca	active	Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	



VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
303	enet	100303	1500	-	-	-	-	-	0	0
304	enet	100304	1500	-	-	-	-	-	0	0
305	enet	100305	1500	-	-	-	-	-	0	0
1002	enet	101002	1500	-	-	-	-	-	0	0
1003	enet	101003	1500	-	-	-	-	-	0	0
1004	enet	101004	1500	-	-	-	-	-	0	0
1005	enet	101005	1500	-	-	-	-	-	0	0

3.58.- COMANDO SHOW VLAN EN EL SWITCH ECOTEC

SW-ECOTEC#SHOW VLAN

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig1/1, Gig1/2
306 DireccionEstudiantil	active	Fa0/2
307 Spirit4	active	Fa0/3
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	



VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
303	enet	100303	1500	-	-	-	-	-	0	0
304	enet	100304	1500	-	-	-	-	-	0	0
305	enet	100305	1500	-	-	-	-	-	0	0
1002	enet	101002	1500	-	-	-	-	-	0	0
1003	enet	101003	1500	-	-	-	-	-	0	0
1004	enet	101004	1500	-	-	-	-	-	0	0
1005	enet	101005	1500	-	-	-	-	-	0	0

3.59.- COMANDO SHOW VLAN EN EL SWITCH ECOTEC-1

SW-ECOTEC-1#SHOW VLAN

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
300 Tesorería	active	Fa0/2
301 Biblioteca	active	Fa0/3
302 Spirit	active	Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	



VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
303	enet	100303	1500	-	-	-	-	-	0	0
304	enet	100304	1500	-	-	-	-	-	0	0
305	enet	100305	1500	-	-	-	-	-	0	0
1002	enet	101002	1500	-	-	-	-	-	0	0
1003	enet	101003	1500	-	-	-	-	-	0	0
1004	enet	101004	1500	-	-	-	-	-	0	0
1005	enet	101005	1500	-	-	-	-	-	0	0

3.60.- COMANDO SHOW VLAN EN EL SWITCH ECOTEC-2

SW-ECOTEC-2#SHOW VLAN

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
303 Dirección	active	Fa0/2
304 Bodega	active	Fa0/3
305 Estadística	active	Fa0/4
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	



VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
303	enet	100303	1500	-	-	-	-	-	0	0
304	enet	100304	1500	-	-	-	-	-	0	0
305	enet	100305	1500	-	-	-	-	-	0	0
1002	enet	101002	1500	-	-	-	-	-	0	0
1003	enet	101003	1500	-	-	-	-	-	0	0
1004	enet	101004	1500	-	-	-	-	-	0	0
1005	enet	101005	1500	-	-	-	-	-	0	0

3.61.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER TES

```
TES>enable  
TES#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.
```

```
TES(config)#interface fastethernet 0/0/2
```

Diagrama de anotación para la línea anterior:
- "interface" apunta a "Tipo de interfaz"
- "fastethernet" apunta a "Modulo"
- "0" apunta a "Interfaz"
- "0/0/2" apunta a "Subinterfaz"

```
TES(config-subif)#encapsulation dot1Q 203
```

Diagrama de anotación para la línea anterior:
- "encapsulation" apunta a "Encapsulamiento de vlan"
- "dot1Q" apunta a "Protocolo por el que se comunican las vlan"
- "203" apunta a "Número de vlan"

```
TES(config-subif)#ip address 192.168.5.97 255.255.255.240
```

Diagrama de anotación para la línea anterior:
- "192.168.5.97" apunta a "Dirección de la subinterfaz"
- "255.255.255.240" apunta a "Mascara de la subinterfaz"

```
TES (config-subif)# no shutdown
```

Diagrama de anotación para la línea anterior:
- "no shutdown" apunta a "Activa una interfaz desactivada"

```
TES (config-subif)#exit  
TES (config)#interface fastethernet 0/0.3  
TES (config-subif)#encapsulation dot1Q 204  
TES (config-subif)#ip address 192.168.5.113 255.255.255.240  
TES (config-subif)#no shutdown  
TES (config-subif)#exit  
TES (config)#interface fastethernet 0/0.4  
TES (config-subif)#encapsulation dot1Q 205  
TES (config-subif)#ip address 192.168.5.129 255.255.255.240  
TES (config-subif)#no shutdown  
TES (config-subif)#exit  
TES (config)#interface fastethernet 0/0.5  
TES (config-subif)#encapsulation dot1Q 206  
TES (config-subif)#ip address 192.168.5.145 255.255.255.240  
TES (config-subif)#no shutdown  
TES (config-subif)#exit
```



3.62.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER TES-1

```
TES-1>enable
TES-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TES-1(config)#interface fastethernet 0/0.2
TES-1(config-subif)#encapsulation dot1Q 202
TES-1(config-subif)#ip address 192.168.3.1 255.255.255.224
TES-1(config-subif)#no shutdown
TES-1(config-subif)#exit
TES-1(config)#interface fastethernet 0/0.3
TES-1(config-subif)#encapsulation dot1Q 201
TES-1(config-subif)#ip address 192.168.3.33 255.255.255.240
TES-1(config-subif)#no shutdown
TES-1(config-subif)#exit
TES-1(config)#interface fastethernet 0/0.4
TES-1(config-subif)#encapsulation dot1Q 200
TES-1(config-subif)#ip address 192.168.3.49 255.255.255.240
TES-1(config-subif)#no shutdown
TES-1(config-subif)#exit
```

3.63.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER UEES

```
UEES>enable
UEES#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UEES(config)#interface fastethernet 0/0.2
UEES(config-subif)#encapsulation dot1Q 106
UEES(config-subif)#ip address 192.168.6.9 255.255.255.248
UEES(config-subif)#no shutdown
UEES(config-subif)#exit
UEES(config)#interface fastethernet 0/0.3
UEES(config-subif)#encapsulation dot1Q 107
UEES(config-subif)#ip address 192.168.6.17 255.255.255.240
UEES(config-subif)#no shutdown
UEES(config-subif)#exit
```



3.64.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER UEES-1

```
UEES-1>enable
UEES-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UEES-1 (config)#interface fastethernet 0/0.2
UEES-1 (config-subif)#encapsulation dot1Q 100
UEES-1 (config-subif)#ip address 192.168.2.1 255.255.255.248
UEES-1 (config-subif)#no shutdown
UEES-1 (config-subif)#exit
UEES-1 (config)#interface fastethernet 0/0.3
UEES-1 (config-subif)#encapsulation dot1Q 101
UEES-1 (config-subif)#ip address 192.168.2.9 255.255.255.248
UEES-1 (config-subif)#no shutdown
UEES-1 (config-subif)#exit
UEES-1 (config)#interface fastethernet 0/0.4
UEES-1 (config-subif)#encapsulation dot1Q 102
UEES-1 (config-subif)#ip address 192.168.2.17 255.255.255.240
UEES-1 (config-subif)#no shutdown
UEES-1 (config-subif)#exit
```

3.65.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER UEES-2

```
UEES-2>enable
UEES-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UEES-2 (config)#interface fastethernet 0/0.2
UEES-2 (config-subif)#encapsulation dot1Q 100
UEES-2 (config-subif)#ip address 192.168.2.33 255.255.255.240
UEES-2 (config-subif)#no shutdown
UEES-2 (config-subif)#exit
UEES-2 (config)#interface fastethernet 0/0.3
UEES-2 (config-subif)#encapsulation dot1Q 101
UEES-2 (config-subif)#ip address 192.168.2.49 255.255.255.240
UEES-2 (config-subif)#no shutdown
UEES-2 (config-subif)#exit
UEES-2 (config)#interface fastethernet 0/0.4
UEES-2 (config-subif)#encapsulation dot1Q 102
UEES-2 (config-subif)#ip address 192.168.2.65 255.255.255.240
UEES-2 (config-subif)#no shutdown
UEES-2 (config-subif)#exit
```

3.66.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER ECOTEC

```
ECOTEC>enable
ECOTEC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ECOTEC (config)#interface fastethernet 0/0.2
ECOTEC (config-subif)#encapsulation dot1Q 306
ECOTEC (config-subif)#ip address 192.168.6.65 255.255.255.224
ECOTEC (config-subif)#no shutdown
ECOTEC (config-subif)#exit
ECOTEC (config)#interface fastethernet 0/0.3
ECOTEC (config-subif)#encapsulation dot1Q 307
ECOTEC (config-subif)#ip address 192.168.6.97 255.255.255.224
ECOTEC (config-subif)#no shutdown
ECOTEC (config-subif)#exit
```

3.67.- CONFIGURACIÓN DE LAS SUBINTERFACES EN EL ROUTER ECOTEC-1

```
ECOTEC-1>enable
ECOTEC-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ECOTEC-1 (config)#interface fastethernet 0/0.2
ECOTEC-1 (config-subif)#encapsulation dot1Q 300
ECOTEC-1 (config-subif)#ip address 192.168.4.1 255.255.255.248
ECOTEC-1 (config-subif)#no shutdown
ECOTEC-1 (config-subif)#exit
ECOTEC-1 (config)#interface fastethernet 0/0.3
ECOTEC-1 (config-subif)#encapsulation dot1Q 301
ECOTEC-1 (config-subif)#ip address 192.168.4.9 255.255.255.248
ECOTEC-1 (config-subif)#no shutdown
ECOTEC-1 (config-subif)#exit
ECOTEC-1 (config-subif)#encapsulation dot1Q 302
ECOTEC-1 (config-subif)#ip address 192.168.4.17 255.255.255.240
ECOTEC-1 (config-subif)#no shutdown
ECOTEC-1 (config-subif)#exit
```



3.68.- CONFIGURACION DE LAS SUBINTERFACES EN EL ROUTER ECOTEC-2

```

ECOTEC-2>enable
ECOTEC-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ECOTEC-2 (config)#interface fastethernet 0/0.2
ECOTEC-2 (config-subif)#encapsulation dot1Q 303
ECOTEC-2 (config-subif)#ip address 192.168.4.33 255.255.255.224
ECOTEC-2 (config-subif)#no shutdown
ECOTEC-2 (config-subif)#exit
ECOTEC-2 (config)#interface fastethernet 0/0.3
ECOTEC-2 (config-subif)#encapsulation dot1Q 304
ECOTEC-2 (config-subif)#ip address 192.168.4.65 255.255.255.224
ECOTEC-2 (config-subif)#no shutdown
ECOTEC-2 (config-subif)#exit
ECOTEC-2 (config-subif)#encapsulation dot1Q 305
ECOTEC-2 (config-subif)#ip address 192.168.4.81 255.255.255.240
ECOTEC-2 (config-subif)#no shutdown
ECOTEC-2 (config-subif)#exit

```

3.69.- COMANDO SHOW INTERFACES EN EL ROUTER

Muestra las estadísticas completas de todas las interfaces del router.

```

UEES# Show Interfaces
FastEthernet 0 /0 is up, line protocol is up (connected)

```

```

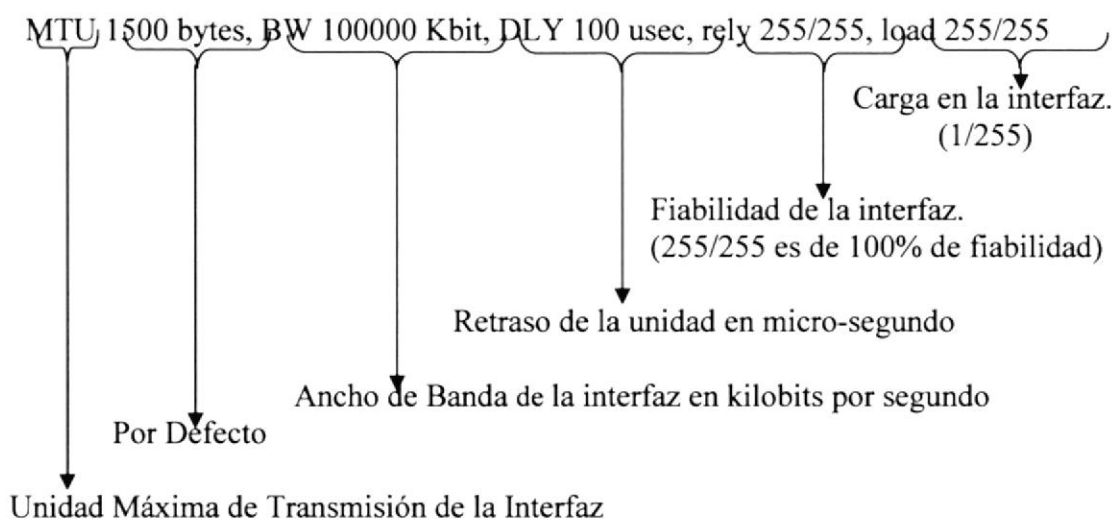
Hardware is Lance, address is 0060.3e62.6c01 (bia 0060.3e62.6c01)

```

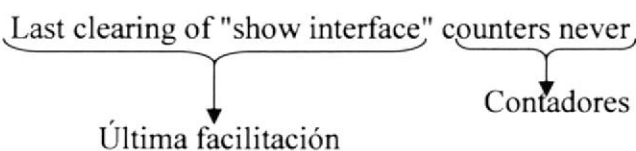
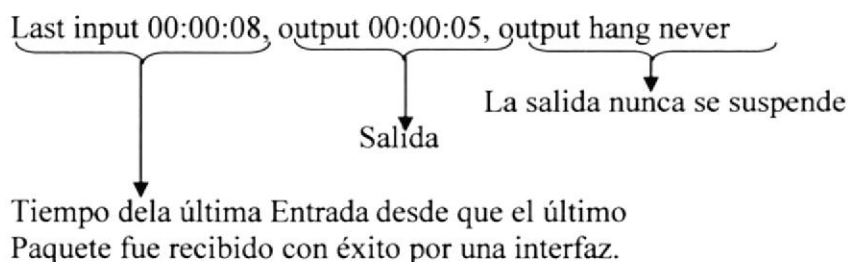
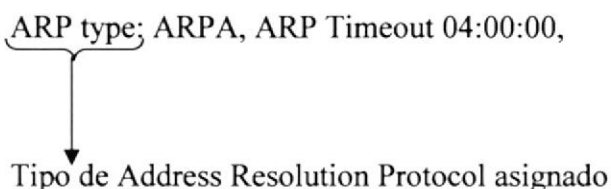
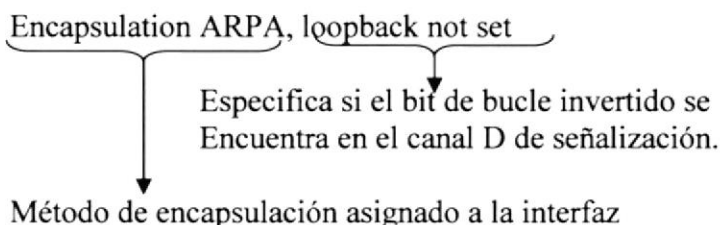
```

Internet address is 192.168.5.65 /27

```



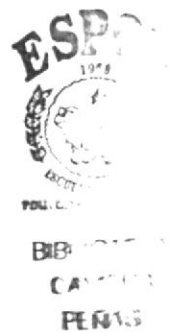
1500 bytes: Describe el paquete más grande que puede ser enviado a través de la interfaz antes de que se fragmenta el paquete.



BIBLIOTECA
CAMPUS
PEÑAS

Queueing strategy: fifo
Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 60 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
1349 packets output, 102524 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.2 is up, line protocol is up (connected)
Hardware is PQUICC_FEC, address is 0060.3e62.6c01 (bia 0060.3e62.6c01)
Internet address is 192.168.5.97/28
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 203
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 52 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
28 packets output, 2128 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out



3.70.- COMANDO SHOW INTERFACES EN EL ROUTER TES-1

```
TES-1#show interfaces
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0060.70ad.9301 (bia 0060.70ad.9301)
  Internet address is 192.168.1.129/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 8 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    4 packets output, 304 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.2 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0060.70ad.9301 (bia 0060.70ad.9301)
  Internet address is 192.168.3.1/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 202
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last clearing of "show interface" counters never
FastEthernet0/0.3 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0060.70ad.9301 (bia 0060.70ad.9301)
  Internet address is 192.168.3.33/28
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 201
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last clearing of "show interface" counters never
```



3.71.- COMANDO SHOW INTERFACES EN EL ROUTER UEES

UEES#show interfaces

FastEthernet0/0 is up, line protocol is up (connected)

Hardware is Lance, address is 000a.41e5.4401 (bia 000a.41e5.4401)

Internet address is 192.168.6.1/29

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00,

Last input 00:00:08, output 00:00:05, output hang never

Last clearing of "show interface" counters never

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 79 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 input packets with dribble condition detected

18 packets output, 3540 bytes, 0 underruns

0 output errors, 0 collisions, 1 interface resets

0 babbles, 0 late collision, 0 deferred

0 lost carrier, 0 no carrier

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/0.2 is up, line protocol is up (connected)

Hardware is PQUICC_FEC, address is 000a.41e5.4401 (bia 000a.41e5.4401)

Internet address is 192.168.6.9/29

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation 802.1Q Virtual LAN, Vlan ID 106

ARP type: ARPA, ARP Timeout 04:00:00,

Last clearing of "show interface" counters never

FastEthernet0/0.3 is up, line protocol is up (connected)

Hardware is PQUICC_FEC, address is 000a.41e5.4401 (bia 000a.41e5.4401)

Internet address is 192.168.6.17/28

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation 802.1Q Virtual LAN, Vlan ID 107

ARP type: ARPA, ARP Timeout 04:00:00,

Last clearing of "show interface" counters never

3.72.- COMANDO SHOW INTERFACES EN EL ROUTER UEES-1

```
UEES-1#show interfaces
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0004.9ab2.9a01 (bia 0004.9ab2.9a01)
  Internet address is 192.168.1.65/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 122 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    23 packets output, 8270 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.2 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0004.9ab2.9a01 (bia 0004.9ab2.9a01)
  Internet address is 192.168.2.1/29
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 100
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last clearing of "show interface" counters never
FastEthernet0/0.3 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0004.9ab2.9a01 (bia 0004.9ab2.9a01)
  Internet address is 192.168.2.9/29
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 101
  ARP type: ARPA, ARP Timeout 04:00:00,
```



3.73.- COMANDO SHOW INTERFACES EN EL ROUTER UEES-2

UEES-2#show interfaces

```
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0001.c73a.6a01 (bia 0001.c73a.6a01)
  Internet address is 192.168.1.97/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 132 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    43 packets output, 17350 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.2 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0001.c73a.6a01 (bia 0001.c73a.6a01)
  Internet address is 192.168.2.33/28
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 103
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last clearing of "show interface" counters never
FastEthernet0/0.3 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0001.c73a.6a01 (bia 0001.c73a.6a01)
  Internet address is 192.168.2.49/28
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 104
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last clearing of "show interface" counters never
FastEthernet0/0.4 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0001.c73a.6a01 (bia 0001.c73a.6a01)
  Internet address is 192.168.2.65/28
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 105
```

```

ARP type: ARPA, ARP Timeout 04:00:00,
Last clearing of "show interface" counters never
FastEthernet0/1 is administratively down, line protocol is down (disabled)
Hardware is Lance, address is 0001.c73a.6a02 (bia 0001.c73a.6a02)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 input packets with dribble condition detected
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 2 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out

```

3.74.- COMANDO SHOW INTERFACES EN EL ROUTER ECOTEC

```

ECOTEC#show interfaces
FastEthernet0/0 is up, line protocol is up (connected)
Hardware is Lance, address is 0090.0ca2.a701 (bia 0090.0ca2.a701)
Internet address is 192.168.6.33/27
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 77 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 input packets with dribble condition detected
  115 packets output, 26030 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred

```



0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.2 is up, line protocol is up (connected)
Hardware is PQUICC_FEC, address is 0090.0ca2.a701 (bia 0090.0ca2.a701)
Internet address is 192.168.6.65/27
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 306
ARP type: ARPA, ARP Timeout 04:00:00,
Last clearing of "show interface" counters never
FastEthernet0/0.3 is up, line protocol is up (connected)
Hardware is PQUICC_FEC, address is 0090.0ca2.a701 (bia 0090.0ca2.a701)
Internet address is 192.168.6.97/27
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q Virtual LAN, Vlan ID 307
ARP type: ARPA, ARP Timeout 04:00:00,
Last clearing of "show interface" counters never
FastEthernet0/1 is administratively down, line protocol is down (disabled)
Hardware is Lance, address is 0090.0ca2.a702 (bia 0090.0ca2.a702)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

3.75.- COMANDO SHOW INTERFACES EN EL ROUTER ECOTEC-1

```
ECOTEC-1#show interfaces
FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0090.0c6a.d201 (bia 0090.0c6a.d201)
  Internet address is 192.168.1.161/27
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 120 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    112 packets output, 46480 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
FastEthernet0/0.2 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0090.0c6a.d201 (bia 0090.0c6a.d201)
  Internet address is 192.168.4.1/29
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 300
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last clearing of "show interface" counters never
FastEthernet0/0.3 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0090.0c6a.d201 (bia 0090.0c6a.d201)
  Internet address is 192.168.4.9/29
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 301
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last clearing of "show interface" counters never
FastEthernet0/0.4 is up, line protocol is up (connected)
  Hardware is PQUICC_FEC, address is 0090.0c6a.d201 (bia 0090.0c6a.d201)
  Internet address is 192.168.4.17/28
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID 302
```



ARP type: ARPA, ARP Timeout 04:00:00,
Last clearing of "show interface" counters never
FastEthernet0/1 is administratively down, line protocol is down (disabled)
Hardware is Lance, address is 0090.0c6a.d202 (bia 0090.0c6a.d202)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Serial1/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 192.168.1.30/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 114 bits/sec, 0 packets/sec
5 minute output rate 40 bits/sec, 0 packets/sec
194 packets input, 44900 bytes, 0 no buffer
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
114 packets output, 15820 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out



3.76.- COMANDO SHOW INTERFACES EN EL ROUTER ECOTEC-2

ECOTEC-2#show interfaces

FastEthernet0/0 is up, line protocol is up (connected)

Hardware is Lance, address is 00e0.f976.b501 (bia 00e0.f976.b501)

Internet address is 192.168.1.193/27

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00,

Last input 00:00:08, output 00:00:05, output hang never

Last clearing of "show interface" counters never

Queueing strategy: fifo

Output queue :0/40 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 132 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 input packets with dribble condition detected

123 packets output, 52430 bytes, 0 underruns

0 output errors, 0 collisions, 1 interface resets

0 babbles, 0 late collision, 0 deferred

0 lost carrier, 0 no carrier

0 output buffer failures, 0 output buffers swapped out

FastEthernet0/0.2 is up, line protocol is up (connected)

Hardware is PQUICC_FEC, address is 00e0.f976.b501 (bia 00e0.f976.b501)

Internet address is 192.168.4.33/27

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation 802.1Q Virtual LAN, Vlan ID 303

ARP type: ARPA, ARP Timeout 04:00:00,

Last clearing of "show interface" counters never

FastEthernet0/0.3 is up, line protocol is up (connected)

Hardware is PQUICC_FEC, address is 00e0.f976.b501 (bia 00e0.f976.b501)

Internet address is 192.168.4.65/28

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation 802.1Q Virtual LAN, Vlan ID 304

ARP type: ARPA, ARP Timeout 04:00:00,

Last clearing of "show interface" counters never

FastEthernet0/0.4 is up, line protocol is up (connected)

Hardware is PQUICC_FEC, address is 00e0.f976.b501 (bia 00e0.f976.b501)

Internet address is 192.168.4.81/28

MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation 802.1Q Virtual LAN, Vlan ID 305

```
ARP type: ARPA, ARP Timeout 04:00:00,  
Last clearing of "show interface" counters never  
FastEthernet0/1 is administratively down, line protocol is down (disabled)  
Hardware is Lance, address is 00e0.f976.b502 (bia 00e0.f976.b502)  
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00,  
Last input 00:00:08, output 00:00:05, output hang never  
Last clearing of "show interface" counters never  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 0 bits/sec, 0 packets/sec  
0 packets input, 0 bytes, 0 no buffer  
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort  
0 input packets with dribble condition detected  
0 packets output, 0 bytes, 0 underruns  
0 output errors, 0 collisions, 2 interface resets  
0 babbles, 0 late collision, 0 deferred  
0 lost carrier, 0 no carrier  
0 output buffer failures, 0 output buffers swapped out
```

3.77.- COMANDO SHOW INTERFACES EN EL ROUTER ISP

ISP#SHOW INTERfACES

```
FastEthernet0/0 is up, line protocol is up (connected)  
Hardware is Lance, address is 0060.2f82.3401 (bia 0060.2f82.3401)  
Internet address is 200.10.1.33/27  
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255  
Encapsulation ARPA, loopback not set  
ARP type: ARPA, ARP Timeout 04:00:00,  
Last input 00:00:08, output 00:00:05, output hang never  
Last clearing of "show interface" counters never  
Queueing strategy: fifo  
Output queue :0/40 (size/max)  
5 minute input rate 0 bits/sec, 0 packets/sec  
5 minute output rate 50 bits/sec, 0 packets/sec  
0 packets input, 0 bytes, 0 no buffer  
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort  
0 input packets with dribble condition detected  
137 packets output, 24170 bytes, 0 underruns  
0 output errors, 0 collisions, 1 interface resets  
0 babbles, 0 late collision, 0 deferred
```



0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
FastEthernet0/1 is administratively down, line protocol is down (disabled)
Hardware is Lance, address is 0060.2f82.3402 (bia 0060.2f82.3402)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
Serial1/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 200.10.1.2/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 64 bits/sec, 0 packets/sec
5 minute output rate 81 bits/sec, 0 packets/sec
501 packets input, 42984 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
506 packets output, 41664 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out

3.78.- COMANDO SHOW PROTOCOLS EN EL ROUTER TES

Muestra el estado global e interfaz de cualquier protocolo de capa 3 que haya sido configurado.

TES#show protocols

Global values:

Internet Protocol routing is enabled

FastEthernet0/0 is up, line protocol is up

Indica que la línea esta en estado levantado

Estado

Tipo y número de interfaz

Internet address is 192.168.5.65/27

FastEthernet0/0.2 is up, line protocol is up

Internet address is 192.168.5.97/28

FastEthernet0/0.3 is up, line protocol is up

Internet address is 192.168.5.113/28

FastEthernet0/0.4 is up, line protocol is up

Internet address is 192.168.5.129/28

FastEthernet0/0.5 is up, line protocol is up

Internet address is 192.168.5.145/28

FastEthernet0/1 is administratively down, line protocol is down

Serial1/0 is up, line protocol is up

Internet address is 192.168.1.18/30

Serial1/1 is up, line protocol is up

Internet address is 192.168.1.22/30

Serial1/2 is up, line protocol is up

Internet address is 192.168.1.25/30

Serial1/3 is up, line protocol is up

Internet address is 200.10.1.1/30



3.79.- COMANDO SHOW PROTOCOLS EN EL ROUTER TES-1

TES-1#show protocols

Global values:

Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.129/27
FastEthernet0/0.2 is up, line protocol is up
Internet address is 192.168.3.1/27
FastEthernet0/0.3 is up, line protocol is up
Internet address is 192.168.3.33/28
FastEthernet0/0.4 is up, line protocol is up
Internet address is 192.168.3.49/28
FastEthernet0/1 is administratively down, line protocol is down
Serial1/0 is up, line protocol is up
Internet address is 192.168.1.26/30
Serial1/1 is administratively down, line protocol is down

3.80.- COMANDO SHOW PROTOCOLS EN EL ROUTER UEES

UEES#SHOW PROTOCOLS

Global values:

Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.6.1/29
FastEthernet0/0.2 is up, line protocol is up
Internet address is 192.168.6.9/29
FastEthernet0/0.3 is up, line protocol is up
Internet address is 192.168.6.17/28
FastEthernet0/1 is administratively down, line protocol is down
Serial1/0 is up, line protocol is up
Internet address is 192.168.1.2/30
Serial1/1 is up, line protocol is up
Internet address is 192.168.1.10/30
Serial1/2 is up, line protocol is up
Internet address is 192.168.1.13/30
Serial1/3 is up, line protocol is up
Internet address is 192.168.1.17/30



3.81.- COMANDO SHOW PROTOCOLS EN EL ROUTER UEES-1

UEES-1#SHOW PROTOCOLS

Global values:

Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.65/27
FastEthernet0/0.2 is up, line protocol is up
Internet address is 192.168.2.1/29
FastEthernet0/0.3 is up, line protocol is up
Internet address is 192.168.2.9/29
FastEthernet0/0.4 is up, line protocol is up
Internet address is 192.168.2.17/28
FastEthernet0/1 is administratively down, line protocol is down
Serial1/0 is up, line protocol is up
Internet address is 192.168.1.5/30
Serial1/1 is up, line protocol is up
Internet address is 192.168.1.1/30
Serial1/2 is administratively down, line protocol is down

3.82.- COMANDO SHOW PROTOCOLS EN EL ROUTER UEES-2

UEES-2#SHOW PROTOCOLS

Global values:

Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.97/27
FastEthernet0/0.2 is up, line protocol is up
Internet address is 192.168.2.33/28
FastEthernet0/0.3 is up, line protocol is up
Internet address is 192.168.2.49/28
FastEthernet0/0.4 is up, line protocol is up
Internet address is 192.168.2.65/28
FastEthernet0/1 is administratively down, line protocol is down
Serial1/0 is up, line protocol is up
Internet address is 192.168.1.9/30
Serial1/1 is up, line protocol is up
Internet address is 192.168.1.6/30
Serial1/2 is administratively down, line protocol is down

3.83.- COMANDO SHOW PROTOCOLS EN EL ROUTER ECOTEC

ECOTEC#SHOW PROTOCOLS

Global values:

Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.6.33/27
FastEthernet0/0.2 is up, line protocol is up
Internet address is 192.168.6.65/27
FastEthernet0/0.3 is up, line protocol is up
Internet address is 192.168.6.97/27
FastEthernet0/1 is administratively down, line protocol is down
Serial1/0 is up, line protocol is up
Internet address is 192.168.1.14/30
Serial1/1 is up, line protocol is up
Internet address is 192.168.1.29/30
Serial1/2 is up, line protocol is up
Internet address is 192.168.1.33/30
Serial1/3 is up, line protocol is up
Internet address is 192.168.1.21/30
Vlan1 is administratively down, line protocol is down

3.84.- COMANDO SHOW PROTOCOLS EN EL ROUTER ECOTEC-1

ECOTEC-1#SHOW PROTOCOLS

Global values:

Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.161/27
FastEthernet0/0.2 is up, line protocol is up
Internet address is 192.168.4.1/29
FastEthernet0/0.3 is up, line protocol is up
Internet address is 192.168.4.9/29
FastEthernet0/0.4 is up, line protocol is up
Internet address is 192.168.4.17/28
FastEthernet0/1 is administratively down, line protocol is down
Serial1/0 is up, line protocol is up
Internet address is 192.168.1.30/30
Serial1/1 is up, line protocol is up
Internet address is 192.168.1.38/30
Serial1/2 is administratively down, line protocol is down



3.85.- COMANDO SHOW PROTOCOLS EN EL ROUTER ECOTEC-2

ECOTEC-2# SHOW PROTOCOLS

Global values:

Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.193/27
FastEthernet0/0.2 is up, line protocol is up
Internet address is 192.168.4.33/27
FastEthernet0/0.3 is up, line protocol is up
Internet address is 192.168.4.65/28
FastEthernet0/0.4 is up, line protocol is up
Internet address is 192.168.4.81/28
FastEthernet0/1 is administratively down, line protocol is down
Serial1/0 is up, line protocol is up
Internet address is 192.168.1.34/30
Serial1/1 is administratively down, line protocol is down
Serial1/2 is up, line protocol is up
Internet address is 192.168.1.37/30
Serial1/3 is administratively down, line protocol is down

3.86.- COMANDO SHOW PROTOCOLS EN EL ROUTER ISP

ISP#SHOW PROTOCOLS

Global values:

Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
Internet address is 200.10.1.33/27
FastEthernet0/1 is administratively down, line protocol is down
Serial1/0 is up, line protocol is up
Internet address is 200.10.1.2/30
Serial1/1 is administratively down, line protocol is down

3.87.2.- ACTIVAR EL MODO DE ADMINISTRACIÓN REMOTA

```
TES(config)# line vty 0 4
```

Diagrama de anotación del comando anterior:

- Una línea vertical con una flecha hacia abajo apunta a "Comando" desde el texto "line".
- Una línea vertical con una flecha hacia abajo apunta a "# de conexiones concurrentes remotas" desde el texto "vty".
- Una línea vertical con una flecha hacia abajo apunta a "Conexiones Remotas" desde el texto "0 4".

```
TES(config-line)#password cisco
TES(config-line)#login
TES(config-line)#exit
```

3.88.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER TES-1

```
TES-1(config)#line console 0
TES-1(config-line)#password cisco
TES-1(config-line)#login
TES-1(config-line)#exit
TES-1(config)#enable secret cisco
TES-1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
TES-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
TES-1(config)#line vty 0 4
TES-1(config-line)#password cisco
TES-1(config-line)#login
TES-1(config-line)#exit
```



3.89.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER UEES

```
UEES(config)#line console 0
UEES(config-line)#password cisco
UEES(config-line)#login
UEES(config-line)#exit
UEES(config)#enable secret cisco
UEES(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
UEES#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UEES(config)#line vty 0 4
UEES(config-line)#password cisco
UEES(config-line)#login
UEES(config-line)#exit
```

3.90 .- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER UEES-1

```
UEES-1(config)#line console 0
UEES-1(config-line)#password cisco
UEES-1(config-line)#login
UEES-1(config-line)#exit
UEES-1(config)#enable secret cisco
UEES-1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
UEES-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UEES-1(config)#line vty 0 4
UEES-1(config-line)#password cisco
UEES-1(config-line)#login
UEES-1(config-line)#exit
```



BIBLIOTECA
CAMPUS
PEÑAS

3.91.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER UEES-2

```
UEES-2(config)#line console 0
UEES-2(config-line)#password cisco
UEES-2(config-line)#login
UEES-2(config-line)#exit
UEES-2(config)#enable secret cisco
UEES-2(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
UEES-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UEES-2(config)#line vty 0 4
UEES-2(config-line)#password cisco
UEES-2(config-line)#login
UEES-2(config-line)#exit
```

3.92.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER ECOTEC

```
ECOTEC(config)#line console 0
ECOTEC(config-line)#password cisco
ECOTEC(config-line)#login
ECOTEC(config-line)#exit
ECOTEC(config)#enable secret cisco
ECOTEC(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
ECOTEC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ECOTEC(config)#line vty 0 4
ECOTEC(config-line)#password cisco
ECOTEC(config-line)#login
ECOTEC(config-line)#exit
```

3.93.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER ECOTEC-1

```
ECOTEC-1(config)#line console 0
ECOTEC-1(config-line)#password cisco
ECOTEC-1(config-line)#login
ECOTEC-1(config-line)#exit
ECOTEC-1(config)#enable secret cisco
ECOTEC-1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
ECOTEC-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ECOTEC-1(config)#line vty 0 4
ECOTEC-1(config-line)#password cisco
ECOTEC-1(config-line)#login
ECOTEC-1(config-line)#exit
```

3.94.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER ECOTEC-2

```
ECOTEC-2(config)#line console 0
ECOTEC-2(config-line)#password cisco
ECOTEC-2(config-line)#login
ECOTEC-2(config-line)#exit
ECOTEC-2(config)#enable secret cisco
ECOTEC-2(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
ECOTEC-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ECOTEC-2(config)#line vty 0 4
ECOTEC-2(config-line)#password cisco
ECOTEC-2(config-line)#login
ECOTEC-2(config-line)#exit
```



BIBLIOTECA
CAMPUS
PEÑAS

3.95.- ASIGNACIÓN DE CONTRASEÑA PARA PROTEGER EL ACCESO AL ROUTER ISP

```
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#enable secret cisco
ISP(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
```



3.96.- LISTAS DE CONTROL DE ACCESO

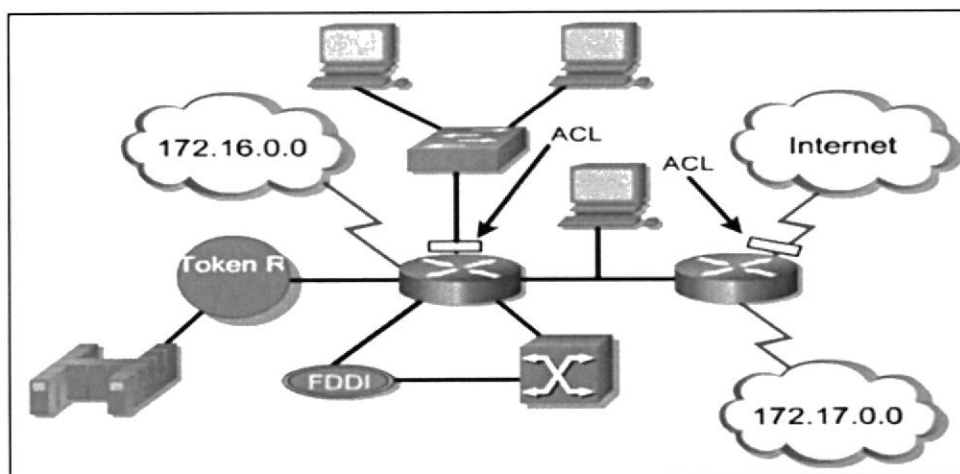


Figura 3 -11: ACL

Las listas de acceso son el mecanismo por excelencia para seleccionar tráfico. Una vez que un conjunto de paquetes ha sido seleccionado el router puede realizar diversas tareas sobre ellos. Uno de los usos más extendidos de las listas de acceso es el de controlar el flujo de tráfico entrante y saliente de un router, pero hemos visto otras muchas aplicaciones prácticas. El proceso de configuración de listas de acceso consta de dos pasos generales, la creación de la lista de acceso en si y su aplicación en la interfaz correspondiente (o, de forma más general, en el proceso deseado). Hay que tomar unas precauciones generales a la hora de aplicar listas de acceso. Hay tres mecanismos para prevenir o corregir los problemas derivados de una mala configuración, recuerde: reload, reset y loopback.

La siguiente tabla muestra los rangos de listas de acceso numeradas:

- IP estándar: 1-99 y 1300-1999
- IP extendida: 100-199 y 2000-2699

3.96.1.-Estructura Básica

Las reglas que componen las listas de acceso tienen tres partes: un número que identifica la lista, una instrucción deny o permit y una condición
 access-list número_identificador [permit|deny] condición
 El número utilizado para identificar una lista concreta debe ser seleccionado de un rango numérico acorde con el uso concreto de la lista.



BIBLIOTECA
CAMPUS
PEÑAS

Nos centraremos especialmente en las listas IP, en sus formas Estándar y Extendida.

PROTOCOLO	TIPO	RANGO	FILTRA POR
IP	Estándar	1-99 y 1300-1999	el origen
IP	Extendidas	100-199 y 2000-2699	El origen, destino, protocolo, puerto...
Ethernet	Código (Type)	200-299	el tipo de código Ethernet
DECnet	Protocol Suite	300-399	el Origen
Appletalk	Protocol Suite	600-699	el Origen
Ethernet	Direcciones	799-799	la dirección MAC
IPX	Estándar	800-899	el origen
IPX	Extendida	900-999	el origen, destino, protocolo, puerto...
IPX	SAP	1000-1099	tipo de aplicación (SAP, Service Access Point)

Tabla 3 -8: Numeración de las Listas de Accesos

3.96.2.-MÁSCARA DE WILDCARD

Las listas de acceso estándar y extendidas utilizan una máscara de WILDCARD. Al igual que un a dirección IP, una máscara de wildcard es una cantidad de 32 bits escrita en un formato decimal con puntos. La máscara wildcard le indica al Router qué bits de la dirección usar en las comparaciones. Los bits de direcciones correspondientes a los bits de máscara wildcard establecidas en 1 se ignoran en las comparaciones, mientras que los bits de direcciones de máscara wildcard establecidos en 0 se usan en las comparaciones.

3.96.3.-TIPO DE ACL: ESTÁNDAR

Las listas de acceso estándar permiten o prohíben paquetes en base a la dirección IP de origen del paquete. El resultado es el permiso o la denegación de la salida del paquete por parte del protocolo, basándose en la dirección IP de la red-subred-host de origen.

Sintaxis:

access-list(número) (deny|permit) (ip origen) (wildcard origen)

3.96.3.1.- COMO SE CONFIGURAN ACL ESTÁNDAR

Los pasos generales para configurar ACLs son 3:

- Crear la ACL en modo de configuración global
- Aplicar la ACL en una interfaz indicando la dirección del tráfico al que se le va a aplicar
- Verificar su funcionamiento

La creación de la ACL consiste en crear una secuencia de reglas con un mismo identificador, cuyo orden filtre el tráfico según los objetivos. Cada regla tiene la forma:

```
access-list <n> [ permit | deny ] <referencia1> <wildcard1>
```

Donde n es el número que identifica la ACL (0 a 99 ó 1300 a 1999 para ACLs estándar) y referenciaN/wildcardN son los pares con los que se compararán los paquetes para aplicarles la acción. Entonces una ACL tiene la forma:

```
access-list <n> permit <referencia1> <wildcard1>
```

```
access-list <n> deny <referencia2> <wildcard2>
```

Como todas las reglas coinciden en el número (n), la ACL está compuesta por todas las reglas listadas. Para simplificar, puse permit y deny pero en las reglas se puede elegir cualquiera de las dos según los objetivos perseguidos. Todas las ACLs terminan implícitamente en una regla deny any, es decir, al final de la lista, cualquier paquete que no haya correspondido con ninguna regla se va a descartar por defecto.

Para aplicar una ACL, ésta ya debe estar creada. Las listas de acceso se aplican en una interfaz, por lo tanto hay que ingresar en modo de interfaz y el comando tiene la forma

```
ip access-group <n> [in | out]
```

Donde n es el número común a todas las reglas de la ACL y las palabras in/out indican en qué sentido se aplicarán las reglas y esto tiene importantes implicaciones: el tráfico en una dirección tiene ciertas direcciones IP origen pero en la otra dirección éstas mismas direcciones serán IP destino.

```
interface serial 0/0
```

```
ip access-group <n> [in|out]
```

Finalmente verificar la ACL se hace con varios comandos.

Uno es `show access-list`, que muestra todas las listas de acceso activas y cuántos paquetes han correspondido (match) con cada regla.

El comando que muestra si una interfaz tiene una ACL aplicada y en qué dirección es `show ip interface`, este comando muestra mucha información, por la mitad de toda esa información dice inbound ACL Outbound ACL.

```
show access-list
```

```
show ip interface serial 0/0
```

3.96.4.-TIPO DE ACL: EXTENDIDA

Las listas de acceso extendidas comprueban tanto la dirección de origen como la de destino de cada paquete. También pueden verificar protocolos especificados, números de puerto y otros parámetros. Una vez creada, una ACL debe asociarse a una interfaz de la siguiente manera:

Sintaxis:

```
access-list (número) (deny-permit) (protocolo) (IP origen) (wildcard origen) (IP destino) (wildcard destino) [(operador) (operando)]
```

3.96.5.- LISTA DE ACCESO ENTRANTE

Los paquetes entrantes son procesados antes de ser enrutados a una interfaz de salida, si el paquete pasa las pruebas de filtrado, será procesado para su enrutamiento (evita la sobrecarga asociada a las búsquedas en las tablas de enrutamiento si el paquete ha de ser descartado por las pruebas de filtrado).

3.96.6. -LISTA DE ACCESO SALIENTE

Los paquetes entrantes son enrutados a la interfaz de salida y después son procesados por medio de la lista de acceso de salida antes de su transmisión. Las listas de acceso expresan el conjunto de reglas que proporcionan un control añadido para los paquetes que entran en interfaces de entrada, paquetes que se transmiten por el router, y paquetes que salen de las interfaces de salida del router. Las listas de acceso no actúan sobre paquetes originados en el propio router, como las actualizaciones de enrutamiento a las sesiones Telnet salientes.

3.96.7. FUNCIONAMIENTO DE LAS ACL

El orden en el que se ubican las sentencias de la ACL es importante. El software Cisco IOS verifica si los paquetes cumplen cada sentencia de condición, en orden, desde la parte superior de la lista hacia abajo.

Una vez que se encuentra una coincidencia, se lleva a cabo la acción de aceptar o rechazar y no se verifican otras sentencias ACL. Si una sentencia de condición que permite todo el tráfico está ubicada en la parte superior de la lista, no se verifica ninguna sentencia que esté por debajo.

3.96.8.-QUE CONSIDERACIONES HAY QUE TENER PARA INSTALAR ACLS

3.96.8.1.-DENEGACIÓN POR DEFECTO Y LOG

La primera consideración importante es tener en cuenta siempre que las listas de acceso terminan en denegación por defecto, por lo tanto, si una ACL sólo tiene reglas de denegación lo único que logra es denegar TODO el tráfico.

Una ACL debe tener siempre por lo menos una regla de permitir. Algunos administradores prefieren poner una regla final, sea deny any o permit any de manera explícita para poder ver con show access-list cuántos paquetes se han filtrado por la última regla o mejor, cuántos paquetes no han correspondido con ninguna otra regla. Otros administradores usan la lista de acceso para recolectar información sobre el tráfico de la red, combinando reglas que terminan con la palabra log que hace que la ACL genere entradas de registro como si fueran mensajes del sistema. Combinar reglas permit con log hace que la acl evidencie algún tráfico que se necesita saber cómo se está comportando.

3.97.- REGLAS ESPECIFICAS Y GENERALES

Como cada regla se verifica en secuencia comenzando por la primera, si una regla es general, es decir, abarca más direcciones o flujos de datos que otra, ésta regla debería ir después de las más específicas. Para ilustrar esto, observe el siguiente ejemplo: yo quiero bloquear un host de la red 192.168.1.0/24 pero permitir el resto de esta red, necesito dos reglas: permitir la red y denegar el host, como la regla para la red es más general e incluye el host mismo, ponerla de primera va a tener como efecto que nunca se mire la regla que dice denegar el host, porque siempre aplicará la primera y no se

verificarán más reglas, permitiendo al host transmitir información cuando el objetivo era denegar precisamente ese host.

La regla se debería escribir de la siguiente manera:

```
access-list 1 deny 192.168.1.1 0.0.0.0
```

```
access-list 1 permit 192.168.1.0 0.0.0.255
```

La anterior ACL tiene como resultado, cuando se aplica a una interfaz, que sólo el tráfico perteneciente a la red 192.168.1.0, excepto el host 192.168.1.1, puede salir por la interfaz en la que se aplique. Lo anterior siempre y cuando, el tráfico tenga como orígenes éstas direcciones.

Finalmente, cierto tráfico proveniente del enrutador no pasa por las listas de acceso, por ejemplo, el acceso a VTY (telnet/ssh) al enrutador no es examinado por las ACL, por lo tanto hay que poner una regla especial para este tráfico.

La regla se llama access-group <n> y debe ser ACL estándar. Una regla de este tipo limita el acceso por telnet al enrutador sólo a los hosts que correspondan a la lista especificada.

3.98.-TELNET

Es un protocolo de comunicación que permite al usuario una computadora con conexión a internet establecer una sesión como terminal remoto de otro sistema de la red. Si el usuario no dispone de una cuenta en el ordenador o compilador remoto, puede conectarse como usuario anónimo o también por (www).

Puerto 23 Realizar conexiones Telnet o rsh mediante túneles SSH no tiene ningún sentido, ya que SSH es ya el protocolo para shell remota de forma segura. En escenarios realmente extraños podría emplearse eventualmente para acceder, por ejemplo, desde un host de Internet a un servidor de una extranet que sólo tiene el puerto 23 abierto. En este caso podría establecerse una conexión SSH segura a un host en la frontera de la extranet con Internet, y de ahí realizar la comunicación al puerto 23 de forma insegura (suponiendo que el interior de la extranet no sea conflictivo).

3.99.-PING (ICMP)

Es una petición al emisor para verificar o comprobar el estado del enlace trabajar con un paquete de comunicaciones llamado echo.

3.100.-FTP

Es un protocolo de transferencia de archivos que se utiliza en internet y otras redes para transferir archivos entre servidores o entre un usuario o un servidor.

Puerto 21 A nivel general, FTP tiene algunos aspectos reseñables:

- FTP tiene dos conexiones distintas: una para los comandos (control) y otra para la transmisión de ficheros (datos). La manera estándar de hacer un túnel SSH en una conexión FTP se centra únicamente en la protección de la conexión de control, es decir, del login/password de la sesión y de los comandos utilizados. Los ficheros se intercambiarán sin utilizar el túnel SSH.
- Es necesario usar el modo pasivo ("passive mode") para la conexión de datos o de lo contrario el servidor FTP tratará de conectar con la máquina remota que se encuentre al otro lado del túnel SSH (típicamente la propia máquina servidora) y no con la máquina cliente que realiza la petición.
- Al usar el modo pasivo, la conexión de datos provendrá de una dirección IP distinta a la usada en la conexión de datos. Esto suele ser un problema para la gran mayoría de servidores FTP, ya que por defecto deniegan este hecho como medida de seguridad (para prevenir "hijacking" o "spoofing" en las conexiones). Deberemos, por lo tanto, configurar el servidor FTP para permitir esto.

Debido a estos problemas de seguridad, y gracias a las nuevas prestaciones de la versión 2 de SSH, el SSH tunneling en conexiones FTP está siendo reemplazado por conexiones "sftp", que proporcionan protección tanto de datos como de comandos, sin necesidad de modificar el servidor FTP existente.

Ejemplos:

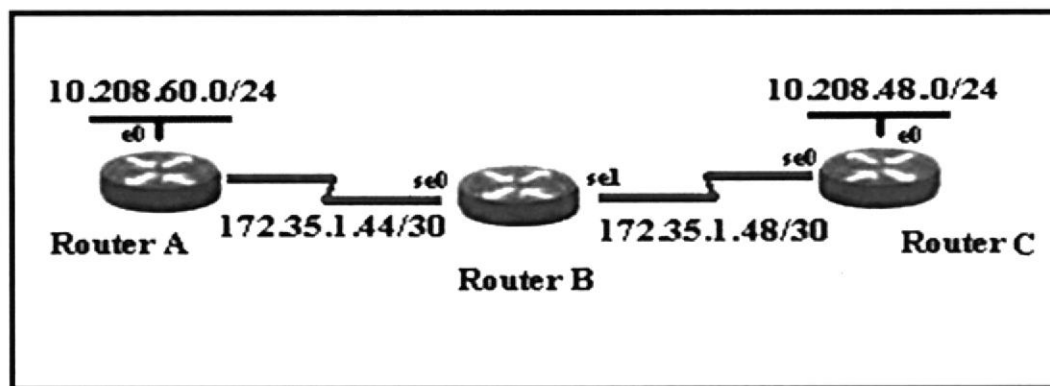


Figura 3 -12: SSH

Concretamente asignaremos las siguientes direcciones IPs por interfaz:

```
10.208.60.1/24 eth ---[router A]--- se0 172.35.1.46/30 --WAN LINK-- 172.35.1.45/30
se0 ---[router B]--- se1 172.35.1.49/30 --WAN LINK-- 172.35.1.50/30 se0 ---[router
C]--- eth 10.208.48.1/24
```

3.100.1.-CONTROL SENCILLO DE TRAFICO MEDIANTE LISTAS DE ACCESO

Queremos filtrar en el router B aquellos paquetes que provienen de las máquinas 10.208.60.10 y 10.208.60.25, pertenecientes a la red local del router

```
A
access-list 1 deny 10.208.60.10 0.0.0.0
access-list 1 deny 10.208.60.25 0.0.0.0
access-list 1 permit any
```

Por cierto, podemos configurar lo anterior de una forma más compacta mediante el uso de host:

```
access-list 1 deny host 10.208.60.10
access-list 1 deny host 10.208.60.25
access-list 1 permit any
algo).
```

```
access-list 1 deny 10.208.60.10 0.0.0.0
access-list 1 deny 10.208.60.25 0.0
```

3.101.-SSH

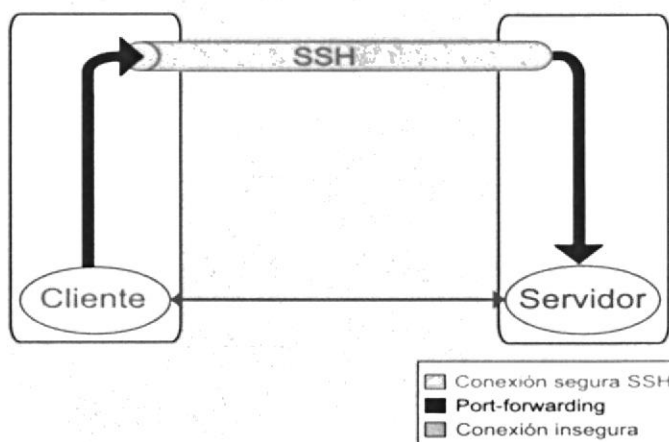


Figura 3 -13: SSH

SSH es un protocolo seguro y un conjunto de herramientas para reemplazar otras más comunes (inseguras). Fue diseñado desde el principio para ofrecer un máximo de seguridad y permitir el acceso remoto a servidores de forma segura. SSH se puede utilizar para asegurar cualquier tráfico basado en red, configurándolo como un pipe (p. ej., vinculándolo a cierto puerto en ambos extremos).

Además de esto, los componentes del servidor se ejecutan en la mayoría de sistemas UNIX, y NT, y los componentes del cliente se ejecutan en casi cualquier cosa.

No existen tantos problemas con el SSH per se como existen con telnet, todo el tráfico de la sesión va cifrado y el intercambio de llaves se hace de forma relativamente segura (opcionalmente se pueden precargar las llaves al final, para evitar que sean transmitidas y ser vulnerables a ataques tipo 'man in the middle', hombre de por medio).

SSH se suele ejecutar como un demonio, y se puede cerrar utilizando el fichero `sshd_config`. También se puede ejecutar `sshd` desde `inetd`, y de tal forma utilizar `TCP_WRAPPERS`, y por defecto los rpm's de `ftp://ftp.replay.com/` tienen la opción de `TCP_WRAPPERS` compilada. De modo que utilizar "`sshd: blahblah`" en `hosts.allow` y `hosts.deny` te permite restringir con facilidad el acceso a ssh. Por favor, ten en cuenta que las primeras versiones de ssh contienen bugs, y se han hackeado sitios (generalmente con ataques tipo 'man in the middle' o problemas de desbordamientos de pila en el código ssh), pero la última versión de ssh tiene en cuenta estos problemas.

Lo que sigue es un fichero `sshd-config` típico:

Port 22

se ejecuta en el puerto 22, el standard

ListenAddress 0.0.0.0

escucha en todos los interfaces, quizás sería preferible vincularlo

sólo a un cortafuegos interno, etc.

3.101.1.-Características de SSH

- Para establecer una sesión SSH es necesario autenticación. Si utilizamos autenticación por `passphrase` (además de las correspondientes claves RSA o métodos similares), deberemos prever este hecho en nuestros scripts o nuestras sesiones interactivas o de lo contrario no podremos establecer el túnel SSH.

- Las reglas de protección en `ipchains` o `iptables`. Si tenemos configuradas reglas para bloquear las conexiones entrantes, necesitaremos establecer una excepción a esas reglas para que funcione el "port-forwarding" en local, con algo parecido a esto:

```
# iptables -A INPUT -s 127.0.0.1 -d 127.0.0.1 -i lo -j ACCEPT
# iptables -A OUTPUT -s 127.0.0.1 -d 127.0.0.1 -o lo -j ACCEPT
```



BIBLIOTECA
CAMPUS
PEÑAS

- Si vamos a utilizar puertos privilegiados en nuestra máquina local (con privilegios de root), deberemos tener en cuenta que esos puertos no se hayan empleado para conexiones entrantes. Si, por ejemplo, queremos hacer "port-forwarding" del puerto 110 para que nuestros usuarios puedan acceder de manera segura a su servidor de correo, deberemos tener cuidado ante un posible servidor POP3 escuchando el puerto 110 en nuestra máquina. Revisad vuestras configuraciones de los demonios que están escuchando puertos y en especial el fichero "/etc/inetd.conf".

- Si queremos establecer un túnel para cada conexión y destruirlo cuando ésta acabe, podemos usar una nueva opción incluida en el último parche (-S) para fijar un tiempo de espera o "delay" en el que se atenderán las conexiones SSH. Cuando ese tiempo expire, no se atenderán más conexiones y el comando finalizará cuando todas la conexiones hayan concluido (esto es importante, no termina cuando se consuma el tiempo fijado). Si disponemos de una versión antigua de SSH, podemos hacer esto mismo de la siguiente manera:

```
$ ssh -f -L 110:popmail.correo.net:110 usuario@popmail.correo.net sleep 30
```

esto sería equivalente a:

```
$ ssh -f -S 30 -L 110:popmail.correo.net:110 usuario@popmail.correo.net
```

Así estamos fijando un temporizador de 30 segundos para aceptar conexiones, finalizado el cual se esperará únicamente a que las conexiones ya establecidas terminen.

3.102.-FIREWALL

Un firewall es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red interna de los intrusos.

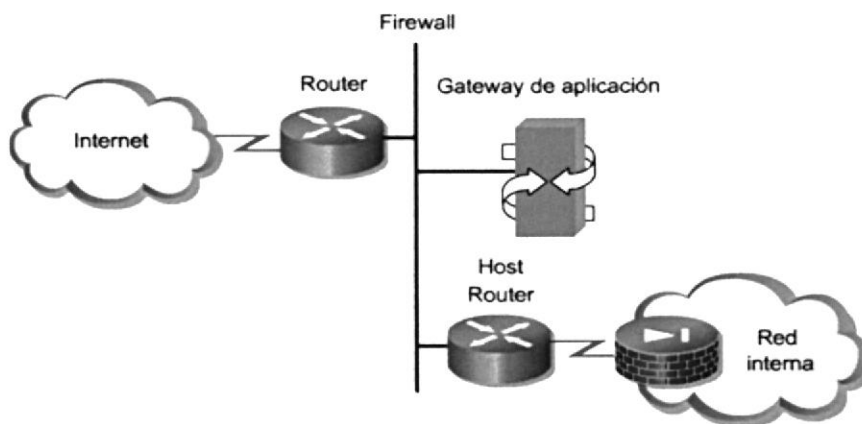


Figura 3 -14: Firewall en las ACL

Se deben utilizar ACL en los routers firewall, que a menudo se sitúan entre la red interna y una red externa, como Internet.

Se necesita configurar las ACL en routers fronterizos, que son aquellos situados en las fronteras de la red, para brindar mayor seguridad.

3.103.-PUERTOS

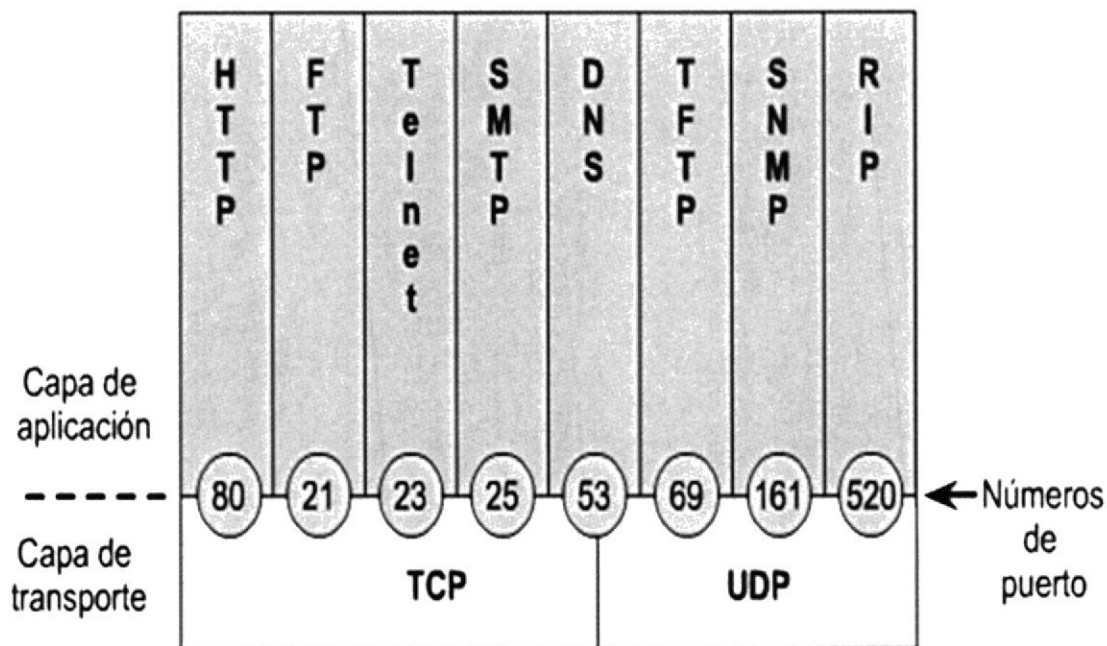


Figura 3 -15:Clases de Puerto Usados en las ACL



BIBLIOTECA
CAMPUS
PEÑAS

3.104.-UBICACIÓN DE UNA ACL

La regla es colocar las ACL extendidas lo más cerca posible del origen del tráfico denegado. Las ACL estándar no especifican las direcciones destino, de modo que se deben colocar lo más cerca posible del destino.

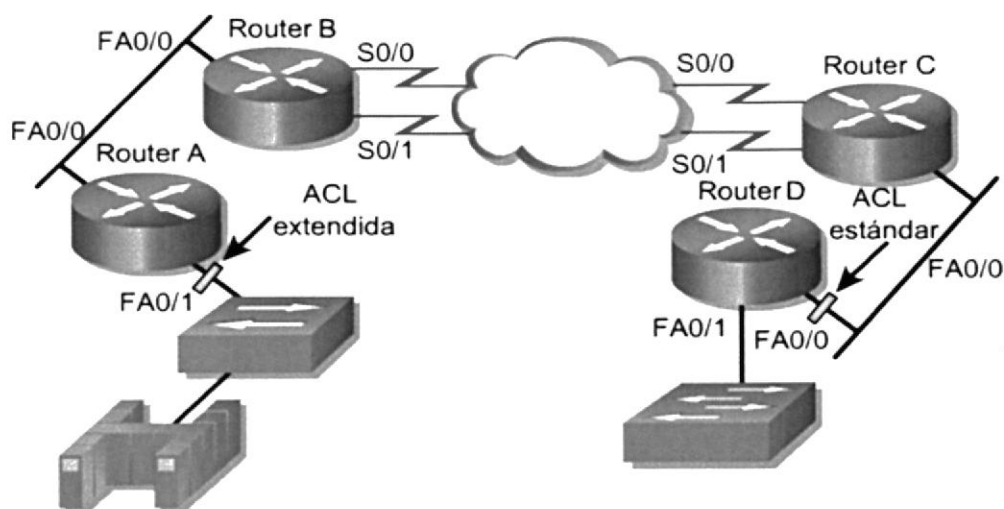


Figura 3 -16: Ejemplo de Ubicación de una ACL



BIBLIOTECA
CAMPUS
PEÑAS

3.105.-CREACIÓN DE LAS ACL

Las ACL se crean en el modo de configuración global. Existen varias clases diferentes de ACLs: estándar, extendidas, IPX, AppleTalk, entre otras.

Cuando configure las ACL en el router, cada ACL debe identificarse de forma única, asignándole un número. Este número identifica el tipo de lista de acceso creado y debe ubicarse dentro de un rango específico de números que es válido para ese tipo de lista.

3.106.-CREACIÓN DE ACCESS LIST EN EL ROUTER TES

TES(config)#access-list 100 permit icmp host 192.168.5.98 host 192.168.3.50 echo

Permite el paso de tráfico cuando hay una sesión establecida.

Host Destino

Host Origen

Protocolo

Permite acción del ping la acl

Número de la lista de acceso

Comando Para Creación de ACL en el router

```

TES(config)#access-list 100 permit icmp host 192.168.5.98 host 192.168.3.34 echo
TES(config)#access-list 100 permit icmp host 192.168.5.98 host 192.168.3.2 echo
TES(config)#access-list 100 permit icmp host 192.168.5.114 host 192.168.3.50 echo
TES(config)#access-list 100 permit icmp host 192.168.5.114 host 192.168.3.34 echo
TES(config)#access-list 100 permit icmp host 192.168.5.114 host 192.168.3.2 echo
TES(config)#access-list 100 permit icmp host 192.168.5.130 host 192.168.3.50 echo
TES(config)#access-list 100 permit icmp host 192.168.5.130 host 192.168.3.34 echo
TES(config)#access-list 100 permit icmp host 192.168.5.130 host 192.168.3.2 echo
TES(config)#access-list 100 permit icmp host 192.168.5.146 host 192.168.3.50 echo
TES(config)#access-list 100 permit icmp host 192.168.5.146 host 192.168.3.34 echo
TES(config)#access-list 100 permit icmp host 192.168.5.146 host 192.168.3.2 echo
TES(config)# access-list 101 permit icmp host 192.168.5.98 host 192.168.2.66 echo
TES(config)#access-list 101 permit icmp host 192.168.5.98 host 192.168.2.50 echo
TES(config)#access-list 101 permit icmp host 192.168.5.98 host 192.168.2.34 echo
TES(config)#access-list 101 permit icmp host 192.168.5.114 host 192.168.2.66 echo
TES(config)#access-list 101 permit icmp host 192.168.5.114 host 192.168.2.50 echo
TES(config)#access-list 101 permit icmp host 192.168.5.114 host 192.168.2.34 echo
TES(config)#access-list 101 permit icmp host 192.168.5.130 host 192.168.2.66 echo
TES(config)#access-list 101 permit icmp host 192.168.5.130 host 192.168.2.50 echo
TES(config)#access-list 101 permit icmp host 192.168.5.130 host 192.168.2.34 echo
TES(config)#access-list 101 permit icmp host 192.168.5.146 host 192.168.2.66 echo
TES(config)#access-list 101 permit icmp host 192.168.5.146 host 192.168.2.50 echo
TES(config)#access-list 101 permit icmp host 192.168.5.146 host 192.168.2.34 echo
TES(config)# access-list 102 permit icmp host 192.168.5.98 host 192.168.2.2 echo
TES(config)#access-list 102 permit icmp host 192.168.5.98 host 192.168.2.10 echo
TES(config)#access-list 102 permit icmp host 192.168.5.98 host 192.168.2.18 echo
TES(config)#access-list 102 permit icmp host 192.168.5.114 host 192.168.2.2 echo

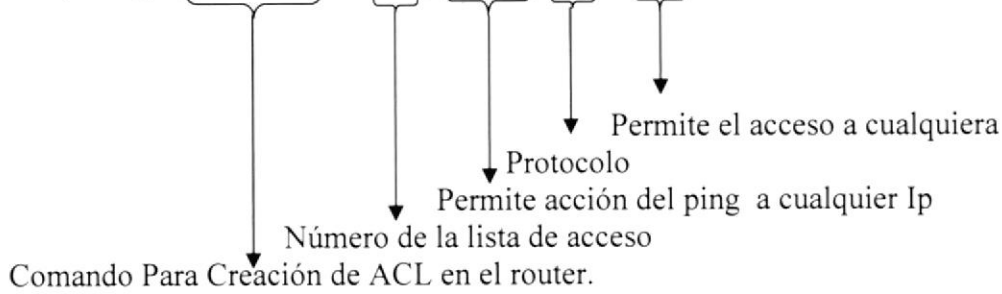
```

TES(config)#access-list 102 permit icmp host 192.168.5.114 host 192.168.2.10 echo
TES(config)#access-list 102 permit icmp host 192.168.5.114 host 192.168.2.18 echo
TES(config)#access-list 102 permit icmp host 192.168.5.130 host 192.168.2.2 echo
TES(config)#access-list 102 permit icmp host 192.168.5.130 host 192.168.2.10 echo
TES(config)#access-list 102 permit icmp host 192.168.5.130 host 192.168.2.18 echo
TES(config)#access-list 102 permit icmp host 192.168.5.146 host 192.168.2.2 echo
TES(config)#access-list 102 permit icmp host 192.168.5.146 host 192.168.2.10 echo
TES(config)#access-list 102 permit icmp host 192.168.5.146 host 192.168.2.18 echo
TES(config)#access-list 103 permit icmp host 192.168.5.98 host 192.168.6.10 echo
TES(config)#access-list 103 permit icmp host 192.168.5.98 host 192.168.6.18 echo
TES(config)#access-list 103 permit icmp host 192.168.5.114 host 192.168.6.10 echo
TES(config)#access-list 103 permit icmp host 192.168.5.114 host 192.168.6.18 echo
TES(config)#access-list 103 permit icmp host 192.168.5.130 host 192.168.6.10 echo
TES(config)#access-list 103 permit icmp host 192.168.5.130 host 192.168.6.18 echo
TES(config)#access-list 103 permit icmp host 192.168.5.146 host 192.168.6.10 echo
TES(config)#access-list 103 permit icmp host 192.168.5.146 host 192.168.6.18 echo
TES(config) access-list 104 permit icmp host 192.168.5.98 host 192.168.6.66 echo
TES(config)#access-list 104 permit icmp host 192.168.5.98 host 192.168.6.98 echo
TES(config)#access-list 104 permit icmp host 192.168.5.114 host 192.168.6.66 echo
TES(config)#access-list 104 permit icmp host 192.168.5.114 host 192.168.6.98 echo
TES(config)#access-list 104 permit icmp host 192.168.5.130 host 192.168.6.66 echo
TES(config)#access-list 104 permit icmp host 192.168.5.130 host 192.168.6.98 echo
TES(config)#access-list 104 permit icmp host 192.168.5.146 host 192.168.6.66 echo
TES(config)#access-list 104 permit icmp host 192.168.5.146 host 192.168.6.98 echo
TES(config)#access-list 105 permit icmp host 192.168.5.98 host 192.168.4.18 echo
TES(config)#access-list 105 permit icmp host 192.168.5.98 host 192.168.4.10 echo
TES(config)#access-list 105 permit icmp host 192.168.5.98 host 192.168.4.2 echo
TES(config)#access-list 105 permit icmp host 192.168.5.114 host 192.168.4.18 echo
TES(config)#access-list 105 permit icmp host 192.168.5.114 host 192.168.4.10 echo
TES(config)#access-list 105 permit icmp host 192.168.5.114 host 192.168.4.2 echo
TES(config)#access-list 105 permit icmp host 192.168.5.130 host 192.168.4.18 echo
TES(config)#access-list 105 permit icmp host 192.168.5.130 host 192.168.4.10 echo
TES(config)#access-list 105 permit icmp host 192.168.5.130 host 192.168.4.2 echo
TES(config)#access-list 105 permit icmp host 192.168.5.146 host 192.168.4.18 echo
TES(config)#access-list 105 permit icmp host 192.168.5.146 host 192.168.4.10 echo
TES(config)#access-list 105 permit icmp host 192.168.5.146 host 192.168.4.2 echo
TES(config)# access-list 106 permit icmp host 192.168.5.98 host 192.168.4.34 echo
TES(config)#access-list 106 permit icmp host 192.168.5.98 host 192.168.4.66 echo
TES(config)#access-list 106 permit icmp host 192.168.5.98 host 192.168.4.82 echo
TES(config)#access-list 106 permit icmp host 192.168.5.114 host 192.168.4.34 echo
TES(config)#access-list 106 permit icmp host 192.168.5.114 host 192.168.4.66 echo
TES(config)#access-list 106 permit icmp host 192.168.5.114 host 192.168.4.82 echo
TES(config)#access-list 106 permit icmp host 192.168.5.130 host 192.168.4.34 echo
TES(config)#access-list 106 permit icmp host 192.168.5.130 host 192.168.4.66 echo
TES(config)#access-list 106 permit icmp host 192.168.5.130 host 192.168.4.82 echo
TES(config)#access-list 106 permit icmp host 192.168.5.146 host 192.168.4.34 echo
TES(config)#access-list 106 permit icmp host 192.168.5.146 host 192.168.4.66 echo
TES(config)#access-list 106 permit icmp host 192.168.5.146 host 192.168.4.82 echo



BIBLIOTECA
CAMPUS
PEÑAS

```
TES(config)# access-list 107 permit icmp host 192.168.5.98 host 200.10.1.34 echo
TES(config)#access-list 107 permit icmp host 192.168.5.114 host 200.10.1.34 echo
TES(config)#access-list 107 permit icmp host 192.168.5.130 host 200.10.1.34 echo
TES(config)#access-list 107 permit icmp host 192.168.5.146 host 200.10.1.34 echo
TES(config)# access-list 108 permit ip any
```



```
TES(config)#EXIT
```

Sale de Modo de Configuración Global

```
TES#WR
```

Guarda los cambios Realizados
Building configuration...
[OK]

3.107.-CREACIÓN DE ACCESS LIST EN EL ROUTER

TES-1

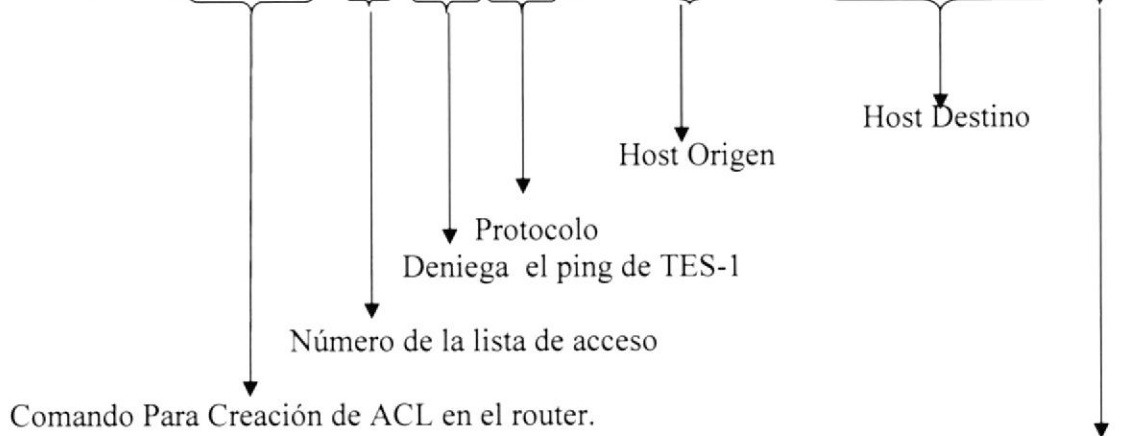
TES-1>enable

Password:

TES-1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

TES-1(config)#access-list 100 deny icmp host 192.168.3.50 host 192.168.5.98 echo



```

TES-1(config)#access-list 100 deny icmp host 192.168.3.50 host 192.168.5.114 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.50 host 192.168.5.130 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.50 host 192.168.5.146 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.34 host 192.168.5.98 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.34 host 192.168.5.114 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.34 host 192.168.5.130 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.34 host 192.168.5.146 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.2 host 192.168.5.98 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.2 host 192.168.5.114 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.2 host 192.168.5.130 echo
TES-1(config)#access-list 100 deny icmp host 192.168.3.2 host 192.168.5.146 echo

```



```

TES-1(config)#access-list 109 deny tcp host 192.168.3.50 eq telnet host 192.168.5.98

```

Diagrama de anotaciones para el comando anterior:

- 109: Número de la lista de acceso
- deny: Deniega el acceso remoto de TES-1
- tcp: Protocolo
- host 192.168.3.50: Host Origen
- eq: Operaciones lógicas pueden especificarse como Igual
- telnet: Nombre Del Puerto Acceso Remoto
- host 192.168.5.98: Host destino

Comando Para Creación de ACL en el router.

```

TES-1(config)#access-list 109 deny tcp host 192.168.3.50 eq telnet host 192.168.5.114
TES-1(config)#access-list 109 deny tcp host 192.168.3.50 eq telnet host 192.168.5.130
TES-1(config)#access-list 109 deny tcp host 192.168.3.50 eq telnet host 192.168.5.146
TES-1(config)#access-list 109 deny tcp host 192.168.3.34 eq telnet host 192.168.5.98
TES-1(config)#access-list 109 deny tcp host 192.168.3.34 eq telnet host 192.168.5.114
TES-1(config)#access-list 109 deny tcp host 192.168.3.34 eq telnet host 192.168.5.130
TES-1(config)#access-list 109 deny tcp host 192.168.3.34 eq telnet host 192.168.5.146
TES-1(config)#access-list 109 deny tcp host 192.168.3.2 eq telnet host 192.168.5.98
TES-1(config)#access-list 109 deny tcp host 192.168.3.2 eq telnet host 192.168.5.114
TES-1(config)#access-list 109 deny tcp host 192.168.3.2 eq telnet host 192.168.5.130
TES-1(config)#access-list 109 deny tcp host 192.168.3.2 eq telnet host 192.168.5.146
TES-1(config)#access-list 110 deny tcp host 192.168.3.50 eq ftp host 192.168.5.98
TES-1(config)#access-list 110 deny tcp host 192.168.3.50 eq ftp host 192.168.5.114
TES-1(config)#access-list 110 deny tcp host 192.168.3.50 eq ftp host 192.168.5.130
TES-1(config)#access-list 110 deny tcp host 192.168.3.50 eq ftp host 192.168.5.146
TES-1(config)#access-list 110 deny tcp host 192.168.3.34 eq ftp host 192.168.5.98
TES-1(config)#access-list 110 deny tcp host 192.168.3.34 eq ftp host 192.168.5.114
TES-1(config)#access-list 110 deny tcp host 192.168.3.34 eq ftp host 192.168.5.130
TES-1(config)#access-list 110 deny tcp host 192.168.3.34 eq ftp host 192.168.5.146
TES-1(config)#access-list 110 deny tcp host 192.168.3.2 eq ftp host 192.168.5.98
TES-1(config)#access-list 110 deny tcp host 192.168.3.2 eq ftp host 192.168.5.114
TES-1(config)#access-list 110 deny tcp host 192.168.3.2 eq ftp host 192.168.5.130
TES-1(config)#access-list 110 deny tcp host 192.168.3.2 eq ftp host 192.168.5.146
TES-1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
TES-1#wr
Building configuration...
[OK]

```



3.108.-CREACIÓN DE ACCESS LIST EN EL ROUTER UEES

```
UEES>enable
Password:
UEES#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UEES(config)#access-list 103 deny icmp host 192.168.6.10 host 192.168.5.98 echo
UEES(config)#access-list 103 deny icmp host 192.168.6.10 host 192.168.5.114 echo
UEES(config)#access-list 103 deny icmp host 192.168.6.10 host 192.168.5.130 echo
UEES(config)#access-list 103 deny icmp host 192.168.6.10 host 192.168.5.146 echo
UEES(config)#access-list 103 deny icmp host 192.168.6.18 host 192.168.5.98 echo
UEES(config)#access-list 103 deny icmp host 192.168.6.18 host 192.168.5.114 echo
UEES(config)#access-list 103 deny icmp host 192.168.6.18 host 192.168.5.130 echo
UEES(config)#access-list 103 deny icmp host 192.168.6.18 host 192.168.5.146 echo
UEES(config)#access-list 111 deny tcp host 192.168.6.10 eq telnet host 192.168.5.98
UEES(config)#access-list 111 deny tcp host 192.168.6.10 eq telnet host 192.168.5.114
UEES(config)#access-list 111 deny tcp host 192.168.6.10 eq telnet host 192.168.5.130
UEES(config)#access-list 111 deny tcp host 192.168.6.10 eq telnet host 192.168.5.146
UEES(config)#access-list 111 deny tcp host 192.168.6.18 eq telnet host 192.168.5.98
UEES(config)#access-list 111 deny tcp host 192.168.6.18 eq telnet host 192.168.5.114
UEES(config)#access-list 111 deny tcp host 192.168.6.18 eq telnet host 192.168.5.130
UEES(config)#access-list 111 deny tcp host 192.168.6.18 eq telnet host 192.168.5.146
UEES(config)#access-list 112 deny tcp host 192.168.6.10 eq ftp host 192.168.5.98
UEES(config)#access-list 112 deny tcp host 192.168.6.10 eq ftp host 192.168.5.114
UEES(config)#access-list 112 deny tcp host 192.168.6.10 eq ftp host 192.168.5.130
UEES(config)#access-list 112 deny tcp host 192.168.6.10 eq ftp host 192.168.5.146
UEES(config)#access-list 112 deny tcp host 192.168.6.18 eq ftp host 192.168.5.98
UEES(config)#access-list 112 deny tcp host 192.168.6.18 eq ftp host 192.168.5.114
UEES(config)#access-list 112 deny tcp host 192.168.6.18 eq ftp host 192.168.5.130
UEES(config)#access-list 112 deny tcp host 192.168.6.18 eq ftp host 192.168.5.146
UEES(config)#exit

%SYS-5-CONFIG_I: Configured from console by console
UEES#wr
Building configuration...
[OK]
```

3.109.-CREACIÓN DE ACCESS LIST EN EL ROUTER

UEES-1

```
UEES-1>enable
```

```
Password:
```

```
UEES-1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.18 host 192.168.5.98 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.18 host 192.168.5.114 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.18 host 192.168.5.130 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.18 host 192.168.5.146 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.10 host 192.168.5.98 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.10 host 192.168.5.114 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.10 host 192.168.5.130 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.10 host 192.168.5.146 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.2 host 192.168.5.98 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.2 host 192.168.5.114 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.2 host 192.168.5.130 echo
```

```
UEES-1(config)#Access-list 102 deny icmp host 192.168.2.2 host 192.168.5.146 echo
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.18 eq telnet host 192.168.5.98
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.18 eq telnet host
```

```
192.168.5.114
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.18 eq telnet host
```

```
192.168.5.130
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.18 eq telnet host
```

```
192.168.5.146
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.10 eq telnet host 192.168.5.98
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.10 eq telnet host
```

```
192.168.5.114
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.10 eq telnet host
```

```
192.168.5.130
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.10 eq telnet host
```

```
192.168.5.146
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.2 eq telnet host 192.168.5.98
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.2 eq telnet host 192.168.5.114
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.2 eq telnet host 192.168.5.130
```

```
UEES-1(config)#Access-list 113 deny tcp host 192.168.2.2 eq telnet host 192.168.5.146
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.18 eq ftp host 192.168.5.98
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.18 eq ftp host 192.168.5.114
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.18 eq ftp host 192.168.5.130
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.18 eq ftp host 192.168.5.146
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.10 eq ftp host 192.168.5.98
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.10 eq ftp host 192.168.5.114
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.10 eq ftp host 192.168.5.130
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.10 eq ftp host 192.168.5.146
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.2 eq ftp host 192.168.5.98
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.2 eq ftp host 192.168.5.114
```

```
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.2 eq ftp host 192.168.5.130
UEES-1(config)#Access-list 114 deny tcp host 192.168.2.2 eq ftp host 192.168.5.146
UEES-1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
UEES-1#wr
Building configuration...
[OK]
```



BIBLIOTECA
CAMPUS
PEÑAS

3.110.-CREACIÓN DE ACCESS LIST EN EL ROUTER UEES-2

```
UEES-2>enable
Password:
UEES-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
UEES-2(config)#access-list 101 deny icmp host 192.168.2.66 host 192.168.5.98 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.66 host 192.168.5.114 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.66 host 192.168.5.130 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.66 host 192.168.5.146 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.50 host 192.168.5.98 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.50 host 192.168.5.114 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.50 host 192.168.5.130 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.50 host 192.168.5.146 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.34 host 192.168.5.98 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.34 host 192.168.5.114 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.34 host 192.168.5.130 echo
UEES-2(config)#access-list 101 deny icmp host 192.168.2.34 host 192.168.5.146 echo
UEES-2(config)#access-list 115 deny tcp host 192.168.2.66 eq telnet host 192.168.5.98
UEES-2(config)#access-list 115 deny tcp host 192.168.2.66 eq telnet host
192.168.5.114
UEES-2(config)#access-list 115 deny tcp host 192.168.2.66 eq telnet host
192.168.5.130
UEES-2(config)#access-list 115 deny tcp host 192.168.2.66 eq telnet host
192.168.5.146
UEES-2(config)#access-list 115 deny tcp host 192.168.2.50 eq telnet host 192.168.5.98
UEES-2(config)#access-list 115 deny tcp host 192.168.2.50 eq telnet host
192.168.5.114
UEES-2(config)#access-list 115 deny tcp host 192.168.2.50 eq telnet host
192.168.5.130
UEES-2(config)#access-list 115 deny tcp host 192.168.2.50 eq telnet host
192.168.5.146
UEES-2(config)#access-list 115 deny tcp host 192.168.2.34 eq telnet host 192.168.5.98
UEES-2(config)#access-list 115 deny tcp host 192.168.2.34 eq telnet host
192.168.5.114
UEES-2(config)#access-list 115 deny tcp host 192.168.2.34 eq telnet host
192.168.5.130
```

```

UEES-2(config)#access-list 115 deny tcp host 192.168.2.34 eq telnet host
192.168.5.146
UEES-2(config)#access-list 116 deny tcp host 192.168.2.66 eq ftp host 192.168.5.98
UEES-2(config)#access-list 116 deny tcp host 192.168.2.66 eq ftp host 192.168.5.114
UEES-2(config)#access-list 116 deny tcp host 192.168.2.66 eq ftp host 192.168.5.130
UEES-2(config)#access-list 116 deny tcp host 192.168.2.66 eq ftp host 192.168.5.146
UEES-2(config)#access-list 116 deny tcp host 192.168.2.50 eq ftp host 192.168.5.98
UEES-2(config)#access-list 116 deny tcp host 192.168.2.50 eq ftp host 192.168.5.114
UEES-2(config)#access-list 116 deny tcp host 192.168.2.50 eq ftp host 192.168.5.130
UEES-2(config)#access-list 116 deny tcp host 192.168.2.50 eq ftp host 192.168.5.146
UEES-2(config)#access-list 116 deny tcp host 192.168.2.34 eq ftp host 192.168.5.98
UEES-2(config)#access-list 116 deny tcp host 192.168.2.34 eq ftp host 192.168.5.114
UEES-2(config)#access-list 116 deny tcp host 192.168.2.34 eq ftp host 192.168.5.130
UEES-2(config)#access-list 116 deny tcp host 192.168.2.34 eq ftp host 192.168.5.146
UEES-2(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
UEES-2#wr
Building configuration...
[OK]

```

3.111.-CREACIÓN DE ACCESS LIST EN EL ROUTER ECOTEC

```

Ecotec>enable
Password:
Ecotec#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ecotec(config)#access-list 104 deny icmp host 192.168.6.66 host 192.168.5.98 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.66 host 192.168.5.114 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.66 host 192.168.5.130 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.66 host 192.168.5.146 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.98 host 192.168.5.98 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.98 host 192.168.5.114 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.98 host 192.168.5.130 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.98 host 192.168.5.146 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.98 host 192.168.5.146 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.98 host 192.168.5.146 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.98 host 192.168.5.146 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.98 host 192.168.5.146 echo
Ecotec(config)#access-list 104 deny icmp host 192.168.6.98 host 192.168.5.146 echo
Ecotec(config)#access-list 117 deny tcp host 192.168.6.66 eq telnet host 192.168.5.98
Ecotec(config)#access-list 117 deny tcp host 192.168.6.66 eq telnet host 192.168.5.114
Ecotec(config)#access-list 117 deny tcp host 192.168.6.66 eq telnet host 192.168.5.130
Ecotec(config)#access-list 117 deny tcp host 192.168.6.66 eq telnet host 192.168.5.146
Ecotec(config)#access-list 117 deny tcp host 192.168.6.98 eq telnet host 192.168.5.98

```



```
Ecotec(config)#access-list 117 deny tcp host 192.168.6.98 eq telnet host 192.168.5.114
Ecotec(config)#access-list 117 deny tcp host 192.168.6.98 eq telnet host 192.168.5.130
Ecotec(config)#access-list 117 deny tcp host 192.168.6.98 eq telnet host 192.168.5.146
Ecotec(config)#access-list 118 deny tcp host 192.168.6.66 eq ftp host 192.168.5.98
Ecotec(config)#access-list 118 deny tcp host 192.168.6.66 eq ftp host 192.168.5.114
Ecotec(config)#access-list 118 deny tcp host 192.168.6.66 eq ftp host 192.168.5.130
Ecotec(config)#access-list 118 deny tcp host 192.168.6.66 eq ftp host 192.168.5.146
Ecotec(config)#access-list 118 deny tcp host 192.168.6.98 eq ftp host 192.168.5.98
Ecotec(config)#access-list 118 deny tcp host 192.168.6.98 eq ftp host 192.168.5.114
Ecotec(config)#access-list 118 deny tcp host 192.168.6.98 eq ftp host 192.168.5.130
Ecotec(config)#access-list 118 deny tcp host 192.168.6.98 eq ftp host 192.168.5.146
Ecotec(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Ecotec#wr
Building configuration...
[OK]
```

3.112.-CREACIÓN DE ACCESS LIST EN EL ROUTER ECOTEC-1

```
ECOTEC-1>enable
Password:
ECOTEC-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.18 host 192.168.5.98
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.18 host 192.168.5.114
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.18 host 192.168.5.130
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.18 host 192.168.5.146
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.10 host 192.168.5.98
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.10 host 192.168.5.114
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.10 host 192.168.5.130
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.10 host 192.168.5.146
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.2 host 192.168.5.98 echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.2 host 192.168.5.114
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.2 host 192.168.5.130
echo
ECOTEC-1(config)#access-list 105 deny icmp host 192.168.4.2 host 192.168.5.146
echo
```

```
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.18 eq telnet host
192.168.5.98
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.18 eq telnet host
192.168.5.114
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.18 eq telnet host
192.168.5.130
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.18 eq telnet host
192.168.5.146
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.10 eq telnet host
192.168.5.98
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.10 eq telnet host
192.168.5.114
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.10 eq telnet host
192.168.5.130
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.10 eq telnet host
192.168.5.146
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.2 eq telnet host
192.168.5.98
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.2 eq telnet host
192.168.5.114
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.2 eq telnet host
192.168.5.130
ECOTEC-1(config)#access-list 119 deny tcp host 192.168.4.2 eq telnet host
192.168.5.146
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.18 eq ftp host 192.168.5.98
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.18 eq ftp host
192.168.5.114
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.18 eq ftp host
192.168.5.130
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.18 eq ftp host
192.168.5.146
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.10 eq ftp host 192.168.5.98
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.10 eq ftp host
192.168.5.114
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.10 eq ftp host
192.168.5.130
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.10 eq ftp host
192.168.5.146
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.2 eq ftp host 192.168.5.98
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.2 eq ftp host 192.168.5.114
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.2 eq ftp host 192.168.5.130
ECOTEC-1(config)#access-list 120 deny tcp host 192.168.4.2 eq ftp host 192.168.5.146
ECOTEC-1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
ECOTEC-1#wr
Building configuration...
[OK]
```



3.113.-CREACIÓN DE ACCESS LIST EN EL ROUTER ECOTEC-2

```
ECOTEC-2>enable
Password:
ECOTEC-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.34 host 192.168.5.98
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.34 host 192.168.5.114
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.34 host 192.168.5.130
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.34 host 192.168.5.146
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.66 host 192.168.5.98
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.66 host 192.168.5.114
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.66 host 192.168.5.130
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.66 host 192.168.5.146
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.82 host 192.168.5.98
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.82 host 192.168.5.114
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.82 host 192.168.5.130
echo
ECOTEC-2(config)#access-list 106 deny icmp host 192.168.4.82 host 192.168.5.146
echo
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.82 eq telnet host
192.168.5.98
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.82 eq telnet host
192.168.5.114
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.82 eq telnet host
192.168.5.130
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.82 eq telnet host
192.168.5.146
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.66 eq telnet host
192.168.5.98
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.66 eq telnet host
192.168.5.114
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.66 eq telnet host
192.168.5.130
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.66 eq telnet host
192.168.5.146
```

```
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.34 eq telnet host
192.168.5.98
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.34 eq telnet host
192.168.5.114
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.34 eq telnet host
192.168.5.130
ECOTEC-2(config)#access-list 121 deny tcp host 192.168.4.34 eq telnet host
192.168.5.146
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.34 eq ftp host 192.168.5.98
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.34 eq ftp host
192.168.5.114
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.34 eq ftp host
192.168.5.130
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.34 eq ftp host
192.168.5.146
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.66 eq ftp host 192.168.5.98
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.66 eq ftp host
192.168.5.114
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.66 eq ftp host
192.168.5.130
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.66 eq ftp host
192.168.5.146
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.82 eq ftp host 192.168.5.98
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.82 eq ftp host
192.168.5.114
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.82 eq ftp host
192.168.5.130
ECOTEC-2(config)#access-list 122 deny tcp host 192.168.4.82 eq ftp host
192.168.5.146
ECOTEC-2(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
ECOTEC-2#wr
Building configuration...
[OK]
```

3.114.-CREACIÓN DE ACCESS LIST EN EL ROUTER ISP

```
ISP >enable
Password:
ISP#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#access-list 107 permit icmp host 200.10.1.43 host 192.168.4.98 echo
ISP(config)#access-list 107 permit icmp host 200.10.1.43 host 192.168.4.114 echo
ISP(config)#access-list 107 permit icmp host 200.10.1.43 host 192.168.4.130 echo
ISP(config)#access-list 107 permit icmp host 200.10.1.43 host 192.168.4.146 echo
ISP(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
```

```
ISP#wr
Building configuration...
[OK]
```

3.115.- SHOW ACCESS-LISTS EN EL ROUTER TES



```
TES>enable
```

Instrucción para entrar en modo privilegiado
Password:
TES# show access-lists

Muestra el contenido de todas las ACL en el router.

```
Extended IP access list 100
```

Este Rango identifica el tipo de ACL extendidas para Router TES-1

Lista de Control de Acceso o ACL
Este es el parámetro que permite o deniega accesos a una o más acl.

```
permit icmp host 192.168.5.98 host 192.168.3.50 echo
```

Permit deja pasar ese tráfico de la red

Protocolo

Host Origen

Host Destino

Permite el paso de tráfico cuando hay una sesión establecida.

```
permit icmp host 192.168.5.98 host 192.168.3.34 echo
permit icmp host 192.168.5.98 host 192.168.3.2 echo
permit icmp host 192.168.5.114 host 192.168.3.50 echo
permit icmp host 192.168.5.114 host 192.168.3.34 echo
permit icmp host 192.168.5.114 host 192.168.3.2 echo
permit icmp host 192.168.5.130 host 192.168.3.50 echo
permit icmp host 192.168.5.130 host 192.168.3.34 echo
permit icmp host 192.168.5.130 host 192.168.3.2 echo
permit icmp host 192.168.5.146 host 192.168.3.50 echo
permit icmp host 192.168.5.146 host 192.168.3.34 echo
permit icmp host 192.168.5.146 host 192.168.3.2 echo
```

Extended IP access list 101



Identifica el tipo de ACL extendidas para UEES-2

```

permit icmp host 192.168.5.98 host 192.168.2.66 echo
permit icmp host 192.168.5.98 host 192.168.2.50 echo
permit icmp host 192.168.5.98 host 192.168.2.34 echo
permit icmp host 192.168.5.114 host 192.168.2.66 echo
permit icmp host 192.168.5.114 host 192.168.2.50 echo
permit icmp host 192.168.5.114 host 192.168.2.34 echo
permit icmp host 192.168.5.130 host 192.168.2.66 echo
permit icmp host 192.168.5.130 host 192.168.2.50 echo
permit icmp host 192.168.5.130 host 192.168.2.34 echo
permit icmp host 192.168.5.146 host 192.168.2.66 echo
permit icmp host 192.168.5.146 host 192.168.2.50 echo
permit icmp host 192.168.5.146 host 192.168.2.34 echo

```

Extended IP access list 102



Identifica el tipo de ACL extendidas para UEES-1

```

permit icmp host 192.168.5.98 host 192.168.2.2 echo
permit icmp host 192.168.5.98 host 192.168.2.10 echo
permit icmp host 192.168.5.98 host 192.168.2.18 echo
permit icmp host 192.168.5.114 host 192.168.2.2 echo
permit icmp host 192.168.5.114 host 192.168.2.10 echo
permit icmp host 192.168.5.114 host 192.168.2.18 echo
permit icmp host 192.168.5.130 host 192.168.2.2 echo
permit icmp host 192.168.5.130 host 192.168.2.10 echo
permit icmp host 192.168.5.130 host 192.168.2.18 echo
permit icmp host 192.168.5.146 host 192.168.2.2 echo
permit icmp host 192.168.5.146 host 192.168.2.10 echo
permit icmp host 192.168.5.146 host 192.168.2.18 echo

```

Extended IP access list 103



Identifica el tipo de ACL extendidas para UEES

```

permit icmp host 192.168.5.98 host 192.168.6.10 echo
permit icmp host 192.168.5.98 host 192.168.6.18 echo
permit icmp host 192.168.5.114 host 192.168.6.10 echo
permit icmp host 192.168.5.114 host 192.168.6.18 echo
permit icmp host 192.168.5.130 host 192.168.6.10 echo
permit icmp host 192.168.5.130 host 192.168.6.18 echo
permit icmp host 192.168.5.146 host 192.168.6.10 echo
permit icmp host 192.168.5.146 host 192.168.6.18 echo

```



Extended IP access list 104

Identifica el tipo de ACL extendidas para ECOTEC

```
permit icmp host 192.168.5.98 host 192.168.6.66 echo
permit icmp host 192.168.5.98 host 192.168.6.98 echo
permit icmp host 192.168.5.114 host 192.168.6.66 echo
permit icmp host 192.168.5.114 host 192.168.6.98 echo
permit icmp host 192.168.5.130 host 192.168.6.66 echo
permit icmp host 192.168.5.130 host 192.168.6.98 echo
permit icmp host 192.168.5.146 host 192.168.6.66 echo
permit icmp host 192.168.5.146 host 192.168.6.98 echo
Extended IP access list 105
```

Identifica el tipo de ACL extendidas para ECOTEC-1

```
permit icmp host 192.168.5.98 host 192.168.4.18 echo
permit icmp host 192.168.5.98 host 192.168.4.10 echo
permit icmp host 192.168.5.98 host 192.168.4.2 echo
permit icmp host 192.168.5.114 host 192.168.4.18 echo
permit icmp host 192.168.5.114 host 192.168.4.10 echo
permit icmp host 192.168.5.114 host 192.168.4.2 echo
permit icmp host 192.168.5.130 host 192.168.4.18 echo
permit icmp host 192.168.5.130 host 192.168.4.10 echo
permit icmp host 192.168.5.130 host 192.168.4.2 echo
permit icmp host 192.168.5.146 host 192.168.4.18 echo
permit icmp host 192.168.5.146 host 192.168.4.10 echo
permit icmp host 192.168.5.146 host 192.168.4.2 echo
Extended IP access list 106
```

Identifica el tipo de ACL extendidas para ECOTEC-2

```
permit icmp host 192.168.5.98 host 192.168.4.34 echo
permit icmp host 192.168.5.98 host 192.168.4.66 echo
permit icmp host 192.168.5.98 host 192.168.4.82 echo
permit icmp host 192.168.5.114 host 192.168.4.34 echo
permit icmp host 192.168.5.114 host 192.168.4.66 echo
permit icmp host 192.168.5.114 host 192.168.4.82 echo
permit icmp host 192.168.5.130 host 192.168.4.34 echo
permit icmp host 192.168.5.130 host 192.168.4.66 echo
permit icmp host 192.168.5.130 host 192.168.4.82 echo
permit icmp host 192.168.5.146 host 192.168.4.34 echo
permit icmp host 192.168.5.146 host 192.168.4.66 echo
permit icmp host 192.168.5.146 host 192.168.4.82 echo
```



Extended IP access list 107



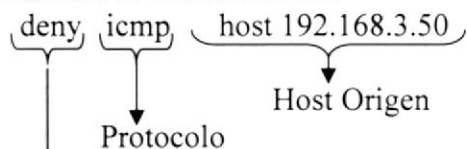
Identifican el tipo de ACL extendidas para el ISP

```
permit icmp host 192.168.5.98 host 200.10.1.34 echo
permit icmp host 192.168.5.114 host 200.10.1.34 echo
permit icmp host 192.168.5.130 host 200.10.1.34 echo
permit icmp host 192.168.5.146 host 200.10.1.34 echo
Extended IP access list 108
permit ip any any
```

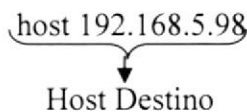
3.116.-SHOW ACCESS-LISTS EN EL ROUTER TES-1

TES-1#show access-lists

Extended IP access list 100



Deniega el ping de la sucursal UEES -1



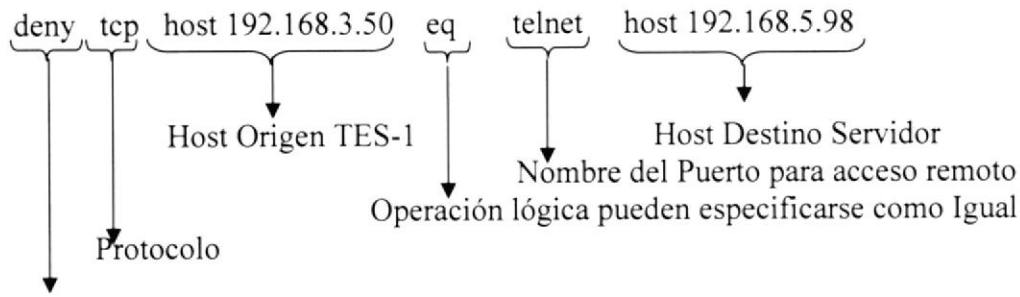
Permite el paso de Tráfico cuando hay Una sesión establecida.

```
deny icmp host 192.168.3.50 host 192.168.5.114 echo
deny icmp host 192.168.3.50 host 192.168.5.130 echo
deny icmp host 192.168.3.50 host 192.168.5.146 echo
deny icmp host 192.168.3.34 host 192.168.5.98 echo
deny icmp host 192.168.3.34 host 192.168.5.114 echo
deny icmp host 192.168.3.34 host 192.168.5.130 echo
deny icmp host 192.168.3.34 host 192.168.5.146 echo
deny icmp host 192.168.3.2 host 192.168.5.98 echo
deny icmp host 192.168.3.2 host 192.168.5.114 echo
deny icmp host 192.168.3.2 host 192.168.5.130 echo
deny icmp host 192.168.3.2 host 192.168.5.146 echo
```

Extended IP access list 109



Identifica el tipo de ACL extendidas para el Grupo TES-1

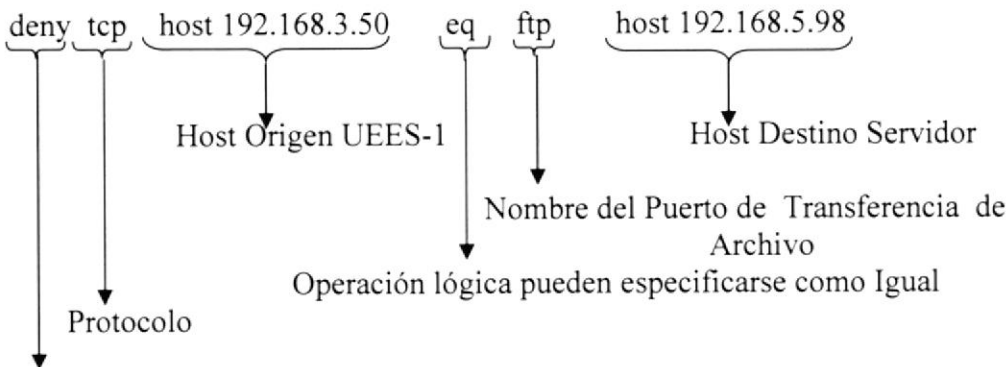


Deniega la entrada de paquetes por el protocolo tcp del Router TES-1

```
deny tcp host 192.168.3.50 eq telnet host 192.168.5.114
deny tcp host 192.168.3.50 eq telnet host 192.168.5.130
deny tcp host 192.168.3.50 eq telnet host 192.168.5.146
deny tcp host 192.168.3.34 eq telnet host 192.168.5.98
deny tcp host 192.168.3.34 eq telnet host 192.168.5.114
deny tcp host 192.168.3.34 eq telnet host 192.168.5.130
deny tcp host 192.168.3.34 eq telnet host 192.168.5.146
deny tcp host 192.168.3.2 eq telnet host 192.168.5.98
deny tcp host 192.168.3.2 eq telnet host 192.168.5.114
deny tcp host 192.168.3.2 eq telnet host 192.168.5.130
deny tcp host 192.168.3.2 eq telnet host 192.168.5.146
```

Extended IP access list 110

Identifica el tipo de ACL extendidas para el Grupo TES-1



Deniega la entrada de paquetes por el protocolo tcp de la sucursal TES -1

```
deny tcp host 192.168.3.50 eq ftp host 192.168.5.114
deny tcp host 192.168.3.50 eq ftp host 192.168.5.130
deny tcp host 192.168.3.50 eq ftp host 192.168.5.146
deny tcp host 192.168.3.34 eq ftp host 192.168.5.98
deny tcp host 192.168.3.34 eq ftp host 192.168.5.114
deny tcp host 192.168.3.34 eq ftp host 192.168.5.130
deny tcp host 192.168.3.34 eq ftp host 192.168.5.146
deny tcp host 192.168.3.2 eq ftp host 192.168.5.98
deny tcp host 192.168.3.2 eq ftp host 192.168.5.114
```



```
deny tcp host 192.168.3.2 eq ftp host 192.168.5.130  
deny tcp host 192.168.3.2 eq ftp host 192.168.5.146
```

3.117.-SHOW ACCESS-LISTS EN EL ROUTER UEES

```
UEES#show access-lists  
Extended IP access list 103  
deny icmp host 192.168.6.10 host 192.168.5.98 echo  
deny icmp host 192.168.6.10 host 192.168.5.114 echo  
deny icmp host 192.168.6.10 host 192.168.5.130 echo  
deny icmp host 192.168.6.10 host 192.168.5.146 echo  
deny icmp host 192.168.6.18 host 192.168.5.98 echo  
deny icmp host 192.168.6.18 host 192.168.5.114 echo  
deny icmp host 192.168.6.18 host 192.168.5.130 echo  
deny icmp host 192.168.6.18 host 192.168.5.146 echo  
Extended IP access list 111  
deny tcp host 192.168.6.10 eq telnet host 192.168.5.98  
deny tcp host 192.168.6.10 eq telnet host 192.168.5.114  
deny tcp host 192.168.6.10 eq telnet host 192.168.5.130  
deny tcp host 192.168.6.10 eq telnet host 192.168.5.146  
deny tcp host 192.168.6.18 eq telnet host 192.168.5.98  
deny tcp host 192.168.6.18 eq telnet host 192.168.5.114  
deny tcp host 192.168.6.18 eq telnet host 192.168.5.130  
deny tcp host 192.168.6.18 eq telnet host 192.168.5.146  
Extended IP access list 112  
deny tcp host 192.168.6.10 eq ftp host 192.168.5.98  
deny tcp host 192.168.6.10 eq ftp host 192.168.5.114  
deny tcp host 192.168.6.10 eq ftp host 192.168.5.130  
deny tcp host 192.168.6.10 eq ftp host 192.168.5.146  
deny tcp host 192.168.6.18 eq ftp host 192.168.5.98  
deny tcp host 192.168.6.18 eq ftp host 192.168.5.114  
deny tcp host 192.168.6.18 eq ftp host 192.168.5.130  
deny tcp host 192.168.6.18 eq ftp host 192.168.5.146
```



3.118.-SHOW ACCESS-LISTS EN EL ROUTER UEES-1

```
UEES-1#show access-lists  
Extended IP access list 102  
deny icmp host 192.168.2.18 host 192.168.5.98 echo  
deny icmp host 192.168.2.18 host 192.168.5.114 echo  
deny icmp host 192.168.2.18 host 192.168.5.130 echo  
deny icmp host 192.168.2.18 host 192.168.5.146 echo  
deny icmp host 192.168.2.10 host 192.168.5.98 echo  
deny icmp host 192.168.2.10 host 192.168.5.114 echo  
deny icmp host 192.168.2.10 host 192.168.5.130 echo  
deny icmp host 192.168.2.10 host 192.168.5.146 echo
```

```
deny icmp host 192.168.2.2 host 192.168.5.98 echo
deny icmp host 192.168.2.2 host 192.168.5.114 echo
deny icmp host 192.168.2.2 host 192.168.5.130 echo
deny icmp host 192.168.2.2 host 192.168.5.146 echo
Extended IP access list 113
deny tcp host 192.168.2.18 eq telnet host 192.168.5.98
deny tcp host 192.168.2.18 eq telnet host 192.168.5.114
deny tcp host 192.168.2.18 eq telnet host 192.168.5.130
deny tcp host 192.168.2.18 eq telnet host 192.168.5.146
deny tcp host 192.168.2.10 eq telnet host 192.168.5.98
deny tcp host 192.168.2.10 eq telnet host 192.168.5.114
deny tcp host 192.168.2.10 eq telnet host 192.168.5.130
deny tcp host 192.168.2.10 eq telnet host 192.168.5.146
deny tcp host 192.168.2.2 eq telnet host 192.168.5.98
deny tcp host 192.168.2.2 eq telnet host 192.168.5.114
deny tcp host 192.168.2.2 eq telnet host 192.168.5.130
deny tcp host 192.168.2.2 eq telnet host 192.168.5.146
Extended IP access list 114
deny tcp host 192.168.2.18 eq ftp host 192.168.5.98
deny tcp host 192.168.2.18 eq ftp host 192.168.5.114
deny tcp host 192.168.2.18 eq ftp host 192.168.5.130
deny tcp host 192.168.2.18 eq ftp host 192.168.5.146
deny tcp host 192.168.2.10 eq ftp host 192.168.5.98
deny tcp host 192.168.2.10 eq ftp host 192.168.5.114
deny tcp host 192.168.2.10 eq ftp host 192.168.5.130
deny tcp host 192.168.2.10 eq ftp host 192.168.5.146
deny tcp host 192.168.2.2 eq ftp host 192.168.5.98
deny tcp host 192.168.2.2 eq ftp host 192.168.5.114
deny tcp host 192.168.2.2 eq ftp host 192.168.5.130
deny tcp host 192.168.2.2 eq ftp host 192.168.5.146
```



3.119.-SHOW ACCESS-LISTS EN EL ROUTER UEES-2

```
UEES-2#show access-lists
Extended IP access list 101
```

```
deny icmp host 192.168.2.66 host 192.168.5.98 echo
deny icmp host 192.168.2.66 host 192.168.5.114 echo
deny icmp host 192.168.2.66 host 192.168.5.130 echo
deny icmp host 192.168.2.66 host 192.168.5.146 echo
deny icmp host 192.168.2.50 host 192.168.5.98 echo
deny icmp host 192.168.2.50 host 192.168.5.114 echo
deny icmp host 192.168.2.50 host 192.168.5.130 echo
deny icmp host 192.168.2.50 host 192.168.5.146 echo
deny icmp host 192.168.2.34 host 192.168.5.98 echo
deny icmp host 192.168.2.34 host 192.168.5.114 echo
deny icmp host 192.168.2.34 host 192.168.5.130 echo
deny icmp host 192.168.2.34 host 192.168.5.146 echo
```

Extended IP access list 115

```
deny tcp host 192.168.2.66 eq telnet host 192.168.5.98
deny tcp host 192.168.2.66 eq telnet host 192.168.5.114
deny tcp host 192.168.2.66 eq telnet host 192.168.5.130
deny tcp host 192.168.2.66 eq telnet host 192.168.5.146
deny tcp host 192.168.2.50 eq telnet host 192.168.5.98
deny tcp host 192.168.2.50 eq telnet host 192.168.5.114
deny tcp host 192.168.2.50 eq telnet host 192.168.5.130
deny tcp host 192.168.2.50 eq telnet host 192.168.5.146
deny tcp host 192.168.2.34 eq telnet host 192.168.5.98
deny tcp host 192.168.2.34 eq telnet host 192.168.5.114
deny tcp host 192.168.2.34 eq telnet host 192.168.5.130
deny tcp host 192.168.2.34 eq telnet host 192.168.5.146
```

Extended IP access list 116

```
deny tcp host 192.168.2.34 eq ftp host 192.168.5.98
deny tcp host 192.168.2.34 eq ftp host 192.168.5.114
deny tcp host 192.168.2.34 eq ftp host 192.168.5.130
deny tcp host 192.168.2.34 eq ftp host 192.168.5.146
deny tcp host 192.168.2.66 eq ftp host 192.168.5.98
deny tcp host 192.168.2.66 eq ftp host 192.168.5.114
deny tcp host 192.168.2.66 eq ftp host 192.168.5.130
deny tcp host 192.168.2.66 eq ftp host 192.168.5.146
deny tcp host 192.168.2.50 eq ftp host 192.168.5.98
deny tcp host 192.168.2.50 eq ftp host 192.168.5.114
deny tcp host 192.168.2.50 eq ftp host 192.168.5.130
deny tcp host 192.168.2.50 eq ftp host 192.168.5.146
```



3.120.-SHOW ACCESS-LISTS EN EL ROUTER ECOTEC

Ecotec#show access-lists

Extended IP access list 104

```
deny icmp host 192.168.6.66 host 192.168.5.98 echo
deny icmp host 192.168.6.66 host 192.168.5.114 echo
deny icmp host 192.168.6.66 host 192.168.5.130 echo
deny icmp host 192.168.6.66 host 192.168.5.146 echo
deny icmp host 192.168.6.98 host 192.168.5.98 echo
deny icmp host 192.168.6.98 host 192.168.5.114 echo
deny icmp host 192.168.6.98 host 192.168.5.130 echo
deny icmp host 192.168.6.98 host 192.168.5.146 echo
```

Extended IP access list 117

```
deny tcp host 192.168.6.66 eq telnet host 192.168.5.98
deny tcp host 192.168.6.66 eq telnet host 192.168.5.114
deny tcp host 192.168.6.66 eq telnet host 192.168.5.130
deny tcp host 192.168.6.66 eq telnet host 192.168.5.146
deny tcp host 192.168.6.98 eq telnet host 192.168.5.98
deny tcp host 192.168.6.98 eq telnet host 192.168.5.114
```

```
deny tcp host 192.168.6.98 eq telnet host 192.168.5.130
deny tcp host 192.168.6.98 eq telnet host 192.168.5.146
Extended IP access list 118
deny tcp host 192.168.6.66 eq ftp host 192.168.5.98
deny tcp host 192.168.6.66 eq ftp host 192.168.5.114
deny tcp host 192.168.6.66 eq ftp host 192.168.5.130
deny tcp host 192.168.6.66 eq ftp host 192.168.5.146
deny tcp host 192.168.6.98 eq ftp host 192.168.5.98
deny tcp host 192.168.6.98 eq ftp host 192.168.5.114
deny tcp host 192.168.6.98 eq ftp host 192.168.5.130
deny tcp host 192.168.6.98 eq ftp host 192.168.5.146
```

3.121.-SHOW ACCESS-LISTS EN EL ROUTER ECOTEC-1

ECOTEC-1#show access-lists

Extended IP access list 105

```
deny icmp host 192.168.4.18 host 192.168.5.98 echo
deny icmp host 192.168.4.18 host 192.168.5.114 echo
deny icmp host 192.168.4.18 host 192.168.5.130 echo
deny icmp host 192.168.4.18 host 192.168.5.146 echo
deny icmp host 192.168.4.10 host 192.168.5.98 echo
deny icmp host 192.168.4.10 host 192.168.5.114 echo
deny icmp host 192.168.4.10 host 192.168.5.130 echo
deny icmp host 192.168.4.10 host 192.168.5.146 echo
deny icmp host 192.168.4.2 host 192.168.5.98 echo
deny icmp host 192.168.4.2 host 192.168.5.114 echo
deny icmp host 192.168.4.2 host 192.168.5.130 echo
deny icmp host 192.168.4.2 host 192.168.5.146 echo
```

Extended IP access list 119

```
deny tcp host 192.168.4.18 eq telnet host 192.168.5.98
deny tcp host 192.168.4.18 eq telnet host 192.168.5.114
deny tcp host 192.168.4.18 eq telnet host 192.168.5.130
deny tcp host 192.168.4.18 eq telnet host 192.168.5.146
deny tcp host 192.168.4.10 eq telnet host 192.168.5.98
deny tcp host 192.168.4.10 eq telnet host 192.168.5.114
deny tcp host 192.168.4.10 eq telnet host 192.168.5.130
deny tcp host 192.168.4.10 eq telnet host 192.168.5.146
deny tcp host 192.168.4.2 eq telnet host 192.168.5.98
deny tcp host 192.168.4.2 eq telnet host 192.168.5.114
deny tcp host 192.168.4.2 eq telnet host 192.168.5.130
deny tcp host 192.168.4.2 eq telnet host 192.168.5.146
```

Extended IP access list 120

```
deny tcp host 192.168.4.18 eq ftp host 192.168.5.98
deny tcp host 192.168.4.18 eq ftp host 192.168.5.114
deny tcp host 192.168.4.18 eq ftp host 192.168.5.130
deny tcp host 192.168.4.18 eq ftp host 192.168.5.146
```



```
deny tcp host 192.168.4.10 eq ftp host 192.168.5.98  
deny tcp host 192.168.4.10 eq ftp host 192.168.5.114  
deny tcp host 192.168.4.10 eq ftp host 192.168.5.130  
deny tcp host 192.168.4.10 eq ftp host 192.168.5.146  
deny tcp host 192.168.4.2 eq ftp host 192.168.5.98  
deny tcp host 192.168.4.2 eq ftp host 192.168.5.114  
deny tcp host 192.168.4.2 eq ftp host 192.168.5.130  
deny tcp host 192.168.4.2 eq ftp host 192.168.5.146
```

3.122.-SHOW ACCESS-LISTS EN EL ROUTER ECOTEC-2

ECOTEC-2#show access-lists

Extended IP access list 106

```
deny icmp host 192.168.4.34 host 192.168.5.98 echo  
deny icmp host 192.168.4.34 host 192.168.5.114 echo  
deny icmp host 192.168.4.34 host 192.168.5.130 echo  
deny icmp host 192.168.4.34 host 192.168.5.146 echo  
deny icmp host 192.168.4.66 host 192.168.5.98 echo  
deny icmp host 192.168.4.66 host 192.168.5.114 echo  
deny icmp host 192.168.4.66 host 192.168.5.130 echo  
deny icmp host 192.168.4.66 host 192.168.5.146 echo  
deny icmp host 192.168.4.82 host 192.168.5.98 echo  
deny icmp host 192.168.4.82 host 192.168.5.114 echo  
deny icmp host 192.168.4.82 host 192.168.5.130 echo  
deny icmp host 192.168.4.82 host 192.168.5.146 echo
```

Extended IP access list 121

```
deny tcp host 192.168.4.82 eq telnet host 192.168.5.98  
deny tcp host 192.168.4.82 eq telnet host 192.168.5.114  
deny tcp host 192.168.4.82 eq telnet host 192.168.5.130  
deny tcp host 192.168.4.82 eq telnet host 192.168.5.146  
deny tcp host 192.168.4.66 eq telnet host 192.168.5.98  
deny tcp host 192.168.4.66 eq telnet host 192.168.5.114  
deny tcp host 192.168.4.66 eq telnet host 192.168.5.130  
deny tcp host 192.168.4.66 eq telnet host 192.168.5.146  
deny tcp host 192.168.4.34 eq telnet host 192.168.5.98  
deny tcp host 192.168.4.34 eq telnet host 192.168.5.114  
deny tcp host 192.168.4.34 eq telnet host 192.168.5.130  
deny tcp host 192.168.4.34 eq telnet host 192.168.5.146
```

Extended IP access list 122

```
deny tcp host 192.168.4.82 eq ftp host 192.168.5.98  
deny tcp host 192.168.4.82 eq ftp host 192.168.5.114  
deny tcp host 192.168.4.82 eq ftp host 192.168.5.130  
deny tcp host 192.168.4.82 eq ftp host 192.168.5.146  
deny tcp host 192.168.4.66 eq ftp host 192.168.5.98  
deny tcp host 192.168.4.66 eq ftp host 192.168.5.114  
deny tcp host 192.168.4.66 eq ftp host 192.168.5.130
```



```
deny tcp host 192.168.4.66 eq ftp host 192.168.5.146
deny tcp host 192.168.4.34 eq ftp host 192.168.5.98
deny tcp host 192.168.4.34 eq ftp host 192.168.5.114
deny tcp host 192.168.4.34 eq ftp host 192.168.5.130
deny tcp host 192.168.4.34 eq ftp host 192.168.5.146
```

3.123.-SHOW ACCESS-LISTS EN EL ROUTER ISP

```
ISP#show access-lists
Extended IP access list 107
  permit icmp host 200.10.1.43 host 192.168.4.98 echo
  permit icmp host 200.10.1.43 host 192.168.4.114 echo
  permit icmp host 200.10.1.43 host 192.168.4.130 echo
  permit icmp host 200.10.1.43 host 192.168.4.146 echo
```

3.124.-SHOW RUNNING-CONFIG EN EL ROUTER PRINCIPAL TES

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

```
Current configuration : 7129 bytes
```

```
!
```

```
Version 12.4
```

```
no service password-encryption
```

```
!
```

```
hostname TES
```

```
!
```

```
Nombre del Router
```

```
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
```

Muestra la contraseña encriptada del usuario Administrador

```
enable password cisco
```

Muestra la contraseña del usuario



```
!  
!  
ip ssh versión 1
```

Línea de comando de acceso remoto seguro

```
!  
!
```

```
interface FastEthernet0/0  
ip address 192.168.5.65 255.255.255.224
```

Muestra la dirección Ip y dirección de máscara de subred del router

```
duplex auto
```

Comunicación simultánea

```
speed auto
```

```
!
```

```
interface FastEthernet0/0.2
```

SubInterfaz Virtual

```
encapsulation dot1Q 203
```

Protocolo en las que se comunican las Vlan

Permite el encapsulamiento entre Vlan

```
ip address 192.168.5.97 255.255.255.240
```

Dirección del host y máscara de Subred

```
interface FastEthernet0/0.3  
encapsulation dot1Q 204  
ip address 192.168.5.113 255.255.255.240
```

```
!
```

```
interface FastEthernet0/0.4  
encapsulation dot1Q 205  
ip address 192.168.5.129 255.255.255.240
```

```
!
```

```

interface FastEthernet0/0.5
encapsulation dot1Q 206
ip address 192.168.5.145 255.255.255.240
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
ip address 192.168.1.18 255.255.255.252

```

Muestra la dirección serial y máscara de la subred

```

!
interface Serial1/1
ip address 192.168.1.22 255.255.255.252
!
interface Serial1/2
ip address 192.168.1.25 255.255.255.252
clock rate 64000
!
interface Serial1/3
ip address 200.10.1.1 255.255.255.252
clock rate 64000

```

Muestra la dirección serial, máscara y Nivel de Sincronización de reloj de la interface serial

```

!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.1.16 0.0.0.3 area 0
network 192.168.1.20 0.0.0.3 area 0
network 192.168.1.24 0.0.0.3 area 0
network 192.168.5.64 0.0.0.31 area 0
network 192.168.5.96 0.0.0.15 area 0
network 192.168.5.112 0.0.0.15 area 0
network 192.168.5.128 0.0.0.15 area 0
network 192.168.5.144 0.0.0.15 area 0

```



```
network 200.10.1.0 0.0.0.3 area 0
```

Muestra la dirección de red, wildcard y área del router ospf

```
ip classless
```

```
!
```

```
!
```

```
access-list 100 permit icmp host 192.168.5.98 host 192.168.3.50 echo
```

```
access-list 100 permit icmp host 192.168.5.98 host 192.168.3.34 echo
```

Muestra la regla de permit o deny de acceso al ping

```
access-list 100 permit icmp host 192.168.5.98 host 192.168.3.2 echo
access-list 100 permit icmp host 192.168.5.114 host 192.168.3.50 echo
access-list 100 permit icmp host 192.168.5.114 host 192.168.3.34 echo
access-list 100 permit icmp host 192.168.5.114 host 192.168.3.2 echo
access-list 100 permit icmp host 192.168.5.130 host 192.168.3.50 echo
access-list 100 permit icmp host 192.168.5.130 host 192.168.3.34 echo
access-list 100 permit icmp host 192.168.5.130 host 192.168.3.2 echo
access-list 100 permit icmp host 192.168.5.146 host 192.168.3.50 echo
access-list 100 permit icmp host 192.168.5.146 host 192.168.3.34 echo
access-list 100 permit icmp host 192.168.5.146 host 192.168.3.2 echo
access-list 101 permit icmp host 192.168.5.98 host 192.168.2.66 echo
access-list 101 permit icmp host 192.168.5.98 host 192.168.2.50 echo
access-list 101 permit icmp host 192.168.5.98 host 192.168.2.34 echo
access-list 101 permit icmp host 192.168.5.114 host 192.168.2.66 echo
access-list 101 permit icmp host 192.168.5.114 host 192.168.2.50 echo
access-list 101 permit icmp host 192.168.5.114 host 192.168.2.34 echo
access-list 101 permit icmp host 192.168.5.130 host 192.168.2.66 echo
access-list 101 permit icmp host 192.168.5.130 host 192.168.2.50 echo
access-list 101 permit icmp host 192.168.5.130 host 192.168.2.34 echo
access-list 101 permit icmp host 192.168.5.146 host 192.168.2.66 echo
access-list 101 permit icmp host 192.168.5.146 host 192.168.2.50 echo
access-list 101 permit icmp host 192.168.5.146 host 192.168.2.34 echo
access-list 102 permit icmp host 192.168.5.98 host 192.168.2.2 echo
access-list 102 permit icmp host 192.168.5.98 host 192.168.2.10 echo
access-list 102 permit icmp host 192.168.5.98 host 192.168.2.18 echo
access-list 102 permit icmp host 192.168.5.114 host 192.168.2.2 echo
access-list 102 permit icmp host 192.168.5.114 host 192.168.2.10 echo
access-list 102 permit icmp host 192.168.5.114 host 192.168.2.18 echo
access-list 102 permit icmp host 192.168.5.130 host 192.168.2.2 echo
access-list 102 permit icmp host 192.168.5.130 host 192.168.2.10 echo
access-list 102 permit icmp host 192.168.5.130 host 192.168.2.18 echo
access-list 102 permit icmp host 192.168.5.146 host 192.168.2.2 echo
access-list 102 permit icmp host 192.168.5.146 host 192.168.2.10 echo
```



```
access-list 102 permit icmp host 192.168.5.146 host 192.168.2.18 echo
access-list 103 permit icmp host 192.168.5.98 host 192.168.6.10 echo
access-list 103 permit icmp host 192.168.5.98 host 192.168.6.18 echo
access-list 103 permit icmp host 192.168.5.114 host 192.168.6.10 echo
access-list 103 permit icmp host 192.168.5.114 host 192.168.6.18 echo
access-list 103 permit icmp host 192.168.5.130 host 192.168.6.10 echo
access-list 103 permit icmp host 192.168.5.130 host 192.168.6.18 echo
access-list 103 permit icmp host 192.168.5.146 host 192.168.6.10 echo
access-list 103 permit icmp host 192.168.5.146 host 192.168.6.18 echo
access-list 104 permit icmp host 192.168.5.98 host 192.168.6.66 echo
access-list 104 permit icmp host 192.168.5.98 host 192.168.6.98 echo
access-list 104 permit icmp host 192.168.5.114 host 192.168.6.66 echo
access-list 104 permit icmp host 192.168.5.114 host 192.168.6.98 echo
access-list 104 permit icmp host 192.168.5.130 host 192.168.6.66 echo
access-list 104 permit icmp host 192.168.5.130 host 192.168.6.98 echo
access-list 104 permit icmp host 192.168.5.146 host 192.168.6.66 echo
access-list 104 permit icmp host 192.168.5.146 host 192.168.6.98 echo
access-list 105 permit icmp host 192.168.5.98 host 192.168.4.18 echo
access-list 105 permit icmp host 192.168.5.98 host 192.168.4.10 echo
access-list 105 permit icmp host 192.168.5.98 host 192.168.4.2 echo
access-list 105 permit icmp host 192.168.5.114 host 192.168.4.18 echo
access-list 105 permit icmp host 192.168.5.114 host 192.168.4.10 echo
access-list 105 permit icmp host 192.168.5.114 host 192.168.4.2 echo
access-list 105 permit icmp host 192.168.5.130 host 192.168.4.18 echo
access-list 105 permit icmp host 192.168.5.130 host 192.168.4.10 echo
access-list 105 permit icmp host 192.168.5.130 host 192.168.4.2 echo
access-list 105 permit icmp host 192.168.5.146 host 192.168.4.18 echo
access-list 105 permit icmp host 192.168.5.146 host 192.168.4.10 echo
access-list 105 permit icmp host 192.168.5.146 host 192.168.4.2 echo
access-list 106 permit icmp host 192.168.5.98 host 192.168.4.34 echo
access-list 106 permit icmp host 192.168.5.98 host 192.168.4.66 echo
access-list 106 permit icmp host 192.168.5.98 host 192.168.4.82 echo
access-list 106 permit icmp host 192.168.5.114 host 192.168.4.34 echo
access-list 106 permit icmp host 192.168.5.114 host 192.168.4.66 echo
access-list 106 permit icmp host 192.168.5.114 host 192.168.4.82 echo
access-list 106 permit icmp host 192.168.5.130 host 192.168.4.34 echo
access-list 106 permit icmp host 192.168.5.130 host 192.168.4.66 echo
access-list 106 permit icmp host 192.168.5.130 host 192.168.4.82 echo
access-list 106 permit icmp host 192.168.5.146 host 192.168.4.34 echo
access-list 106 permit icmp host 192.168.5.146 host 192.168.4.66 echo
access-list 106 permit icmp host 192.168.5.146 host 192.168.4.82 echo
access-list 107 permit icmp host 192.168.5.98 host 200.10.1.34 echo
access-list 107 permit icmp host 192.168.5.114 host 200.10.1.34 echo
access-list 107 permit icmp host 192.168.5.130 host 200.10.1.34 echo
access-list 107 permit icmp host 192.168.5.146 host 200.10.1.34 echo
access-list 108 permit ip any any
!
```

```
!  
line con 0  
password cisco  
login
```

Muestra la contraseña de acceso al router

```
line vty 0 4  
password cisco  
login
```

Muestra la contraseña de acceso al router, a modo de administración remota

```
!  
!  
End
```

3.125.-SHOW RUNNING-CONFIG EN EL ROUTER TES-1

```
TES-1#show running-config  
Building configuration...
```

Current configuration : 4032 bytes

```
!  
version 12.4  
no service password-encryption  
!  
hostname TES-1  
!  
!  
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0  
enable password cisco  
!  
!  
!  
ip ssh version 1  
!  
!  
interface FastEthernet0/0  
ip address 192.168.1.129 255.255.255.224  
duplex auto  
speed auto  
  
!  
interface FastEthernet0/0.2
```



```
encapsulation dot1Q 202
ip address 192.168.3.1 255.255.255.224
!
interface FastEthernet0/0.3
encapsulation dot1Q 201
ip address 192.168.3.33 255.255.255.240
!
interface FastEthernet0/0.4
encapsulation dot1Q 200
ip address 192.168.3.49 255.255.255.240
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
ip address 192.168.1.26 255.255.255.252
!
interface Serial1/1
no ip address
shutdown
!
interface Serial1/2
no ip address
shutdown
!
interface Serial1/3
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 192.168.1.128 0.0.0.31 area 0
network 192.168.1.24 0.0.0.3 area 0
network 192.168.3.0 0.0.0.31 area 0
network 192.168.3.32 0.0.0.31 area 0
network 192.168.3.0 0.0.0.7 area 0
network 192.168.3.48 0.0.0.15 area 0
!
ip classless
!
!
```

```

access-list 101 deny icmp host 192.168.5.8 any echo
access-list 101 deny icmp host 192.168.5.18 any echo
access-list 101 deny icmp host 192.168.5.34 any echo
access-list 101 deny icmp host 192.168.5.42 any echo
access-list 101 deny icmp host 192.168.5.46 any echo
access-list 102 deny tcp any any eq telnet
access-list 100 deny icmp host 192.168.3.50 host 192.168.5.98 echo
access-list 100 deny icmp host 192.168.3.50 host 192.168.5.114 echo
access-list 100 deny icmp host 192.168.3.50 host 192.168.5.130 echo
access-list 100 deny icmp host 192.168.3.50 host 192.168.5.146 echo
access-list 100 deny icmp host 192.168.3.34 host 192.168.5.98 echo
access-list 100 deny icmp host 192.168.3.34 host 192.168.5.114 echo
access-list 100 deny icmp host 192.168.3.34 host 192.168.5.130 echo
access-list 100 deny icmp host 192.168.3.34 host 192.168.5.146 echo
access-list 100 deny icmp host 192.168.3.2 host 192.168.5.98 echo
access-list 100 deny icmp host 192.168.3.2 host 192.168.5.114 echo
access-list 100 deny icmp host 192.168.3.2 host 192.168.5.130 echo
access-list 100 deny icmp host 192.168.3.2 host 192.168.5.146 echo
access-list 109 deny tcp host 192.168.3.50 eq telnet host 192.168.5.98
access-list 109 deny tcp host 192.168.3.50 eq telnet host 192.168.5.114
access-list 109 deny tcp host 192.168.3.50 eq telnet host 192.168.5.130
access-list 109 deny tcp host 192.168.3.50 eq telnet host 192.168.5.146
access-list 109 deny tcp host 192.168.3.34 eq telnet host 192.168.5.98
access-list 109 deny tcp host 192.168.3.34 eq telnet host 192.168.5.114
access-list 109 deny tcp host 192.168.3.34 eq telnet host 192.168.5.130
access-list 109 deny tcp host 192.168.3.34 eq telnet host 192.168.5.146
access-list 109 deny tcp host 192.168.3.2 eq telnet host 192.168.5.98
access-list 109 deny tcp host 192.168.3.2 eq telnet host 192.168.5.114
access-list 109 deny tcp host 192.168.3.2 eq telnet host 192.168.5.130
access-list 109 deny tcp host 192.168.3.2 eq telnet host 192.168.5.146
access-list 110 deny tcp host 192.168.3.50 eq ftp host 192.168.5.98
access-list 110 deny tcp host 192.168.3.50 eq ftp host 192.168.5.114
access-list 110 deny tcp host 192.168.3.50 eq ftp host 192.168.5.130
access-list 110 deny tcp host 192.168.3.50 eq ftp host 192.168.5.146
access-list 110 deny tcp host 192.168.3.34 eq ftp host 192.168.5.98
access-list 110 deny tcp host 192.168.3.34 eq ftp host 192.168.5.114
access-list 110 deny tcp host 192.168.3.34 eq ftp host 192.168.5.130
access-list 110 deny tcp host 192.168.3.34 eq ftp host 192.168.5.146
access-list 110 deny tcp host 192.168.3.2 eq ftp host 192.168.5.98
access-list 110 deny tcp host 192.168.3.2 eq ftp host 192.168.5.114
access-list 110 deny tcp host 192.168.3.2 eq ftp host 192.168.5.130
access-list 110 deny tcp host 192.168.3.2 eq ftp host 192.168.5.146
!
!
line con 0
password cisco
login
line vty 0 4

```



```
password cisco
login
!
!
end
```

3.126.-SHOW RUNNING-CONFIG EN EL ROUTER UEES

```
UEES#show running
Building configuration...
```

```
Current configuration : 2825 bytes
!
version 12.4
no service password-encryption
!
hostname UEES
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
ip address 192.168.6.1 255.255.255.248
duplex auto
speed auto
!
interface FastEthernet0/0.2
encapsulation dot1Q 106
ip address 192.168.6.9 255.255.255.248
!
interface FastEthernet0/0.3
encapsulation dot1Q 107
ip address 192.168.6.17 255.255.255.240
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial1/0
```

```
ip address 192.168.1.2 255.255.255.252
!
interface Serial1/1
ip address 192.168.1.10 255.255.255.252
!
interface Serial1/2
ip address 192.168.1.13 255.255.255.252
clock rate 64000
!
interface Serial1/3
ip address 192.168.1.17 255.255.255.252
clock rate 64000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
redistribute rip subnets
network 192.168.1.16 0.0.0.3 area 0
!
router rip
version 2
redistribute ospf 1 metric 1
network 192.168.1.0
network 192.168.6.0
!
ip classless
!
!
access-list 103 deny icmp host 192.168.6.10 host 192.168.5.98 echo
access-list 103 deny icmp host 192.168.6.10 host 192.168.5.114 echo
access-list 103 deny icmp host 192.168.6.10 host 192.168.5.130 echo
access-list 103 deny icmp host 192.168.6.10 host 192.168.5.146 echo
access-list 103 deny icmp host 192.168.6.18 host 192.168.5.98 echo
access-list 103 deny icmp host 192.168.6.18 host 192.168.5.114 echo
access-list 103 deny icmp host 192.168.6.18 host 192.168.5.130 echo
access-list 103 deny icmp host 192.168.6.18 host 192.168.5.146 echo
access-list 111 deny tcp host 192.168.6.10 eq telnet host 192.168.5.98
access-list 111 deny tcp host 192.168.6.10 eq telnet host 192.168.5.114
access-list 111 deny tcp host 192.168.6.10 eq telnet host 192.168.5.130
access-list 111 deny tcp host 192.168.6.10 eq telnet host 192.168.5.146
access-list 111 deny tcp host 192.168.6.18 eq telnet host 192.168.5.98
access-list 111 deny tcp host 192.168.6.18 eq telnet host 192.168.5.114
access-list 111 deny tcp host 192.168.6.18 eq telnet host 192.168.5.130
access-list 111 deny tcp host 192.168.6.18 eq telnet host 192.168.5.146
access-list 112 deny tcp host 192.168.6.10 eq ftp host 192.168.5.98
```

```
access-list 112 deny tcp host 192.168.6.10 eq ftp host 192.168.5.114
access-list 112 deny tcp host 192.168.6.10 eq ftp host 192.168.5.130
access-list 112 deny tcp host 192.168.6.10 eq ftp host 192.168.5.146
access-list 112 deny tcp host 192.168.6.18 eq ftp host 192.168.5.98
access-list 112 deny tcp host 192.168.6.18 eq ftp host 192.168.5.114
access-list 112 deny tcp host 192.168.6.18 eq ftp host 192.168.5.130
access-list 112 deny tcp host 192.168.6.18 eq ftp host 192.168.5.146
!
!
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
!
!
end
```

3.127.-SHOW RUNNING-CONFIG EN EL ROUTER UEES-1

```
UEES-1#show running
Building configuration...
```

```
Current configuration : 3576 bytes
```

```
!
version 12.4
no service password-encryption
!
hostname UEES-1
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
ip address 192.168.1.65 255.255.255.224
duplex auto
```



```
speed auto
!  
interface FastEthernet0/0.2  
encapsulation dot1Q 100  
ip address 192.168.2.1 255.255.255.248  
!  
interface FastEthernet0/0.3  
encapsulation dot1Q 101  
ip address 192.168.2.9 255.255.255.248  
!  
interface FastEthernet0/0.4  
encapsulation dot1Q 102  
ip address 192.168.2.17 255.255.255.240  
!  
interface FastEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial1/0  
ip address 192.168.1.5 255.255.255.252  
clock rate 64000  
!  
interface Serial1/1  
ip address 192.168.1.1 255.255.255.252  
clock rate 64000  
!  
interface Serial1/2  
no ip address  
shutdown  
!  
interface Serial1/3  
no ip address  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
router rip  
version 2  
network 192.168.1.0  
network 192.168.2.0  
!  
ip classless  
!  
!
```



```
access-list 102 deny icmp host 192.168.2.18 host 192.168.5.98 echo
access-list 102 deny icmp host 192.168.2.18 host 192.168.5.114 echo
access-list 102 deny icmp host 192.168.2.18 host 192.168.5.130 echo
access-list 102 deny icmp host 192.168.2.18 host 192.168.5.146 echo
access-list 102 deny icmp host 192.168.2.10 host 192.168.5.98 echo
access-list 102 deny icmp host 192.168.2.10 host 192.168.5.114 echo
access-list 102 deny icmp host 192.168.2.10 host 192.168.5.130 echo
access-list 102 deny icmp host 192.168.2.10 host 192.168.5.146 echo
access-list 102 deny icmp host 192.168.2.2 host 192.168.5.98 echo
access-list 102 deny icmp host 192.168.2.2 host 192.168.5.114 echo
access-list 102 deny icmp host 192.168.2.2 host 192.168.5.130 echo
access-list 102 deny icmp host 192.168.2.2 host 192.168.5.146 echo
access-list 113 deny tcp host 192.168.2.18 eq telnet host 192.168.5.98
access-list 113 deny tcp host 192.168.2.18 eq telnet host 192.168.5.114
access-list 113 deny tcp host 192.168.2.18 eq telnet host 192.168.5.130
access-list 113 deny tcp host 192.168.2.18 eq telnet host 192.168.5.146
access-list 113 deny tcp host 192.168.2.10 eq telnet host 192.168.5.98
access-list 113 deny tcp host 192.168.2.10 eq telnet host 192.168.5.114
access-list 113 deny tcp host 192.168.2.10 eq telnet host 192.168.5.130
access-list 113 deny tcp host 192.168.2.10 eq telnet host 192.168.5.146
access-list 113 deny tcp host 192.168.2.2 eq telnet host 192.168.5.98
access-list 113 deny tcp host 192.168.2.2 eq telnet host 192.168.5.114
access-list 113 deny tcp host 192.168.2.2 eq telnet host 192.168.5.130
access-list 113 deny tcp host 192.168.2.2 eq telnet host 192.168.5.146
access-list 114 deny tcp host 192.168.2.18 eq ftp host 192.168.5.98
access-list 114 deny tcp host 192.168.2.18 eq ftp host 192.168.5.114
access-list 114 deny tcp host 192.168.2.18 eq ftp host 192.168.5.130
access-list 114 deny tcp host 192.168.2.18 eq ftp host 192.168.5.146
access-list 114 deny tcp host 192.168.2.10 eq ftp host 192.168.5.98
access-list 114 deny tcp host 192.168.2.10 eq ftp host 192.168.5.114
access-list 114 deny tcp host 192.168.2.10 eq ftp host 192.168.5.130
access-list 114 deny tcp host 192.168.2.10 eq ftp host 192.168.5.146
access-list 114 deny tcp host 192.168.2.2 eq ftp host 192.168.5.98
access-list 114 deny tcp host 192.168.2.2 eq ftp host 192.168.5.114
access-list 114 deny tcp host 192.168.2.2 eq ftp host 192.168.5.130
access-list 114 deny tcp host 192.168.2.2 eq ftp host 192.168.5.146
!
!
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
!
!
End
```

3.128.-SHOW RUNNING-CONFIG EN EL ROUTER UEES-2

```
UEES-2#show running  
Building configuration...
```

```
Current configuration : 3572 bytes
```

```
!  
version 12.4  
no service password-encryption  
!  
hostname UEES-2  
!  
!  
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0  
enable password cisco  
!  
!  
!  
!  
ip ssh version 1  
!  
!  
interface FastEthernet0/0  
ip address 192.168.1.97 255.255.255.224  
duplex auto  
speed auto  
!  
interface FastEthernet0/0.2  
encapsulation dot1Q 103  
ip address 192.168.2.33 255.255.255.240  
!  
interface FastEthernet0/0.3  
encapsulation dot1Q 104  
ip address 192.168.2.49 255.255.255.240  
!  
interface FastEthernet0/0.4  
encapsulation dot1Q 105  
ip address 192.168.2.65 255.255.255.240  
!  
interface FastEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!
```



```
interface Serial1/0
ip address 192.168.1.9 255.255.255.252
clock rate 64000
!
interface Serial1/1
ip address 192.168.1.6 255.255.255.252
!
interface Serial1/2
no ip address
shutdown
!
interface Serial1/3
no ip address
shutdown
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
network 192.168.1.0
network 192.168.2.0
!
ip classless
!
!
access-list 101 deny icmp host 192.168.2.66 host 192.168.5.98 echo
access-list 101 deny icmp host 192.168.2.66 host 192.168.5.114 echo
access-list 101 deny icmp host 192.168.2.66 host 192.168.5.130 echo
access-list 101 deny icmp host 192.168.2.66 host 192.168.5.146 echo
access-list 101 deny icmp host 192.168.2.50 host 192.168.5.98 echo
access-list 101 deny icmp host 192.168.2.50 host 192.168.5.114 echo
access-list 101 deny icmp host 192.168.2.50 host 192.168.5.130 echo
access-list 101 deny icmp host 192.168.2.50 host 192.168.5.146 echo
access-list 101 deny icmp host 192.168.2.34 host 192.168.5.98 echo
access-list 101 deny icmp host 192.168.2.34 host 192.168.5.114 echo
access-list 101 deny icmp host 192.168.2.34 host 192.168.5.130 echo
access-list 101 deny icmp host 192.168.2.34 host 192.168.5.146 echo
access-list 115 deny tcp host 192.168.2.66 eq telnet host 192.168.5.98
access-list 115 deny tcp host 192.168.2.66 eq telnet host 192.168.5.114
access-list 115 deny tcp host 192.168.2.66 eq telnet host 192.168.5.130
access-list 115 deny tcp host 192.168.2.66 eq telnet host 192.168.5.146
access-list 115 deny tcp host 192.168.2.50 eq telnet host 192.168.5.98
access-list 115 deny tcp host 192.168.2.50 eq telnet host 192.168.5.114
access-list 115 deny tcp host 192.168.2.50 eq telnet host 192.168.5.130
access-list 115 deny tcp host 192.168.2.50 eq telnet host 192.168.5.146
access-list 115 deny tcp host 192.168.2.34 eq telnet host 192.168.5.98
```



```

access-list 115 deny tcp host 192.168.2.34 eq telnet host 192.168.5.114
access-list 115 deny tcp host 192.168.2.34 eq telnet host 192.168.5.130
access-list 115 deny tcp host 192.168.2.34 eq telnet host 192.168.5.146
access-list 116 deny tcp host 192.168.2.34 eq ftp host 192.168.5.98
access-list 116 deny tcp host 192.168.2.34 eq ftp host 192.168.5.114
access-list 116 deny tcp host 192.168.2.34 eq ftp host 192.168.5.130
access-list 116 deny tcp host 192.168.2.34 eq ftp host 192.168.5.146
access-list 116 deny tcp host 192.168.2.66 eq ftp host 192.168.5.98
access-list 116 deny tcp host 192.168.2.66 eq ftp host 192.168.5.114
access-list 116 deny tcp host 192.168.2.66 eq ftp host 192.168.5.130
access-list 116 deny tcp host 192.168.2.66 eq ftp host 192.168.5.146
access-list 116 deny tcp host 192.168.2.50 eq ftp host 192.168.5.98
access-list 116 deny tcp host 192.168.2.50 eq ftp host 192.168.5.114
access-list 116 deny tcp host 192.168.2.50 eq ftp host 192.168.5.130
access-list 116 deny tcp host 192.168.2.50 eq ftp host 192.168.5.146
!
!
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
!
!
end

```



3.129.-SHOW RUNNING-CONFIG EN EL ROUTER ECOTEC

```

Ecotec#show running
Building configuration...

Current configuration : 2848 bytes
!
version 12.4
no service password-encryption
!
hostname Ecotec
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!

```

```
!  
!  
!  
ip ssh version 1  
!  
!  
interface FastEthernet0/0  
ip address 192.168.6.33 255.255.255.224  
duplex auto  
speed auto  
!  
interface FastEthernet0/0.2  
encapsulation dot1Q 306  
ip address 192.168.6.65 255.255.255.224  
!  
interface FastEthernet0/0.3  
encapsulation dot1Q 307  
ip address 192.168.6.97 255.255.255.224  
!  
interface FastEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial1/0  
ip address 192.168.1.14 255.255.255.252  
!  
interface Serial1/1  
ip address 192.168.1.29 255.255.255.252  
clock rate 64000  
!  
interface Serial1/2  
ip address 192.168.1.33 255.255.255.252  
clock rate 64000  
!  
interface Serial1/3  
ip address 192.168.1.21 255.255.255.252  
clock rate 64000  
!  
interface Vlan1  
no ip address  
shutdown  
!  
router ospf 1  
log-adjacency-changes  
redistribute rip subnets  
network 192.168.1.20 0.0.0.3 area 0
```

```
!  
router rip  
version 2  
redistribute ospf 1 metric 1  
network 192.168.1.0  
network 192.168.6.0  
!  
ip classless  
!  
!  
access-list 104 deny icmp host 192.168.6.66 host 192.168.5.98 echo  
access-list 104 deny icmp host 192.168.6.66 host 192.168.5.114 echo  
access-list 104 deny icmp host 192.168.6.66 host 192.168.5.130 echo  
access-list 104 deny icmp host 192.168.6.66 host 192.168.5.146 echo  
access-list 104 deny icmp host 192.168.6.98 host 192.168.5.98 echo  
access-list 104 deny icmp host 192.168.6.98 host 192.168.5.114 echo  
access-list 104 deny icmp host 192.168.6.98 host 192.168.5.130 echo  
access-list 104 deny icmp host 192.168.6.98 host 192.168.5.146 echo  
access-list 117 deny tcp host 192.168.6.66 eq telnet host 192.168.5.98  
access-list 117 deny tcp host 192.168.6.66 eq telnet host 192.168.5.114  
access-list 117 deny tcp host 192.168.6.66 eq telnet host 192.168.5.130  
access-list 117 deny tcp host 192.168.6.66 eq telnet host 192.168.5.146  
access-list 117 deny tcp host 192.168.6.98 eq telnet host 192.168.5.98  
access-list 117 deny tcp host 192.168.6.98 eq telnet host 192.168.5.114  
access-list 117 deny tcp host 192.168.6.98 eq telnet host 192.168.5.130  
access-list 117 deny tcp host 192.168.6.98 eq telnet host 192.168.5.146  
access-list 118 deny tcp host 192.168.6.66 eq ftp host 192.168.5.98  
access-list 118 deny tcp host 192.168.6.66 eq ftp host 192.168.5.114  
access-list 118 deny tcp host 192.168.6.66 eq ftp host 192.168.5.130  
access-list 118 deny tcp host 192.168.6.66 eq ftp host 192.168.5.146  
access-list 118 deny tcp host 192.168.6.98 eq ftp host 192.168.5.98  
access-list 118 deny tcp host 192.168.6.98 eq ftp host 192.168.5.114  
access-list 118 deny tcp host 192.168.6.98 eq ftp host 192.168.5.130  
access-list 118 deny tcp host 192.168.6.98 eq ftp host 192.168.5.146  
!  
!  
!  
line con 0  
password cisco  
login  
line vty 0 4  
password cisco  
login  
!  
!  
End
```



3.130.-SHOW RUNNING-CONFIG EN EL ROUTER ECOTEC-1

```
ECOTEC-1#show running
Building configuration...
```

```
Current configuration : 3563 bytes
```

```
!
version 12.4
no service password-encryption
!
hostname ECOTEC-1
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
ip address 192.168.1.161 255.255.255.224
duplex auto
speed auto

!
interface FastEthernet0/0.2
encapsulation dot1Q 300
ip address 192.168.4.1 255.255.255.248
!
interface FastEthernet0/0.3
encapsulation dot1Q 301
ip address 192.168.4.9 255.255.255.248
!
interface FastEthernet0/0.4
encapsulation dot1Q 302
ip address 192.168.4.17 255.255.255.240
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
shutdown
```

```
!  
interface Serial1/0  
ip address 192.168.1.30 255.255.255.252  
!  
interface Serial1/1  
ip address 192.168.1.38 255.255.255.252  
clock rate 64000  
!  
interface Serial1/2  
no ip address  
shutdown  
!  
interface Serial1/3  
no ip address  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
router rip  
version 2  
network 192.168.1.0  
network 192.168.4.0  
!  
ip classless  
!  
!  
access-list 105 deny icmp host 192.168.4.18 host 192.168.5.98 echo  
access-list 105 deny icmp host 192.168.4.18 host 192.168.5.114 echo  
access-list 105 deny icmp host 192.168.4.18 host 192.168.5.130 echo  
access-list 105 deny icmp host 192.168.4.18 host 192.168.5.146 echo  
access-list 105 deny icmp host 192.168.4.10 host 192.168.5.98 echo  
access-list 105 deny icmp host 192.168.4.10 host 192.168.5.114 echo  
access-list 105 deny icmp host 192.168.4.10 host 192.168.5.130 echo  
access-list 105 deny icmp host 192.168.4.10 host 192.168.5.146 echo  
access-list 105 deny icmp host 192.168.4.2 host 192.168.5.98 echo  
access-list 105 deny icmp host 192.168.4.2 host 192.168.5.114 echo  
access-list 105 deny icmp host 192.168.4.2 host 192.168.5.130 echo  
access-list 105 deny icmp host 192.168.4.2 host 192.168.5.146 echo  
access-list 119 deny tcp host 192.168.4.18 eq telnet host 192.168.5.98  
access-list 119 deny tcp host 192.168.4.18 eq telnet host 192.168.5.114  
access-list 119 deny tcp host 192.168.4.18 eq telnet host 192.168.5.130  
access-list 119 deny tcp host 192.168.4.18 eq telnet host 192.168.5.146  
access-list 119 deny tcp host 192.168.4.10 eq telnet host 192.168.5.98  
access-list 119 deny tcp host 192.168.4.10 eq telnet host 192.168.5.114  
access-list 119 deny tcp host 192.168.4.10 eq telnet host 192.168.5.130  
access-list 119 deny tcp host 192.168.4.10 eq telnet host 192.168.5.146
```



```
access-list 119 deny tcp host 192.168.4.2 eq telnet host 192.168.5.98
access-list 119 deny tcp host 192.168.4.2 eq telnet host 192.168.5.114
access-list 119 deny tcp host 192.168.4.2 eq telnet host 192.168.5.130
access-list 119 deny tcp host 192.168.4.2 eq telnet host 192.168.5.146
access-list 120 deny tcp host 192.168.4.18 eq ftp host 192.168.5.98
access-list 120 deny tcp host 192.168.4.18 eq ftp host 192.168.5.114
access-list 120 deny tcp host 192.168.4.18 eq ftp host 192.168.5.130
access-list 120 deny tcp host 192.168.4.18 eq ftp host 192.168.5.146
access-list 120 deny tcp host 192.168.4.10 eq ftp host 192.168.5.98
access-list 120 deny tcp host 192.168.4.10 eq ftp host 192.168.5.114
access-list 120 deny tcp host 192.168.4.10 eq ftp host 192.168.5.130
access-list 120 deny tcp host 192.168.4.10 eq ftp host 192.168.5.146
access-list 120 deny tcp host 192.168.4.2 eq ftp host 192.168.5.98
access-list 120 deny tcp host 192.168.4.2 eq ftp host 192.168.5.114
access-list 120 deny tcp host 192.168.4.2 eq ftp host 192.168.5.130
access-list 120 deny tcp host 192.168.4.2 eq ftp host 192.168.5.146
!
!
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
!
!
end
```

3.131.-SHOW RUNNING-CONFIG EN EL ROUTER ECOTEC-2

```
ECOTEC-2#show running
Building configuration...
```

```
Current configuration : 3620 bytes
```

```
!
version 12.4
no service password-encryption
!
hostname ECOTEC-2
!
!
enable secret 5 $1$mERr$hX5rVt7rPNoS4wqbXKX7m0
enable password cisco
!
```

```
!  
!  
!  
ip ssh version 1  
!  
!  
interface FastEthernet0/0  
ip address 192.168.1.193 255.255.255.224  
duplex auto  
speed auto  
!  
interface FastEthernet0/0.2  
encapsulation dot1Q 303  
ip address 192.168.4.33 255.255.255.224  
!  
interface FastEthernet0/0.3  
encapsulation dot1Q 304  
ip address 192.168.4.65 255.255.255.240  
!  
interface FastEthernet0/0.4  
encapsulation dot1Q 305  
ip address 192.168.4.81 255.255.255.240  
!  
interface FastEthernet0/1  
no ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial1/0  
ip address 192.168.1.34 255.255.255.252  
!  
interface Serial1/1  
no ip address  
shutdown  
!  
interface Serial1/2  
ip address 192.168.1.37 255.255.255.252  
!  
interface Serial1/3  
no ip address  
shutdown  
!  
interface Vlan1  
no ip address  
shutdown  
!  
router rip
```

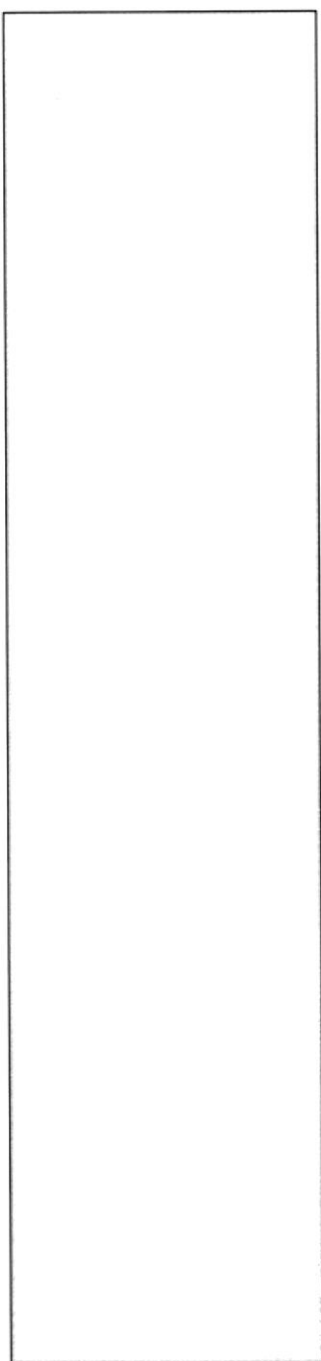


BIBLIOTECA
CAMPUS
PEÑAS

```
version 2
network 192.168.1.0
network 192.168.4.0
!
ip classless
!
!
access-list 106 deny icmp host 192.168.4.34 host 192.168.5.98 echo
access-list 106 deny icmp host 192.168.4.34 host 192.168.5.114 echo
access-list 106 deny icmp host 192.168.4.34 host 192.168.5.130 echo
access-list 106 deny icmp host 192.168.4.34 host 192.168.5.146 echo
access-list 106 deny icmp host 192.168.4.66 host 192.168.5.98 echo
access-list 106 deny icmp host 192.168.4.66 host 192.168.5.114 echo
access-list 106 deny icmp host 192.168.4.66 host 192.168.5.130 echo
access-list 106 deny icmp host 192.168.4.66 host 192.168.5.146 echo
access-list 106 deny icmp host 192.168.4.82 host 192.168.5.98 echo
access-list 106 deny icmp host 192.168.4.82 host 192.168.5.114 echo
access-list 106 deny icmp host 192.168.4.82 host 192.168.5.130 echo
access-list 106 deny icmp host 192.168.4.82 host 192.168.5.146 echo
access-list 121 deny tcp host 192.168.4.82 eq telnet host 192.168.5.98
access-list 121 deny tcp host 192.168.4.82 eq telnet host 192.168.5.114
access-list 121 deny tcp host 192.168.4.82 eq telnet host 192.168.5.130
access-list 121 deny tcp host 192.168.4.82 eq telnet host 192.168.5.146
access-list 121 deny tcp host 192.168.4.66 eq telnet host 192.168.5.98
access-list 121 deny tcp host 192.168.4.66 eq telnet host 192.168.5.114
access-list 121 deny tcp host 192.168.4.66 eq telnet host 192.168.5.130
access-list 121 deny tcp host 192.168.4.66 eq telnet host 192.168.5.146
access-list 121 deny tcp host 192.168.4.34 eq telnet host 192.168.5.98
access-list 121 deny tcp host 192.168.4.34 eq telnet host 192.168.5.114
access-list 121 deny tcp host 192.168.4.34 eq telnet host 192.168.5.130
access-list 121 deny tcp host 192.168.4.34 eq telnet host 192.168.5.146
access-list 122 deny tcp host 192.168.4.66 eq ftp host 192.168.5.146
access-list 122 deny tcp host 192.168.4.82 eq ftp host 192.168.5.98
access-list 122 deny tcp host 192.168.4.82 eq ftp host 192.168.5.114
access-list 122 deny tcp host 192.168.4.82 eq ftp host 192.168.5.130
access-list 122 deny tcp host 192.168.4.82 eq ftp host 192.168.5.146
access-list 122 deny tcp host 192.168.4.66 host 192.168.5.98
access-list 122 deny tcp host 192.168.4.66 eq ftp host 192.168.5.98
access-list 122 deny tcp host 192.168.4.66 eq ftp host 192.168.5.114
access-list 122 deny tcp host 192.168.4.66 eq ftp host 192.168.5.130
access-list 122 deny tcp host 192.168.4.34 eq ftp host 192.168.5.98
access-list 122 deny tcp host 192.168.4.34 eq ftp host 192.168.5.114
access-list 122 deny tcp host 192.168.4.34 eq ftp host 192.168.5.130
access-list 122 deny tcp host 192.168.4.34 eq ftp host 192.168.5.146
!
!
!
line con 0
```

```
password cisco  
login  
line vty 0 4  
password cisco  
login  
!  
!  
end
```





GLOSARIO

GLOSARIO

A

Access Point.- Es un punto de acceso inalámbrico privado, para conectar sus computadoras a Internet sin necesidad de cables, permitiendo compartir recursos de red.

Antivirus.- Que detecta la presencia de virus y puede neutralizar sus efectos.

ARP type.- Tipo de Address Resolution Protocol asignado.

B

Broadcast .- Son mensajes que se envían a toda la red y como tal ocasionan congestión en la misma.

BW.- Ancho de Banda de la interfaz en kilobits por segundo.

C

Clock rate.- Permite asignar sincronización de reloj en interfaz DCE

Configure terminal.- Configura la terminal manualmente desde la terminal de consola

Connect dirección_ipnombre.- Permite conectarse remotamente a un host

Copy flash tftp.- Copia la imagen del sistema desde la memoria Flash a un servidor TFTP.

Copy running-config startup-config.- Guarda la configuración activa en la NVRAM

Counters never.- Contadores

Ctrl+A .- Permite desplazarse al principio de la línea de comandos

Ctrl+B (o Flecha Izquierda).- Permite desplazarse un carácter hacia atrás

Ctrl+C.- Cancela la ejecución del Dialogo de configuración inicial o Setup

Ctrl+E.- Permite desplazarse hasta el final de la línea de comandos

Ctrl+F (o Flecha Derecha).- Permite desplazarse un carácter hacia delante

Ctrl+N (o Flecha Abajo).- Muestra el comando más reciente

Ctrl+P (o Flecha Arriba).- Muestra el último comando ingresado

Ctrl+Shift+6.- Permite interrumpir intentos de ping, traceroute y traducciones de nombres

Ctrl+Z (o end).- Estando en cualquier modo de configuración regresa al modo EXEC Privilegiado.

D

Database.- Ingresa en el modo base de datos de VLAN

Default .- Por defecto utilizado para el administrador

Deny.- Deniega la entrada de paquetes por el protocolo tcp.

Dimensiones.- una de las propiedades del espacio. El espacio, tal y como lo conocemos, es tridimensional. Para definir un volumen se necesitan tres medidas (dimensiones): longitud, anchura y altura.

DIMM.- Dual In-line Memory Module, módulo de memoria en línea doble. Hace referencia a su sistema de comunicación con la placa base, que se gestiona en grupos de datos de 64 bits

Disco Duro.- unidad de almacenamiento permanente de gran capacidad. Está formado por varios discos apilados dos o más, normalmente de aluminio o vidrio, recubiertos de un material ferromagnético.

Disconnect conexión.-Desconecta una sesión telnet establecida desde el router

DLY.- Retraso de la unidad en micro-segundo.

DNS.- Sistemas de Nombres De Dominios.Su función es convertir nombres de dominios a dirección IP.

DRAM .- Tipo de memoria de acceso aleatorio almacenan la información en circuitos integrados que contienen condensadores.

E

Echo.- Permite el paso de tráfico cuando hay una sesión establecida.

Enable password contraseña.-Establece una contraseña local para controlar el acceso a los diversos niveles de privilegio. Ej: enable password class

Enable secret contraseña.-Especifica una capa de seguridad adicional mediante el comando enable password. Ej: enable secret class

Enable.-Ingresa al modo EXEC Privilegiado

Encapsulation ARPA.- Método de encapsulación asignado a la interfaz

Erase flash.-Borra el contenido de la memoria Flash

Erase startup-config.-Borra el contenido de la NVRAM

Esc+B .-Permite desplazarse una palabra hacia atrás

Exit.-Estando en el modo de configuración global o cualquiera de sus submodos regresa al modo anterior. Estando en los modos EXEC Usuario o EXEC Privilegiado, cierra la sesión.

F

Fast ethernet .- Envía en tramas de longitud variable que contienen la información de control y hasta 1.500 bytes de datos.

Fibra Óptica.- fibra o varilla de vidrio u otro material transparente con un índice de refracción alto que se emplea para transmitir luz. Cuando la luz entra por uno de los extremos de la fibra, se transmite con muy pocas pérdidas incluso aunque la fibra esté curvada.

Frecuencia.- término empleado en física para indicar el número de veces que se repite en un segundo cualquier fenómeno periódico.

Full duplex Back.- Transmite datos simultáneamente en ambas direcciones, emitiendo y recibiendo al mismo tiempo, se dice que operan en modo.

H

Half Duplex.- Sólo puede transmitir uno de ellos y el otro simplemente actúa de receptor, el modo de operación

Hardware is Lance.- Este campo describe el tipo de hardware que la interfaz está conectado.

Hardware.- se refiere a los componentes materiales de un sistema informático. La función de estos componentes suele dividirse en tres categorías principales: entrada, salida y almacenamiento.

Hostname nombre.- Modifica el nombre del router. Ej: hostname Lab_A

Hp.- Hewlett-Packard, fabricante productos y mantiene plantas de fabricación, centros de investigación y desarrollo.

I

IMPRESORA.- periférico para ordenador o computadora que traslada el texto o la imagen generada por computadora a papel u otro medio, como transparencias o diversos tipos de fibras.

Interface fastethernet.- Entra al modo de configuración de interfaz de la ethernet

Interface serial.- Entra al modo de configuración de interfaz del serial

Interface tipo número.- Configura un tipo de interfaz y entra al modo de configuración de interfaz.

INTERNET.- Internet, interconexión de redes informáticas que permite a los ordenadores o computadoras conectadas comunicarse directamente.

Ip access-list.- Permite crear una ACL nombrada. Se debe indicar el tipo. Este comando ingresa al router al submodo de configuración que puede reconocerse por el prompt

Ip address.- Asigna una dirección IP y máscara de subred para las rutas.

Ip classless.- Permite que el router no tome en cuenta los límites con definición de clases de las redes en su tabla de enrutamiento y simplemente transmita hacia la ruta por defecto

Ip default-network dirección_red.- Establece una ruta por defecto. Ej: ip default-network 210.32.45.0

Ip route dirección_red máscara_dir_ip_salto.- Establece rutas estáticas. Ej: ip route 210.42.3.0 255.255.255.0 211.1.2.1

ISP.- Proveedor De Servicio Internet.

L

LAN.- Local Area Network Las computadoras de una red de área local.

Last input.- Tiempo de la última Entrada desde que el último Paquete fue recibido con éxito por una interfaz.

Line protocol is up.- Línea del protocolo, está en estado levantado

Line tipo número.- Identifica una línea específica para la configuración e inicia el modo de reunión de comandos de configuración.

Logout.- Sale del modo EXEC

Loopback not set.- Especifica si el bit de bucle invertido se encuentra en el canal D de señalización.

M

Mac.- Es una dirección Física asignada por el fabricante de la tarjeta de red .Se puede utilizar con fines administrativos para asignar políticas en la red.

Mail.- Correo electrónico, sistema de envío y recepción de correo mediante el uso de un ordenador o computadora u otro dispositivo electrónico, de manera que se utilice una red de área local.

Memoria Flash.- chip de memoria no volátil su contenido permanece aunque el aparato se desconecte de la corriente, que se puede reescribir. En cierto sentido se considera una variante de la EEPROM (Electrically Erasable Programmable Read-OnlyMemory, memoria de lectura solamente borrable y programable eléctricamente).

Memoria.- Los circuitos que permiten almacenar y recuperar la información. En un sentido más amplio, puede referirse también a sistemas externos de almacenamiento, como las unidades de disco o de cinta.

Metric.-Metrica que se utiliza en el OSPF.

Microtik.- Logra enlaces de datos inalámbricos de alta velocidad.

Modo de configuración de interfaces: Permite utilizar comandos de configuración de interfaces (Direcciones IP, mascarar, etc.).

Modo de configuración de línea: Permite configurar una línea (ejemplo: acceso al router por Telnet).

Modo de configuración global: Permite utilizar los comandos de configuración generales del router.

Modo espacial: RXBoot Modo de mantenimiento que puede servir, especialmente, para reinicializar las contraseñas del router.

Modo usuario: Permite consultar toda la información relacionada al router sin poder modificarla.

MTU.- Unidad Máxima de Transmisión de la Interfaz.

N

Netware.- Permite a los usuarios compartir archivos y recursos del sistema, como los discos duros y las impresoras.

Network.- Asigna una dirección de red a la cual el router se encuentra directamente conectado

Nic.- O tarjeta de Red

No debug all.-Desactiva todas las depuraciones activadas en el dispositivo

No shutdown.- Reinicia una interfaz desactivada.

O

OSPF.- Es un protocolo de enrutamiento del estado de enlace basado en estándares abiertos.

P

Peso.- Medida de la fuerza gravitatoria ejercida sobre un objeto.

Ping.-Envía una petición de eco para diagnosticar la conectividad básica de red.

Procesador.- Unidad central de proceso, formado por uno o dos chips.

Proxy.- Un ordenador o computadora se dice que es de 64 bits si utiliza procesadores de 64-bit.

R

RAM Buffer.- Crea el buffer de los paquetes (RAM compartida).

Reload.-Reinicia el router

Rely.- Fiabilidad de la interfaz.

Resume Conexión.-Resume una sesión telnet interrumpida con la secuencia CTRL+SHIFT+6 y X.

RIP.- Son las siglas de Routing Information Protocol. (Protocolo De Información De Enrutamiento)

Router protocolo de enrutamiento.-Inicia un proceso de enrutamiento definiendo en primer lugar un protocolo de enrutamiento IP. Ej: router rip ó router igrp 120

Routers.- permite la comunicación entre diferentes segmentos de Red. El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados.

S

S.O.-Sistema Operativo.

Service password-encryption.-Habilita la función de cifrado de la contraseña

Servidor.- Computadora conectada a una red que pone sus recursos a disposición del resto de los integrantes de la red. Suele utilizarse para mantener datos centralizados o para gestionar recursos compartidos.

Setup.-Entra a la facilidad de Diálogo de configuración inicial

Show access-lists.-Muestra el contenido de todas las ACL en el router. Para ver una lista específica, agregue el nombre o número de ACL como opción a este comando

Show arp.-Muestra la asignación de direcciones IP a MAC a Interfaz del router

Show cdp entry.-Muestra información acerca de un dispositivo vecino registrado en una tabla CDP

Show cdp interfaces.-Muestra información acerca de las interfaces en las que CDP está habilitado

Show cdp neighbors.-Muestra los resultados del proceso de descubrimiento de CDP

Show cdp traffic.-Muestra los contadores CDP, incluyendo el número de paquetes enviados y recibidos, y los errores de checksum

Show cdp.-Muestra el intervalo entre publicaciones CDP, tiempo de validez y versión de la publicación

Show clock.-Muestra la hora y fecha del router

Show controllers.-Muestra información importante como que tipo de cable se encuentra conectado

- Show debugging.**-Muestra información acerca de los tipos de depuraciones que están habilitados
- Show flash.**-Muestra la disposición y contenido de la memoria Flash
- Show history.**-Muestra el historial de comandos ingresados
- Show hosts.**-Muestra una lista en caché de los nombres de host y direcciones
- show interfaces.**-Muestra estadísticas para la/las interfaces indicadas
- Show ip interface brief.**-Muestra un breve resumen de la información y del estado de una dirección IP
- Show ip interface.**-Muestra los parámetros de estado y globales asociados con una interfaz
- Show ip protocols.**-Muestra los parámetros y estado actual del proceso de protocolo de enrutamiento activo
- Show ip rip database.**-Muestra el contenido de la base de datos privada de RIP
- Show ip route.**-Muestra el contenido de la tabla de enrutamiento IP. El parámetro dirección permite acotar la información que se desea visualizar, exclusivamente a la dirección ingresada. El parámetro protocolo permite indicar la fuente de aprendizaje de las rutas que se desean visualizar, como por ejemplo rip, igrp, static y connected
- Show memory.**-Muestra estadísticas acerca de la memoria del router, incluyendo estadísticas de memoria disponible
- Show processes.**-Muestra información acerca de los procesos activos
- Show protocols.**-Muestra los protocolos de capa 3 configurados
- Show running-config.**-Muestra la configuración actual en la RAM
- Show sessions.**-Muestra las conexiones Telnet establecidas en el router
- Show sessions.**-Muestra las conexiones Telnet establecidas en el router
- Show stacks.**-Controla el uso de la pila de procesos y rutinas de interrupción y muestra la causa del último re arranque del sistema
- Show startup-config.**-Muestra la configuración que se ha guardado, que es el contenido de la NVRAM
- Show versión.**-Muestra información sobre el Cisco IOS y la plataforma
- Software.**- Programas de computadoras. Son las instrucciones responsables de que el hardware (la máquina) realice su tarea. Como concepto general, el software puede dividirse en varias categorías basadas en el tipo de trabajo realizado.
- Switch .-** El switch que usa es D-Link y pertenece a la capa 1 del modelo OSI cabe recalcar que no es administrable.
- Switchport access vlan.**- Comando para tener acceso a un puerto de la vlan
- Switchport mode.**- Configura el modo de pertenencia VLAN para un puerto.

T

- Tecla Tabulador.**-Completa el comando ingresado parcialmente
- Telnet.**- Nombre del Puerto servicio que permite acceder de manera remota a un dispositivo. Permite conectarse remotamente a un host
- Terminal editing.**-Reactiva las funciones de edición avanzada
- Terminal history size numero_líneas .-**Establece el tamaño del buffer del historial de comandos.
- Terminal monitor.**-Si se utiliza una sesión por telnet para examinar el router, entonces, permite redirigir el resultado y los mensajes del sistema hacia a terminal remota
- Terminal no editing.**-Deshabilita las funciones de edición avanzada

ThreatSense .- Protege proactivamente contra malware conocido y desconocido logrando altísimos niveles de detección de códigos maliciosos para proteger su sistema.

Topología.- Varias computadoras individuales conectadas entre sí forman una red de área local.

Traceroute dirección_ip.-Muestra la ruta tomada por los paquetes hacia un destino

Transciver.-En términos informáticos convierte la luz a impulsos eléctricos.

Transmisión.- Transferencia de datos, en informática, transmisión de información de un lugar a otro, tanto dentro de un ordenador o computadora

Trunhing Port.- (PUERTO TRUNCADO) Permite Reducir el nivel de congestionamiento entre 2 Switch.

Trunk.- Especifica un puerto como punto extremo para un tronco VLAN

Undebug all .-Desactiva todas las depuraciones activadas en el dispositivo.

U

UPS.- Uninterrupted Power Supply baterías que permiten mantener el sistema informático en funcionamiento, por lo menos el tiempo necesario para apagarlo sin pérdida de datos. Sin embargo, la única forma de garantizar la integridad física de los datos es mediante copias de seguridad.

Usuario privilegiado: Permite visualizar el estado del router e importar o exportar imágenes de IOS.

V

Velocidad.- Transferencia máxima se ajusta automáticamente en función de la cobertura y calidad de la transmisión.

Vlan.- Virtual local area network .Permite reducir los dominios de Broadcast.

W

Wildcard.-Máscara de longitud inversa.Es la máscara de subred que se utiliza con el protocolo de enrutamiento OSPF y aplicarlas en las ACL.

Wireless.-Red sin cable .Transmisión Only Direccional y Unidireccional.

Wlan.- Es una red de comunicaciones de datos que cubre una extensa área geográfica.

